LUT
Lappeenranta
University of Technology

Jussi Laakkonen

AN APPROACH FOR DISTINCT INFORMATION PRIVACY RISK ASSESSMENT

Thesis for the degree of Doctor of Science (Technology) to be presented with due permission for public examination and criticism in the Auditorium of the Student Union House at Lappeenranta University of Technology, Lappeenranta, Finland on the 18th of November, 2017, at noon.

Acta Universitatis
Lappeenrantaensis 766

Supervisors Jari Porras
LUT School of Business and Management
Lappeenranta University of Technology
Finland

Pekka Jäppinen
LUT School of Business and Management
Lappeenranta University of Technology
Finland

Reviewers Josef Noll
Department of Informatics
The Faculty of Mathematics and Natural Sciences
University Graduate Center (UniK)
University of Oslo
Norway

Samant Khajuria
Department of Electronic Systems
Center for Communication, Media and Information Technologies
The Faculty of Engineering and Science
Aalborg University
Denmark

Opponents Samant Khajuria
Department of Electronic Systems
Center for Communication, Media and Information Technologies
The Faculty of Engineering and Science
Aalborg University
Denmark

Prof. M. Jean Vanderdonckt
Louvain Interaction Lab
Université Catholique de Louvain
Belgium

ISBN 978-952-335-149-3
ISBN 978-952-335-150-9 (PDF)
ISSN-L 1456-4491
ISSN 1456-4491
Lappeenrannan teknillinen yliopisto
Yliopistopaino 2017

Abstract

Jussi Laakkonen

An approach for distinct information privacy risk assessment

Lappeenranta November 2017
312 pages

Acta Universitatis Lappeenrantaensis 766
Diss. Lappeenranta University of Technology
ISBN 978-952-335-149-3, ISBN 978-952-335-150-9 (PDF)
ISSN-L 1456-4491, ISSN 1456-4491

Privacy is a a basic human right and a foundational issue of the digital world but also a complex concept to comprehend; the term is commonly misunderstood through secrecy. The struggle with privacy has been, and will be between liberty and control. An equal balance between the two is difficult to achieve, hence the different motivators and agendas of the involved parties. New definitions of different aspects of privacy, such as PII 2.0 and legislative regulations can help in moving towards a suitable compromise. However, before a new definition is devised, the systems withholding private information must be protected to ensure privacy of individuals. The first step in protecting the systems is assessing information privacy risks, to which the contribution of this thesis is an answer to.

In information privacy identifiability of information is the key issue. In legislation private information is the data that can identify an individual or that can be linked to an individual. In order to maintain information privacy it is required to guarantee the individual autonomy of an individual by encompassing both integrity and confidentiality of the identified or identifiable information. This thesis begins with a survey of privacy state of art that is derived from existing research on, models and approaches of, and legal definitions on privacy.

Contribution of this thesis is an approach for assessing information privacy risk in ecosystems collecting information about individuals. The approach is a mid-level tool for assessing information privacy risk that operates between abstract and concrete methods to offer indicative results about the ecosystem under study. The approach is intended to be used as a tool in detecting the areas of the ecosystem where more protection is needed. Based on the results resources can be then allocated and prioritized to problematic areas of the ecosystem. The approach operates on abstract task, functional and component levels and consists of two contributions: (1) an abstraction method and iterative framework and (2) an assessment model. Contribution 1 offers details about information flows between the tasks and functions of the ecosystem components. Contribution 2 establishes a qualitative information privacy risk value on component basis utilizing both qualitative and quantitative attributes of information privacy.

Keywords: privacy, information privacy, risk assessment, privacy legislation

Acknowledgements

This study was done in Lappeenranta University of Technology throughout years 2011 and 2015. Writing, correcting and editing process of this thesis began in 2015 and was finished at the end of September 2017. Most parts of this thesis were written in 2015.

I thank the personnel of our department of many names throughout the years and the fellow Ph.D. students with whom I discussed, argued and drank motivational spirits with. Especially I like to thank Prof. Jari Porras, who I regard as the best boss I've had so far, for being an excellent mentor challenging my thinking and bringing my ideas to the next level during the ca. eight years I worked at LUT. Also, I like to thank my supervisor Pekka Jäppinen for making my job difficult in a good sense that I would keep on trying to find new, better solutions instead of just settling with the first applicable one. And additionally I like to thank Prof. Ahmed Seffah, who acted as an unofficial supervisor during the last years of my research, for sparring me on difficult issues when writing the last papers and giving me the extra boost in motivation when all seemed lost.

I would like to thank the consortium of Smart Grid and Energy Markets (funded by Cleen Oy), the consortium of MobiServ project (funded by EU) and the consortium of Game Cloud (funded by TEKES) for making this research possible. Each project gave an interesting environment to study from different viewpoints in order to gain knowledge and data for this research.

Also I appreciate the grants I received from ISACA Finland chapter (http://www.isaca.org/chapters1/finland) and FUUG (https://fuug.fi/) to support my research. This made me feel that at least someone believed in my work, although my own faith was crumbling.

I hail all the Single Malt Whisky distilleries in Scotland. You produce the source of inspiration to pull through this tough, least rewarding and most frustrating era in my life, to conduct this painstaking research and to spend countless hours in writing this thesis. A liquid to sustain life, *uisge beatha*, the water of life, easer of stress, reliever of pain. Without Single Malt Whisky, I would have never finished this work. This is an never ending love story. *Slainté*.

In the final year of research and in the beginning of writing this thesis I met you, Eeva-Stiina, and now I'm feeling happy once again. You took me in your arms when I was feeling down and devastated because of the setbacks I encountered. You listened, cared and pulled me back on my feet. I do not know any other way could I repay this but by staying by your side and giving you all the support you need.

Last but not least I want to thank my parents who have supported my studies and fed my enthusiasm towards computers way before they, or even I, did realize it.

The very first computer you bought started this all. This is just one of the fruits it produced. It is funny to think that all those days and nights spent on playing computer games and tweaking the computer to get more performance out of it in one day results in a Ph.D. thesis. Mom and dad, I thank you for your patience with me.

As final notes: this is a work effort struggled away with stubbornness and determination. Motivation to finish this was lost on multiple occasions. The following joke reflects my feelings toward a certain group of people*:*

What is the difference between a crowbar and a bureaucrat?

Sometimes one is able to bend the crowbar.

Permanently.

... The world is entering a new dark age.

Jussi Laakkonen
October 2017
Lappeenranta, Finland

Nomenclature

AID	Actor Identifier
API	Application Programming Interface
CDIS	Customer Data Information System
DEA	Drug Enforcement Agency
DGP	Digital Games Platform
DPD	Data Protection Directive
DSO	Distribution System Operator
DSR	Design Science Research
DSRM	Design Science Reserach Methodology
EC	European Commission
EDI	Electronic Data Interchange
ETSI	European Telecommunications Standards Institute
EU	European Union
FIP	Fair Information Practice
GPS	Global Positioning System
ILS	Independent Living Support
IP	Internet Protocol
LAN	Local Area Network
MDIS	Measurement Data Information System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OECD	Organization of Economic Cooperation and Development
ORU	Optical Recognition Unit
PbD	Privacy by Design
PIAF	Privacy Impact Assessment Framework
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information

PLC	Power Line Communication
PP	Privacy Principle
PRU	Physical Robotic Unit
RQ	Research Question
RSQ	Research Sub-Question
SGEM	Smart Grids and Energy Markets
SHACU	Smarthome Automation and Communication Unit
SLA	Service Level Agreeement
UML	Unified Modeling Language
US	United States
VAS	Value-added Service
VPN	Virtual Private Network
WHSU	Wearable Health Status Unit
WLAN	Wireless Local Area Network

Contents

Preface

> Plunging into a new found / Age of advanced observeillance / A world-wide, foolproof cage
>
> Privacy and intimacy as we know it / Will be a memory / Among many to be passed down / To those who never knew
>
> Living in the pupil of 1, 000 eyes
>
> Was it overlooked in front of all our faces? / Now, the mistakes and secrets / Cannot be erased
>
> Viewing the blind complexity / By which laws were justified / To erase simplicity
>
> To the left and to the right / From behind, they're out of sight
>
> © *Chuck Schuldiner / Roadrunner Records 1995*

The above lyrical inscription (used here with the right of quotation, section 22 of Finnish copyright law[1]) was written by a personal idol of mine, Chuck Schuldiner (RIP) the frontman of band *Death,* for their 6th long play *Symbolic*[2] that was released in 1995. The song from which the lyrical chapter is taken from is titled *1,000 Eyes*[3]. This particular song was always one of my favorites from the album. First it was the musical composition, the riffs, the guitar leads and pace changes that caught my attention. A bit later, the lyrics dealing with societal issues in speculative manner began to interest. Almost 20 years later these lyrics start to make more sense from an another viewpoint I had when I first heard the song and went through the booklet of the album. Back then I had practically no knowledge on information privacy since Internet was then in its infancy.

Now we all have 1,000 eyes behind us, watching, monitoring, analyzing and evaluating us. The eyes can be seen as a metaphor for devices constructed by men to allow surveillance and to observe others to fulfill the needs of few to be in control. If we go on an uncontrolled path in information privacy, we may overlook the mistakes and secrets that cannot be erased, which will haunt humanity for years to come. The culprits can be indeed out of sight, protected by the thick shroud of legislation to justify their actions. People would be living in a cage. Monitored and controlled like animals. Like in an Orwellian (1984) [1] scenario, where people have lost their freedom, their liberty. Unless we let it happen.

By nature we, homo sapiens are curious. We like to learn new things and concepts. We want to know how the universe works. But now, our attention is on digitalization of the societies and the surveillance possibilities it opens. This draws the curiosity of many, which might rise from the fear that something that is regarded

[1] http://www.finlex.fi/fi/laki/kaannokset/1961/en19610404.pdf

[2] https://www.emptywords.org/Symbolic.htm

[3] https://www.emptywords.org/LyricsSymbolic.htm

as private is misused by an another individual, company, advertisers or even government. Our society needs the curious people to reveal the problems as it guides our understanding (of privacy) into new level. By understanding the problem and adapting new thoughts about privacy, especially into the legislation, the potential harm to individuals in case of a breach, for instance, can be mitigated. This work is an attempt of one curious mind to do one's bit for the society to help with this problem.

Part I

Introductory chapters

This part begins with an introduction to the context of this thesis summarizing also the research that is presented as well as the contributions. The second section continues with a more detailed description and definition of privacy state of art from multiple viewpoints, such as the foundations of privacy, legislation and the role of privacy in modern world.

1 Introduction

Surveillance of individuals has reached a new level in this millennium. Security agencies feel the need to observe individuals and their actions on the Internet so dangerous ones can be filtered out and counteractions and preventative measures can be placed in time[4]. This course of action has been widely criticized by people [2], media (a broad summary exists in Wikipedia[5]) and even legislation [3]. Meanwhile, people are still sharing more and more personal data[6] through various media [4] and using services that have stated that they do not really respect the privacy of their customers[7,8]. Legislators are now attempting to enforce new ways to protect our basic right, privacy, in these services. In a wide study on privacy [5], the authors stated that the directions for the quest for privacy are ambiguous and it will be a continuous race as it has been with cryptography. The study authors also noted [5] that the world should find a correct balance with privacy, which will not be an easy task and takes time.

1.1 Privacy and a balance between liberty and control

Privacy is about liberty vs. control, as Bruce Schneier aptly states [6]. He also states that freedom should not be sacrificed for security. The nothing to hide argument is invalid [7] when dealing with privacy. Privacy should not be confused with security, as although they are interlinked they are different concepts [8]. Without security, there would be no privacy [9]. But giving up too much for security will make us lose our liberty and our freedom [6]. It will end up in too much control for a selected few, a totalitarian state, where every move is watched and controversial acts are punished, as George Orwell described in *1984* [1].

In the late 19th century, a new definition was publicized that every man has the right to privacy [10]. However, current technological and social development changed this definition rapidly. New technological methods for observing and monitoring individuals are about to take that right away [11]. Now it seems that the trend is to put more and more of our daily lives into a digital, analyzable form for visible and life-benefiting needs. The benefits, however, come with obscure and mysterious hidden possibilities unknown to users [11]. Who would have guessed that smart meters enable monitoring of television-watching behavior [12]?

However, the world does not have to go into that direction. As the means for surveillance evolve, people's worries increase, too. Anxiety about the unknown is

[4] http://www.theguardian.com/uk-news/2014/dec/02/youre-the-bomb-are-you-at-risk-from-anti-terrorism-algorithms-automated-tracking-innocent-people

[5] https://en.wikipedia.org/wiki/Reactions_to_global_surveillance_disclosures

[6] http://www.sharethis.com/blog/2015/01/21/q4-2014-consumer-sharing-trends-report/

[7] http://www.businessinsider.com/gmail-privacy-google-court-brief-2013-8

[8] http://www.zdnet.com/article/70-dont-trust-facebook-with-their-personal-information/

a common trait in humans [13], and that particular anxiety increases the curiosity [14] of some individuals [15]. Through the curiosity of many, we have starting to see that as the technological skills of many improve through education and open information available over the Internet, more and more problems with the new technological solutions are being found, such as the recent findings about Samsung's Smart TV speech recording[9]. Without these kinds of people, many things would go unnoticed in new technology.

Most of the newfound problems are related to privacy and the handling of private information in the new technology. Some reports about these problems result in manufacturers making changes to their policies and products[10], but also legislation and government behavior have been changed because of the resulting oppression of individuals. The latter was the case in the Netherlands where the smart metering law was found to contravene the European Convention of Human Rights, and the installation of smart meters is now voluntary [16, 17].

1.2 Privacy is complicated and threatened

Privacy is a foundational issue of the digital world [5]. It is a complex, multidisciplinary issue [18, 19] that is understood [8, 7] and valued [18] differently by different individuals, data holders, courts and legislations [20]. For privacy is a human-made concept [21] that evolves with us and with the society surrounding us [19]. Now, the functions of our society are being digitalized. As many revelations about different surveillance programs[11,12], and especially the U.S. National Security Agency (NSA) [3], data theft[13,14] and poor protection of systems[15] in the media show, it is not all good, especially for individuals as "living a public life is becoming the new default" [5] and the transition to this kind of life will introduce problems. Meanwhile, new definitions and regulations are being devised to ease the transition.

The digital world introduced the need for a more definitive meaning of privacy, especially information privacy. The European Union (EU) has reacted to this challenge by trying to establish a consensus on new data protection regulation [22, 23]. The slow progression of defining the regulation (the debate started in 2011, and continues), indicates that not only the term privacy is challenging but also all the connected issues are as well. Nevertheless, some progress has been achieved.

[9] http://www.theregister.co.uk/2015/02/17/samsung_smart_tv_privacy_rewind/

[10] http://www.cnet.com/news/samsung-changes-smarttv-privacy-policy-in-wake-of-spying-fears/

[11] http://www.theguardian.com/us-news/the-nsa-files

[12] http://en.wikipedia.org/wiki/Global_surveillance_disclosures_(2013–present)

[13] http://www.forbes.com/sites/moneybuilder/2015/01/13/the-big-data-breaches-of-2014/

[14] http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

[15] http://www.zdnet.com/article/one-billion-records-leaked-designer-vulnerability-use-rose-in-2014/

First, the protection of personal information is required to be strengthened under the threat of large fines. Second, all systems that handle and process moderately large amounts of personal data (5,000 transactions in a year) have to be assessed for information privacy risks, and it must be proved that protecting measures are in place. Third, all negligence in information protection must be severely penalized without the possibility of complaining to local authorities; instead, all complaints go through the European Court of Justice.

In light of the NSA revelations, for instance, accompanied by all the leakage, break-in and information misuse news [3], people have also taken to the barricades[16] and developed means such as Tor Tails[17] to guarantee privacy in Internet services. Many systems made to help our daily lives are the ones that can threaten our privacy. People are now worried about the peripheral information available about them from seemingly harmless sources [8]. The main worry is that the information is combined by a third party to generate an accurate profile or to find out something about that individual [5]. Combining such data gives details about an individual, which the individual might not be willing to share with anyone.

1.3 Increasing the collection of data about people

People are now aware that someone is collecting data about them [8]. But who and for what purpose? Multiple new technologies, such as Independent Living Support (ILS) systems (e.g. MobiServ [24]), gaming platforms (such as Game Cloud [25] or the best-known one, Steam[18]), smart grids [26, 27, 28] and, of course, social media [29], collect vast amounts of information not only from the use of the services but also from the service users. These new technologies are not without problems. For example, data from smart grids offers a lot of information about the individuals inside a residence [12, 30, 31], and many countermeasures have been devised [32, 33, 34, 35, 36] to reduce the effect of data leakage. In addition, the data that different gaming platforms and the games themselves generate can be used for a huge variety of purposes [37, 38], which opens up the possibility of establishing a psychological profile of a player [39, 40] with the proper tools [41]. The problems with social media privacy protection and the risks have been known for a while [29, 42] and are almost continuously circulating in various media[19,20,21] after data is leaked. A gruesome example are the leaks on popular adult

[16] https://www.eff.org/deeplinks/2013/10/polls-continue-show-majority-americans-against-nsa-spying

[17] https://tails.boum.org

[18] http://store.steampowered.com

[19] http://en.wikipedia.org/wiki/2012_LinkedIn_hack

[20] http://www.huffingtonpost.com/2013/06/27/facebook-leak-data_n_3510100.html

[21] https://gigaom.com/2014/12/17/everything-you-need-to-know-about-the-recent-snapchat-leaks/

dating[22] and cheating[23] sites; the information on these sites can be harmful to one's reputation. In an ILS research project (MobiServ [24]), part of this research was conducted, it was noted that the aspects of security differ from those of privacy [43], and therefore there is a clear need for a method for assessing privacy risks in addition to the common security analysis [44].

This need was the starting point for the work presented in this thesis. Later, the work reached out to smart grid areas to offer an *abstraction method* to detect privacy risk [45], as well as to build privacy-aware gaming platforms with a framework helping to incorporate Privacy by Design (PbD) principles into the development [46]. The smart grid and gaming platform examples show that the situation is complicated. The abuse of poorly protected information is not clearly visible until the leak is publicized or the information is abused. People are getting worried about what is hidden from them [19], what even peripheral information is available about them [8] and why it is even collected? Post-processing of collected data (through data mining) is a worrisome aspect that is not clearly recognized by legislation [11, 47]. The current European legislation on data protection [48] provides many of rights for an individual to access his or her own information [49], as well as the right to be forgotten [22], but has no clear stance on anonymized information being processed to be identified information. Instead, it seems that the European Commission is acting under the pretense that "Anonymous data is easy to deal with." and has no risk[24].

With the proposed regulation [22], the EU is attempting to ease the situation by forcing many companies, corporations and organizations to detect the problems and react to them. If all systems containing private information are equally protected, some portions of the problem are removed but not all. Identification of an individual is a key issue here as stated in Amendment 6, Recital 23 [23]:

> *The principles of data protection should apply to any information concerning an identified or identifiable natural person. To determine whether a person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by any other person to identify or single out the individual directly or indirectly.*

Protecting identifiable information inside the systems is imperative, but first the problems with protection have to be detected in order to apply the protection. Aptly, the clause on identifiability is continued with a requirement to take into consideration the current technical development [23]:

> *To ascertain whether means are reasonably likely to be used to iden-*

[22] http://www.channel4.com/news/adult-friendfinder-dating-hack-internet-dark-web

[23] http://krebsonsecurity.com/2015/07/online-cheating-site-ashleymadison-hacked/

[24] http://europa.eu/rapid/press-release_SPEECH-13-269_en.htm

> *tify the individual, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration both available technology at the time of the processing and technological development.*

1.4 Goal, statement and scope of this research

This thesis focuses on the problem of detecting the risks in information privacy handling in any ecosystem. With the new data protection regulation, the EU has clearly shown [22, 23] that there is a need for a method for assessing information privacy risks in any kind of information system. As the scope of the proposed regulation suggests, there will be a wide range of needs to assess the risk in varied systems with various expertise. According to the literature review presented later, no such method exists that is flexible for any ecosystem to allow non-experts in the area to conduct an assessment. In addition to the need proposed by the MobiServ project [24], this Europe-wide requirement [22, 23] for a method or tool for assessing privacy risks in a flexible manner shows that the work presented in this thesis is necessary.

1.4.1 Research objectives

The objective of this research is to devise **an approach for assessing information privacy risk** that:

1. produces reusable and clear results
2. allows comparison of the results of the analysis
3. is usable without the need for expert knowledge
4. requires only average resource consumption without interrupting the ecosystem's operations

Furthermore, the approach must be usable in any ecosystem for analyzing existing (eco-)systems, as well as developing new ones (objective 5).

1.4.2 Research questions

The scope of this thesis is limited by presenting the three main research questions (RQs) and three research sub-questions (RSQs) to be answered later in this thesis.

RQ1: What attributes define information privacy? First and foremost, the initial question is about what kind of information needs to be protected and what information is regarded as private information. Since this research deals intensively with the information that we all generate in the systems collecting, analyzing and making decisions based on that information, it is imperative to discover the different attributes of information that makes it identifiable to an individual and useful for analytical purposes. In other words, what are the characteristics that make information private? Both, quantitative and qualitative attributes must be accounted for to make an analysis of information privacy risk possible. This leads to the following research sub-question:

RSQ1.1: What is the relation between the different attributes of private information? The model aims to encompass all attributes of information privacy, but what is the relation between these attributes, and which attributes are related to other attributes? The different types of attributes (quantitative and qualitative) have their own role. Which of these is to be applied to the evaluation and calculation of information privacy risk is the question here.

RQ2: How to gather information about where to apply privacy protection? Another question is related to the systems that collect and store the data since they have a multitude of different characteristics. In order to find out the risks in the systems without going into too many details to find out the places where the information should be protected, an abstraction of the ecosystems is needed. The question is, how to abstract the ecosystems that collect and use information about their users or customers into basic tasks? This leads to the following sub-question that what are the generic tasks of different actors in the ecosystems, and are these tasks dependent on each other and how?

As these two aforementioned research questions (RQ1 and RQ2) relate to the abstraction of the ecosystem to gain deeper knowledge about the ecosystem, modeling information privacy has its own specific research questions. The different characteristics and the concrete attributes of information privacy bring challenges in making connections between attributes, and the ecosystem and legislation agnosticism introduce issues of their own.

RQ3: How to model information privacy in an user-friendly way (legislation and ecosystem agnostic)? How the attributes of private information relate to each other brings up the question of how to introduce an easy-to-use aspect in the model. How can the different attributes of information privacy be utilized in the model to make it self-balancing to allow it to be more user friendly. This leads to two research sub-questions about legislation and ecosystem agnosticism.

RSQ3.1: How to create a legislation-agnostic model for information privacy? First, how to include legislative requirements for privacy in the model to answer the actual need for this kind of method? Legislation tends to seldom be changed but it might not be reasonable to tie the model into one law. Instead, the definitions of legislation might be more useful as guidelines in the use of the developed model of information privacy.

RSQ3.2: How to achieve an ecosystem-agnostic model for information privacy? Second, the question is about whether the model is suitable for the particular task but also for assessing any ecosystem or scenario. This is an important issue worthy of investigation as the model is intended to be ecosystem agnostic.

These research questions introduce all necessary aspects of establishing the approach for assessing information privacy risk for the goal. RQ1 and RSQ1.1 require knowledge about information privacy classifications, and RQ2 introduces the need for details about the contexts in which information is managed, transferred and maintained. Answering RQ3 requires that the research also focuses on finding the aspects that will guarantee the resulting tool is not for experts only. RSQ3.1 pushes one of the main motivators, the proposed EU regulation and its needs, into the research. RSQ3.2, as the final question, requires that the resulting approach is evaluated.

1.4.3 Statement and limitations of the research

The work presented in this thesis is a mid-level tool [50] for addressing the problem of assessing information privacy on an asset basis in ecosystems that collect, maintain and process private, sensitive information. Information privacy is assessed with an approach consisting of three layers, each of which will increase the depth of knowledge about the (eco-)system and its details. These three layers utilize details of the task and functional and component levels of each asset. Additionally, the three-level classification of Personally Identifiable Information (PII) 2.0 is utilized in assessing the identifiability of the information within the ecosystem. Similarly, by applying quantitative and qualitative attributes of information privacy an accurate privacy risk value is established.

This research offers only an approach for detecting risks to information privacy and takes no stance on how the risks may be mitigated. It would be ideal to present the approach in the form of a software tool, thus, the potential extent of its use because of the new Europe-wide requirements [23], but the development of such software and its more detailed specifications are future work. The approach presented in this thesis is the design documentation for such a software tool. The software would not only make the use of the approach more proficient but would also enable graphical representations of the ecosystem under study. This, in turn, would enable to present the assessment result with varying levels of detail for different focus groups (e.g., different for executives and analysts).

Privacy is closely tied to the societal laws we have created around us. In this work, a re-definition of privacy or information privacy is not introduced, but insights into the history and current situation of both are offered in addition to the presented working definition of information privacy. Therefore, the focus of this research is on information privacy and not on data protection, which is more related to security. Therefore, this research does not include security attributes directly. Furthermore, the *assessment mode*l does not include the purpose of use in the qualitative risk calculation as the purpose is an attribute of data protection.

1.4.4 Scope of the research contribution

The work that is presented in this thesis is an approach for assessing information privacy in any system, meant to be used as a mid-level tool [50] in the assessment. Campbell and Stamp [50] refer to mid-level tools as a mix of abstract and concrete methods, where abstract methods have a broad application with a high requirement of expertise whereas concrete methods require a low level of expertise in the form of user knowledge and have a narrow application. The higher level methods (abstract) lose the granularity of the detail, and in contrast, the lower-level methods (concrete) have finer-grained detail.

The approach presented here falls in between these two classifications in expertise and in the scopes of detail and application. The expert knowledge requirement is reduced through the design of the assessment requirements, and the scope of application is kept on "medium altitude" [50] to fulfill a design decision of being a multi-use approach applicable to a broad domain. Thus, this results in medium granularity of detail. This is intended as the approach is designed to give indicative results that can help analysts to allocate resources to problematic areas. By being a mid-level tool with indicative results, the tool can be of economic benefit to the analysis of many different ecosystems as further, more detailed concrete analysis processes can be prioritized using the results of the tool.

1.5 Contribution of this thesis

In this thesis, a solution for the problem of information privacy risk assessment in a flexible manner without the need for expert knowledge is presented. This work is only *a* solution, emphasis on the a, since the concept of privacy is human devised and, therefore, can have no singular definition as it is always a construct from innate properties of humans from the perspective of humans [21].

The approach is formed of two main contributions: (1) an *abstraction method* (in assessing an existing solution) or an *iterative framework* (in creating new systems) and (2) an *assessment model* encompassing all attributes of information privacy on the asset level to establish a qualitative risk value. This approach is aimed at assessing information privacy risks in systems that collect information about the daily or other activities of individuals. The approach helps to gain more understanding of the underlying system and to detect the information privacy risks on high abstract and functional levels, and on a component basis.

The first contribution is the first assessment in which information flows between different tasks and functions of the components of the ecosystem under study, as well as the system components themselves, are analyzed. This generates information that is used for analyzing potential information privacy risks within the ecosystem and to offer details about the more detailed assessment conducted with the second contribution.

The second contribution introduces the second assessment in which the information privacy risks of each component in the system are assessed in more detail with a model encompassing all aspects that affect information privacy risk. The model establishes a qualitative risk value utilizing qualitative and quantitative attributes, which are based on categorization of the key aspects of information privacy.

In the following sections, the scope of the contribution is described, and then the two contributions are briefly introduced. A full detailed description of both contributions is presented later in this thesis.

1.5.1 Contribution 1: the abstraction method and the iterative framework

The first part of the approach has two distinct uses. The basic work flow is the same in both uses; the system is abstracted at high level, and the functionalities are mapped to abstract tasks, which enables analysis of information flows inside and outside the system(s). In this thesis, this theory referred to as an *abstraction method* when existing solutions are analyzed and as a (iterative) framework when the method is used alongside development of a new (eco-)system.

First, the *abstraction method* can be used as a analysis tool for detecting information flows in existing systems utilizing high-level abstraction of the tasks and functions of the (eco-)system [45]. This helps to detect how the components of a system or systems utilize information and what kind of information is exchanged offering a clear overview of the system's information flows. By utilizing this knowledge, a common layout of multiple systems can be established, or existing systems can be compared to each other in order to see which is the most suitable solution.

Second, the *iterative framework* enables the possibility of incorporating PbD principles into the design process of a new system through iterative analysis and can be used as a framework in the process [46]. In each iteration round, the component layout of the system is reevaluated and assessed and compared to the previous one to see what effects the changes had to information flows and privacy. This process forces the creation of a lot of documentation that can help to show to, for example, the EU that the design of the system enables privacy by default (a PbD principle). The documentation can also show that certain problems in privacy protection are taken care of. These claims can be backed up by the results the second part of the approach, the model, offer.

1.5.2 Contribution 2: an assessment model

The model for information privacy risk assessment (the *assessment model*) is aimed to be the more definitive and analytical tool of the approach. The *assessment model* produces a qualitative information privacy risk value for each component of the ecosystem. The information privacy risk value is calculated from all attributes that define information privacy with relation-based mapping of the attributes in the form of a model. There are total of 18 attributes each of which has one or more connections to other attributes of information privacy. The multiplicity of relations is accounted for in the model as the attributes are connected either directly or indirectly. The attributes and their relations form the model for calculating information privacy risk. The attributes are classified with predefined scales, and the calculations for both styles of relations are either done as an average (direct) or with connection-specific matrices (indirect). To avoid consuming a vast amount of resources, the model requires that only nine attributes are to be assessed and valued by the analyst using the model.

Usage of the model benefits from the preliminary work of the first contribution (*abstraction method* and the *iterative framework*) for classifying different attributes of information privacy. The *assessment model* makes it possible to compare the risk values of previous layouts of the ecosystem if used alongside *the iterative framework*, for instance. The results of the *assessment model* give more details and offer more insight for the following iterations of *the iterative framework*, if a new system is being designed with the help of this whole approach. In addition, with the *assessment model*, the established ecosystem layout can be compared to other similar ecosystem layouts in order to see why the existing architectures have smaller or higher risk values if used with the *abstraction method*.

Therefore, the results generated by the *assessment model* can back up the changes introduced through the use of the *iterative framework* and strengthen the claims in the documentation in order to satisfy the new requirements of EU regulation [22, 23] for proof that an attempt has been made to protect private information from privacy infractions. Therefore, if the sanctions proposed by the EU can be avoided, or even reduced, in the case of a breach, then the *assessment model* and the approach in general have an economic impact. However, these are not the main points of the method, albeit they are still important. The importance lies in the usable results, ease of use and correctness of the model.

These are not the only benefits of the *assessment model*. In order to value each accounted attribute of information privacy, the person doing the analysis (not necessarily an analyst) has to think about the components in more detail and perhaps propose a design change based on the findings and analysis.

Furthermore, as the method here is focused on the systems collecting information about individuals, in the *assessment model* the individual is put at the center of the assessment. Some of the attributes are viewed from the companies' viewpoints, but most of the attributes value the aspects from the view of individuals' privacy, or its loss if the information is disclosed without authorization. This approach in putting the individual at the center is the same in, for example, Privacy Impact Assessments (PIAs) [51, 52] and some privacy risk assessment models, such as [53].

Moreover, as the first contribution enables incorporating of all of the PbD principles [45], the *assessment model* can strengthen these decisions. The model helps to incorporate four of the seven (1st, 2nd, 5th and 6th) PbD principles into the design.

1.6 Research methodologies

The design processes of both contributions follow the process of design science research (DSR) methodology [54] and are detailed in part III. The contributions (*abstraction method*, *iterative framework* and *assessment model*), are evaluated during the DSR process; thus, the evaluation of design artifacts is an integral part of DSR [54]. How these processes are located on the time line of the research and on the time lines of the projects in this research, are presented in Appendix A on page 247. The time line descriptions also include the research publications, which are presented in Appendix B on page 251.

The first contribution was developed with the principle of abstraction and generalization, a part of interpretive studies [55] using data from a questionnaire and experts' insights into the smart grid environment. Whereas the information and details were derived using the principle of abstraction and generalization, the complete development process of the *abstraction method* and the *iterative framework* followed the process of DSR methodology [54].

The second contribution is a direct solution to a real-world assessment problem. Thus, it was developed with DSR [54] utilizing theoretical definitions and real-world requirements stemming from legislative regulation and analysis needs.

In section 6, the foundations of the two research paradigms, DSR [54] and the principle of abstraction and generalization [55], and are detailed. They are presented in part III along the descriptions of the research to create the contributions because the results of the research, and the two contributions are closely tied to the two research paradigms. Thus, it is not feasible to present the research paradigms in detail in this section. In the following, these methodologies are briefly introduced.

Design science research: Design science research is a methodology for designing a solution to a specific real-world problem utilizing existing theories and approaches. In this thesis, DSR is used as a process for development and is described in this thesis as activity driven. The guidelines, different components, design cycles and questions to be asked during the DSR process are briefly introduced in section 6.

Abstraction and generalization: The process of abstraction and generalization is a combination of the principles of the hermeneutic circle and contextualization [55]. Hermeneutic circle is an iterative method to gain deeper knowledge about the relations of different contexts and their details. Contextualization principle is a method to put the issue under research into its social and historical context to better understand the different relationships within the context. Abstraction and generalization apply the iteration from the hermeneutic circle and the relevance mapping of contexts from contextualization in order to establish theoretical connections through logical reasoning within the research context.

1.7 Terminology

In order to make this thesis easier to read, certain often confused terms are clarified. The following also gives insight into how these terms are used in this thesis.

1.7.1 Ecosystem vs. environment vs. system

Each of the terms, system, ecosystem and environment, has a specific scope. However, they are connected:

- An ecosystem is a system of interconnected components that is established through the interaction of organisms within their environment working toward a common goal[25].
- An environment defines the surroundings or conditions around an organism that influence it[26].

[25] http://www.merriam-webster.com/dictionary/ecosystem

[26] http://www.merriam-webster.com/dictionary/environment

- A system is a coalition or a group of organisms or components that work together[27].

Therefore, in this thesis the term ecosystem is used to refer all of these because it defines the relationships between all possible components, including human components[28]. The term ecosystem also has a larger definition comprising the environment and the system operating within the environment. However, in some parts of this work the terms environment and (information) system are used, thus their scope.

1.7.2 A distinction between the terms information and data

In some contexts, information and data are used as synonyms, but during this study, it became evident that these terms describe two interlinked concepts. In this thesis, they are treated as separate concepts. Here the differences between the two concepts are described.

It is said[29] that, in the English language, the differences originate from early meanings and definitions. The word “data” is derived from the Latin word “datum” that is “something given”[30], whereas the word “information” is an even older word originating from Old French or Middle English that used to mean “the act of informing”[29]. Therefore, there is a clear distinction between these two commonly mixed-up terms.

Data is a chunk of binary, a block of bytes or a plain text entry in a file, database or cloud describing an action, an event or a reaction or it can be a combination of each producing, for example, a log entry about an individual’s behavior. Data is a single limited occurrence or a collection of occurrences, which may or may not have a connection to any event source, individual or event[31].

Information is a much more wider concept containing data about an event source, individual or event[32]. Information is all the peripheral additional data that can be interconnected with different pieces of data in order to connect the pieces of data to an individual, for instance.

Simply put, data is a raw, unprocessed and unorganized small piece of fact. Information is the processed, structured and organized form of data that can be a

[27] http://www.merriam-webster.com/dictionary/system

[28] http://www.differencebetween.net/language/words-language/difference-between-environment-and-ecosystem/

[29] http://www.diffen.com/difference/Data_vs_Information

[30] http://www.oxforddictionaries.com/definition/english/data

[31] http://www.merriam-webster.com/dictionary/data

[32] http://www.merriam-webster.com/dictionary/information

combination of multiple pieces of data, in raw or processed form, to establish a connection to an action, event or a reaction of an individual.

1.7.3 Information privacy protection is not data protection

In general, data protection is more than just protection of personal information as Francois Gilbert, the author of *Global Privacy and Security Law*, describes [56]. Data protection often means information security, in which personal or otherwise sensitive information is protected through security measures. Therefore, data protection is a much more wider concept than information privacy [52].

Data protection includes such terms as *purpose of use* and many others related to security. Data protection deals with securing the data, as well as the information that enables to establish the connection between data and an action, event or a reaction of an individual. The term is defined as "the protection of the integrity and accessibility of data" [56]. Therefore, data protection is a wide concept encompassing security attributes in order to protect personal data and does not account for the identifiability of the information, a key issue in information privacy.

1.8 Structure of this thesis

This thesis starts with a problem description, continuing through a description of the research questions to the presentation of the research methodology. This is then continued with the description and assessment of the real work, and the thesis is concluded with ideas for future development and final remarks. This thesis consists of five parts, and the structure is detailed as follows.

Part I

The first part begins with an introduction to the subject that is dealt with in this thesis.

Section 1: This section offers an overview of the problem with privacy in the modern world. In addition, some state of art related to privacy is introduced, which is more detailed in the second section. Next, the goal of the research, the research questions, the statement of the research and the limitations of the research are presented. Last, the contribution of this thesis is summarized with a short discussion about both parts of the contribution, and the research methodologies are introduced. Finally, this section concludes with this description of the content of this thesis.

Section 2: In the second section, the difficulties in understanding and defining privacy, especially information privacy, including a bit from the history of privacy and from the current situation, are described. This chapter is then continued with a presentation of real-world privacy threats followed by a definition of information privacy. After information privacy is defined, the more specific privacy threats are discussed, and legal aspects are introduced. The differentiation between two often confused terms, information and data, is described next and is followed by a definition of risk and information privacy risk. This is continued with a literature review of various methods, approaches and tools that are used either for security or privacy assessment to show the influences and background work for the development of the method as a whole. Last, an overview of the state of art is presented in light of this research offering a discussion of risks, privacy threats, methods and definitions of risk, privacy and information privacy presented earlier.

Part II

In the second part, the contributions of this thesis are presented.

Section 3: In the third section, the first part of the contribution, the *abstraction method* and the *iterative framework* is described. First, the fundamental concepts of the abstract and functional models of the *abstraction method* and the *iterative framework* are presented, and use of the concepts within the models is detailed. This is continued with a discussion about the differences between the uses of the *abstraction method* and the *iterative framework*. Last, the key benefits of the *abstraction method* and the *iterative framework* use are presented.

Section 4: In the fourth section, the *assessment model* is presented in full detail. The description begins with an introduction of the scope, focus and goals of the model and is continued with a detailed presentation of the requirements, constraints and attributes of the model. This is followed by the description of the *assessment model* and all of its more specific details and components. Last, the model usage is described with an introduction of how to select different values for calculation and how to generate the value with three-step approach.

Section 5: In the fifth section use of the contribution of this thesis is summarized. This section presents the steps necessary to conduct the assessment with the approach consisting of contributions 1 and 2.

Part III

The third part begins with a description of the research paradigms and principles used in the research and continues by describing the design processes to create the contributions of this thesis. Each design process is described as an activity-driven DSR process in which evaluation is an integral part. Each resulting artifact (*abstraction method*, *iterative framework* and *assessment model*) is evaluated against the devised criteria in the fifth DSR activity.

Section 6: In the sixth section, the research paradigms and principles, the principle of abstraction and generalization and design science research methodology are described.

Section 7: In the seventh section, the development process of the *abstraction method* is presented first. This is continued with a description of the process to establish the *iterative framework*.

Section 8: In the eight section, the process of developing the *assessment model* is detailed.

Part IV

This part concludes the thesis. A discussion about future development is presented along the final remarks about this research in separate sections.

Section 9: The ninth section offers a discussion about the future development of the complete approach and its sub-components, the *abstraction method* and the *iterative framework*, the *assessment model*. The development directions, which could not be carried out due to a lack of time, such as software implementation of the approach, are also described in this section.

Section 10: This section concludes the thesis. Final remarks on the whole research, as well as the research results, are given.

Part V

This part contains the appendices for the thesis. Seven appendices are included: (A) the research process time line, (B) the list of publications, (C) a description of the MobiServ environment layout, (D) the seven DSR guidelines, (E) a presentation of the use of the complete approach to build a new ecosystem through a case example of the Game Cloud development process, (F) the results produced by the model for the Game Cloud case example, (G) the questionnaire created in Smart Grids and Energy Markets (SGEM) [57] project, including the answers to the questionnaire, and (H) presents the value matrices devised for the dependency calculations of the second *assessment model* prototype.

2 Privacy state of art; the concept, definitions, meanings and solutions

In this section, the real-world problem to which the approach is an answer, is described. Privacy issues are examined from multiple perspectives involving societal, legislative, research and real-world contexts. The threats to privacy are also discussed in this section through three example cases of real-world implementations and their use of personal data. Risk, privacy risk and the more definitive information privacy risk are defined by drawing knowledge and influences from existing research on, methods of and definitions of privacy, risk and assessment of these two. Last, a literature review of risk assessment methods is presented. This section is concluded with a discussion about the foundations of privacy in relation to this thesis.

Some parts of the digital game platform threat example (2.3.3) are taken from the author's fourth publication [58] (see Appendix B). The section describing new legislation on information privacy (2.4.2) has portions of text taken from the author's fifth unpublished manuscript [59]. The sections in which the definitions of risk (2.5.1) and information privacy risk (2.5.2) are presented are taken from the unpublished fifth manuscript [59]. Some parts of the literature review presented in eighth sub-section (2.6) also come from the unpublished fifth manuscript [59].

2.1 Privacy as a concept of cultural norms and behavior patterns

Privacy is essentially a human devised concept [21] to protect ourselves from another human-devised constitution: the governing party, the government in current times [6]. The main idea behind privacy is to give individuals the freedom to be whoever they want to be, to believe in what they want and to have the freedom of thought, whether controversial to mainstream ideas [60]. But the beauty of privacy lies deep within it. Allowing an individual to think controversial thoughts can, in the long run, benefit the community as a whole [11], even in larger meaning that the people in that community can understand. The ideas devised in the protection of privacy may be those that drive the development of the whole society in a completely new direction.

2.1.1 Historic perspective

Not many of the people who so fiercely guarded their religion-based mainstream ideas about geocentricism would in their time believe that the controversial idea of Galileo Galilei would become the new mainstream. This one controversial, scientifically proven theory was at first disowned, since another, The Aristotelian truth, was acknowledged. However, in retrospect, Galilei devised his idea of heliocentrism in private and only when he had some evidence, i.e., a new (strong) theory, did he go public with it. He first explained to Grand Duchess Christina[33] that his theory did not conflict with the mainstream ideas [61], and after these letters were sent to Roman Inquisition, Galilei had to defend his ideas in person.

Unfortunately, during Galileo's period, unlike today, the scientific world was controlled by the Church and the theory was regarded as heresy [62]. However, with his theory Galilei brought benefits to research on astronomy and expanded our understanding of the universe around us. Being controversial at the time of creation does not mean that the idea or theory is not possible or not acceptable or not beneficial for the future of the human race.

One could speculate that, in that era, if there had been a network for sharing ideas in real time that could also be monitored Galileo might have been arrested at the early stages of his groundbreaking work. This is one example of why we need privacy. It gives us the freedom to be curious and creative [11], to think freely, to think outside the box, to see the universe as we see fit and to share our ideas without fear of being locked away because of our thoughts. Controversial ideas are those that might drive the thinking into new directions and open up the barred eyes of many.

2.1.2 Privacy is a human construct

It is unfortunate that even among the people who call themselves scientists some ideas seem to be preposterous or impossible at first glance. The world around us is an interesting place that we can view through our limited senses, and through the devices that we create with our limited understanding of how the universe around us really works[34]. The evolution of the human species has perhaps required that our senses are limited in order to favor other abilities, such as certain fine motor skills, logical reasoning and empathy. But the last ability also creates many problems with our logical reasoning. If we can draw a basic theory from our understanding of how the environment around us works, it can be declared an exact science. Laws of nature are quite well understood, such as physics, and if we base our understanding on that, we have, a strong basis as the grounding theory is proven and approved. But if the theory involves a concept devised by humans or a collection of humans to protect ourselves from groups of other humans, then the definition is not exact. The main reason is that we humans also feel, and, therefore, humans can be highly irrational on some occasions [63, 64].

Privacy, as mentioned, is a human construct [21]. Therefore, the definition is con-

[33] http://inters.org/galilei-madame-christina-Lorraine

[34] http://www.huffingtonpost.com/entry/what-the-worlds-first-cyborg-can-teach-us-about-color-identity-and-art_559c5693e4b042b0befa2ba5

tinuously evolving; the definition is never exact. It can never have a singular definition because people develop, societies develop and the needs of both develop as well. Privacy is a continuously fluctuating concept in an ever-flowing stream of ideas, theories, changes, development and the fears of man. The definition of privacy is drawn from the thought patterns of irrational bio-chemical organisms, but these organisms, us, have certain basic needs. In addition to the need for nutrition there are five levels of need defined by Maslow [65]: self-actualization, esteem, love, safety and psychological needs; self-transcendence was added later.

In addition to these needs there is another one: the right to be left alone, i.e., right to privacy, which is also referred to as an aspect of human dignity [66]. The United Nations declares this a basic human right [60], but for Finns, whom the author also represents, privacy has been a construct that we take for granted [67]. It is built into our societal norms [68]. In Finnish society, people prefer silence and do not waste time on small talk because we are uneasy about talking to strangers [69]. By leaving other individuals alone, we respect their privacy [69] and expect them to do the same for us. Not all people understand this, and many societies do not work this way. Privacy as a concept in all modern civilized societies shares many similarities around the world [5]. However, the concept of privacy is not universal, and thus, many differences exist making it difficult to achieve a consensus on the matter [5]. In Europe, the definition is uniform, but compared to the understanding of privacy in the United States (US) there are major differences in legislation and how people perceive the concept of privacy [19, 20].

The first steps toward a modern understanding of individual privacy were drawn during the imperialistic period in Europe, but the first actual writing about privacy was created on the other side of Atlantic [19]. In the late 19th century, Warren and Brandeis wrote an article [10] on everyone's right to privacy that defined the basis for the human need for privacy. In the article, "right to life" was extended to cover the "right to enjoy life" and the "right to be let alone." The latter is more interesting from a legal point of view, whereas the former states that everyone has the right to pursue happiness, a basic human need for an enjoyable life that should be de facto for all human beings. But the legal view is more apt for the scope of this thesis. As the concept of privacy was previously introduced as a construct to protect ourselves from government intrusion, Warren and Brandeis' declaration [10] is the origin of it. Although the need originated in 18th century Britain [19], this is the first published article about the issue that was adopted to legal definitions.

2.1.3 Into the digital era: more options, more freedom, more risk and no privacy?

The "right to be left alone" was an apt declaration before the society was digitalized. The right covered, even in legislation, all the private premises of an individual. In that time, a man's home was his castle. Home searches required, and still require, a warrant. The digitalization of our world has changed this situation and put it in overdrive to its full extent. It is said that the Internet of Things can make it even worse [5].

What can now be considered as individual's personal space? It is challenging to define it since now most of the information an individual creates (actions, writings, music/movie preferences, web browsing and game playing) are done with digital equipment. Even if the actions are done within walls without a directly connected device, some home appliances can still monitor and record the actions (e.g., Samsung TVs[35]). If all data can be controlled within the home network of an individual, then the data is under the control of that individual and is, therefore, private and protected by the definition of physical privacy. But cloud services used over the Internet may obscure this situation. If there is an external interface (accessible from outside, e.g., the Internet) into the home network that is not protected allowing data transfers to, e.g., a cloud-based service, can that particular information within a home network be regarded as private? The information should be considered private, but if the information is freely accessible without any means of intrusion, it becomes a legally challenging issue. Is it espionage related to wire-tapping if an external person monitors the information through a "hole in the wall"? However, if one agrees with the terms of service, the "espionage" is justified.

What about a scenario where the devices communicate over an unprotected wireless network? In such a network anyone in the vicinity can monitor the traffic as all wireless devices are omni-directional. It is more of a scenario where an individual pushes his or her information into the surroundings without even knowing or recognizing the situation.

The previous example is not a big issue and can be regarded as eavesdropping on a single individual. Almost all the same information can be retrieved by looking through an open window. But the digital information is more accurate, and it can be kept in the memory. The human-based storage system usually tends to push some things deeper into entangled organic synapse-driven data storage filled with memories of new and old, from which retrieval is sometimes slow or just impossible. With digital information, there is always the possibility that the device could fail, and information is lost. However, some things can be always retrieved. This is not the thing with dead humans -– at least not yet. In this case, the data will be lost. Therefore, the distribution of one's own life in digital form is much more risky than leaving the curtains open at home. Furthermore, the secure deletion of data from digital media is challenging, and some things might be retrievable even after a careful wipe [70].

When the information is by default stored on a server managed by a third party, a cloud operator, for instance, the issue becomes reality. Many purchased devices

[35] http://www.dailymail.co.uk/sciencetech/article-2959928/Samsung-TVs-left-vulnerable-hackers-Security-expert-reveals-recorded-voice-commands-aren-t-fully-encrypted.html

and appliances, such as televisions[36], mobile phones[37] and even refrigerators[38] can send information about use to the manufacturer's servers. Or as Samsung Smart TV's do, the information is sent directly to a third party[39] – unencrypted[35]. More and more people are becoming interested in the features these devices offer, as well as how the devices send and process the data as, for example, hacking Smart TV's is legal[40] and easy to use[41,42]. Many different problems and direct faults because of negligence are found, which may decrease the popularity of certain manufacturers in the eyes of their customers. This may be expected since it is shown that when people learn about privacy flaws in a service, people lose trust in the service [71]. Samsung reacted to the accusations and problems by encrypting the collected data (as claimed in the article of The Register[39]), thus protecting the privacy of their customers.

Not only is the collection of information problematic, but also sheer extent of such collection is becoming a worrying issue, not only for the cloud service providers, system maintainers and researchers but also customers. The vast amounts of collected information introduce new kinds of threats to privacy because so many different services are collecting information from various sources. This is the key issue worrying people. People are getting worried about even seemingly peripheral information that is available about them [8], accessible over various information networks and processed by various participants for a multitude of purposes.

2.1.4 New systems, new opportunities and new threats

Technological solutions are seen as a way to enhance our quality of life, and in some cases, life expectancy. The intent in many new technologies is to make things in life easier and better, and to support better monitoring of one's life.

Now, monitoring of one's life is an interesting factor for many as the sales figures of different body monitoring devices project[43]. Additionally, internal body monitoring devices are listed as one of the top trends of 2016 by Ericsson Consumerlab[44]. People now can measure their heart rate and even blood pressure at any time without the expense of a visit to a doctor. Furthermore, these measure-

[36] http://www.darkreading.com/compliance/lg-admits-smart-tvs-spied-on-users/d/d-id/1112755

[37] http://arstechnica.com/security/2013/11/smart-tv-from-lg-phones-home-with-users-viewing-habits-usb-file-names/

[38] http://www.digitaltrends.com/home/ge-firstbuild-chillihub-smart-fridge/

[39] http://www.theregister.co.uk/2015/02/17/samsung_smart_tv_privacy_rewind/

[40] http://www.hollywoodreporter.com/thr-esq/is-legal-hack-a-smart-834835

[41] https://hackaday.com/tag/smart-tv-hack/

[42] https://iicybersecurity.wordpress.com/2015/07/07/how-to-easily-hack-your-smart-tv-samsung-and-lg/

[43] http://www.theguardian.com/society/2015/may/19/digital-fitness-technology-data-heath-medicine

[44] http://www.ericsson.com/res/docs/2015/consumerlab/ericsson-consumerlab-10-hot-consumer-trends-2016-report.pdf

ments can be done without any interaction with the individual. Everything can be logged and analyzed later with the device manufacturer's services, which are usually in the cloud. The storage of such data is growing, and the data is a big opportunity for all participants. The individuals also benefit from this as they are able to compare themselves to others, but the data is useful for other parties, too.

Monitoring is not limited to bodily functions with devices voluntarily bought by individuals. Daily routines, even inside one's residence can be tracked and analyzed with smart meters [12, 30, 31, 36, 72], the daily routes one uses can be tracked with Global Positioning System (GPS) systems tracking the location of individuals' vehicles and regular customer cards offered by daily product market chains, offer details about purchasing behavior. Health services also store data about patients in digital form enabling details of an individual's illnesses and allergies that can be used to cause direct harm. Services that offer ILS for elderly individuals collect the daily routines of the individuals in addition to accurate health data. Furthermore, the personality of an individual can be formed by utilizing data from various data sources, such as social media [29, 42] and games [37]. On social media, many already publish a lot of information about themselves that can be used to profile, track or cause direct harm to the individual, but games are a completely new area. With proper tools [41], the data the games generate, especially for new services [46], can be analyzed from multiple viewpoints [38] to form a psychological profile [37, 39] of a player.

These are examples of the new ways that enable more detailed monitoring, collection and analysis of an individual. In addition, there are existing ways to track a person utilizing browsing behavior, cookies on websites, IP address tracking, purchasing behavior on e-stores and credit card payment tracking. These methods also give details about an individual and his or her location but with much less detail than the new technological solutions enable. However, the old and the new technologies can support each other. When data is combined from multiple seemingly harmless sources, it establishes a complete information package of an individual, which becomes a real problem if a third party or governments use this kind of information for their benefit without the individual knowing about the collection and combining of the data [19]. This is what people are now worried about [8]. It has become public that certain government agencies collect and analyze information about different, even innocent individuals with all means necessary. In light of the NSA revelations, the EU, for example, has published a document [3] explaining how the different surveillance programs of U.S. agencies affect the fundamental rights of European citizens.

This is a worrying issue for many as information collection is getting out of hand as monitoring increases without control. Not only the legal use of information is worrying but also the monitoring of individuals' lives is a big opportunity for people operating in the gray areas of data analysis (marketing) and completely on the dark side (criminals). Abuse of the collected data opens up possibilities not only for targeting spam or phishing emails with specific topics [73, 74] by, for example, following TV-watching habits [12] or tracking buying history [42]. Data allows the criminals to track an individual for invading the residence of an individual when he or she is not at home or attacking while the individual is sleeping [75]. But on the other side of the law, such monitoring can be used for some good, too. In the US, police and Drug Enforcement Agency (DEA) have monitored abnormal electricity usage in residential areas to reveal individuals who are more likely to grow or manufacture illegal pharmaceuticals or drugs [26, 76], although there are false positives, too[45].

Therefore, it is a question of whose life these new technologies make better: the people or companies or the law enforcement, or are the people who want to be in control the only ones benefiting? In general, it should ease the lives of every group without sacrificing others. The current state, however, shows that regular people, the end users, are the only ones who suffer. But it is not the technology's fault. This situation is caused by the information that is created and collected or gathered with the new technology. For this, we need to have ways to force privacy into new systems to guarantee that privacy issues are taken care of. First, we need frameworks to apply in the design phase and methods to analyze the design decisions for privacy risks. Second, information privacy has to be enforced with legislation that requires companies, corporations and organizations to assess and react to the information privacy risks found in their new or existing systems.

2.1.5 Perception of privacy fluctuates

The information that is collected about individuals changes our understanding of privacy. Laws have to be re-designed to accommodate the new needs introduced by the information. The traditional understanding of privacy no longer directly applies to this world of binary forms. Rarely is this data, collected by household appliances or personal mobile devices, kept within one's residence or within the personal limit of an individual. For information ownership this is problematic; the data collected from the actions of an individual should belong to the individual. The raw data might belong to the individual, but the processed data used for making decisions may belong to the company collecting the data or to the company that later processes the data.

For example, in European legislation the definition of private information is tied to close links between the event and the person [49]. The data, therefore, has to be identifiable information to the individual for the laws to apply. Currently, there is no stance on information derived through data mining that can be linked to an individual but not directly.

[45] http://www.computerworld.com/article/2469854/internet/bitcoin-miners-busted–police-confuse-bitcoin-power-usage-for-pot-farm.html

2.2 Information privacy: the definition

Daniel Solove states in his study [7] that:

> *The term "privacy" is best used as a shorthand umbrella term for a related web of things. Beyond this kind of a use, the term "privacy" has little purpose. In fact, it can obfuscate more than clarify.*

The same study [7] also showed that in the US people tend to perceive privacy through security. They tend to understand privacy as a fallacy *"I've got nothing to hide."* We all have something we want to hide. We live inside personally managed, if not owned, houses or apartments, and we draw curtains over the windows if we undress. Or at least most of us do. Therefore, we all have a basic human need for privacy. For this reason, privacy is a part of basic human rights [60].

The struggle with privacy is about giving away freedom in favor of control, or to balance the two [6]. The Universal Declaration of Human Rights by the United Nations [60] states that every human should be free from oppression and have freedom of speech and thought as a basic right. Privacy is a right we all should have [10, 60], the right to be free. However, in the digital world maintaining privacy is difficult, and it has been speculated that in the future, privacy will become a luxury [5]. "Dataveillance" is increasing [5], and it seems that this basic right can no longer be taken for granted. But with moderate societal control over an individual, for example, through legislation and regulations that limit and control information use, individuals can have the freedom to which they have the right.

Identifiability is one of the key issues in information privacy. Only when the information can be connected to an individual can it be used to harm the individual autonomy of an individual through, for example, an identity theft. Protecting privacy rarely has any direct benefits for an individual, and the benefits come in the form of prevented harms to an individual. Private information is the data that can identify an individual [77] or information that can be identifiable to an individual as referred in European definitions [48, 49].

Therefore, privacy cannot be qualified only by the damage done [7], nor should it be regarded as a form of secrecy [6]. Information privacy is about maintaining the individual autonomy of an individual by encompassing the integrity and confidentiality of the individual in the digital world. In this context, identifiability is a core component of integrity and confidentiality.

2.3 What is the actual threat?

Data in its binary form is not the issue that threatens individuals' privacy. At issue is the information containing all related connections between the individual and the binary data. Identifiability is one of the key issues. Data in its binary form is of no use to anyone until it can be connected to an identity. The EU, for example [49], refers to private information as information that can be linked to an individual. Another key issue is the nature of the data and the possibilities it opens up. It has been found that gaming data can enable psychological profiling of players through psychographics [37], for instance. If the information that is identifiable with an individual also enables the formation of a psychological profile of that individual based on the actions the individual, it is the complete package of an individual in digital form. The collected information, therefore, can be used to establish a digital identity of an individual that goes way beyond the digital realm grasping many features of an individual that used to be limited to perceptions observed in the real world.

In the following the potential threats in three scenarios are described. In each scenario, information is collected about the users or from their actions within the scenario in different ways for different purposes.

2.3.1 Too smart electricity: the case of smart grids

Years ago, the European Parliament published an agenda [78] about equipping 80% of European residences with smart meters to support a wide variety of smart grid operations by the end of 2020. It is an ambitious goal to achieve a good cause: to enable more efficient electricity distribution systems. A smart grid has many benefits either for the companies generating and delivering the electricity or directly for customers, the consumers of the electricity. With a smart grid the companies get (1) more rapid and detailed responses on error situations, (2) more control over the electricity network, (3) more details about energy usage to apply smart, localized load balancing of the electricity network and, most importantly, (4) hourly changing tariffs for electricity in order to establish accurate billing. These are major benefits for the companies, but the customers are getting something in return; monitoring of their own consumption in real time with expense estimation. Now the customer is seen as a active resource in the system who has the ability to impact the long- and short-term energy consumption through accurate, real-time monitoring of own consumption to moderate electricity consumption.

But the new system is not without challenges from emerging threats. The threats emerge from the consumption information, thus, its accuracy and the details that can be derived from it. In the Netherlands this was seen as a big problem, and the local law on smart metering was contravening the European Convention of Human Rights [16, 17]. In other European countries, privacy laws may have their own peculiarities that restrict information collection, storage or processing. For example, in Finland, data has to be stored for six years [79] (to demonstrate the extent of the data: 200 terabytes of data is created every year with a half a million customers if data is measured four times an hour [80]). This creates stress on the party controlling the data: how to maintain security of the data for the storage period and how to retain the privacy of their customers for the time period. To get back to the situation in the Netherlands, the verdict about smart metering and citizen privacy resulted in voluntary installation of smart meters. This may have a negative effect on the EU's agenda [78] but demonstrates that trust and transparency are important in new systems and their deployment.

With smart meter installations, privacy rose as the central issue. People felt that their privacy was at stake, and they started complaining. The government was not the only party that noticed the increasing concern. The research on smart meter privacy is an ongoing and possibly never-ending issue. Now it is known that electricity consumption data is exploitable in a multitude of ways [12, 30, 31]. The possibilities range from monitoring TV-watching habits [12] and identifying use of home appliances [30] (e.g., computers, TVs and media players, since each device has its own unique energy fingerprint [81]) to accurate monitoring of sleeping cycles and presence in the residence [31]. This data, when connected to an individual, can be used to perhaps not to directly harm but at least affect an individual's privacy. Exploitation of the data can enable a criminal to, for example, execute an home invasion while the resident is away or asleep.

The severity of the problem has been acknowledged and shown in the wide range of countermeasures to hide the identity of the individual in smart metering systems [32, 33, 34, 35, 36, 82, 83]. In addition, the research on smart metering and smart cities is attempting to find solutions to maintain the privacy of individuals involved in the system operations [27, 28, 36, 72, 84, 85, 86, 87]. Furthermore, the National Institute of Standards and Technology (NIST) has also listed the potential privacy impacts on smart metering data [26]. The consensus is that the data is private (personal data in legislation [49]), and it must be protected and anonymized. However, some approaches, such as aggregation, are not good for companies as such approaches can create inaccuracies [83]. A way has to be found that satisfies all involved parties and helps to maintain the customers' trust. It seems an ongoing battle where the individual is put in the center as the source and the controller of the flow. However, all the threats point to that individual.

2.3.2 Assisted and spied upon: the case of independent living support systems

Whereas the smart metering system is meant to give control to the individual by putting the individual at the center so does the individual who resides in the center (of attention) in ILS. These systems have a completely different scope: The aim is to aid and assist the individual in daily tasks to make it possible to live in one's own home as long as possible. This is usually achieved with a set of cameras, smart sensors (e.g., smart clothing) and robot companions as in MobiServ [24]. The main points of these systems are constant monitoring of daily routines (eating, drinking), monitoring of health status (e.g., heart rate) and observing daily exercises and the need for further assistance (e.g., medical assistance), all of which require that an individual is monitored inside the private residence. Or, as in the case of MobiServ [24], a care home, which still falls under private premise regulation. One of the main problems here is that the residents might not be able to understand the privacy risks of such monitoring, and getting feedback from the residents is difficult, due to their lack of technical knowledge.

Designing the whole system and even eliciting the requirements are difficult [44]. The constant monitoring of the resident puts a lot of pressure on security and privacy design. The sensors and cameras can be highly intrusive and collect data that can be later exploited to harm the resident's privacy. In such a system, the security has to be thoroughly assessed on a component basis [44] to detect weak spots [43] to strengthen them to meet the security needs. But even with proper security measures, the resident's privacy cannot be guaranteed. In this system, privacy must be assessed in a different scope than security [44] by including non-technical aspects, such as legislative requirements and the rights of an individual in the process.

Since the resident is under constant monitoring, the recorded images as well as the rest of the sensory data are to be anonymized in order to avoid identifying the individual and connecting the data to an individual. The images or videos from one's home alone are enough to harm privacy by gaining knowledge about daily routines (e.g., sleeping, showering), places where valuables are kept or physical deficiencies in case of a planned burglary, for instance. In addition to videos and images, the MobiServ system [43], for example, contains many different networked components (portrayed and explained in Appendix C) that either store the sensory and analyzed data or offer an interface to the maintenance or control of the ILS system. In addition, some external systems allow remote monitoring and interaction with the user. These systems are separate computers or systems that are not considered integral parts of the system but are included in the security analysis of MobiServ [43].

All of these systems, if poorly protected, can jeopardize privacy by allowing a malicious party to spy upon the elderly resident, who is likely to be unaware of such possibilities. The intelligence obtained by spying on discussions, daily activities and health status may put the resident in danger by allowing the malicious parties to execute tailored scams or identity theft. These attacks and exploits can be done on a large scale if the whole system is being compromised (e.g., through 0-day vulnerability) and the victims might be unaware of the severity of the problem.

In this case, the security of the system plays a key role in protecting privacy. However, the need for security in various places comes not only from the security needs to protect the system and its operation but also from the privacy needs of the resident. Therefore, the severe threats and the privacy requirements are the foundations for establishing a secure system that also protects the users of the system, not the system itself. This is imperative in user-centric environments, such as games.

2.3.3 Psychology of a gamer: the case of digital games platforms

The privacy threats in games were not in the news until the emergence of Net 2.0, and collection of such data with the help of new digital games platforms. Psychological experimentation with games is not new. Since the 1970s, the games have been used as a means to gather data and to observe human behavior [88]. For many years, after the era of violent, aggressive and stimulating computer games in the 1990s (e.g., id Software's Doom[46]), the consensus was that games increase aggression [89, 90, 91] and desensitization to violence [92, 93], but a recent study [94] debunked the theory. In this study, frustration or the inability to progress in the game were the biggest factors that increased aggression, not the game itself.

In games, the possibilities have expanded to support different mechanisms ranging from updating the player's status and achievements to real-time interaction, i.e., on-line gaming against or with other players. What these styles have in common is the collection of player statistics that are saved to a single game server or as is the current trend, to cloud-based storage. Some of the games collect only statistics about how the games are played to help the developers, for instance. The new digital game platforms (DGPs) enable combining and processing of data from multiple games and external sources in a way that has been difficult as the platforms have been mostly separate. In addition to more accurate data collection, these emerging DGPs enable formation of an accurate player behavioral profile.

The behavioral data can be used for multiple different purposes most of which benefit the player [37], but some can invade privacy, and some, such as psychological profiling, can be harmful to players. The accuracy and identifiability of the data make it useful for psychological purposes, as well as for marketing. Marketing is not limited to game developers and publishers trying to sell sequels or other games to their existing customers; other advertisers are interested in the data. In either use, the aim is to generate additional revenue with the collected data.

The opportunities the new digital games platforms open up [58] are not limited to player behavioral analysis, better in-game statistics for players and developers and purchasing behavior data for targeted marketing. The players' benefits are also significant as better services can be constructed for them, through which the players get more content and continuity for their games in the form of game content transfers. But collecting personal data to such extent is not without privacy

[46] http://en.wikipedia.org/wiki/Doom_(1993_video_game)

implications.

Gaming data is utilized in games to benefit the player, but there are also numerous other ways [37] that might not be that useful or beneficial for the player. One possibility the data opens up is the creation of a player psychological behavioral profile. From the players' perspective, this behavioral profiling can sound a bit scary that their data is used for such purposes. From another point of view, the player behavior data and profiling of the players may be seen as completely harmless for privacy as it contains actions only in a game world. However, there is a possibility that hidden perks of one's personality can be revealed by doing something in an environment one thinks is safe from prying eyes and will not hurt anyone, such as games [58]. While the actions do not hurt anyone, the leak of these actions might hurt the one who made the action: you.

If an individual constantly steals items from another players, does that individual behave similarly in real life? Does the individual who in a shooting game attempts to cheat in order to win do the same on school exams? Should that player be put under active surveillance by teaching staff? Players would definitely say no, but psychologists might find a deeper meaning in the data. With respect to computer games, the data can be analyzed from multiple viewpoints [38] in order to understand the games and more importantly, the players [41].

Psychologists may be eager to analyze and to understand player behavior, thus establishing some valid diagnoses. However, like any new technique in its infancy, there are challenges in establishing a valid diagnosis without false positives, which enable incorrect labeling of the individuals. Using psychographics, in which the psychological characteristics of an individual are quantified using collected sensory or behavioral data, analysis of players is possible [37]. The old theories about games causing aggression have been disproved [94]. Now it is known that the reason behind an individual's aggression is connected to the player, not the game. This is one of the many reasons why gaming data enabling psychological analysis of an individual should be protected [58].

A recent study [8] has shown that people now are more worried about unauthorized access to information, even seemingly peripheral that is available online about them, by their family, friends or roommates, than about hackers or thieves. Behavioral data, when connected to a certain individual, might not be seen as a problem if fellow players get their hands on it, but the other people close to you might not understand the potentially violent and obnoxious behavior.

Furthermore, gaming data and in-game chat messages can provide insight into the personality [40, 95] and behavior [39] of the individual, e.g., through motivation analysis [38], whereas data collected from other sources, e.g., mobile phones [96], may reveal physical condition, illnesses and allergies, location, behavioral patterns or predilections. Combining and identifying all this information with an individual reveals too much and can be used to harm individuals' privacy. Therefore, it can be argued that it is equally important to protect gaming data in comparison to other electronically collected information. If the collected, even peripheral game behavior data, when processed by an analyst or a digitalized service, reveals more than is visible to the naked eye, should it be treated as private information? This brings us to the question whether the gaming data should be considered private. In [58], it was suggested that gaming data should receive the same status as health data for these reasons.

2.3.4 Summary of the three cases

A summary of the three cases is presented mainly from the information privacy point of view. In addition, the common factors in each are also discussed after the key points of each case are presented.

The key points of the case smart grid:

- Accurate consumption information can be used to violate end-user privacy, and the consumption information reveals many actions within the residence. Therefore, details about electricity consumption should be regarded as personal data, but ownership of such data is a matter to be solved with legislation.
- People's trust in smart metering has deteriorated as privacy issues are emphasized by researchers.
- Problems have been acknowledged, and a vast number of new ways to preserve customer privacy have been devised to regain customers' trust.
- The customer, the individual using electricity, is at the center as the privacy threats are aimed toward that particular individual.

Key points of the ILS case:

- Constant monitoring of an individual puts a lot of stress on the security and privacy designs of an ILS system. This is especially important because the individual, an elderly resident, may not be able to protect himself or herself or even to begin to comprehend the potential risks of such monitoring.
- The data that is collected through monitoring of many different aspects inside the residence with different means can be used to establish an exact profile of the resident. This includes sleeping cycles (as it could also be done with smart meters) and physical and medical weaknesses, to name only few.
- Real-time spying on the resident is also made possible by the video and audio monitoring required for nutrition detection. Elderly residents have to

trust the caretakers and the architects of an ILS system that the system does not allow any unauthorized behavior conducted from within the system or from outside.

- The resident, the elderly individual whose life in the residence is aided by the devised system, is at the center as all privacy threats are aimed at that individual.

Key points of the DGP case:

- The data that can be collected through played games is accurate enough to establish a behavioral profile of a player. With further analysis, the data can be useful for psychological purposes and marketing, but the data can also be used for the player's benefit.
- The collected data may be used for other purposes than for which it was collected, and it can even be sold to third parties. This, however, may have major implications for players' trust in the DGP, especially if the data is used for psychological purposes in which a decision is made in the real world on the grounds of the behavior data collected from the games.
- By combining the game-world data, and real-world data an accurate profile of a player can be created. This profile may be used only for player identification, but the profile enables much more, even privacy-threatening possibilities (e.g., identity theft).
- The player is at the center of it all. The systems are built to benefit the player using the data from player's actions, which, in the wrong hands, can be used to damage the player's privacy.

These three example cases showed that information collected from the actions of an individual may be used in many different ways. But it all comes down to identification of an individual and to unveiling the behavior of an individual. No matter how the information is collected, if it is accurate enough, it will introduce privacy problems since the focus is on the individual in question in each scenario. Even worse, if the information can be further analyzed to reveal something that is not desired and the results of the analysis are used for a completely different purpose than was intended.

This brings us to the culmination of the issue presented by the three cases; trust. If the new system is not trusted by the individuals, there is a high probability that the system is not even used, or it is used in a way that reveals too little and is of no use for the system's operation. All of these issues clearly show that privacy issues must be resolved before the systems are released to the public in order to first gain and then to maintain the trust of the people. After all, in each system the individual is at the center of the system, the individual is most vital asset in it.

2.4 New needs require new solutions: discussion about techniques, legislation and information ownership

In the world in which we currently live, almost everything is being digitalized. Old documents are converted into digital form in one way or another, by copying the information or scanning the originals. Our new actions are being tracked, monitored and analyzed by various services that were originally invented to ease our daily lives. In addition, new ways to analyze old actions from old log files in retrospect, for instance, have been devised. Data mining is the term used for shifting through vast amounts of information and the connected binary/text: the data.

By using various sources of information, data mining can be effective in analyzing the behavior of an individual. Especially in health informatics, there is a wide variety of applications where data mining has opened up new paths for analysis [97]. In addition, in targeted marketing [98, 99, 100], as well as crime analysis [101], this has been found to be very useful, but these are also the things people are really worried about [8].

New techniques protect information, and legislation forces such techniques. But to whom the information belongs and what is allowed to be done with the information is a question difficult to answer and to define, even from the legislative point of view. In the following, these issues are discussed and introduced.

2.4.1 Privacy by Design

One of the ways to tackle problems before they even emerge is with design solutions that take into account the risks of the potential problems and attempt to prevent them from happening and causing harm to the system, to the users of the system or the information contained by the system. Privacy by Design (PbD) [9] is a framework for incorporating privacy by default into new systems during the design phase. The seven foundational principles of PbD are designed for the universal need to integrate privacy into every standard, protocol and process that touches our lives as a means for preserving our freedom and personal control over our data flows [9]:

1. Proactive, not Reactive; Preventative, not Remedial: Privacy threats should be anticipated and prevented before they can happen. It is important to establish strong privacy practices in early stages of the system design and to maintain them throughout the development in a consistent manner.

2. Privacy as the Default: Privacy must be the default design choice for systems and policies delivering the maximum degree of privacy for the individuals. The created policies have to follow the fair information practices (FIPs) for

purpose specification, collection limitation, data minimization and use, retention and disclosure limitation.

3. Privacy Embedded into Design: The design and architecture of the system must have privacy protection incorporated into the core. Privacy has to be embedded in a holistic, integrative and creative way to support a systematic approach at every step of development, even after deployment. The means for protecting privacy should be integral parts and not bolted-on mechanisms.

4. Full Functionality - Positive-Sum, not Zero-Sum: The means employed and integrated for protecting privacy should not impair the functionality of the system. In addition, the incorporation of privacy requirements should not be a compromise to establish a zero-sum situation but to offer benefits that do not impair other functionality (as mentioned in the third principle).

5. End-to-End Security -– Lifecycle protection: Privacy must be protected in every part of the system and its operating domain, and the data is to be protected as well during the whole lifecycle. In addition to protection of privacy and data, accountability must be maintained throughout the domain and lifecycle. In addition to the confidentiality, integrity and availability of data, security standards have to offer methods for secure destruction, appropriate encryption and strong access control and logging methods.

6. Visibility and Transparency: All operations follow the stated promises and objectives allowing the components and operations to remain visible and transparent to all parties involved. In general, FIPs must be followed, but especially *accountability, openness* and *compliance* are the most important in achieving transparency and visibility.

   (a) First, the privacy policies must be documented and communicated to an individual involved, and in information transfers to third parties, the protection must be kept on the same level as in internal systems.

   (b) Second, the policies and practices for personal information protection must be open for individuals. This, and transparency in operations, can lead to full accountability.

   (c) Third, the policies and procedures must be monitored, evaluated and verified to ensure compliance with complaint and redress mechanisms.

7. Respect for User Privacy: The interfaces for human-machine interaction should be human-centered, user-centric and user-friendly that users can manage their own data and, thus, may prevent abuse and misuse of privacy and personal data. The individual should be the center of operations involving the use and collection of personal data.

2.4.2 New legislation on information privacy

In Europe, the European Parliament has been working on a new data protection regulation to replace the former, currently outdated one. The directive laid out in 1995 [48] covers all main issues of data protection but is falling behind in the development of new technologies and the possibilities opened up by them. Still, the old directive gives the individual a wide range of rights to information concerning oneself. According to the EU Handbook on Data Protection law [49], based on the 1995 directive [48], an individual has the authority to:

- access his or her own information from any controller processing it
- rectify information if it is inaccurate
- delete information
- object to the use of information processing or decision making (automated decisions or marketing)

But the challenges introduced by the new technologies require more pressing, definitive, restrictive and up-to-date legislation to enforce that European citizens' right to privacy is respected and maintained. The proposed European Commission (EC) privacy legislation [22, 23] aims to introduce a common set of rules for private information handling in modern information systems. One aspect of this is that requirements for private information protection are toughened and individuals' rights to their information are strengthened. Another aspect is that every information privacy infraction will be taken seriously, and if it is caused by negligence or poor design, a penalty will be issued to the responsible company, organization or corporation.

Currently, the penalties are set to be based on a percentage of the annual turnover, ranging from 0.5% to 5% [23]. The regulation also concerns the public sector and other non-profitable organizations, where exact limits for fines, ranging from €0.25 million to €1 hundred million, are used [23]. The fine amount depends on the severity of the infraction. For example, the highest fine can be given for not complying with the regulation, and a fine of 2% or €1 million can be given for repeated infractions (amendment 188) [23]. Any breach has to be reported within 72 hours to the supervisory authority and to everyone whose private information is at stake (amendment 43) [23]. The quantities of the fines and the time limits, as well as the regulations in general, are still being debated.

A third big aspect of the new regulation is that every data holder has to assess the privacy risks [22, 23] if the criteria for private information processing are met (5,000 transactions in a month). For companies, organizations and corporations, this means that they have to be able to detect problematic areas in private information handling in order to employ the necessary protective measures. It is also stated that privacy should be enabled by default into new systems, thus requiring implementation of the PbD principles previously introduced.

The new regulation proposal [22, 23] incorporates the eight privacy principles (PPs) defined by the Organization of Economic Cooperation and Development (OECD), as the 1995 directive [48] incorporated the OECD privacy principles of that time. The OECD PPs are more of FIPs) that are generally introduced to all parties dealing with private information. In brief, the eight OECD PPs define: the following

PP1. The limitation of information collection

PP2. The use of information without consent of the individual

PP3. Information should be relevant to the use

PP4. The purpose of the information collection should be clearly specified

PP5. Information must be reasonably protected

PP6. The collector of the information can be held accountable for any infraction

PP7. Access to individuals' own information should be retained

PP8. Any changes in policies with respect to personal information must be reported to the individual

Still, with an issue so multi-faceted and complex as privacy that involves continuously developing technological services, the legislation is always behind the current state of affairs in the digital world. The laws enacted to protect individuals' rights would have to be refined every year to keep up with the progress of the various services, but as the case with the new European regulation shows, the processes for improving the legislation take a long time as it is not a simple task. If the different legislation cannot keep up with the changing world, we need researchers' feedback and ideas to improve the definitions that can be adapted in courts, for instance, without changing the legislation.

One aspect is the definition of PII, which in courts serves as a jurisdictional trigger for evaluating whether to apply privacy law [20] but also is a definition for the identifiable information in information systems. The NIST [102] uses the following definition for PII:

> *PII is "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records;*

> *and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.*"

PII is used more frequently in U.S. legislation, but it has also been used in European legislation, in which the term *personal data* [48] is the equivalent term. *Personal data* is defined in European legislation [49] as:

> *Data are personal data if they relate to an identified or at least identifiable person, the data subject.*

Both define the same issue with different terms: If the information identifies an individual it is private. However, information and data have different scopes, and this is discussed later in this thesis.

Whereas the two legislations tend to differ in many ways, not only in privacy regulations, they tend to understand PII and especially privacy quite differently [20]. For this particular reason, a new version was introduced. The proposed PII 2.0 [20] promotes a common understanding of privacy on both sides of the Atlantic and can be regarded as a modern definition that helps legislative bodies' analysts to determine the need for privacy law and to assess privacy risks. PII 2.0 introduces coherent boundaries for determining the involvement of private information through three open-ended benchmark categories. The categories are the following:

1. Identified information: Information that is linked to an identity. The meaning is the same in European legislation.

2. Identifiable information: Information that can later be linked to an identity. This corresponds to the term *pseudonymized data* in European legislation [49].

3. Non-identifiable information: Information that is anonymized and cannot be linked to an identity. This corresponds to the term *anonymized data* in European legislation [49].

The rights to one's own personal information [48, 49], the fair information practices [77] and new classification categories for PII [20] are the key blocks for defining what information legislators regard as private. Therefore, it is in the hands of lawyers, judges and jurors to decide whether your behavior data was private to begin with and to decide whether the privacy laws can be applied. First, personal data needs a more exact definition since the amount of data collected from our everyday lives is continuously growing and reaching completely new areas of industry. Second, the protection of such data is required, which goes without saying. However, in order to protect private information, it is imperative to know exactly what can be classified as private. Only way to solve this chicken-egg problem is to do it iteratively and continuously improve the situation. New definitions, such as PII 2.0 [20], will drive us in the right direction, but meanwhile, we need to have the proper vehicle and a good driver to achieve the goal. Industry can drive its own benefits in this matter and attempt to circumvent the rights to access the data.

2.4.3 Privacy legislation and data mining

The legislation on information privacy regarding the results of data mining is not unambiguous. PII should be the trigger for determining whether to apply privacy legislation. It should then be a clear black-and-white issue. The problem comes from the understanding of privacy. In European legislation, the *close link* between the event and the individual is not clear enough to specify the privacy of the individual through identifiability. Various data mining techniques can be used to later connect pieces of data, collected from seemingly harmless sources, to identify an individual. However, privacy-preserving data mining techniques are being constantly developed [103, 104, 105, 106, 107] to overcome the problem.

In the U.S. the definition of “reasonable expectation of privacy” is an ambiguous way to define the need for privacy legislation [20]. This definition has been shown to be prone to misuse, even on government levels [20] to circumvent the privacy law in gathering intelligence on their own or foreign people.

In Europe, the definition of *close link* is another way to describe the situation, which seems more definite than the corresponding definition in U.S. legislation. In addition, the European legislation recognizes two additional levels for data, anonymized and pseudonymized data. Anonymized data is defined as [49]:

> *Data are anonymised if they no longer contain any identifiers; they are pseudonymised if the identifiers are encrypted.*

The pseudonymized data is regarded as personal data [49], thus, the encryption of identifiers. But here is the actual problem with this classification. In which category would the result of data mining belong? The *close link* between an event and an object in seemingly peripheral data is hard to find, and in this case, the result of data mining would be beyond the scope of privacy legislation. If the data contains no identifiers, it is not pseudonymized either but anonymized. And anonymized data cannot be considered private, but it can be connected to other data to reveal the identity behind the anonymized data [108, 109] as it is challenging to properly anonymize data [110].

This problematic issue is not defined in legislation, and, therefore, it can be stated that the definition is vague. It is not possible to define a limit for anonymized data that, for example, only the data that can be connected later to an identity is private. But how would this apply to new developing techniques, in which all data could be connected to an identity? Defining all data generated by an individual or collected from the actions of one as private information would undermine many current businesses that base their business model on analyzing anonymized data for various purposes, such as targeted marketing.

The new classifications for private identifiable information, such as PII 2.0 [20] are attempting to drive the discussion and understanding forward. However, progression is possible only if the legislation catches up, adapts and perhaps refines these definitions. PII 2.0 [20] contains three categories for information: non-identifiable, identifiable and identified.

2.4.4 Ownership and control of information

In customer service relationships, information ownership issues are a bit problematic. Can one fully control the data deletions, for instance, if some other party actually stores and manages that data? In many cases, one cannot, it is a matter of trust.

Naïvely it can be thought that in services the copyright to and ownership of user created (private) information should stay with the customer, but End User License Agreements of services or service level agreements (SLAs) can attempt to define otherwise. In Europe, these, agreements are, however, subject to EU legislation and directives. It has been suggested [111] that service providers could come forward with SLAs to protect the privacy of their customers. This is a move in the right direction, but the SLAs alone have no legal binding. To help users of business services and service providers find common ground, the EC has devised guidelines for standardizing cloud SLAs [112]. This way, the SLAs can be written in accordance with the law and, therefore, would pose no problems between users, service providers and legislators in the case of a violation of the terms.

The party offering the service should provide appropriate information protection if private information is stored [77]. The OECD recommends [77] that even if information is handled by a service provider the ownership to that information should stay with the individual. In the EU Data Protection Directive (DPD) [48] an individual has been granted the right to access his or her own information that is stored or collected by another party. The Handbook on European data protection law describes the rights of the data subjects (individuals) in accordance with current regulations [49].

Furthermore, an example of the European stance on private information ownership can be found in electricity market directives. In directive 2009/73/EC for electricity markets [113], it is recommended that information collected from the actions of the user is shared with the service provider to a limited extent and the ownership of information stays with the user. This approach has been seen as a means to increase customer trust in the case of smart grids not only from the researchers' view [80]. In addition, the government institutes for standardization on both sides of the Atlantic, the NIST and the European Telecommunications Standards Institute (ETSI), have similar views on the matter [114, 115].

The individual, therefore, is in control. If an individual wants information to stay private, it should stay private. It can be also argued that if the individual is given the full authority over the his or her information, then the individual also owns that particular information. However, it has been shown that in current systems this is not the case [29]. In personalization services, it is difficult to draw a line between user-generated information and information that is a byproduct of a website visit [29], for instance. Ownership in such cases, according to European legislation [49], would stay with the user, since the byproduct of a website visit can be identified with an individual. However, there must be a *close link* between the event and the individual for the legislative definition (right to information) to apply [49].

Economists view [18] individuals' ownership of their own private information as harmful to information markets and the economy in general. However, it is also stated [18] that potential harm could be resolved with the help of correctly set property rights and that the governed regulation of information privacy is more effective than contractual agreements.

2.5 Definition of risk and assessment of risk

The definition of risk in security systems and risk assessments is well-known but how to define information privacy risk? This is clarified by deducing the aspects of traditional risk definition leading to the definition of information privacy risk.

2.5.1 Traditional risk definition: what are the aspects?

In security risk assessments, the risk is defined through the threat likelihood, vulnerability and the value of the asset [116]. These three aspects are valued, depending on the assessment methodology and the nature of the assessment (qualitative or quantitative), to form a value describing how big the risk of loss is in the event of an attack.

With logical deduction, it can be reasoned that the important issues are covered by three simple keywords: how, who and why, if the focus is on information security.

- First, how can the asset or the data be accessed? This can mean legal and illegal access, not ruling out the potential human errors. The connectivity of an asset largely covers this issue, and other devices offering access to the asset play a big role, too.

- Second, who can access the asset and the information it contains? Since data access introduces the people aspect, access to data has to be separated from asset access. The different roles of different users of the system (customers, maintainers, employees) allow different types of access to the asset itself, to the data or to both.
- Third, why would anyone attack the asset or try to access the data? The answer is simple. The benefits that can be gained are tempting, or the attack path is easy to exploit and, therefore, profitable. The potential and nature of the data play a big role in tempting the attacker.

From the above, it can be concluded that the emphasis is on the likelihood, data and asset access, nature and potential of the data, data quantity and potential damage. In addition, in some information security methods [117] the qualitative value for information is calculated with the definition of the information importance, the age of the information and the potential losses in the event of an attack.

2.5.2 Definition of information privacy risk

This discussion introduces the attributes for defining information privacy risk, and additional attributes can be drawn from the earlier discussion about the concept of information privacy. The aspect of data protection is not included in this discussion since data protection has a broader scope than privacy [51]. Thus, only aspects that directly affect information privacy are included. The following examples present what attributes the existing models for privacy risk assessment emphasize.

Hong et al. [53] use social, organizational and technological contexts in defining privacy risk value. The categories they focus on from the social and organizational contexts are who are the users, what kind of information is stored, information access, sociological relationships between actors and types of the actors, including potentially malicious ones. From the technological context, the focus is on how information is collected, how information is accessed, how much information there is, what is the quality (significance) of the information and what is the storage time of information.

In the privacy risk model presented in the Global Technology Audit Guide [118], which assesses privacy risk on a larger scale similar to Hong et al. [53] by including also the societal context, the threat is seen as a direct consequence for an individual. The threat to individuals is composed of privacy damage, the nature of the information, the potential of the information (capability), access to information and the amount of information. The Privacy Impact Assessment Framework (PIAF) describes six common privacy risks [52]: data profiling, transaction monitoring, identification of individuals, physical observation of individuals, publishing or redistribution of public databases containing personal information and lack of doubtful legal authority.

From these examples, and from the earlier discussion about information privacy, it can be deduced that when assessing the risk to information, whether from the security or privacy point of view, the emphasis is on the following:

- The nature or the quality of the information
- Access to the information or to the asset
- The quantity of information
- The storage time of the information
- The likelihood of an attack
- Damage to the individual or to the asset
- The identifiability of the information (linkability)
- The purpose of use

2.6 Risk assessment methods

Existing methods and models approach risk assessment from a viewpoint that usually includes monetary losses [116, 119, 120], security infractions [121, 122] and the impact of the infractions [123], loss [124] or disclosure of information [123] and/or assets[47] [119]. The specific privacy risk assessment methods involve the users' societal contexts on a broad scale [53, 118], on a smaller scale as asset centric [125] or act as a guidelines [51, 52]. From the literature review, it can be concluded that many assessment methods are criticized for producing subjective [120], speculative [126], or non-reusable results [116].

2.6.1 How security and privacy risk assessment methods coincide

Security risk assessment concentrates more on the safety of the systems and its assets, financial losses, the vulnerabilities of the systems, threats against the systems and the effectiveness of the security measures and policies. The financial repercussion is mainly used to define the loss [120], but also qualitative values are used to define the impact on the business [116] or even on the individual through the nuisance caused by an attack. The security risk assessment, therefore, is focused on unauthorized access and use of resources, whether they are physical assets or information.

[47] In this context, an asset is a component, a device or an actor in the environment fulfilling one or more tasks related to the operation of that particular environment or organization.

The problem with privacy has been argued to be more Kafkaesque (The Trial) than Orwellian (1984) [19] because surveillance and information collecting are not the only aspects; withholding the collected information about the individuals from the individuals is the more troublesome aspect. People are more concerned about unrestricted access to their information than privacy and are uneasy about even peripheral information that is available and could later reveal something about them in the event of unauthorized disclosure [8]. The collected information is prone to cause more harm to individuals' privacy (reputation, e.g., online) than to the party controlling the information. However, the party controlling the information will lose reputation but in different terms, for example, loss of users and income or generally the trust of the people. The reputation loss caused by severe privacy infractions can exceed the direct monetary losses in the long run. The privacy risk assessment, therefore, concerns both sides, while assessing the risk of losing individual autonomy and the confidentiality of individuals' identity.

It is evident that both of these, security and privacy risk assessment go hand in hand. If there are no security measures or policies, private information is impossible to protect [9], but the measures are ineffective and useless if there is no knowledge about what should be protected. A privacy risk assessment offers the what and where, and a security risk assessment gives insight into how the measures are effective in protecting the information or assets (what) in correct locations (where).

2.6.2 Methods for risk assessment

The risk assessment methods used for evaluating risk to security and/or privacy are divided into two types: qualitative and quantitative. Most security risk assessment methods for enterprise needs are quantitative estimating the monetary loss or business impact using, for example, annual loss expectancy on an asset basis [116, 120].

Quantitative enterprise-level risk assessment methods, such as CRAMM [119], INFOSEC Assessment Methodology [123] and OCTAVE [124], focus on protecting assets, including the information held, and mitigating the impact of potential attacks by enhancing security or applying countermeasures. Qualitative methods can also take into account the business impact of security risk. This is, for example, the case with the "root pattern for all enterprise concerns" approach [116]. Qualitative risk analysis methods, such as SQUARE [122] and OCTAVE-S [124], as well as the approach in [116], are used to estimate the need for security; what kind of security properties should be applied and where. Most of the methods, both quantitative and qualitative, are aimed at larger enterprises. The methods do not solely concentrate on information systems and information held but take into account every asset in the domain of the enterprise. The disadvantages of these kind of methods can be summarized as that the results might not be reusable between consecutive assessments [116], or the results are subjective [120] or speculative [126].

Existing methods for assessing privacy risk usually concentrate on a single information system [127], as in “Use and Misuse Cases with privacy enhancement” [125] and are, therefore, system oriented [127]. In this study, these kind of methods are referred to as narrow scoped methods. These methods are suitable for assessing separate systems, but, for example, in new emerging technologies, privacy risk assessment has to be done on a much broader scale. In the new emerging technologies multiple different actors are involved, and the information systems are only part(s) of a larger ecosystem. Each actor has a separate, special role in the ecosystem, which introduces more complex challenges for privacy risk assessment. The privacy in such systems that collect and use vast amounts of information about users has to be defined and assessed in a different, much broader way. For example, in the same way as existing enterprise-level risk assessment methods designed for security already do.

Well-known examples of broad methods are the PIA methods, e.g., the European PIAF [51], which approach privacy from a wider perspective. PIAs aim generally to assess the impact of privacy infractions, but the methods cover a much wider concept than mere information privacy [51]. PIAs are high-level guidelines about how to conduct the assessment. Whereas the existing privacy assessment methods are usually system oriented [127], PIA methods put the individual at the center of the assessment [52] as does Hong et al.’s privacy risk model [53]. PIA guidelines [128] state that potential damage to the individual must take precedence over organizational risks. Additionally, in [53] it is suggested that a risk analysis approach can be used to identify user-centered privacy risks.

In the scope of assessing risks in new emerging technologies, the narrow scope methods and the methods designed for large enterprises collide; both can be used by applying specific areas to the process. Or the one providing broader scope can be used as a higher-level analysis process, and the other one providing a narrower scope can be used to focus on an single actor. This way, a fully detailed analysis of a large ecosystem could be formed.

2.6.3 Influences drawn for this work

The model presented later focuses on the privacy of the individual, while offering an applicable method for broad scope analysis, but the basic characteristics are drawn from risk analysis. This way, the model is not limited to a certain sized ecosystem and with a small adaptation can be used as a narrow-scoped method to assess a single system, for instance. In addition, the individual is put at the center of the assessment without disregarding the view of the company, corporation or organization since privacy infractions affect them as well in terms of, for example, reputation loss.

2.7 Discussion about the foundations of privacy and risk: a summary

Privacy is a human construct with a strong societal connection and is included in legislation around the world, but understanding of it differs. This is not limited to legislation, different people tend to perceive privacy in many different ways. Many confuse privacy with security or assume that privacy is part of security. It is no wonder since the term can confuse more than it clarifies [7]. The problem with privacy can be regarded as an issue of hiding the information, which is obtained through various means, from the individual [19] than as an issue about monitoring everyone.

Security merely protects the system and its assets for unauthorized use. Security is not meant to protect the information about the individual in the same manner. However, security means can protect the individual itself and the assets that belong to the individual, e.g., two-phase authentication in online banking. But use of the information collected during the an online banking visit can reveal something else completely than the balance of one's account. It can reveal the location, the Internet service provider and the device used to access the online banking account, to name only a few. Thus, privacy protection for the information and handling of it is needed.

These new digital means bring new opportunities and open up new possibilities for people to interact with each other and with various companies. This, however, introduces problems as the information used in the transactions and communications can be easily captured legally or illegally. Management of information collected from individuals, is a delicate issue in which the privacy and trust of the individuals are the key factors. If the new systems offering new possibilities cannot be trusted by the individuals the systems may not be used to the extent that the system is profitable for the service provider. In this type of system, the individual is at the center of attention, and the threats. The collected information that is or can be connected to the individual has to be protected in order to gain individual's trust. But when the trust is once lost, it is hard to regain as infractions or failures decrease customer loyalty [129]. People who learn about privacy infractions lose trust [71]; thus, maintaining privacy protection is imperative. Therefore, it would be beneficial to detect the potential threats in the early design stages to avoid loss of trust and, in conjecture, loss of reputation.

Protecting the information collected is imperative also because as the systems offering new services develop so do the analysis methods for seeking out anomalies in data or creating a profile based on information about an individual, for instance. A digitalized society not only means that we are allowed to do many things that used to be tied to a certain location from anywhere in the world but also the monitoring of our actions increases as well. The media attention the mishaps of the globally operating intelligence agencies received (a broad summary exists in Wikipedia[48]) indicates that people are not happy about the way the world is evolving. In addition to detecting privacy threats, privacy of the individuals must be retained to restrict government agencies' access to the information and to use it as they see fit. There must be restrictions, not only in legislation but also in the systems withholding the information. By following some basic principles, such as PbD [9], the OECD Privacy Principles [77] and the new definition of PII [20], basic protection can be established. By improving legislation, the issues regarding information use restrictions can be strengthened. The world cannot be changed overnight. Multiple small steps are required to change it, slowly.

Previous discussions about information privacy indicate that the whole concept is understood in different ways, and it has multiple meanings in different societies. Information privacy needs a uniform definition in order to enable an efficient and grounded analysis. In addition to the consensus about the definition of information privacy, the legislation has to catch up with new definitions. The three levels of PII 2.0 [20] are a good start and offer clear guidelines for how to classify personal information in common consensus and legislation.

However, the definition of information privacy guides in the making of the solution presented in this thesis. For the problem of privacy, this thesis presents an approach that helps in designing new systems to be more privacy preserving and aids in modification of existing systems to achieve the same goal.

[48] https://en.wikipedia.org/wiki/Reactions_to_global_surveillance_disclosures

Part II

Contribution

The contribution of this thesis is an ecosystem-agnostic approach for assessing the information privacy risk on a qualitative scale. The approach consists of two components; (contribution 1) an *abstraction method* and the *iterative framework* and (contribution 2) an *assessment model*. In this part, both contributions are detailed in sections 3 and 4. Use of the contribution is summarized in section 5. A more detailed presentation of the contribution use is available in the Appendix on page 261 in which the contribution is presented through a case example of Game Cloud to establish a new privacy-preserving ecosystem for interconnected games.

3 Contribution 1: an abstraction method and the iterative framework

The first part of the contribution of this thesis is a method for assessing information flows inside a system that has two distinct purposes. The method can be used either for (1) analyzing existing architectures and solutions to find the commonalities in them to be used for information privacy analysis and to establish a common reference architecture or for (2) detecting information flows and the risks and threats inside a system during multiple development iterations. The processes for establishing both are presented in sections 7.1 and 7.2. Here, both styles of the method use, the *abstraction method* and the *iterative framework*, are described. These descriptions are summaries of the research processes, and both are presented in a generic form.

3.1 The method in general

Briefly, the method described here is a high-level information privacy analysis method that helps in detecting information flows between the actors of an information-centric ecosystem collecting information about their users. The method is used to seek out commonalities by dividing the topic under study into smaller elements with the principle of abstraction and generalization [55] in order to gain deeper understanding of the topic. As a result, two high-level models of the ecosystem under study are created. The method is developed to help in evaluating and assessing information privacy issues in large ecosystems by offering an information-centric bird's-eye view. The two models, abstract and functional, present the unique instances, tasks and functions, and the connections between them in a clear and descriptive manner.

3.1.1 Definition of a task

A task is a high-level description of a single unique operative instance in an information-centric ecosystem. In the context of the *abstraction method*, a task is the highest-level representation. Each task describes one basic abstract role in general terms. The more descriptive definition is always case specific in which the abstract task is connected to a more detailed context.

For example, in DGPs there can be multiple information sources that offer details from different types of actions. In Game Cloud [46], there are two distinct sources for information: a game and a third-party service. Both can be represented with one generic task: the source as they both generate information from the user actions for the system to process. The game generates information based on the actions of the players within the game-world context, and the service does the same thing but in the context of the third-party service.

This mapping of a task to an actor is essential part of the abstraction and generalization principle [55]. This is the theoretical connection of a unique instance to a concrete instance within the context of study. The connections are detailed in a similar fashion to the descriptions presented in sections 7.1.4 and 7.2.4.

3.1.2 The process of finding out tasks

In order to map the tasks and to find out the tasks within the ecosystem, the details of the topic under study must be examined. In the abstract model, seven distinct tasks must be found within the context:

1. Controlling task: The task in which the (information) source (2) is controlled.
2. (Information) source task: The task in which the information essential for the ecosystem is generated.
3. Reading task: The task in which the information from the source (2) is read.
4. Processing task: The task in which the information read (3) from the source (2) is processed, analyzed or anonymized.
5. Storing task: The task in which the information read from the source (2) or the processed information from the processing task (4) is kept and maintained.
6. Low-level accessing task: An accessing task in which all the (unprocessed) information withheld by the storing task (5) can be accessed. Additionally, this task is meant to have the characteristics of an administrator of the system under study. Therefore, the parameters, configurations and logs of the actors executing tasks 4 and 5 may be accessed by the actor executing this task.
7. High-level accessing task: The task for high-level access to the processed information contained by the system (e.g., web access).

In order to find out the tasks and the connections to the concrete instances within the contextm the following five-step process is devised:

1. The first step is to research the ecosystem in question from the information use point of view. It is imperative to find out what kind of information generally is transferred in the context. This can be done by looking into existing similar solutions, generally accepted reference architectures, design documents or literature dealing with issues in the context ecosystem.

2. The second step is to research the actors that comprise the ecosystem. In this step, the roles, information handled and transferred, connections to other actors and location inside the ecosystem layout are investigated and mapped out. It is useful to describe the layout in a similar fashion as the presentation in Figure 7.5 on page 142 to help the next steps.

3. In the third step the information offered by the previous two steps is analyzed with the principle of abstraction and generalization. In this step, the information is sifted through to seek out the seven unique instances within the context. The unique instances are connected with logical reasoning to the concrete instances found in step 2 to support the theoretical findings. Each found unique instance, a task, has to have an actor that executes the task within the context. This step may require multiple iterations over the information to find all connections between the tasks.

4. In the fourth step the information transferred between the tasks is laid out. This is done by combining the task (unique instance) specification from step 3 with the generic information offered by the first step and the details about the information transferred between the actors that was mapped in step 2.

5. As the final step the layout of the abstract tasks and the information transferred between the tasks, the abstract model, is established. It is useful to insert the information that is transferred between the tasks in an abstract form into the model to increase readability. The model is devised to show the most generic layout of the tasks and on some occasions, changes are required in the layout. These changes may include changes to information flow directions or reducing the directionality of the information flows. These differences can be seen by comparing the abstract models of the smart grid architecture (Figure 7.1 on page 120) and the Game Cloud platform (Figure 7.8 on page 148).

3.1.3 The abstract model

The abstract model contains the generic tasks and their generic connections with the generic information that is transferred between them within any information-centric system. The layout of the tasks is presented in a generic form in Figure 3.1.

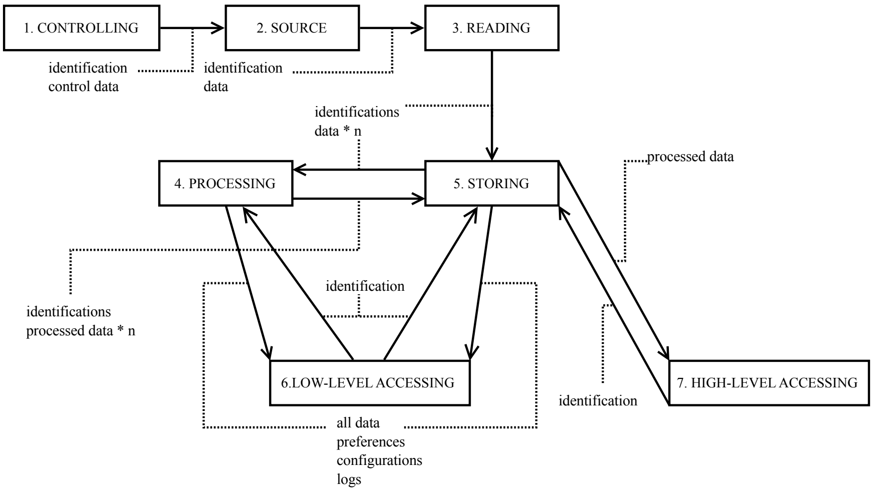


Figure 3.1: The final version of the abstract model

The arrows in the figure represent the directionality of the information flow between the tasks. The dotted connections to the arrows show the generic form of the information transferred between the tasks.

The layout takes no stance on the multiplicity of the tasks within the system as it is not needed for abstract, high-level analysis. The amount of each task is included in the descriptions of the tasks. However, if the analysis would seem to benefit from it, the multiplicity of each actor can be included in the model with a notation similar to the UML class multiplicity notation[49].

For example, the multiplicity of the controlling, source and reading tasks in the context of Game Cloud [46] are shown in Figure 3.2. Other tasks of the abstract model are omitted from the figure as these three clearly demonstrate the issue.

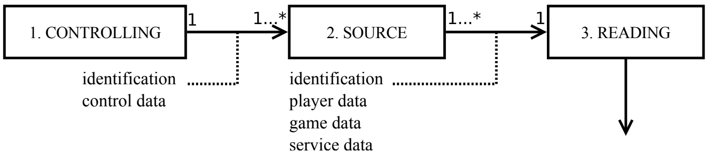


Figure 3.2: An example of multiplicity in the connections between the tasks in the abstract model

One of the benefits the abstract model and the required work on background information offer is the depth of the knowledge obtained during the process. The model itself presents the highest-level overview of the system and its information

[49] http://www.uml-diagrams.org/multiplicity.html

flows, which does not give many details about the real ecosystem. However, with further research on the functions within the ecosystem, these tasks can be mapped to concrete functions within the system. The tasks alone can be mapped to the actors found in the second step (see, e.g., the mapping of tasks to Game Cloud actors in Table 7.5 on page 144) for the initial analysis of the system, but with the functional model the depth of knowledge about the internal workings is increased.

3.1.4 Definition of a function

Whereas tasks are regarded as the highest-level representations of the instances within the context, a function is a concrete instance of an operation existing within the context (a real-world operation). Therefore, a function is a more detailed representation of a unique instance within the system than a task. Each function describes a single generic concrete operation that is participated in by many different actors.

For example, in Game Cloud [46] one of the functions is *player data processing* in which the information generated by the *game* is analyzed. Two Game Cloud actors participate in this function: the *database* and the *ontology engine*. The database maintains the information and by request sends the requested information to the *ontology engine* for processing. This processed data is then saved back to the *database*.

The previous example shows that a function is not solely part of the repertoire of a single actor but has a wider scope. This shows that a function describes a larger operation that may involve multiple actors in the context.

3.1.5 The process of finding out functions

Research on the functions within the ecosystem is also done with the principle of abstraction and generalization [55]. The knowledge about the system gained in the previous process of seeking out the abstract tasks and their connections is used here as the basis for analysis of the functions. Similarly to the process of finding the tasks, the functions are to be mapped to each other based on the information that is transferred between them.

To find out the functions and their connections, the following five-step process is devised. The steps are described as follows:

1. The process starts by searching the most commonly occurring verbs from the background information. This is another way of using the abstraction and generalization principle to find unique instances within the context. The list of these verbs is the basis for determining the functions within the system.

2. In the second step, the list of verbs is analyzed, and with logical reasoning, the basic functions are determined. The functions are described by their concrete operation in the context.

3. After the functions are detected, the information flows between them are determined. This requires that the information that is transferred is categorized on a highly abstract level. For example, in smart grids five high-level types of information were found: smart meter id, customer id, customer personal identifiable information, consumption data and processed consumption data. In this step, the use of these abstract information types in the different functions are analyzed. A mapping similar to the Table 7.1 on page 123 can be used to detail the information use in each function.

4. Next, the relations between each task and function are determined. This part pulls together the tasks, functions and actors. With the help of this step, a mapping of these three can be represented as shown in Table 7.2 on page 126 for creating a concrete reference architecture of the context. With the representation of information use created in the third step, an information-centric analysis of the context ecosystem can be performed.

5. Finally, a model of the functions of the context is created. The model can be represented without the information transferred between the functions as in Figure 7.2 on page 123 by showing only the directionality of the information flows. The model can also show the transferred information in a similar fashion to the abstract model (Figure 3.1 on page 70), but in this research, an approach in which the information required by each function is shown (see, e.g., Table 7.6 on page 146) was preferred for clarity. It was seen to be more beneficial to first present the information used by functions and then summarize the transfers in the layout of the (eco-)system (e.g., Figure 7.9 on page 151), for instance.

3.1.6 The functional model

The functional model is always case specific as it contains and presents the real-world functions and their respective connections within the application context. The purpose of the functional model is to show the connection between the functions, as well as to map the tasks to functions. Or the functions and tasks can be at this stage be mapped directly to the actors found.

Although the functional model is case specific, there are some commonalities in the function descriptions of both research processes (presented in sections 7.1 and 7.2). The following seven functions exist in both: (1) *measurement*, (2) *generation*, (3) *management*, (4) *processing*, (5) *monitoring*, (6) *statistics creation* (or *billing*) and (7) *value-added* (*third-party*) *services*. The eighth function, *administration*, existed only in the Game Cloud research process but is included as a function in the generic functional model as it can be regarded as a generic function in every digital system.

From these functions and the connections between them, a generic functional model, presented in Figure 3.3, can be established. In the figure, the connections (directional information flows) between the functions are presented as a result of analyzing the models devised during the research processes presented in sections 7.1 and 7.2. Some connections that exist in both, but some are present only in one of the scenarios.

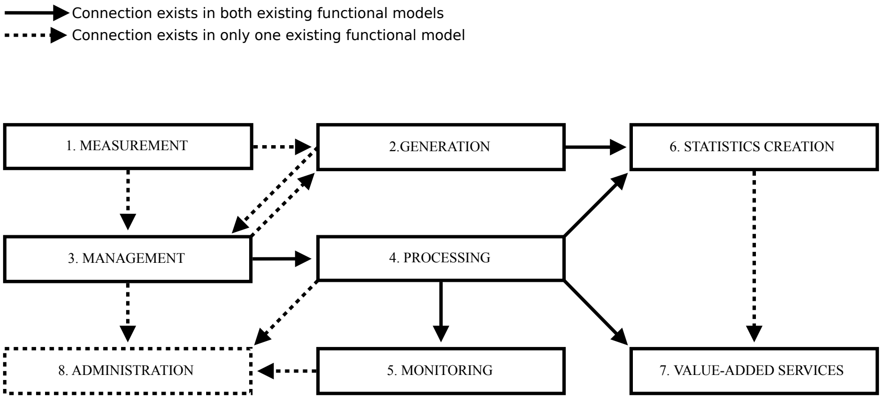


Figure 3.3: First version of a generic functional model

However, it is worthy to note that the presented generic model is established from the results of only two different systems, and more ecosystems would have to be analyzed in order to establish a reliable and correct generic model of the functions in information-centric systems. For this reason, the model presented in Figure 3.3 should be used only as a basis for developing the case-specific functional model. More examples of functional models established from the information from the smart grid and DGP contexts can be found from the research process descriptions starting on pages 123 and 147. In the functional model, there is no use defining the multiplicity of the functions because multiple different actors can participate in a single function as it was earlier defined in the function definition section 3.1.4.

The presentation of the model is one aspect of the purpose of the functional model. The mapping of the information use for each function as it was presented in the third step in the process of finding out the functions is the second aspect. This helps in analyzing the information use and flows within the system after the functions and tasks are mapped to the actors. This cannot be represented as a generic presentation because the information usage of functions differs a lot in different contexts, as well as does the types of data collected and transferred within the system.

3.2 Details of the use and key benefits of the method

The two distinct uses of method as an (1) *abstraction method* and as an (2) *iterative framework* are quite similar in the sense that the process of seeking out the tasks and functions and mapping the information between them are the same. However, some small differences exist between the use of these two. Here, the details of method use as an (1) *abstraction method* and as an (2) *iterative framework* are described in addition to the presentation of the key benefits found during the use of both.

3.2.1 Details of use of the abstraction method

The *abstraction method* was developed to analyze the common architecture of smart grid layouts in Finland based on questionnaire data (Appendix G on page 287.), pilots [130, 131] and existing reference architectures of NIST [114] and ETSI [115]. This was described as a research process in section 7.1 and is also presented in [45].

From the described process, it is evident that a vast amount of background knowledge is required in addition to the details about current implementations if the desire is to establish a common reference architecture from a certain application context. The key purpose of the *abstraction method* is to help create this common reference, but this method can also be used to research information flows and to help conduct an initial analysis of information privacy issues on high level on a single system without generating a common layout.

When the *abstraction method* is used to establish a common reference architecture, the method helps to detect privacy issues by detecting the usage, storage and handling of information within the system under study. The mapping of data collected, maintained and transferred to the tasks and functions helps to conduct the analysis, but in order to establish the reference architecture, they must be mapped to the actors (as in Table 7.2 on page 126) found during the process. The layout with the connections between the actors can be established by analyzing the information flows in the established abstract and functional models and the mapping of actors, tasks and functions.

3.2.2 Details of iterative framework use

The *abstraction method* was utilized in the Game Cloud development [46] as an *iterative framework* to improve privacy in the developed platform. The changes made to the process were not big as is presented in section 7.2 on page 131.

As the name suggests, the analysis is to be performed multiple times during the development iteration. The beginning of the process of the *iterative framework* does not differ from the processes described for finding out the tasks and functions. The abstract task and function analysis is required to be done only once because they are not usually changed during the design. However, if the scope and design direction change drastically, it is recommended to revise the abstract task and function descriptions and to reanalyze the system if changes are detected.

The tasks and functions must be mapped in each iteration. This is because as the design develops the tasks can be allocated to new actors, and the function participation can change. This was noted during the Game Cloud design process [46]. In each iteration, a new layout of the system with the information transferred between the actors is to be created. This and the mapping of tasks and functions to the actors enable the possibility comparing the new and old design and detecting what effects the changes had on the information flows and information privacy.

3.2.3 Key benefits of the method

The key benefits that are gained by utilizing the *abstraction method* and the *iterative framework* in the information privacy risk assessment as a high-level tool are the following:

- An increase in the depth of the knowledge obtained from analyzing the ecosystem from a different point of view. The knowledge is increased through the process of dividing the topic into smaller elements and finding commonalities between different actors within the topic.
- A detailed description of the information used and transferred inside and outside the system on high-level making it possible to concentrate on the relevant information.
- Requires the maintenance of information-centric documentation during the design process when used as a *iterative framework*. This requires additional steps but is seen as a benefit, since additional effort put into documentation returns its worth. This is because the requirements for (private) information handling are tightening [22, 23], and documentation will help to prove that the directive is adhered to.
- Elaborating about tasks and functions detects potential flaws in the design that might not be visible in the design documents.
- Creation of a clear, information-centered bird's-eye view of the system. Compared to, for example, the architectures devised by NIST [26] and ETSI [115] for smart grid privacy analysis, the method presented is a lightweight approach separating domain-specific issues, such as electricity generation in the smart grid domain [26], from the analysis [45]. Thus, the core issues

concerning information privacy in a system can be focused on to conduct the analysis more efficiently.

- Applying a generic architecture with a focus on privacy assessment to existing implementations.
- Ability to analyze information flows at a high level during development.
- The *iterative framework* helps to incorporate PbD principles into the design of the new system [46]. To be more specific, the *iterative framework* in general assists in fulfilling the first five principles by (1) enabling continuous improvement with the iterative design process that (2) enables built-in privacy into the system, (3) using privacy as a design requirement from the start and (4) improving the design by accommodating privacy needs through a positive sum approach and (5) guiding the implementation of security measures to the correct areas. Fulfilling the remaining two principles is domain specific and will not be discussed here.

4 Contribution 2: an assessment model

In this section, all the details of the model for an asset-centric information privacy risk assessment is described. Most of the text in this section is directly taken from the author's fourth manuscript [59] (see Appendix B), which has yet to be published.

This part presents the last, final version of the model, which contains only small modifications in comparison to the third prototype presented in section 8.3.5 on page 187. The illustration of the model, the scales and the dependency calculations are almost similar to the ones that are presented in section 8.3.5, but for clarity of the presentation, they are also shown also. This way the model for information privacy assessment is described in a coherent manner including the usage.

The different attributes within the model are also described with a little more detail in comparison to the presentations of the complete research process (in section 8 on page 155). The presentation in the following sections is meant to give more insight into the model without the need to go through the whole research process of the model. Ergo, this part of thesis is a compact presentation of the second part of the approach described in this thesis.

4.1 Asset-centric model for information privacy risk assessment

A model is a theoretical construct of an idea or a concept. The model represents the author's working definition of information privacy risk and the aspects affecting such risk. The description and concept of information privacy were used to derive a list of requirements and constraints, which led to the development of the model. The presented model is asset centric, taking into account the information privacy needs of an individual from the perspectives of disclosure and misuse.

The model is divided into multiple connected attributes, which encompass all the requirements for information privacy. Each term and definition that are later used in the model presentation, as well as model attribute descriptions, are presented in Table 4.1 on the following page.

To respond to the challenge of estimating the information privacy risks in a feasible and cost-effective way, the model (depicted in Figure 4.1) was built. The model is expressed using Unified Modeling Language (UML) notation. The requirements are accounted for in a single model consisting of a multitude of attributes. The attributes are divided into three different types, each of which is connected, either directly or indirectly, to the values of the other attributes. Each attribute is valued on a scale of one to six similar to that in [53, 116].

Table 4.1: Definitions of the terms in the model

Definition	Description
Asset network	The type of the network the asset is in. The asset network value is defined using the definition of public, private and protected with access restrictions.
Asset misuse potential	The level of potential harm the authorized or unauthorized user can inflict on the individual through asset misuse.
Asset role	The necessity of the asset in the environment from the individuals' perspective.
Asset value	The combined value of the asset from the individuals' perspective.
Attack	An attack conducted by an unauthorized user or a misuse attempt by an authorized user.
Attacker	Authorized (internal) or unauthorized (external) user attempting to misuse or disclose private information.
Attack actualization	How probable the attack or misuse is when the amount of effort is accounted for.
Attack gain	The amount of reward the attacker can get by misusing private information.
Attack likelihood	How probable it is the asset will be attacked (internal or external).
Damage level	The combined estimated amount of damage the attack or misuse of data causes the individual.
Data	The data derived from the information concerning an individual.
Data access	The number of authorized users who can access the data.
Data capabilities	The level of usefulness of the data for the attacker accounting also for the linkability of data.
Data quantity	The amount of data contained in the asset.
Data significance	The meaningfulness of the data for the individual or to the asset operation.
Data storage time	The time the asset contains the data.
Data value	The combined value of the data contained by the asset.
Impact on privacy	The level of privacy damage caused by a successful attack to the asset or misuse of data.
Privacy damage	The direct amount of damage misuse of the data causes to an individual's privacy.
Privacy risk	The level of privacy risk for the asset.
User damage	How big effect the attack or misuse of the asset has on the individual's life quality.

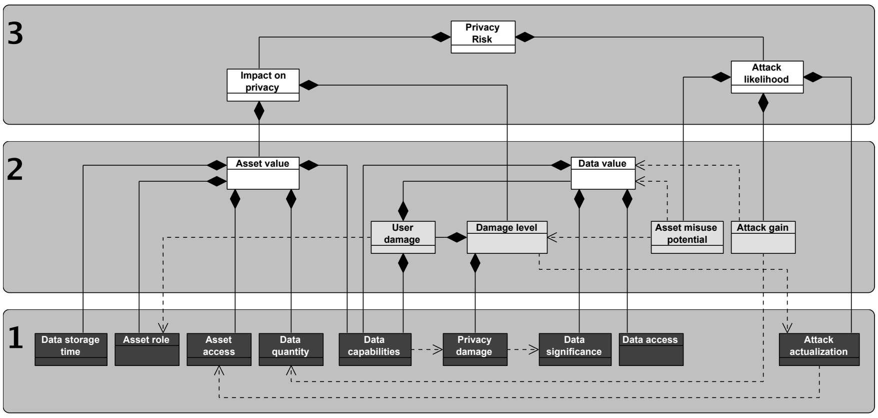


Figure 4.1: Model for privacy risk assessment on an asset basis

The three types of attributes are as follows:

- Calculable, the white color in Figure 4.1, which is directly calculated from the values of the other attributes. Calculation is done by taking an average of all attribute values that are composites of the attribute of this type.
- Definable, the light gray color in Figure 4.1, which are either valued by using a specific matrix or the value is first calculated from the values of the other attributes and then adjusted with a specific matrix.
- Assessable, the dark gray color and white text in Figure 4.1, which are given an initial estimate by the analyst. The initial estimate can be adjusted by some other attribute value on which this attribute is dependent.

The topmost attribute in Figure 4.1, the *privacy risk*, is the result the model produces for each asset. The *privacy risk* is a calculable attribute that is composed of two other calculable type attributes, *impact on privacy* and *attack likelihood*. This is similar to the approach for *privacy risk* presented by Hong et al. [53], where the *privacy risk* is calculated from the values of *likelihood* and *damage*. The model, however, has an extended range of parameters since the risk is analyzed on an asset basis, where the characteristics of the asset have to be accounted for in the *privacy risk* value.

The values for these attributes are formed of more complex relations between different definable and assessable type attributes. The relations between each attribute in the model are derived through an attempt to generalize all aspects affecting an asset holding private information. Two different types of UML relationships are used in the model, composition (direct) and dependency (indirect). The composition is a basic UML composition; each composite has an equal effect on the value of the attribute that is calculated. The dependency referred to as indirect is a supplier–client relationship [132] between the attributes in which the client connects to the supplier. For example, *Attack gain* in Figure 4.1 is a composite that has two suppliers, *data quantity* and *data value*, and therefore, also acts as a client. The indirect dependencies have a case-specific effect on the values of the client attributes and are expressed as two-dimensional matrices. The initial estimation charts for the assessable attributes and the two-dimensional matrices are explained in more detail later in this section.

The model has a total of 18 attributes, of which nine have to be assessed per asset before the model can be used to calculate the privacy risk. The initial values are most likely to be changed during the process, thus the dependencies between different attributes. Some assessable attributes, such as *data access* and *asset role*, are constant throughout the model lifetime at this phase. It is, however, intended to connect some of the assessable attributes, at least the two previously mentioned assets, to other assets or to attributes of other assets in the ecosystem in order to produce more accurate privacy risk results throughout the ecosystem.

The attributes are divided into three levels according to Figure 4.1. The three levels represent the flow of the assessment, and the steps are taken in number order, starting from number one. The first level in the model consists only of the assessable type attributes, which get initial estimates from the analyst. The second level contains all definable type attributes and one calculable, *data value*, since many definable type attributes depend on the value of that particular attribute. The third level consists of three calculable attributes including the result of the model, the *privacy risk*.

4.2 The attributes explained

In the following, each of the assessable, calculable and definable attributes is detailed. The attributes are presented by grouping each directly or indirectly dependent attribute under the attributes (calculable and definable) of which the value is defined or calculated from the values of the dependent attributes.

4.2.1 Privacy Risk

The *privacy risk* value in the model comes from the impact of a successful attack on privacy and the likelihood of the attack. The *impact on privacy* (corresponds to *damage* in [53]) is composed of two values: the value of the asset and the damage the attack can cause to the privacy of that individual. *Attack likelihood* is a composition of *attack actualization* and *attack gain* accompanied by the asset capabilities that defines the *asset misuse potential.*

The direct damage to the user (e.g., physical through a vital asset) or to the surroundings can be accounted for, but they are more of security attributes and are part of future study. Instead, the damage (reduction in quality of life) to the user whose information is at stake is accounted for in addition to the privacy damage.

4.2.2 Impact on privacy

The impact is viewed from the individual's point of view, which can be highly subjective depending on the person executing the assessment if evaluated as a separate attribute. However, here the impact is defined through the legislative definition and many other attributes that affect either directly or indirectly the value of *impact on privacy*, thus reducing subjectivity. The more valuable the data held by the asset, the bigger is the impact on reputation privacy. Furthermore, it is more reasonable and less subjective to evaluate the impact by utilizing the legal perspective than the needs and the requirements of an individual user because it does not require the involvement of the individuals. Therefore, companies, corporations and organizations can evaluate the risks independently. As a future work, an additional component may be added to the model, where individuals' perspectives on sensitiveness of data can be included. Thus, the model can be used for evaluating privacy risk also from an individual's perspective.

The integrity of an individual can be harmed by direct damage to the individual's privacy or by attacking the asset that opens access to the information belonging to that individual. Therefore, *impact on privacy* is composed of the *asset value* and the *damage level.* The impact of the information disclosure is taken into account through the *asset value* and the attributes forming that value in addition to the *damage level*, which is formed indirectly by the *data value* through *user damage*.

4.2.3 Attack likelihood

Schumacher et al. [116] define the frequency of occurrence, i.e., the event likelihood, as "an event or attack that could cause damage." It is a probability affected by unresolved vulnerabilities, available exploits, actualization of the attacks, the reward for the attacker and the value of the targeted asset. The full definition of likelihood [116] covers a lot more attributes, which are mainly aimed for security risk assessment, but these attributes are those that are reasonable to accommodate in the model. In the model, the *attack actualization* and the *attack gain* for the attacker are the most important for determining the *attack likelihood,* but also the capabilities of the asset must be accounted for. In [116], the *asset value* is used in the *attack likelihood* estimation. In the model, the usefulness of the asset for the attacker is covered by the *asset misuse potential.*

Asset misuse potential: *Asset misuse potential* is about the access the asset provides the attacker and what type of damage the attacker can do with it. The potential in asset misuse comes from the value of the data and how much damage this asset allows the attacker to inflict. Even with low-valued data, the damage can be significant (reidentification of data [108]). Therefore, the combined estimated damage (the *damage level*) is used to account for the damage, and to increase the emphasis of the damage to the user, a direct dependency on the value of the data the asset contains (*data value*) is utilized.

Attack gain: A successful attack gives the attacker (an authorized or unauthorized user) access to personal data, and the *attack gain* is defined through the potential reward [116] that is gained through misuse of the data. The amount of gain is defined by the value of the data (*data value*, which also accounts for the identifiability through *data capabilities*) and the amount of data (*data quantity*). Large amounts of non-sensitive and non-identifiable data is of no interest, but a handful of emails, for instance, is a completely different issue. However, it is also possible that the attacker has motives other than harming the privacy of an individual. The attacker can, for example, benefit from stolen credentials without touching, or even being interested in private information or vice versa. The privacy infraction can be a mere side product of the attack or misuse, and the attacker can also do harm without gaining any information but personal satisfaction. The issue of potential collateral privacy damage caused by other motives of an attacker is not included in the current version of the model but will be addressed in the future.

Attack actualization: *Attack actualization* defines how probable the attack is when the amount of effort required is accounted for. It is most efficiently defined with the help of attack trees, for example, with a privacy taxonomy-based approach [133]. Attack trees show how an asset can or might be attacked and offer a clear estimation of the probability of an attack. Therefore, the actualization of the attacks is also affected by the network the asset is in. In a highly protected network, the actualization of attacks is lower as it would require more resources from the attacker. This, therefore, accounts for authorized and unauthorized users. However, assets in highly protected networks might contain valuable information so they still can be viewed as profitable targets. In addition, the network limits the availability of an asset, not only in the public, external network but also in the internal network. For this reason, in the model, the dependency on the network type (*asset network*) is indirect.

4.2.4 Asset value

The value for the asset containing the data is determined by five assessable attributes using direct dependencies. The value consists of the *asset role*, *asset net-*

work, *data capabilities*, *data quantity* and *data storage time*.

Asset role: To value assets, it is imperative to know what the asset does in the environment, i.e., the role of the asset. The *asset role* defines the relations between the assets in the environment and can be viewed as an inter-asset dependent attribute [134]. The role can be defined through abstraction of the environment into basic tasks [45] or by the relative necessity of an asset [120]. The actual value of an asset is largely defined by the information the asset holds. In addition, the time the data is stored by the asset (*data storage time*) and the amount of data (*data quantity*) held by an asset affect the value.

Data quantity: *Data quantity* is subjective to each environment and requires a classification of its own. The longer the asset stores the data, the more interesting it is in the eyes of the attacker. Devices that store data only temporarily or not at all are not going to interest the attacker.

Data storage time: The time the asset stores the data is subjective to the environment. The *data storage time* needs to be estimated using knowledge about information usage in the environment.

Data capabilities: The value of an asset can be increased if the information can be regarded as useful for the attacker. It is a question about how exploitable or usable (for the attacker) the data is. *Data capability* (potential in [118]) is used to define this value, and it is highly subjective depending on the environment and the type of data. In addition, the legal compliance of the data is included by using identifiability in the *data capability* value assessment. PII 2.0 [20] is used in identifiability classification, but other suitable identifiability models, e.g., the identifiability continuum [108], can be adopted. Furthermore, the *data capability* is affected by the *privacy damage* level. If there is a possibility to inflict lots of damage on individuals' privacy using this asset, then the data has to be useful for the attacker, especially if the data can be linked to an individual.

Asset network: The value of the asset can be lower if the network where the asset resides is well protected from external threats. The *asset network* type defines the basic level of protection the asset has. A private network without any access is of lower value than a public network even with access restrictions. The *asset network* type can also be used to divide the assets into groups. This introduces a grouping approach similar to the asset value definition used in CRAMM [119].

4.2.5 Damage level

The *damage level* is a hybrid attribute of calculable and definable values, which falls somewhere in-between the two attributes. This attribute is treated as definable since the value is adjusted based on other attribute, therefore, this attribute does not produce a purely calculatory value.

The *damage level* gives an estimate of the damage (i.e., the scale of damage as suggested in [53]) a successful attack or misuse of information would cause to privacy. The damage a successful attack would inflict on privacy is determined by the damage to the user (*user damage*) and to the privacy of that user (*privacy damage*). *User damage* defines how big the effect of an attack or data misuse is on the individuals' individual autonomy. *Privacy damage* is an estimation of the damage a successful attack can do to the reputation privacy of an individual. The injury level definition (the loss if the attack is successful) [120] is adopted to accommodate privacy needs by replacing the organizational needs with the privacy needs of an individual. The level of the damage should correlate with the *attack actualization* since more attacks can mean more faults in the short or long term (e.g., denial of service attacks). The relation to *attack actualization* is, therefore, indirect.

User damage: The damage to the user is defined by the hindrance to the user or the degradation of the user's quality of life. It is defined by what other kind of damage than direct reputation privacy damage the attacker can inflict on the individual, that is, the loss of individual autonomy. *User damage*, therefore, depends on the value (*data value*) and the nature and the identifiability (*data capabilities*) of the data the asset contains. Defining *user damage* in this manner reduces the subjectivity of the attribute, and the values of these attributes should correlate in a way that compromising highly valued data does more damage. Therefore, the direct damage that an attack can cause, even indirectly with a successful attack (e.g., a mistake made by an attacker), is included through *data capabilities*.

Asset role: However, *user damage* should take into account the importance of the asset to the everyday life of the user, which is highly subjective to the environment and to the deployment of the assets. In some environments, the damage can be always low or nonexistent if the assets are not essential parts of the user's life. But when they are essential, the damage can be life-threatening (e.g., heart rate monitoring in independent living environments). In the model, the importance of the asset is incorporated in the *user damage* definition through the *asset role* as an indirect dependency, which makes the attribute a hybrid attribute similar to the *damage level*. Therefore, at this point, the subjectivity of the *user damage* attribute is slightly reduced. The intent of future research is to further extend the definition of *user damage* in order to offer a broader perspective and better scaling for the *damage level*. To define the *user damage* in a way that reduces subjectivity, the damage to the user can be defined by the User Impact Factor similar to the Component and System Impact Factors introduced by Hariri et al. [121]. A similar approach could be used to value security values, such as surrounding and system damage, which can be used as an extensions for defining the *damage level*.

Privacy damage: Loss of privacy (*privacy damage*) is defined by estimating what kind of data is lost and how much. The loss of reputation privacy is also included, since the disclosed data, based on its significance, can be used to cause harm. *Privacy damage* has to be estimated closely with the *data significance* and the definition of personal data in the current legislation. The effect of data identifiability is not accounted for in *privacy damage* but in the *damage level* through *user damage*.

4.2.6 Data value

Data is valued from the attackers' and individuals' view; any personal data that can be used to identify or harm an individual is useful data for the attacker and valuable for the individual. The *data value* is composed of the *data significance*, the publicity level, i.e., the *data access* level and the identifiability and potential (*data capability*).

Data access: The number of people accessing the personal data is a matter of access control, and in a security assessment, the methods of access control are verified. But in the model presented in this study, the *data access* is defined only on the basis of how many different persons can access the data. If the data is accessible only by the user, then it is the lowest value; if the data is shared by a handful of people or they should be able to access the data, the value is greatly increased. For some systems, legislation or directives can require an external independent regulator, which naturally increases the *data access* value of the assets the regulator has to access.

Data significance: *Data significance* defines the level of importance of the data for the individual. It is about how necessary the data is for the individual and its significance for system operation. Data can be the login credentials or some profiling data used for system calibration. The *data significance* is not used to define the privacy level for the data, which is defined by the *privacy damage*, which, in turn, affects the value *data capabilities*.

Data capabilities: To account for the identifiability and the nature of the data in the *data value* calculation, the *data capabilities* is included. This brings the attacker aspect into the *data value* calculation by taking account of the misuse potential of the data through identifiability and exploitability.

4.3 How to define and calculate values for the model

The values from the three types of attributes (assessable, calculable and definable) come either from the analyst (assessable) or by calculating the value from different dependencies in the model. (calculable and definable). In the model a qualitative scale (as recommended in [53]), ranging from one to six (also used in [123, 116]), is used to classify each attribute. In this rating, one is defined as negligible (lowest) and six is extreme (highest) [116].

An external method can be used to gain deeper understanding of the environment and to prepare the evaluation of assessable attributes. For example, the previously described abstraction of the environment (in section 3 on page 67) offers the means for detecting information usage and different roles of assets in the environment. The *abstraction method* brings a common understanding of the different groups of stakeholders and will increase the depth and value of the assessment [46]. Abstraction introduces the need for more knowledge about the environment and, therefore, may increase the cost of the process. But the benefits it provides by allowing a generalized overview of the environment can justify the additional resource consumption.

4.3.1 Three types of attributes

The model contains three types of attributes as shown in Figure 4.1 and summarized on page 79. In the following, each of these three types (assessable, definable and calculable)is presented in more detail. This includes the initial estimate scales for the assessable type attributes, which are presented as tables.

Assessable: The assessable attributes can be evaluated manually, but the initial estimates will be more accurate with a task-specific analysis. Small inaccuracies are hidden by the scale for each attribute. Reference values for each assessable attribute are presented in Tables 4.2, 4.3 and 4.4 in a similar form to the risk matrices and the valuation tables [116]. The attributes are divided into three tables based on their connection to the asset that contains the data, to the user whose data is stored or to the system to which the asset belongs. This is the final version of the scales for assessable attributes that focus on the three core aspects in the context of information privacy: data, user and system. Table 4.2 contains values for asset-related attributes, Table 4.3 presents all value attributes from the user perspective and Table 4.4 contains the value attributes from the system perspective. The reference values are normative and require adjustment based on information about the environment to be assessed. Additionally, some of the assessable attributes are adjusted by the value of other assessable attribute by their indirect relationships. Furthermore, there exists one exception with *data capabilities*, which has to be valued again after assessing the initial value (Table 4.3) using the identifiability level of the data according to Table 4.5.

Table 4.2: Attribute values from the asset perspective

Value	Asset network	Asset role	Attack actualization
6	Public network with no access restrictions.	Vital for the user.	Asset is either open or very vulnerable, and attacks will happen.
5	Public network with access restrictions.	Almost vital asset. Short maintenance gaps are tolerated.	Asset has some vulnerabilities that are known and are tried often.
4	Protected network. External restricted access.	Important but not vital asset. Maintenance gaps are tolerated.	Attack requires knowledge, and with reasonable efforts, an attack is successful.
3	Private network. Restricted external access.	Everyday usage appliance, but user can live without it.	Asset is protected, but because of the data, attacks can happen infrequently.
2	Private network. No external access to asset.	An extra appliance that gives some practical benefits.	Breach requires enormous effort, and attacks happen very rarely.
1	No network access.	Not important at all.	Attack is unlikely because a breach requires enormous efforts.

Calculable: The values for the calculable type attributes do not come from the analyst's analysis but are affected by the other, definable and assessable type attributes. In the example described by Schumacher [116], the risk value is composed directly of the attribute values without weighing factors. The risk is formed on an asset basis by summing up the threat likelihood (corresponds to *attack likelihood*) and vulnerability combinations (corresponds to *impact on privacy*) and multiplying this by the asset value. In the model, however, the calculable type attribute values are calculated as an average of the composite attribute values. This results in similar scaling as in [116] but is more coherent throughout the model, and the results are more comparable between different assessments.

Table 4.3: Attribute values from the user perspective

Value	Data capabilities	Data significance	Privacy damage
6	Data can be used to permanently affect user privacy.	Data is either vital for the user or crucial for the system operation. Leak causes severe privacy infractions or opens access to the whole system.	User loses reputation privacy completely. Private data is lost.
5	Privacy is violated with leaked data if not properly anonymized.	Data is important for the user and is needed in system operations. Leak causes harm to privacy or opens up parts of the system to the attacker.	User reputation privacy is lost, and/or personal data is lost.
4	Large amounts of data would threaten privacy.	Data is important for the user and is needed in system operations. Leak causes temporary harm to privacy or opens up access to the asset.	User reputation privacy and personal data are threatened.
3	Leak would increase curiosity but is no real threat. In systems, such data has to be recreated, and the leak causes some offline time.	Data is useful for the user, and the leak of a large amount of data causes privacy issues. In systems, such data has to be replaced, and maintenance is required.	User reputation privacy or personal data is threatened.
2	Leaked data has a meaning only inside the system.	Data has a small role in user's life and a leak causes only annoyance.	No real effect on privacy. Some data is lost.
1	No data or data of no interest.	Not significant, necessary for the user or required in any operation. Leak has no impact.	No effect on privacy. No data leak/loss possibility.

Table 4.4: Attribute values from the system perspective

Value	Data access	Data quantity	Data storage time
6	Open access to shared data.	Contains all user-related private information (e.g., a large database).	Permanent storage for data, and there are backups.
5	Data is publicly shared with access restrictions.	Contains lots of information most of which is identifiable and some is identified (e.g., a home computer or a small database).	Long-term storage (data is stored for years).
4	Accessible by a large number of persons (>10) with access control.	Contains information (some of it is identifiable) that can be wiped out securely (e.g., cache).	Medium-term storage (data is stored for months, less than a year).
3	Accessible by only a small quantity of persons (<10) with access control.	Small amounts of data (some of it is identifiable) are kept at any time.	Short-term storage (wiped out or overwritten now and then).
2	Accessible by only a few persons (<5) with access control.	Contains a copy of transferred data (e.g., a router).	Stores for the time the data is being transferred.
1	Only the user, system component(s) or system maintainer can access the data.	No data.	Does not store anything.

Definable: There are two types of definable attributes in the model. The first are hybrid attributes (*user damage* and *damage level*) that are first calculated using direct relationships and then adjusted with the value of the dependent attributes. The second type is directly defined by the dependent attributes. With hybrid attributes, the value is always first calculated from direct relationships and after that adjusted by the value of the attributes connected with indirect relationships. The value adjustment is done using the respective dependency matrix.

Table 4.5: Data capabilities identifiability classification

Data capability Data identifiability	1	2	3	4	5	6
Non-identifiable	1	1	2	3	4	4
Identifiable	1	3	4	4	5	6
Identified	3	4	5	6	6	6

4.3.2 Relationships between attributes and the value matrices

The direct relationship between attributes is a straightforward UML aggregation relationship. The indirect relationship is defined with UML dependency, which is also described as a supplier-–client relationship, where “the supplier provides something for the client” [132]. In the model, the supplier attribute provides a value for the client, which is used for adjusting the client attribute value using the dependency rules. The effect of each dependency is type specific; each case is a bit different, and the effect varies based on the type of the affecting attribute. When there is only one supplier, the initial value of the client attribute is accounted for in the adjustment. Otherwise, the value of the client is defined by the values of the two suppliers. When the value of one attribute changes, all dependent attributes, or the attributes that are composed of that value, must be updated according to the dependency rules.

The dependencies are defined in the current version with two-dimensional matrices. The values for the matrices were formed by analyzing and assessing the effect of the respective attributes using the definitions in Tables 4.2, 4.3 and 4.4. The dependency matrices are presented as Tables 4.6, 4.7, 4.8, 4.9, 4.10, 4.11 and 4.12.

The value of the attribute in question is determined using the values of the two label attributes of the particular table. For example, the *asset misuse potential* is defined by the *damage level* and the *data value* using Table 4.6, where the value of the *damage level* defines the *column* and the *data value* defines the *row*. With values $(3, 4)$, the value of the *asset misuse potential* would be then set to 3 (the bold number in Table 4.6).

Table 4.6: Asset misuse potential adjustment matrix

Damage level Data value	1	2	3	4	5	6
6	2	4	5	5	6	6
5	1	3	4	5	5	6
4	1	3	**3**	4	5	6
3	1	2	3	4	4	5
2	1	2	2	3	4	4
1	1	1	1	1	1	2

Table 4.7: Attack actualization adjustment matrix

Attack actualization Asset network	1	2	3	4	5	6
6	5	5	5	5	6	6
5	4	4	4	5	5	6
4	2	3	3	4	5	5
3	2	2	3	4	5	5
2	1	2	3	3	3	4
1	1	1	1	2	2	3

Table 4.8: Attack gain adjustment matrix

Data quantity Data value	1	2	3	4	5	6
6	1	5	5	6	6	6
5	1	4	4	5	5	6
4	1	3	4	4	5	5
3	1	2	2	3	4	5
2	1	1	2	2	2	3
1	1	1	1	1	1	2

Table 4.9: Data capabilities adjustment matrix

Data capabilities Privacy damage	1	2	3	4	5	6
6	3	4	5	5	6	6
5	2	3	5	5	5	6
4	1	3	4	4	5	6
3	1	2	3	3	4	5
2	1	2	3	3	3	4
1	1	2	3	3	3	4

Table 4.10: Damage level adjustment matrix

Damage level Attack actualization	1	2	3	4	5	6
6	2	3	4	5	6	6
5	1	2	3	4	5	6
4	1	2	3	4	5	5
3	1	2	3	4	4	5
2	1	2	3	3	4	4
1	1	1	2	2	3	3

Table 4.11: Privacy damage adjustment matrix

Privacy damage Data significance	1	2	3	4	5	6
6	1	2	4	5	6	6
5	1	2	4	5	5	6
4	1	2	3	4	5	6
3	1	2	3	4	5	5
2	1	2	3	4	5	5
1	1	1	2	3	4	5

Table 4.12: User damage adjustment matrix

User damage Asset role	1	2	3	4	5	6
6	4	5	6	6	6	6
5	3	4	5	5	5	6
4	2	3	4	4	5	6
3	1	2	3	4	5	6
2	1	2	3	4	5	6
1	1	2	3	4	5	6

4.3.3 Using the model and the tables

Use of the model is straightforward, and an assessment can be performed for a single asset at a time or simultaneously for all assets. Simultaneous assessment is required when dependencies between assets are implemented. In such an assessment, a software reduces the manual labor and keeps control of the process.

In the following, the process is described in three steps, which follow the layout of the three levels in Figure 4.1. The process begins by assessing the initial estimates for the attributes that are not suppliers for any other attribute. Then the values for the attributes that are the first clients in supplier-–client chains are selected.

Step 1: First, the attributes on level one have to be assessed and valued using Tables 4.2, 4.3 and 4.4. The most suitable value is selected from the tables using "judgment calls based on the best knowledge" [53], in addition to prior knowledge of the environment for each assessable attribute. The selected value is the initial estimate for the attribute. After the initial estimates for the attributes at level one are assessed, the attributes that have a supplier are adjusted based on the dependency matrices. At the first level, the three attributes (*attack actualization*, *privacy damage* and *data capabilities*) are adjusted with the matrices. *Privacy damage* has to be adjusted before *data capabilities*, thus the dependency.

Step 2: Next, the values for the attributes at the second level are to be defined. First, the value for the *data value* attribute has to be calculated from its composites as many other attributes depend on it. Then each definable attribute is calculated from the composites and then adjusted with dependencies, from left to right in the same order as the attributes are laid out in Figure 4.1. The value for the *asset value* attribute comes from direct dependencies and none of the attributes depend on it; therefore, *asset value* can be calculated last. For example, the *damage level* has to be first calculated from the values of *user damage* and *privacy damage* before it can be adjusted using the *attack actualization* value using Table 4.10. The value of *asset misuse potential* cannot be adjusted using Table 4.6 before the value for *damage level* is calculated and adjusted. Similarly, the *attack gain* and the *user damage* can be defined only after *data value* is calculated.

Step 3: In the third and final step, the values for the attributes at the third level are calculated using the composites for each. First, the values for the *impact on privacy* and *attack likelihood* attributes need to be calculated, which produce the values for calculating the *privacy risk* value.

5 Contribution: an overview use of the approach

The previous two sections, three and four, presented the two components of the approach (contribution 1 and 2) in detail. In this section, the use of these two contributions together as an complete approach is presented as an overview. In figure 5.1 the general use of the approach (contribution) is presented. The six steps shown in the figure are detailed in this section. Additionally, a detailed case example of use of the approach to develop a new ecosystem (Game Cloud) is presented in Appendix E. This approach is also presented as a brief and a complete example in the author's fourth publication [58] (see Appendix B).

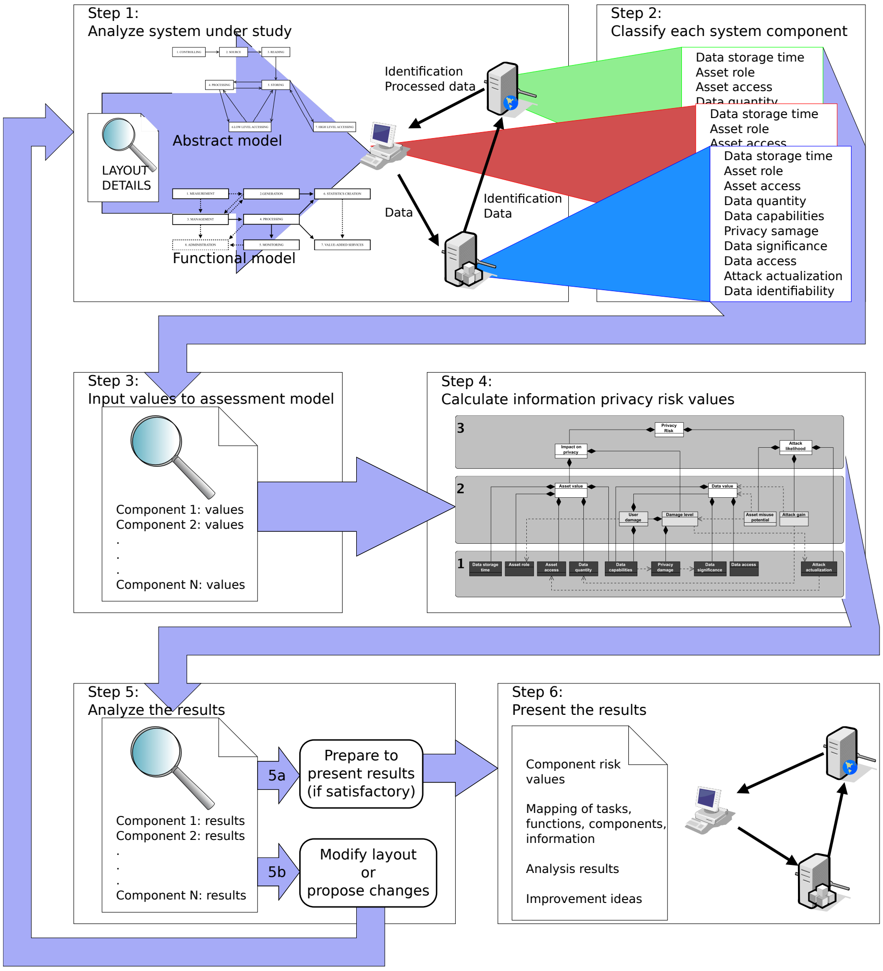


Figure 5.1: An overview of use of the approachin six steps

5.1 Step 1: Analyze the system under study

The first step is to analyze the layout of the system under study for information flows between the system components. This analysis is done with contribution 1. The process is the same in use of the *abstraction method* and the *iterative framework*. This step is divided into the following five minor steps.

If the approach is used to analyze existing systems or to compare existing systems or to establish a reference architecture to present the most common layout, see the details of contribution 1 use as an *abstraction method* in section 3.2.1 on page 74. If the approach is used to develop a new system as an *iterative framework,* see the details of use in section 3.2.2 on page 74.

Step 1.1: Find out what information is transferred within the system, seek out the seven typical abstract tasks in the system and map the information transferred between the tasks. For a detailed process, refer to the five-step approach described in section 3.1.2 on page 68.

Step 1.2: Establish the abstract model of the system under study. For more details, refer to section 3.1.3 on page 69.

Step 1.3: Find out the functions within the system, map out the information use of the functions and seek out the connections between the tasks and functions, including information use. For a detailed process, refer to the five-step approach in section 3.1.5 on page 71.

Step 1.4: Establish the functional model of the system under study. For more details, refer to section 3.1.6 on page 72.

Step 1.5: Make an initial analysis of the system based on the information required to establish the abstract and functional models and with the information the models offer. Detect potential flaws in information handling, transfers and management.

5.2 Step 2: Classify each system component

The second step is to classify each system component using the predefined scales presented in section 4.3 on page 86. This classification of the components is required to be done in order to use the *assessment model* to calculate the risk value. It is required to select initial estimates for the nine attributes presented at the first level in Figure 4.1 on page 79 plus the identifiability of information affecting the *data capabilities* attribute.

Therefore, in total there are 10 attributes to assess for each component. The information obtained from the first step offers insight into the components that helps in selecting the initial estimate. Tables 4.2, 4.3 and 4.4 present the scales to use to assess initial estimates for the nine attributes, and Table 4.5 presents the scales for the *data identifiability* classification.

5.3 Step 3: Input values in the assessment model

This third step is to prepare the values for inputting them in the *assessment model* (contribution 2) and to detect potential errors in classification. Therefore, this step is also an overview of the selected values. It is imperative to analyze the selected values in comparison to the other initial values selected for other system components.

After the overview, the values are to be prepared to be inputted for the calculation. If the *assessment model* is used manually, the values can be put into a spreadsheet for an easy comparison of the initial estimates and the results of the risk value calculation as shown in Figure E.1 on page 262. If the software prototype, available at `https://github.com/lut-projects/iprat`, is used, see Appendix F for more details about using a script and a file containing the initial estimates.

5.4 Step 4: Calculate the information privacy risk values

The fourth step is to utilize the values determined in the previous step to calculate the risk value for each component. The calculation is done with contribution 2, the *assessment model*, either manually or with the help of prototype software.

If the *assessment model* is used directly without the prototype software, it is necessary to follow the three steps defined in section 4.3.3 on page 92. These three steps present the order in which the initial assessment and calculations are to be made.

With the software, there is no need to follow the steps. Only the 10 attributes are to be assessed for the initial estimates and the software processes the values in proper order. For more information on use of the prototype software see Appendix F.

5.5 Step 5: Analyze the results

In this step, the results from steps 1 and 3 are analyzed. This step contains analysis of the abstract model, the functional model, mapping of information use between tasks, functions and systems components, as well as the information privacy risk values calculated for each system component.

Next, the results offered by the abstract model, the functional model and the information privacy risk calculation are analyzed. An example of the result analysis is presented in Appendix E section E.2 on page 263. If contribution 1 is used as:

- an *abstraction method* (5a in Figure 5.1), then move to the final step (six).
- an *iterative framework,* then make the changes to the system layout or propose changes to the system and move to the first step and continue with the next iteration (5b in Figure 5.1) unless the results are satisfactory (5a in Figure 5.1).

5.6 Step 6: Present the results

This is the final step in which the results of the assessment are presented. Establish a layout of the system with the information flows and present the mapping of the tasks, functions and components, as well as the risk values for each component. Create a presentation of the analysis results, introduce potential improvement ideas to layout or system in general to enhance information and privacy protection. Examples of presentations of the results are available in Appendix E.

Part III

Description and evaluation of the research

The research presented in this thesis is grounded in design science research (DSR). In this part, the research paradigms, principles, research process and evaluation of the research are described. The research paradigms and principles used in this research are described in section 6.

In DSR, determining the evaluation criteria and the evaluation of the artifact are considered integral parts of the process [54]. Each design process is presented as an activity-driven DSR process as later depicted in Figure 6.2 on page 107.

This contribution of this thesis consists of two components, and therefore, the process is described separately for each in sections 7 (contribution 1) and 8 (contribution 2). The first component (contribution 1) is divided into two separate processes as its focus is different depending on whether it is used to analyze existing ecosystems (the *abstraction method*) or to develop a new system (the *iterative framework*). Development of contribution 2 is a long process involving multiple iterations and is detailed in its entirety in section 8.

The results of the research, the *abstraction method* and the *iterative framework* (contribution 1) and the *assessment model* (contribution 2), form the complete approach. The first contribution of the research is a high-level method that loses a lot of granularity [50] in the process, but this is intended to show only the necessary details of the assessed ecosystem. The second contribution of the research offers many details and is, therefore, more of a low-level method [50]. The aim is to require a low level of expert knowledge. Together as an approach, they establish a mid-level tool that mixes abstract and concrete methods with a medium level of granularity to establish a method offering a scope with “medium altitude” [50] in the ecosystem under study.

In each description of the research, specific research objectives are declared, which are answered as part of the DSR process in Activity 5. These objectives are not to be confused with the research questions (RQ) presented in section 1.4.2 on page 22. Instead, by meeting the objectives, the research questions of this research are answered. Detailed answers to the research questions are later presented in the conclusion of this thesis in section 10.3 on page 226.

6 Research paradigms and principles

This thesis presents a real solution to an existing problem, and therefore, design science is used as the research methodology in this work. Design science is an apt methodology for developing a solution based on feedback from real environments to solve a specific problem. The solution is developed iteratively involving theory from the literature to support the design decisions, while developing the solution to suit the need better from the practical and theoretical points of view [54].

The presented approach, the contribution of this thesis, in its full extent follows the paradigm of DSR. Both contributions, 1 and 2, are developed using an activity-driven DSR process, but in the development of contribution 1, the *abstraction method* and the *iteration framework*, and the principle of abstraction and generalization [55] is utilized within a DSR process. The abstraction and generalization methodology suits interpretive research to generalize the involved structures and actors in order to establish a deeper understanding of the subject or environment at hand. This is enabled through categorization of the environment to draw general concepts, involving logical reasoning and theory to draw specific implications and to find out the unique inter-related instances in the environment.

6.1 Design science

DSR at its core is a research paradigm for creating an innovative design utilizing existing theories and approaches to solve a specific real-world problem. It is defined by Hevner and Chatterjee [54] as:

> *a research paradigm in which a designer answers questions relevant to human problems via the creation of innovative artifacts, thereby contributing new knowledge to the body of scientific evidence.*

The artifacts mentioned in the quotation are a wide range of constructs made by humans, such as models (abstractions and representations), methods (algorithms and practices) and better design theories [54]. In general, the term means “something that is artificial.” These artifacts should be improvements of existing solutions or to be the first, ground-breaking, solution to solve a new or old real-world problem.

Hereby the work presented in this thesis is developed using DSR as the approach itself is a design of a solution to an existing real-world problem aiming to offer an easier way to map out the risks in the ecosystem. The approach is not regarded here as an artifact, but it consists of two artifacts: the *abstraction method* and the *iterative framework* and the *assessment model* for information privacy risk assessment. Since both are built from multiple smaller parts, they can be divided into more specific sub-artifacts that are detailed in the following section describing the complete research process. In the following subsections, DSR is presented in more detail. Guidelines for conducting DSR are described as a set of seven points presented in Appendix D on page 259.

6.1.1 Iteration cycles and components, the process of design science research

The previously detailed guidelines are, as named, questions the researcher has to ask of himself or herself while conducting the research in order to proceed in the right direction. They offer only the direction. An apt analogy for this is that the guidelines merely point the needle of the compass to north but give no detail about the correct path. The more detailed process offers the details of the path to reach the destination.

The DSR process is defined with an iterative cycle-based approach that has three main components (environment, DSR and *knowledge base*) involving three cycles (relevance, design and rigor cycles) each of which has multiple feedback from the components during the iterations of the cycles. Hevner and Chatterjee emphasize [54] the importance of the three cycles, which should be identifiable in every DSR. In Figure 6.1, the connections between the components and the cycles of the DSR process, including the questions (Q) that are explained later, are illustrated.

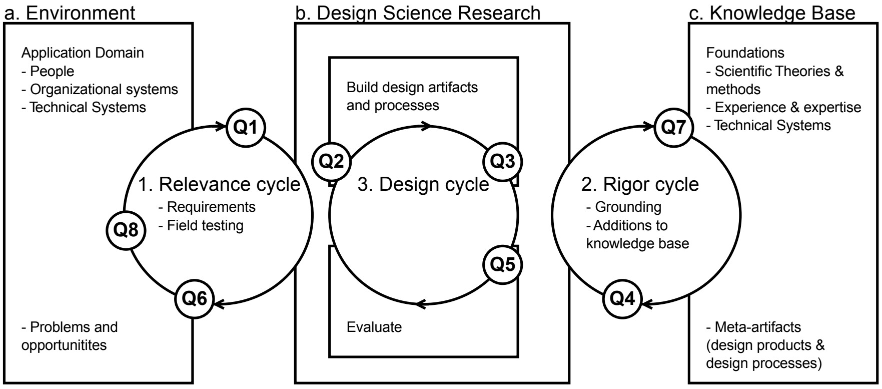


Figure 6.1: The components and cycles of design science research with question mapping. Reproduced from [54].

The components (*a*) environment, (*b*) DSR and (*c*) *knowledge base* are the three contexts the cycles connect in the research and to which the cycles are bound [54]. The environment is the real-world context, an *application domain* involving people, organizational and technical systems, in which the problem exists. DSR is the process in which the artifacts and processes are created and evaluated. The *knowledge base* is the background theory for the research that involves comparing and analyzing existing methods and theories accompanied by experience and expertise. The *knowledge base* also contains the theoretical constructs of the design, or as Hevner and Chatterjee present [54], the design of the meta-artifacts.

The three cycles, (1) relevance, (2) rigor and design (3), are iterations of the research process between or inside the three components. The *relevance cycle* iterates between components *a* and *b,* the *rigor cycle* iterates between *b* and *c* and the *design cycle* is naturally inside the DSR (*b*). The cycles are detailed as follows:

1. Relevance cycle: The *relevance cycle* binds the environment to the research (components *a* and *b*) and is the first step in DSR. Research is initiated in this cycle by inputting the requirements from the application context (environment) in the process. In addition, the evaluation criteria for the research results are defined in this cycle by using the requirements of the environment. The return cycle from the DSR (*b*) gives the output of the research for study and evaluation in the application context of the environment (*a*). The study and evaluation are referred to as *field testing* [54], the results of which will determine the number of iterations required in this cycle. Field testing is meant to evaluate the potential deficiencies and the quality of the research artifact, as well as to assess whether the research artifact has satisfied the requirements. However, the iteration also gives feedback from DSR (*b*) to the *application domain* of the environment (*a*) to restate the requirements if deficiencies are found in them.

2. Rigor cycle: DSR is “grounded on existing ideas drawn from the knowledge base” [54], and the *rigor cycle* is the cycle binding the research (b) to the *knowledge base* (*c*). In the *rigor cycle* the existing theories, experiences, processes and possible artifacts are researched and referenced, as well as compared to the design products, the artifacts of the research, to ensure the innovativeness and usefulness of the research. This cycle is to be executed before and after the design of the artifacts first to gather the background knowledge, i.e., theory, on the matter and then to compare the result to the existing approaches. Each iteration of this cycle will increase the *knowledge base* (*c*) based on the research results (the artifacts, field testing and research experience) by extending and challenging original theories and methods. It is emphasized [54] that the DSR process should make definitive research contributions to the *knowledge base* in order to be accepted as innovative research and not be dismissed as a case of routine design.

3. Design cycle: All main research activities, the design of artifacts and processes, including the evaluation of them, is done within the iterations of the *design cycle*. At each iteration, the feedback from the evaluation is to be used to refine the design. Here, the requirements originating from the environment (*a*) through the *relevance cycle* (1) and the theoretical background that is drawn from the *knowledge base* (*c*) with the help of iterations of the *rigor cycle* (2) are combined to establish a process for artifact design. It is imperative to seek out a balance in the efforts between construction and evaluation of the artifacts [54] as the essence of design science is argued to be in the scientific evaluation of the artifacts [135]. Although the artifacts are the concrete results of the research, neither construction nor evaluation should be more encumbering than the other. Testing of the designed artifacts should be conducted in laboratory and experimental situations before the field tests are executed in real environments as part of the *relevance cycle* [54]. By default, this leads to multiple iterations in this cycle before the contributions are outputted to either of the two other cycles.

6.1.2 Evaluation of design science research process

In addition to the seven guidelines, the DSR process is to be evaluated with more specific questions. Researchers conducting DSR have found some questions to be asked during the progression of their processes to ensure the validity of their research, that it complies with requirements of design science [54]. How these questions should be asked within the process is detailed in Figure 6.1. In the following, the summary of these questions (Q), presented by Hevner and Chatterjee [54], is shown:

Q1. What is the research question (design requirements)?

Q2. What is the artifact? How is the artifact represented?

Q3. What design processes (search heuristics) will be used to build the artifact?

Q4. How are the artifact and the design processes grounded by the *knowledge base*? What, if any, theories support the artifact design and the design process?

Q5. What evaluations are performed during the internal design cycles? What design improvements are identified during each *design cycle*?

Q6. How is the artifact introduced into the application environment, and how is it field tested? What metrics are used to demonstrate artifact utility and improvement over previous artifacts?

Q7. What new knowledge is added to the *knowledge base* and in what form (e.g., peer-reviewed literature, meta-artifacts, new theory, new method)?

Q8. Has the research question been satisfactorily addressed?

6.1.3 The design science research methodology

The guidelines and the process of DSR, including the additional questions asked in various steps of DSR that were presented in the previous subsections, detail all the necessities required to conduct the research. However, they do not describe the process in a methodological manner. For this need, a framework for conducting DSR in information systems has been presented in the form of a methodology [136]. The objective of the process, design science research methodology (DSRM), is to help with recognition of the objectives, processes and outputs of research and to establish a mental model for the characteristics for the research outputs [54]. A mental model is constructed from a perceived, conjured or reasoned rationalization of reality [54] and, thus, is a small-scale representation of it.

This methodology is presented with six activities: problem identification and motivation; definition of the objectives for a solution, design and development; demonstration; evaluation; and communication [54]. Descriptions of research to create and to evaluate the contributions are presented later as activity-driven DSR processes. The activities (A) are described as follows in the execution order:

A1. Problem identification and motivation The first activity is to define the specific research problem and to conceptually atomize the problem to unveil its complexity in order to help with artifact development. In addition, the value of the solution is to be justified in this phase as it accomplishes two things important to the research. First, it motivates to pursue the solution and accept the results, and second, it introduces the researcher's perspective on the problem to help understand the reasoning behind the solution. This activity requires that the state of the problem and the importance of the solution are known.

A2. Define the objectives for a solution The second activity continues from the problem specification (the first activity) by limiting the scope and the objectives of the solution to what is possible and feasible to develop. The objectives, either quantitative (the terms how to compare and assess the superiority of the solution to existing ones) or qualitative (how the developed artifact supports solutions in the case of unbeknownst problems), are to be rationally inferred from the problem specification. This activity requires the knowledge about how the current solutions address existing problems, including their efficiency.

A3. Design and development In this activity, the artifact is created as a construct, model, method, instantiation or new properties of technical, social and/or informational resources. First, the artifact's desired functionality and architecture are determined and then the actual research artifact, in which the research contribution is embedded, is created. This activity requires that the theory behind the solution and problem specification are known in order to develop the solution with it.

A4. Demonstration In the fourth activity the use of the artifact is demonstrated in one or more problem instances. The artifact can be used in any suitable manner to solve a problem, such as in experimentation, simulation or case study. This activity naturally requires that the details of artifact use in problem solving are known to the researcher.

A5. Evaluation The fifth activity is to evaluate the results of the demonstration (the fourth activity) to the objectives laid out in the second activity. In this activity, the applicability of the artifact to the problem domain is assessed through observation and measurements generated in the demonstration utilizing any appropriate empirical evidence or logical proof. Based on the evaluation results, the decision about whether to continue to the next activity or to return to the third activity to improve the artifact is made. The iterations back to activity three can be done as many times as feasible if the research venue allows such action. This activity requires that the researcher is familiar with the relevant metrics and analysis techniques.

A6. Communication In the last activity,the results of the research are to be published, i.e., communicated to the relevant audiences. The results include the problem and its importance, the artifact, its utility and novelty, the rigor of its design and its effectiveness. Knowledge of the disciplinary culture is required in this activity.

6.1.4 Illustration of the DSR process

Figure 6.2 illustrates the overall activity-driven process of DSR methodology. This is an overview of the process that is constructed from the six activities and the components and cycles of DSR, presented in Figure 6.1 on page 102. The DSR process to create the artifacts follows the process described in this diagram.

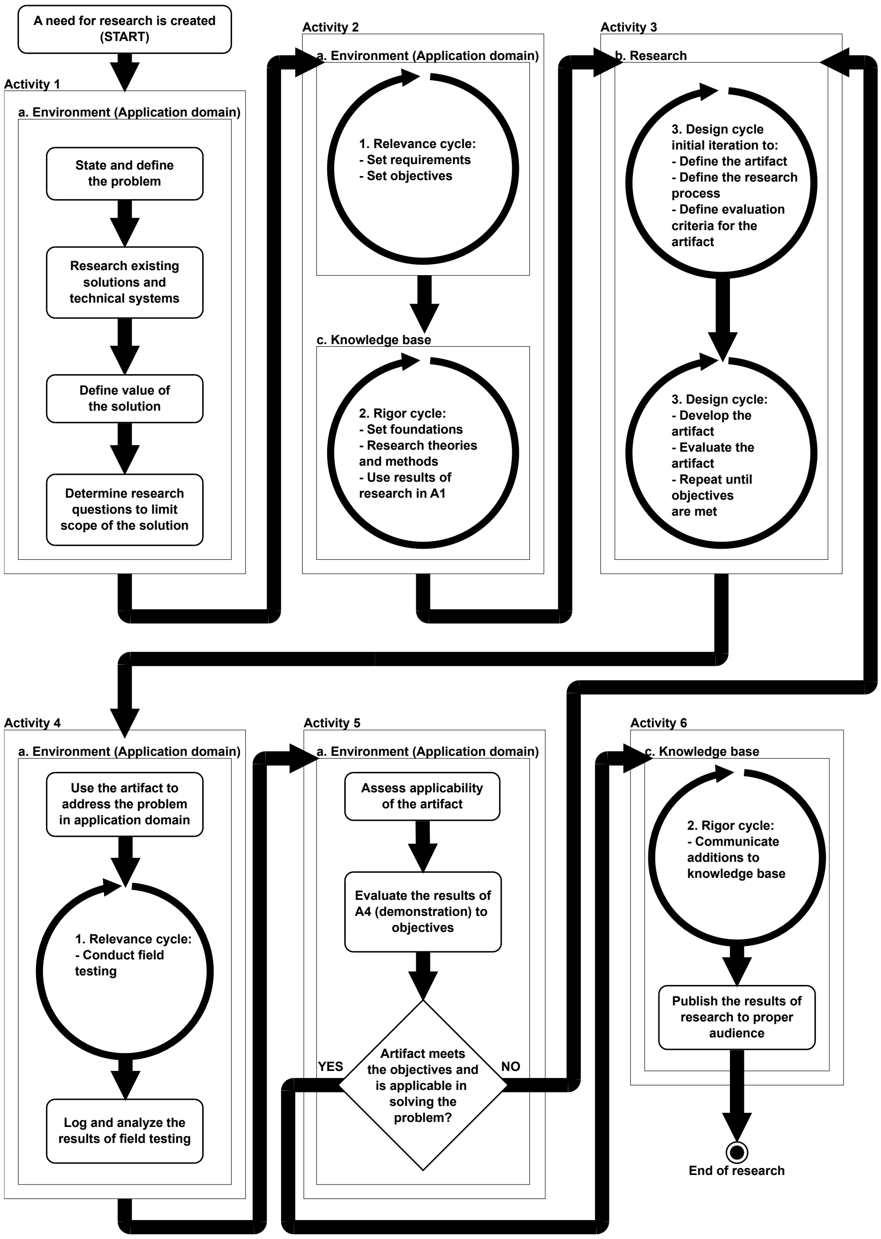

A need for research is created (START)
Activity 1
a. Environment (Application domain)
State and define the problem
Research existing solutions and technical systems
Define value of the solution
Determine research questions to limit scope of the solution
Activity 2
a. Environment (Application domain)
1. Relevance cycle:
- Set requirements
- Set objectives
c. Knowledge base
2. Rigor cycle:
- Set foundations
- Research theories and methods
- Use results of research in A1
Activity 3
b. Research
3. Design cycle initial iteration to:
- Define the artifact
- Define the research process
- Define evaluation criteria for the artifact
3. Design cycle:
- Develop the artifact
- Evaluate the artifact
- Repeat until objectives are met
Activity 4
a. Environment (Application domain)
Use the artifact to address the problem in application domain
1. Relevance cycle:
- Conduct field testing
Log and analyze the results of field testing
Activity 5
a. Environment (Application domain)
Assess applicability of the artifact
Evaluate the results of A4 (demonstration) to objectives
Artifact meets the objectives and is applicable in solving the problem?
YES
NO
Activity 6
c. Knowledge base
2. Rigor cycle:
- Communicate additions to knowledge base
Publish the results of research to proper audience
End of research

Figure 6.2: Activity-driven process of DSR methodology

6.2 Abstraction and generalization

The principle of abstraction and generalization is one of the seven principles for interpretive field research presented by Klein and Myers [55]. In the abstraction and generalization principle, the details revealed by the data are interpreted by utilizing the fundamental principle of the hermeneutic circle and the principle of contextualization to form theoretical relations between human understanding and social actions.

6.2.1 Hermeneutic circle

The core idea of the principle of the hermeneutic circle is that by studying the different parts and interrelationships of different meanings even the most complex entireties can be understood. Klein and Myers [55] present this through a case of translating a sentence into a foreign language where the concept and the related contexts are required to be understood in order to establish an understandable translation. In order to translate the sentence, even the abstract meanings of terms are required. For example, in the sentence "they are playing football," the part "playing" has a multitude of meanings, ranging from "kicking" and "bumping" to "throwing."

The hermeneutic circle is about going into deeper details and relations of different contexts to get an improved understanding of each part [55], in the case of the example, the words. Therefore, an understanding of the matter at hand is gained through iteration, which is the key issue in the hermeneutic circle. It allows the researcher to go into more details layer by layer, each revealing more connections between the contexts through logical reasoning.

6.2.2 Contextualization

In the contextualization principle the issue under research is put into its social and historical context, not only for the researchers but also the audience to see how the current issue emerged [55]. The contextualization principle helps to tie the issue to a certain context in time, or to a moving target. It is said [55] that interpretive research focuses on a moving target. The relationships among people, organizations and technology are continuously in a state of flux so every issue under research has to be tied to a context in interpretive research.

The effect of the research is bidirectional with the contextualization principle; the total history of the organization under research affects the research, and the research affects the future history of the organization [55]. It is important that the researcher views the actors belonging to the organization as producers and not just as products of the organization's history.

6.2.3 The process of abstraction and generalization

In interpretive studies, human affairs are generally regarded as culturally dependent in which natural laws do not apply [55]. The basis for abstraction and generalization in interpretive field studies has emerged from philosophical debates presenting that unique instances can be related to ideas and concepts that apply to multiple situations through abstraction of the categories [55]. In order to present the theoretical insights and connections between the instances in a readable manner, it is important to carefully relate the details obtained from a field study as they were experienced and/or collected during the study. In brief, in abstraction and generalization the theoretic connections are made with logical reasoning through interpreting the details of the system [55, 137].

The details in an example offered by Klein and Meyers [55] of a project involved in developing electronic data interchange (EDI) messages for the Norwegian healthcare sector [138] were interpreted using actor-network theory [139]. In this theory [139], the actors in the (eco-)system are linked together and are pursuing interests that can be inscribed as technical, as well as social, arrangements. This approach offers valuable details of the relations and dependencies inside the (eco-)system.

Utilizing iterations from the principle of the hermeneutic circle and the relevance of the contexts from the contextualization principle, the theoretical connections can be made to establish a generalized model of the issue under research. On each iteration, the depth of detail is increased so abstract connections between instances and actors can be established. This process was used for the initial version of the first part of the approach, the *abstraction method* and the *iterative framework*.

7 Description of research to create and evaluate contribution 1

This section presents the research to develop both uses of contribution 1 of this thesis: *abstraction method* and an *iterative framework*. The research process is an instantiation of the DSR process described in section 6. In this research, design of the artifacts is presented as activity-driven DSR process depicted in Figure 6.2 on page 107.

The research process for contribution 1 began in the SGEM project [57] as Figure A.1 on page 247 in Appendix A portrays and continued throughout the Game Cloud project. This resulted in two separate research processes as there were two distinct problems, and thus, the approach consists of two parts: an *abstraction method* and an *iterative framework*. Both were developed in response to direct needs of the projects and had only a few DSR design iterations as the agenda was to devise a method that could offer help in the analysis or design within the scope of the project. However, the details of the *application domain* and existing technical systems were iterated according to the principle of abstraction and generalization. Therefore, the research on contribution 1, the *abstraction method* and the *iterative framework*, is not research oriented in the way that the processes and resulting artifacts are refined but project oriented; the results of the projects are weighted more.

Parts of the description of the research process of contribution 1: *abstraction method* (sections 7.1.2, 7.1.3, 7.1.4 and 7.1.6) are taken from the author's first publication [45] (see Appendix B). Some parts of the description of the research process of contribution 1: *iterative framework* (the Game Cloud paragraph in section 7.2 and some parts of 7.2.1) are taken from the author's fourth publication [58] (see Appendix B). Portions of the second iteration of contribution 1: *iterative framework* (section 7.2.4) are taken from the author's third publication [46] (see Appendix B).

7.1 Creation and evaluation of the abstraction method

The first context environment (*a* in Figure 6.1) for which the new artifact was to be designed was the smart grid environment. In following the research process is presented as an activity (A)-driven approach described in section 6.1.4.

Two research questions, RQ1 and RQ2 (described in 1.4.2 on page 22), are addressed in this research process. These questions help to limit the scope of the process and are used to establish the requirements for the research process. The DSR-specific questions DSR Q1 to DSR Q8 are answered as follows: Q1 in 7.1.1 on the following page, Q2 and Q3 in 7.1.3 on page 115, Q4 in 7.1.2 on page 114, Q5 in 7.1.3 on page 115, Q6 in 7.1.6 on page 124, and Q7 and Q8 in 7.1.8 on page 130.

7.1.1 A1: Problem

The problem was to analyze information privacy threats in the smart grid environments in a simple way that included only the information flows. There are multiple different actors and components in smart grid environments, such as the customer, distribution system operator, electricity retailer, smart meter and various information systems, to name a few, which transfer roughly the same, standardized information used for calculating the electricity bill [45].

It was found in [45] that existing architectures [114, 115] are too complex for the task. The architectures of NIST [114] and ETSI [115] are meant for checking compliance with industry accepted standards. Both architectures are complete definitions that are difficult to understand completely without expert knowledge about electricity markets, generation or distribution. Thus, they include lots of unnecessary information for information privacy analysis.

Furthermore, it was evident from research on existing pilots [130, 131] and a questionnaire [45] (the questions and the results of questionnaire are presented in Appendix G) that existing smart grid environments do not follow a standardized approach. For example, ETSI [115] introduces recommendations for optimal situations, which were not the reality according to the questionnaire. The summary of the questionnaire, to which 30 distribution system operators (DSOs) in Finland responded, and the research on smart grid pilots are as follows (also presented in [45] with fewer details):

- The reading infrastructure is maintained and owned by the telecommunications operator. The telecommunications operator also offers connectivity to and from the smart meters.
- The telecommunications operator performs the software and tariff updates for the meters and in does reads the consumption data from the meters.
- The meters and the physical maintenance of the meters are of the DSOs' responsibility.
- Ownership of the measurement data information system (MDIS) differed in the pilot and questionnaire results.
  - In [131], it was owned by the telecommunications operator, but in [130], the DSO had full ownership of the information systems.
  - The questionnaire shows that the measurement database is in most of the cases (53%) maintained by the DSO, and in almost all of these

cases, (90%) also the telecommunications operator had full access to the database. When the telecommunications operator maintains the measurement database, the DSO can, in most cases (63%), read from and in half of the cases (50%) write to the database.

- In both pilots, the customers were provided with a web interface to monitor own consumption and to authorize a third party access.

- In the pilots, mobile phone networks were used for communication between the MDIS and the meters. The results of the questionnaire (multiple selections per participant) show that:

  - 70% of the respondents send a reading over private mobile phone network
  - 50% of the respondents send a reading over Power Line Communication (PLC)
  - 30% of the respondents send a reading over a public mobile phone network
  - 13% of the respondents send a reading over a fixed phone lines
  - 10% of the respondents send a reading over unspecified radio frequencies

- It is a common approach to use protected private networks for connections between the DSO and the telecommunications operator.

- Hourly consumption is read once a day; only in 7% of the cases is the consumption read more often.

- In the majority of the cases (60%), the meters store the consumption data for a time period of one to six months, and in almost third (30%) of the cases even longer. In the rest of the cases (10%), the consumption data is stored for less than one month.

- The consumption data in the database is, in the majority of the cases (55%), identified by the source meter ID. In addition, Internet Protocol (IP) addresses (22.5%), physical location (7.5%) and phone numbers (5%) were used. In 10% of the cases, the meter identification and IP addresses were used in combination to identify consumption data.

- The log database about updates and consumption data readings was in most cases (76.7%) accessible and readable also by the telecommunications operator, who had also a copy of the database in the majority of the cases. It is interesting that only in half of the cases (52%), the reading of the meter produced a log entry, whereas in most of the cases (80%), the updates left a log entry.

- Only 60% of the DSOs use some standardized meter access method.

These results clearly indicate that there is a wide variety of divergence among the smart grid implementations. The roles are different, the means of accessing the meters are different, different communications are used etc. Therefore, there is a clear need for a simplified method in order to map out information privacy threats in the environment.

Value of the solution: The value of the solution to address this problem lies within the ease of use without the need of expertise to map out information privacy threats. In addition, as there are many differences between existing implementations of the smart grid environment, the resulting solution must be applicable to any environment without going into the same level as the existing architectures of NIST [114] and ETSI [115].

Research questions specific to this process: This leads to DSR **Q1**: the research questions. First, it is imperative to find out the attributes of information privacy and what information in this environment is private (**RQ1**). And second, it is needed to research about how to gather the information where to apply privacy protection (**RQ2**).

7.1.2 A2: Objectives

This is the first *relevance cycle* (*1*) iteration, which is then continued to the *rigor cycle* (*2*) to research and compare existing solutions and theories, parts of which were conducted in A1. The background research in A1, however, brought the information about how current solutions (of NIST [114] and ETSI [115]) address the problem from one point of view, which helps to fill in the requirements for this activity.

The two research questions (**RQ1** and **RQ2**) help to limit the goals of the solution. The goal here is to devise an approach for assessing information privacy threats using a smart grid as an *application domain*.

Relevance cycle: requirements: The focus must be on information privacy, i.e., on the information that can be used to identify an individual or information that can reveal something about an individual. First, it is required to find out the characteristics of such information and what are the risks and threats in the smart grid environment regarding customer privacy (**objective 1**). Additionally, the existing research focusing on the countermeasures are to be used as a reference to gain deeper knowledge about the risks and threats. This contributes to the *rigor cycle* (*2*) that connects the foundations of the *knowledge base* (*c*) about the application context (*a*). Second, the multiplicity of actors and the components and connections between them are to be accounted for in the research (**objective 2**). It is evident from the background information in A1 that the smart grid environment is complex in terms of the participant connections. This presents challenges about how to find out the information usage in different places and how to gain information about how it is protected in various locations (**objective 3**). In general, the resulting artifact must offer a clear, information-centered bird's-eye view of the application context in order to act as an appropriate tool for assessing information privacy (**objective 4**).

Rigor cycle: foundations: The foundations for the research were laid in A1 with the research on pilots [130, 131], questionnaire [45] and architectures of NIST [114] and ETSI [115]. Furthermore, the various means to protect and detect information usage in a smart grid environment [12, 30, 31, 32, 33, 34, 36, 72, 82, 140] that were presented in [45] offer enough information for grounding the research on something existing. The pilots and the questionnaire detail the environment, i.e., the technical systems, in which the research is done. The other means offer the theories and methods on which the research is based. The information that is used and collected from users of the smart grid environment was analyzed from the pilots, the questionnaire and the NIST and ETSI reference architectures. The information collected contains two parts: (1) identity information (to whom this information is connected and (2) detailed information about electricity consumption for a certain period of time. Additionally, some control information is sent back to the devices residing at customer premises. Grounding of the research process (DSR **Q4**) is at the beginning of this research based on the existing reference architectures, pilots and questionnaire results. The research on theories and methods and existing architectures prove that no approach operates at the desired detail level for this research. Each architecture or method views the environment either from too wide and complex scope or the focus is on a small part of the environment. Therefore, the analysis approach devised in this research is the new knowledge added to the *knowledge base*, which is the answer to DSR **Q7** and concludes the first iteration of the *rigor cycle*.

7.1.3 A3: Design and develop, iteration 1

The decision about what kind of artifact and with what kind of presentation was clear from the beginning. It seemed most logical that the artifact is most useful in form of an approach that starts from the high-level view to get into the depths of the environment in order to establish a reference architecture similar to those of NIST [114] and ETSI [115]. It would be difficult to start from the bottom or the ground level of information as it would require vast amounts of expert information, which contradicts one of the requirements set in A2 on the facing page.

The differences in the behaviors and practices of the different participants (according to the questionnaire [45]) brought up the need to navigate between the different approaches at the abstract level in order to see the commonalities. This was the first step in deriving the most general tasks and functions inside the environment. Since the environment was clearly new for some of the researchers, seeking the common tasks and functions in the smart grid environment helped to understand what information is transferred and where it is being kept.

The artifact: This research resulted in the idea of a research artifact: two separate models operating at different levels (abstract tasks and basic functions) that involve the private information of customers transferred between them, both of which are then used to establish a reference architecture (answer to DSR **Q2**).

Process for research: In order to establish such models, a suitable process for creating them from the background data is needed. The basic idea of the abstraction and generalization [55] research methodology was found to be apt for this research (answer to DSR **Q3**). The abstraction and generalization methodology offers the means to connect abstract instances or theoretical constructs (the tasks) to real concepts (functions) with the information obtained from a field study (the questionnaire).

Evaluation: The following questions are used as a checklist for evaluating the artifact during the internal design cycles to identify improvements during each *design cycle* (answer to DSR **Q5**):

1. Are all existing tasks applied in the approach?
2. Do the connections comply with real-world connections between the tasks?
3. Is the information transferred between the tasks complying with the information transferred in the real-world scenario?
4. Are the tasks generic enough to apply the abstract model to other similar real-world scenarios?
5. Are all existing functions of the smart grid environment included in the functional model?
6. Do all connections between functions comply with the connections in the real-world scenario?
7. Is the information transferred between the functions complying with the information transferred in real-world scenarios?

8. Does the approach include the personal identifiable information (PII) transferred in the smart grid environment in the process?
9. Is it possible to detect information usage in the application context with the approach?
10. Does the approach offer enough knowledge to map the information flows within the application context?
11. Is the resulting artifact better in information-based privacy analysis than the existing solutions?

7.1.4 A3: Design and develop: iteration 2

The first design iteration laid out the design specification for the artifact, as well as the process of establishing the artifact and evaluating it. In the second iteration, they are combined with the requirements from the (*1*) *relevance cycle* and background information from the (*2*) *knowledge base* to develop the actual artifact.

First, the environment is abstracted with the principle of abstraction and generalization [55] to identify high-level tasks and to seek out the interaction between them. This is established by analyzing the information offered by the two reference models of NIST [114] and ETSI [115], the questionnaire (a summary is presented in section 7.1.1 on page 112 and all details are shown in Appendix G) and the smart grid pilots [130, 131]. All this information is later referred to as *background information*. In the analysis, these unique instances found with the abstraction and generalization principle are referred to by the common name *actors.*

Although the layouts were quite different in many ways, it was possible to detect the high-level components and participants in the environment. The analysis of the layouts required multiple iterations, each of which gave more details about the components in the system and their respective connections in terms of information transfers. Certain unique instances were found instantly from the background information. In every smart grid there is a *meter* monitoring the consumption of a *customer*, who, in case of Finland, has to make a contract with an *electricity retailer* to get electricity, which then delivers the electricity with the help of a local *distributor*. This involves many databases where different information is kept, such as customer PII, billing information and electricity consumption history data (which in Finland has to be saved for six years [79]).

It was detected that the meters transfer the information to the distributor or to the retailer, depending on the smart grid architecture. In many of the cases, an external party, a telco, offers the reading infrastructure, thus reading the information from the meters and controlling them. Additionally, some third parties offer increased value in the form of more detailed electricity consumption analysis. By going into deeper details about the connection of the different actors with each iteration, the unique instances in the environment and the connections between them were found with logical reasoning and by cross referencing the layouts.

The unique instances, the actors, grouped by their respective sub-actors, in smart grid are as follows:

1. Customer: The customer who owns the residence, makes the contract with the DSO and decides whether to share consumption data with a Value-added Service (VAS).

    (a) A smart meter: Smart meter keeps track of electricity consumption and other related activities. Contains local log information about the electricity consumption of the residence.

    (b) Meter(s): Various meters used in the residence, e.g., thermostats, water meters, etc. Generates information for the smart meter about the appliances and their energy consumption.

    (c) Sensors: Various sensors in the residence, e.g., temperature sensors. Generates information for the selected meters.

    (d) Resident: The end-user in the residence who is not necessarily the owner of the residence. Monitors his or her own electricity consumption via web-based interfaces.

2. Reader: Smart meter reader responsible for the communication between the smart meter and the MDIS.

    (a) Measurement data information system (MDIS): Information system and database containing all measured consumption data of every customer using smart meters. Provides consumption information for the customer data information system (CDIS) when requested.

3. Distribution System Operator (DSO): Offers electricity distribution to customers via an electricity grid. Maintains the CDIS.

    (a) Customer data information system (CDIS): User database and information system. Contains personal information of the customers, consumption information, etc. Requests consumption information from MDIS.

    (b) Web interface: Interface for the customers for viewing billing information, contract details and personal consumption details. Also used for managing value-added service authorizations and other personal information that is stored in the CDIS.

4. Electricity Retailer: Electricity Retailer, the electricity provider that charges customers based on the readings provided by DSO.

   (a) Billing information system: Information system for billing the customer. Contains the consumption data of each customer.

5. Value-added Services (VAS): Third party offering a service for analyzing long-term consumption data. Data is collected from the CDIS via an interface if a customer has authorized the access.

   (a) Analysis information system: Information system and database of the VAS containing raw and analyzed data of the customers who have made an agreement with the VAS. Information is offered to authenticated customers via a web interface.

   (b) Web interface: Interface for customers to view the analyzed consumption data.

These generic actors are connected by their tasks and functions, forming the layout for each smart grid environment. By cross referencing the layout details and with logical reasoning, the following tasks are identified that are the most general in every smart grid environment:

T1. Controlling: This task involves maintaining and controlling the information source (T2). In a smart grid this task involves updating tariff information, providing software updates to smart meters and accessing log information. This task can be included in the reading task (T3) but usually is separate if the architectural design requires it. There are many information sources (T2) that are controlled by one participant fulfilling the controlling task, and therefore, the connection to T2 is one-to-many.

T2. Source: This task is always executed by the information source that creates the data for analysis. In a smart grid this task belongs to the smart grid located at the customers' premises that monitors electricity consumption and allows authorized parties to read (T3) and control it (T1).

T3. Reading: This task is meant only for getting consumption information from the information source (T2) and in some cases, to control the source. The actor executing this task also has full access to all the data the information source (T2), the smart meter, contains. Therefore, the reading task is one of the key tasks in the smart grid among T2 and T5. There is usually one actor reading from multiple sources (T2) that delivers the data to one or more actors storing the information (T5). The connection to T2 is, therefore, one-to-many and to T5 as well, but in Finland, for example, the connection to T5 is always one-to-one. This is because, according to the background information, the distributor is determined by location, and the distributor is the one that forwards the details about electricity consumption to multiple retailers.

T4. Processing: the information processing task is the part where the individual readings from a customer's smart meters are combined to calculate the total consumption for a certain time period or to analyze the data for load balancing of the electricity grid. The information is requested from the storing task (T5) and in the smart grid environment, there are many actors assigned with this task (T4), and the connection to T5 is many-to-many. This is because there can be many storers (with information of varying granularity and scope) from which the information is requested. The actor of this task can also store the results of the information processing and, therefore, can also be a storer (T5).

T5. Storing: This task is solely for keeping the data generated in the system by different actors. Other tasks T3, T4 and T6 are directly connected to this task for either retrieving information from or pushing information to a database or information system of some sort that fulfills this task. The connection to the processing and accessing tasks is one-to-many, and each task can get information with varying levels of detail. The access level is defined by the task the actor is executing. For example, information for the retailer is of a different granularity than the information delivered for third parties (VAS).

T6. Accessing: This task involves accessing only the consumption information with varying levels of access in terms of information granularity. The information is retrieved from the T5 actor, and in some cases, the actor with this task can be a storer (T5). This task is executed by many actors in the smart grid environment as the task is involved in the information transfer from one information system to another.

The different layouts offered enough details to establish the most generic connections between these tasks. In addition, background data gave details about what information is being transferred and where. The former analysis of the tasks gave details about which tasks are connected and in which way. This resulted in the following abstract model describing the generic tasks and their interactions in the smart grids portrayed in Figure 7.1. The number of participants is not included in the model. The arrows in the model point the direction in which the controls or the information is being transferred. This is the first artifact of the research process part I.

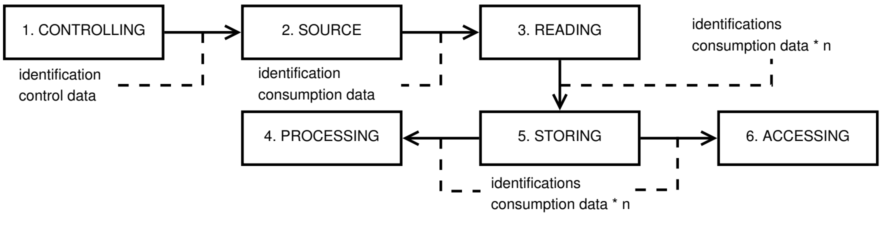


Figure 7.1: Abstract model of the generic tasks in smart grid

Next, the functions in the smart grid environment are to be determined from the background information. The research on the generic tasks helped in this stage as a lot of information about the environment was already sifted. In this stage of the abstraction and generalization the real-world operations inside the environment are detected by seeking out the basic verbs that occur in the specifications of the studied environment. The list of common verbs that were detected during the research are (in alphabetical order) *analyze, authorize, bill, distribute, generate, manage, measure, monitor* and *process*.

From these nine verbs, the seven basic functions of a smart grid can be deduced with logical reasoning. None of the verbs are excluded, but *distribute* and *manage* are put under one function, since the distributor is the one that also manages the electricity grid. In addition, *authorize* is a part of the monitoring and/or analysis of electricity consumption and is not regarded as a separate function. *Authorize* is the action the customer performs in order to give authorization for a third party for value-added analysis of the consumption.

The functions and their descriptions are the following:

F1. Measurement of consumption: Transfers the consumption data from the smart meter to the grid management function.

F2. Grid management: Stores and accesses the data when undertaking operations required for the maintenance of the smart grid. Gives access to the stored data for the consumption data processing function. Informs the electricity generation how much electricity is needed based on current usage demands.

F3. Electricity generation: Provides customers with electricity. To do this efficiently, some data about customers' electricity consumption is required. Delivers the details about the electricity produced to the billing function.

F4. Consumption monitoring: Offers a detailed overview of electricity consumption for customers.

F5. Consumption data processing: Is responsible for the processing of consumption data either by calculating it for the billing function or making it suitable for analysis by the consumption monitoring function and VAS.

F6. Billing: Accesses the given data and provides customers with the bill in exchange for the consumed electricity.

F7. Analysis Services (Value-added services, VAS): Offers an alternative, more analyzed view of customer consumption data. The service is operated by a third party.

The previous iterations on finding the tasks from the background information and the information transferred between the tasks gave details about what information is required by the different functions in the smart grid environment. The information these different functions require can be divided into five components: (1) smart meter ID (M_{id}), (2) customer ID (C_{id}), (3) customer personal identifiable information (C_{PII}), (4) consumption data (C_{data}) and (5) processed consumption data (C_{proc}). M_{id} is linked to the C_{id} of the customer whose consumption the meter is measuring, and the C_{data} is linked to both IDs. The C_{proc} is linked only to the C_{id} as the particular meter is of no interest after the data has been processed. The C_{PII} is linked to the C_{id}, or the C_{id} is included in the C_{PII}.

In an optimal situation, there is no need to use customer identification for consumption measurements as aggregation methods suggest [34, 35, 36]. However, the data has to be somehow identifiable, and the M_{id} would be sufficient. The relation between M_{id} and C_{id} is known by the storer of the data, in this case, the party managing the grid (2). This data, accompanied by the C_{id}, is used in the consumption data processing function (5) to create suitable data for other operations, e.g., billing (6).

In order to charge the customer, it is necessary to know more than just the customer's ID and the electricity consumption. Therefore, in the billing function (6), the C_{PII} of the customer, containing billing information, must be known, which makes it a storer of identities. However, the consumption data does not need to be as accurate if only the total consumption is charged. The same applies to the consumption monitoring (4) and VAS (7) functions, where the latter does not require the C_{id} used in other parts of the environment. It is more likely that the party fulfilling the VAS function has its own internal identification for each customer that is linked to the data of a certain C_{id}.

For the electricity generation function (3), the consumption of individual customers is not needed. The electricity retailer just needs to know to whom the electricity is sold (C_{id}), and the billing function takes care of the rest. However, in order to enable load balancing in the network, some data about the current usage demand is required. The processed consumption data might be enough for electricity generation, but more accurate load balancing information can be provided by the grid management function. This is more reasonable since it reduces data overlap between the functions.

The summary of optimal information use in the smart grid environment and which tasks each function includes, is shown in Table 7.1. The *x*es inside the parentheses define the information as non-mandatory. Since the goal was to establish a common reference architecture with the process, the information use is also generalized to view an optimal use of private information in terms of customer privacy protection.

From this summary and background information, the following functional model, portrayed in Figure 7.2, of the functions in the smart grid environment is established. The arrows in the figure depict the information flow between the functions.

Table 7.1: The optimal information use and included tasks of the real-world functions in the smart grid environment

F#	Functionality	M_{id}	C_{id}	C_{PII}	C_{data}	C_{proc}	Tasks included
1.	Measurement of consumption	x	(x)		x		T1. Controlling T2. Source T3. Reading
2.	Grid management	x	x		x	x	T5. Storing T6. Accessing
3.	Electricity generation		x			(x)	T5. Storing T6. Accessing
4.	Consumption monitoring		x			x	T6. Accessing
5.	Consumption data processing		x		x		T4. Processing T6. Accessing
6.	Billing		x	x		x	T5. Storing T6. Accessing
7.	Analysis services (VAS)		x			x	T4. Processing T6. Accessing

This model is case specific and needs to be constructed for each environment as a part of the analysis process. This is the second artifact of the research process part I.

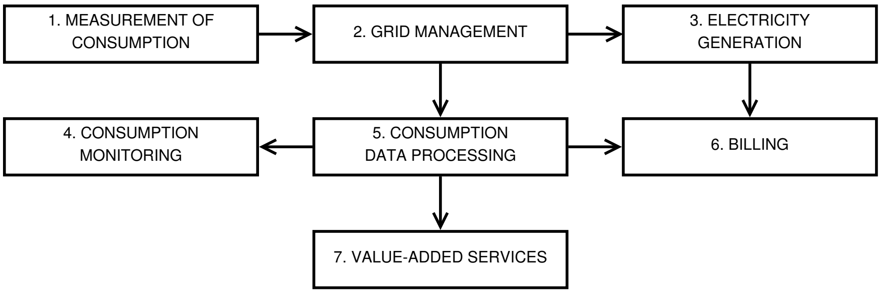

1. MEASUREMENT OF CONSUMPTION
2. GRID MANAGEMENT
3. ELECTRICITY GENERATION
4. CONSUMPTION MONITORING
5. CONSUMPTION DATA PROCESSING
6. BILLING
7. VALUE-ADDED SERVICES

Figure 7.2: Functional model of smart grid real-world operations

7.1.5 A3: Evaluation of the artifact

This is part of *design cycle* (*3*) and is executed after designing the artifacts. The resulting artifacts, the abstract and functional models, are evaluated with the 11 questions presented earlier (on page 116) before the field testing is conducted as a demonstration. The answers to the questions are the following:

1. According to the background information, there are no more generic tasks

in the smart grid environment. These are also the tasks that, through logical reasoning, can be found from any information-centric system.

2. The connections between tasks need more feedback from the demonstration before this question can be answered.

3. The information transferred in a smart grid is formed of two main high-level components, identification and consumption data, which are included in the abstract model.

4. The tasks have been researched on a high enough level to make them fully abstract and to be generic to be applied to any other similar, information-centric system or environment, for information privacy analysis.

5. By analyzing the verbs in the background information, it is evident that the seven functions are the most generic in each layout.

6. The connections between the functions need more feedback from the demonstration before this question can be answered.

7. The more detailed information use, in comparison to the two abstract components of abstract model, consists of five components included in the functional model information use description.

8. PII is included in the functional model; however, it was concluded from the research on background data that in optimal situations PII is required in only one functionality.

9. By analyzing the tasks for the abstract model, including their interactions, and the formation of the functional model with the abstraction and generalization principle reveals many details about information use in the application context. The process helped to detect the usage of the information in the smart grid environment. To fully answer this question, a demonstration of the artifact is required.

10. Answering this question requires a demonstration of the artifact.

11. Answering this question requires a demonstration of the artifact.

The basic models that were formed based on existing implementations, architectures and results of the questionnaire are designed according to the requirements, but some questions can be answered only after field testing the artifact(s).

7.1.6 A4: Demonstration of the artifact

This is the field testing part of the *relevance cycle* (*1*) in which the use of the artifacts, the abstract and functional models, is demonstrated. This is done in the *application domain* of the *environment* (*a*) by constructing a common reference architecture of the smart grid environment utilizing the background information and both models (answer to DSR **Q6**). This architecture contains all the actors and the information flows in the smart grid environment and offers a clear and easily understandable view of the environment. The reference architecture, illustrated as Figure 7.3, is closely based on smart grid environments in Finland, thus the questionnaire data.

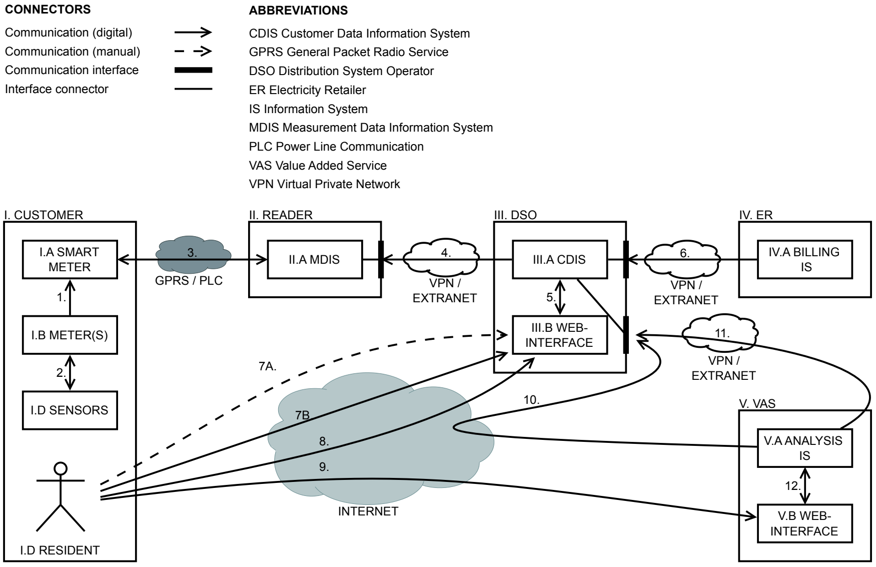


Figure 7.3: Reference architecture of a smart grid

The created reference architecture consists of the different actors, networks and connections between components. The actors in the layout are identified with an actor identifier (AID), and the mapping between the different tasks, functionalities and actors in the layout is presented in Table 7.2.

The management of the different systems containing consumption data of varying details and amounts is divided into three parts. The reader (II) maintains the MDIS (II.A), from which the collected consumption data is retrieved by the customer data information system (CDIS, III.A). The CDIS also contains other customer information required in the operations of the DSO (III) who maintains the CDIS. The billing IS (IV.A) contains customer data and C_{PII} and is maintained by the ER (IV) for billing purposes. For communicating with the smart meters, a mobile phone network is the most common along the PLC. Within and between companies, VPNs are typically used. The companies use a local area network (LAN) for internal information transfers.

Updates and maintenance are assumed to happen via the reader (II), and the DSO

Table 7.2: Mapping of smart grid actors to tasks and functions

AID	Actor name	Tasks	Functions
I	Customer	T2. Source T6. Accessing	F1. Measurement of consumption F4. Consumption monitoring
I.A	Smart Meter	T2. Source	1. Measurement of consumption
I.B	Meter(s)	T2. Source	1. Measurement of consumption
I.C	Sensor(s)	T2. Source	1. Measurement of consumption
I.D	Resident	T6. Accessing	4. Consumption monitoring
II	Reader	T1. Controlling T3. Reading T5. Storing	1. Measurement of consumption
II.A	MDIS	T3. Reading T5. Storing	1. Measurement of consumption
III	DSO	T4. Processing T5. Storing T6. Accessing	2. Grid management 5. Consumption data processing 6. Billing
III.A	CDIS	T4. Processing T5. Storing	5. Consumption data processing 6. Billing
III.B	Web interface	T4. Processing T6. Accessing	5. Consumption data processing
IV	Electricity retailer	T4. Processing T5. Storing T6. Accessing	2. Grid management 3. Electricity producing 5. Consumption data processing 6. Billing
IV.A	Billing information system	T4. Processing T5. Storing	5. Consumption data processing 6. Billing
V	Value-added services	T4. Processing T5. Storing T6. Accessing	4. Consumption monitoring 5. Consumption data processing 7. Analysis services
V.A	Analysis information system	T4. Processing T5. Storing	5. Consumption data processing
V.B	Web interface	T6. Accessing	4. Consumption monitoring

(III) requests consumption data only from the MDIS (II.A). Neither the Electricity Retailer (IV) nor the VAS (V) has direct access to the meter. The connections between the actors in smart grid implementations did not differ as much as the roles of the actors did. In Figure 3, the most common connections between the actors are shown; each is identified with a unique number. The descriptions of the connections in Figure 7.3 are shown in Table 7.3. In Table 7.3, the information that is transferred over each connection is also shown. The details for this information use were analyzed from the information use of different functions presented in Table 7.1 on page 123.

This presentation shows that the created reference architecture has fewer details than the existing architectures of NIST [114] and ETSI [115] but the right amount for information privacy analysis. The designed artifacts are introduced to the *application domain* as a process of establishing an architecture based on existing knowledge, implementations and system. This fully answers **Q6** of the DSR process.

7.1.7 A5: Evaluation of the results of the demonstration

The field testing by creating the reference architecture was the first utilization of the process to establish something concrete with it. This is the part of the *design cycle* (*3*) in which the artifact is evaluated after the demonstration.

The goal of the research process was to design an artifact to be used as a tool for assessing information privacy in the context of the smart grid environment. By developing the artifact using the background information from a specific *application domain*, the result might be too specific and tied to one application context only. However, the methodology used, the principle of abstraction and generalization, should seek out the most common and unique instances within the *application domain*, and this forced the creation of generic models applicable to any similar information-centric environment. This was not the goal of the research at this stage, and to prove such applicability, more research and testing need to be done in another *application domain*. However, the results the demonstration, the creation of a reference architecture, gave shows that the process of establishing both models helps to create an overview of the environment that shows only the necessary information flows. The four objectives set in Activity 2 introduced the specific aims for the designed artifact.

Objective 1: The resulting artifacts required the researcher to seek out what information was transferred between the actors in the environment in order to find the information transferred between the tasks and the functions. The background information, especially the existing architectures and the questionnaire, already detailed the information sent in the environment, and with further research about the tasks and functions, all the characteristics of information were mapped. The

Table 7.3: Description of the connections in the reference architecture with the transferred information

ID	Description	M_{id}	C_{id}	C_{PII}	C_{data}	C_{proc}
1	Home Area Network (HAN) connection that is used to transfer metering data to the smart meter.				x	
2	HAN connection that is used to transfer data from sensors to the meter either by requests from the meter or updates from the sensor.				x	
3	Mobile phone or PLC connection that is used for reading consumption data and controlling the smart meter.	x	x		x	
4	VPN connection that is used by the DSO to get consumption data from the MDIS.		x		x	x
5	LAN connection that is used for delivering consumption data and user information to the web interface.		x			x
6	VPN connection that is used by the ER to get necessary customer information and consumption data.		x	x	x	x
7A	Manual (e.g., a letter) way for the customer to authorize a VAS.	x	x	x		
7B	Digital way for the customer to authorize a VAS.	x	x	x		
8	Internet connection that is used by the resident to monitor own energy consumption and to access own personal information.		x			x
9	Internet connection that is used by the resident to view the result of the analysis.		x			x
10	Internet connection that is used to access the CDIS.		x		x	x
11	VPN connection that is used to access the CDIS.		x		x	x
12	LAN connection that is used for transferring the analysis results to the VAS web interface.		x			x

functional model is required to be constructed separately for each environment under assessment, and therefore, the information usage in each function is required to be always studied. This was the case here as shown in Table 7.1 on page 123. The potential use of the transferred information was left for the grounding step of the *rigor cycle* (*2*), in which a wide variety of research on privacy in smart grids was sifted through. The publications [12, 30, 31, 32, 33, 34, 36, 72, 82, 140] and the documents offered by [114] and ETSI [115] gave enough details and offered motivations for conducting the assessment of privacy risks in smart grids. This information was used in the information mapping of the functions and in the information use of the different connections (Table 7.3 on the facing page) to first present the most optimal information use to mitigate the potential risks and threats, which was then used in the information use mapping of the connections.

Objective 2: The diverse answers on the questionnaire brought the challenge of creating something common from a seemingly dispersed field of actors in smart grid implementations. However, further analysis proved that commonalities exist, and with the principle of abstraction and generalization, the unique instances were found. The demonstration of the artifacts, the process of establishing the reference architecture, shows that by dividing the environment into the most abstract tasks and going from there to more details about the environment through functional and information use analysis, all actors in the environment can be included in the process.

Objective 3: To this objective, the process itself is the answer. The study of the tasks, the functions and the information transferred between them, as well as the construction of the reference architecture forced to seek out the information usage in various places in the smart grid environment.

Objective 4: The constructed reference architecture, shown in Figure 7.3 on page 125, is the fulfillment of this objective. It offers a plain view of the environment by showing only the connections between the generalized actors. However, whether this is an appropriate tool for assessment needs more research. But the establishment of the architecture requires a thorough investigation of the environment and, therefore, offers details for further information privacy assessment.

Furthermore, the answers to the questions laid out in the evaluation of the artifact, which could not be detailed without the results of the demonstration, are as follows:

2. The establishment of the reference architecture required to do more research on the real-world connections in the smart grid environment. This research showed that the connections between the tasks are correct and the tasks can be mapped to the actors in a real-world scenario.

9. Detailed information usage of various types of information transferred in a smart grid was mapped out in Table 7.3 on the facing page. This shows that the whole process can detail the information usage in the required depth of detail.

10. The mapping of information use in Table 7.3 on page 128 shows that the knowledge obtained from the process of establishing the reference architecture through the task and functional models is sufficient.

11. The depth of detail is less than in existing architectures but is enough for establishing the reference architecture to display only the necessary information flows inside the environment. Therefore, the process of establishing such architecture is better for information privacy assessment by reducing the need to go in depth in the details of the smart grid environment.

7.1.8 A6: Communication of the results

Since all of the objectives were met, the transition to the sixth activity was found to be suitable. The designed artifacts were suitable for solving the problem laid out in A1. This is the part of the *rigor cycle* (*2*) in which new additions are contributed to the *knowledge base* (*c*). The process in which the reference architecture is created through intensive analysis and the establishment of both models is the meta-artifact of this research that was published in [45], which partially answers DSR **Q7**.

This activity is not described here in full detail because the process and the results were published in [45]. The publication of the results in the ASE/IEEE conference on Privacy, Security, Risk and Trust in September 2013 in Washington, D.C., is the actual communication of this research to the proper audience. A summary of the first publication [45] is detailed in Appendix B.1 on page 251, and the highlights regarding this research process were the following:

- A survey of the privacy risks and threats in the smart grid environment
- Presentation of the questionnaire results
- Introduction of the process for creating abstract and functional models with the principle of abstraction and generalization
- Creation of the concrete reference architecture with the process and the information offered by the questionnaire and the models
- Discussion about the potential threats regarding the layout presented in the reference architecture
- Discussion about the effects of the changing roles in different smart grid implementations
- Last, an accepted proof for using the designed artifacts in information privacy assessment in the context of smart grids

The new information that was contributed was, therefore, a new method in the form of a meta-artifact that encompasses both designed artifacts in a peer-reviewed research article. This is the full answer to **Q7**. **RQ1** was answered by answering **objective 1,** and **RQ2** was answered by fulfilling the needs of **objective 3** to which the answer of **objective 4** partially contributes. This answers DSR **Q8** and concludes this part of the research.

7.2 Creation and evaluation of the iterative framework

The second context in which the artifact, developed in the previous part I, was not mainly designed for but applied to with slightly changed objectives was the digital games platform (DGP). The purpose of the Game Cloud research project [25] was to establish a DGP that offers increased value for game developers and players. The main purpose of this research project is to evaluate the possibility of using ontologies to standardize game information and to enable transferring of game content between multiple games.

But to establish such a platform, the privacy of the players must be guaranteed in order to gain their trust. The artifacts developed in the previous process of part I were selected as tools for analyzing information privacy in the DGP because both, the DGP and the smart grids, are information-centered environments, the purpose of which is to collect data from the users (players and customers). Before the design process is described, the context in which the research is conducted is explained.

Context: Game Cloud Game Cloud [25] is a new digital games platform operating on top of cloud computing infrastructure enabling collecting, analyzing and using data collected from players using various linked games. The main objective of the project is to standardize game information through ontologies to enable game content transfers between games to offer more continuity and immersion. All of this is enabled by the data collection, gameplay analytics and player profiling offered by the ontology processing engine. Game Cloud offers value for developers and players:

1. Game Cloud offers additional value for developers and players. For developers, the value comes from understanding player behavior by gathering statistics, which enables development of better products.

2. Game Cloud offers continuity and immersion between different games that, in turn, makes it possible for the players to get more value out of their games and connected services.

Research Questions and DSR Questions Similarly to the research process for creating and evaluating the *abstraction method*, the two research questions, RQ1 and RQ2 (described on page 22), are addressed in this research process. The DSR specific questions DSR Q1 to DSR Q8 are answered as follows; Q1 in 7.2.1, Q2 and Q3 in 7.2.3 on page 138, Q4 in 7.2.2 on page 137, Q5 in 7.2.3 on page 138 and 7.2.4 on page 139, Q6 in 7.2.7 on page 150, Q7 in 7.2.2 on page 137 and Q8 in 7.2.9 on page 153.

7.2.1 A1: Problem

The problem was to analyze information privacy risks in the Game Cloud platform during the development of the platform to enable better privacy through system design. The nature of the problem was similar to the previous one for the smart grid environment, since finding out the usage and transfer of PII was one of the key issues. However, the use of the artifacts was different as here a new platform was designed instead of analyzing existing ones. The scope had to be changed to support a design process of the platform in an iterative manner. These platforms, Game Cloud especially, collect data from the actions of the players during gameplay directly or using other connected appliances, such as Kinect [37].

The risks in gaming data use from the literature show [37, 38, 39, 41], as was partially discussed in 2.3.3 on page 46, that the possibilities opened up by accurate gaming data are numerous, privacy threatening and ready to be utilized. Most of the collected data is connected to the PII of the player. The vast survey on gaming data collection and use conducted by Newman and Jerome [37] show that non-PII data can be and is collected[50] by the companies. The non-PII data is collected from other activities than from the activities within the game-world. By combining both, a detailed profile of a player may be established on psychological and behavioral grounds. Handling and storing this type of private player information within the DGPs introduces new challenges for the privacy requirements and privacy needs of the players [37]. In order to maintain trust, information privacy must be built-in to the system [9].

In the survey [37], there is two classifications for collected data: (1) real-world data and (2) player behavior.

1. **Real-world data**: Collecting real-world data is about monitoring other activities and characteristics, such as biometrics, of the player that are not directly analyzable through the game. Biometrics include a player's skeletal and facial features, body movement, voice data, head position and movement, motion of the player, physical location, images from the surround-

[50] http://www.democraticmedia.org/candy-crush-ipo-we-collect-and-store-significant-amounts-information-about-our- players-pii-and-non-p

ings, heart rate, hand movement and even a 3D map[51] of the physical items and room structure surrounding the player [37]. The second aspect of real-world data is the collection and analysis of the player's social activities. The large social networks, such as Facebook and Twitter, offer a lot of information about the player since many games have incorporated the features to connect the game-worlds to the real world through social networks [37]. This results in direct, voluntary identification of a player, which makes it potentially possible to connect everything from the player's friends, contacts, likes and dislikes, education, work history, and physical appearance to the game-world, for example.

2. **Player behavior**: This is the data the games, game platforms or environments collect. Every input, action, reaction, purchase, chat message and information transferred with a client and a server in a online game can be collected [37] and analyzed instantly or much later. Such data is used for a huge variety of purposes. Some of it is used to research the gamer's experience, economic proclivities and to remove issues from games that make it hard or impossible to progress within the game (e.g., bugs) and some other parts of data can be used to analyze the player, even from a psychological perspective [37]. This has also been used for gamers' amusement; in *Silent Hill: Shattered Memories,* the virtual psychiatrist of the game is made to analyze the player within the game by the actions made by the player[52]. In addition to the game actions, the behavioral data can include the types of games the player wants to play, how long the games are played and when.

This behavior data is peculiar in the sense that while some of the actions made by a player can stem from the deep and dark sections of the players' subconscious mind, others can just role play the characters, i.e., act within the game. Psychologists might be willing to use such data for analysis, but the possibility of false-positives may be very high. The context should be fully understood before any decision based on the analysis can be made. For this need, the analysts devise new, more sophisticated methods to predict, for example, player-types through in-game actions, chats and style of play[53]. Using psychographics, where the psychological characteristics of an individual are quantified using the collected real-world and behavioral data, the analysis is possible [37]. This is referred [37] to as game personalization, which is not seen as problematic by players. Instead, players see this aspect as interesting since their own actions within the game-world have an impact on the gameplay and have no problem in sharing their psychographic profile [37].

However, with learning games, things are different. The data collected by such games can reveal a lot, for example, from the players' intelligence, and the data

[51] http://motherboard.vice.com/blog/googles-new-room-mapping-phone-raises-privacy-questions

[52] http://silenthill.wikia.com/wiki/Silent_Hill:_Shattered_Memories

[53] http://arstechnica.com/uncategorized/2007/05/google-patent-for-game-ads-evaluates-user-actions- psychology/

is expected to be treated with the highest confidentiality[54]. By combining the details and skills offered by psychographics, game analytics and psychologists, the collected data may reveal more than meets the eye. False results from the analysis may, for example, harm player privacy through incorrect labeling and the revelation of wrong issues about personality, damage user trust if data is used to manipulate player psychology to create game addiction [37] and damage the company's reputation in the market if the wrongful decisions are publicized. The wrongdoings of a game company are not tolerated well by the players.

One of the biggest examples of this in gaming history was the *Spore* game that was released in 2008 by Electronic Arts. The company included digital rights management software, SecuROM, which is regarded as a rootkit, in the game that was forcefully installed with the game and could not be removed easily [141]. There were class-action lawsuits filed by the players against the company [141], but many resolved the problem by pirating a version of the game, from which the protection was completely removed. This may have had major economic impacts since *Spore* was the most pirated game of 2008 [142]. There are no details about how many players,who legitimately bought the game pirated the game to avoid the installation of SecuROM.

Therefore, players' trust in companies plays an important role in the game industry. Other actions of the company, such as data use without permission, have a big effect, but the impact of data collection on trust is significant. Collecting the data from the games and combining it with real-world data is, therefore, a delicate matter in which players' privacy and the reputation of the companies collecting the data are at stake. Both have significant economic impacts, which in the case of loss of trust can turn negative.

Motivation 1 to collect data: quality The idea behind Game Cloud neatly summarizes the interest from the economic perspective. On such platforms, the most visible reason for collecting and using the data is to provide the players with a service of enhanced quality, but the financial benefits are the ones that push the collection onward. By increasing the quality of the service, the players can get more out of their games. Additionally, the platforms can recommend games to players based on purchasing behavior and offer immersion between the real world and the game world if a player wishes it. Different groups get different benefits from the game behavior data; developers value the data from a qualitative viewpoint similar to players, but the value is quite different for publishers and advertisers. The developers can use the game behavior data to increase the quality of their product by improving gameplay and enhancing the storyline, for instance. For them, the data is also of qualitative value, but the increased quality of their games will eventually result in more revenue.

[54] http://blogs.edweek.org/edweek/DigitalEducation/2014/02/education_leaders_tackle_stude.html

Motivation 2 to collect data: money Publishers and advertisers tend to perceive game behavior data through monetization. The publishers' and advertisers' intent in collecting large amounts of identifiable and accurate data is to trade the data in order to increase revenue, utilize the data for targeted marketing in their own or third-party systems [37] or to spend real-world money [143]. Publishers more likely want to sell more games and games-related products (e.g., action figures), whereas advertisers can see the profit in targeting gaming-related products, such as gaming controllers and gaming chairs, to players. Additionally, the location information of the player can be used in conjunction with other data in third-party services located in the real world. The reasons for collecting data are, therefore, in increasing revenue either through increased quality or by utilizing data for marketing. Revenue is increased with data collected from their customers, the players.

This introduces the clear need to detect the threats at the design stages in DGP development to mitigate the potential long-term impacts. The companies will collect more and more data (the amounts of data collected by Electronic Arts games are insane: 50 terabytes per day [37]) from the actions of the players and will continue to use it for a multitude of purposes, all of which are money-oriented. However, companies should also take care of player privacy to avoid losing the players' trust [37]. In Figure 7.4 on the next page, the long- and short-term impacts of game behavior data from the company's point of view are summarized. In the figure, the positive side impacts increase revenue directly or through increased quality. The negative side impacts are either loss of trust or revenue.

If companies stay on the straight and narrow, gaming data can offer multiple long- and short-term economic benefits as shown on the left side of Figure 7.4 on the following page. In legal use the financial benefits of gaming data are notable, mostly on long-term basis, affecting the economic aspects of a company. In unauthorized use, the effects are more of the loss of trust. In some cases, taking back what was once lost is nearly impossible, therefore, the impact of losing trust has mostly long-term effects. But the loss of trust can have very serious side effects. If the disclosure of data affects players on a large scale, the company can get a very bad reputation, and other nonaffected players can stop using the services altogether. This would result in either gradually or rapidly decreasing revenue.

Value of the solution: To avoid this situation, or at least alleviating the negative impacts, an approach is required to detect the information privacy risks and threats during the design process. Furthermore, to fully meet the requirements of the new European regulation [23], privacy has to be included by default in the developed platform. This can be established by including the seven principles (presented in section 2.4.1 on page 50) in the design process.

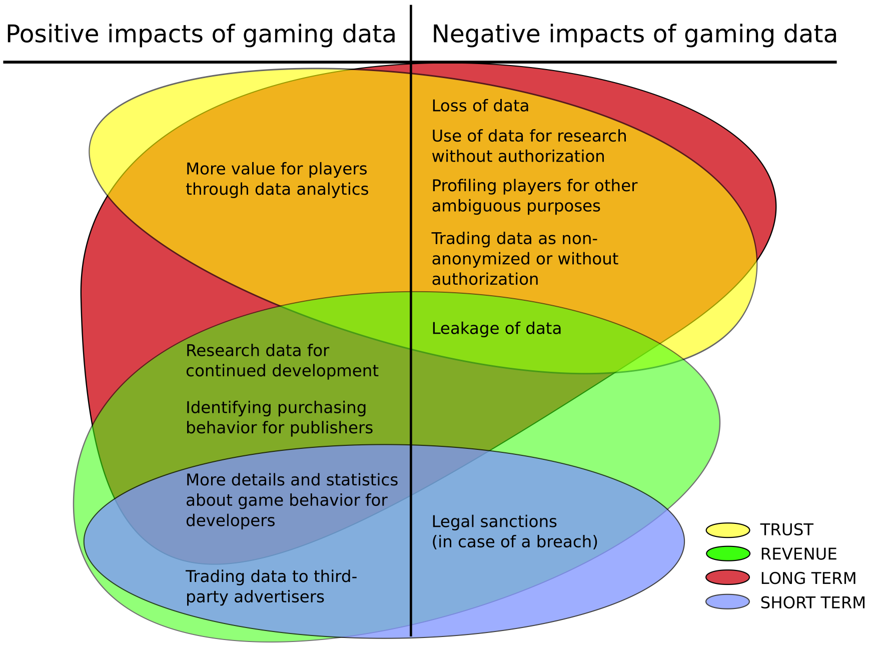

Positive impacts of gaming data
Negative impacts of gaming data
More value for players through data analytics
Loss of data
Use of data for research without authorization
Profiling players for other ambiguous purposes
Trading data as non-anonymized or without authorization
Leakage of data
Research data for continued development
Identifying purchasing behavior for publishers
More details and statistics about game behavior for developers
Legal sanctions (in case of a breach)
Trading data to third-party advertisers
TRUST
REVENUE
LONG TERM
SHORT TERM

Figure 7.4: Positive and negative effects of gaming data use for a company

Utilization of previous solution: In the beginning of the research process, the actors within the Game Cloud platform were detected as having many similarities to the actors in the smart grid. This was mainly because both systems are information intensive and the main purpose is to collect data from users. With a single iteration with the abstraction and generalization principle, the tasks and functions of Game Cloud were found to be similar to those that resulted in the previous research process. Therefore, the previous process was selected to be the basis for this research, and the main aim of the research is to modify the previous process from analyzing existing to analyzing alongside the development of a new system.

Research questions specific to this process: The research questions are almost the same as for the previous process. The attributes of the information used in the platform must be detected (**RQ1**), and the locations of environment in which information has to be protected must be detected (**RQ2**). Additionally, two research questions specific to this part of the research process are (1) how to modify the process to be iterative and (2) how to help incorporate the PbD principles in the design process. This answers DSR **Q1**.

7.2.2 A2: New requirements from Game Cloud

The background information obtained by overviewing the problem in A1 contributes to the knowledge about the *environment* (*a*) and the *application domain* to address the actual problem that offers details for defining the requirements in the *relevance cycle* (*1*). With the same information, grounding the research in the *rigor cycle* (*2*) to the existing technical systems was enabled. The background research in A1 gave a proper overview of the risks and threats in the *application domain* to offer a motivation for detecting them in a newly developed platform. These help in defining the requirements for the resulting artifact, which, in this case, is based on the artifact designed previously.

The research questions limit the scope as for the previous process, but the two new questions, specific to this part of research only, each introduce a new aspect. As a total, this part of the research process has three goals:

1. The first goal is to research the usage of iteration with the previous artifacts, the abstract and functional models.
2. The second goal is to find out how the artifacts can support and help include the PbD principles in the design.
3. The ultimate goal of this research is to develop an approach to assess information privacy risks in DGPs during the development in an iterative manner.

Relevance cycle: requirements As in the previous research process, the focus has to be on information privacy, and the information privacy risks in DGPs must be detected (**objective 1**). Next, the existing artifacts must be further researched so they can be adapted to the iterative development process of an information-centric (eco-)system (**objective 2**). With the modified artifacts, the information privacy risks detected in **objective 1** must be detected during the development process of the DGP (**objective 3**). By detecting the risks during the development some the PbD principles can be included but it is required to help in fulfilling all seven of them during the development (**objective 4**).

Rigor cycle: foundations This research is based on the previous research process in detecting information privacy risks in an information-centric system collecting information from the users, the development documentation of Game Cloud [25] and in the information detailed in A1. The different types of data collected and used by the gaming industry in multiple ways [37, 38, 39, 41] offer details about the information use and small details about what kind of environments are going to be dealt with. The information on the high abstraction level contains two parts as with smart grids; (1) identification and (2) measured or monitored data from the game or another service. Since this research is done for the

Game Cloud project [25], the details for the technical system involved are drawn from the Game Cloud design. The platform design documents offer the basis for grounding the research on something existing, or as in this case, on something new. The grounding of the research is, therefore, on the previous process of creating abstract and functional models and on the design of a new DGP, Game Cloud (answer to DSR **Q4**). The new contribution to the *knowledge base* is the new development of the previous process, but in addition, the added knowledge about how to design the new DGP with the approach is a notable contribution of its own (answer to DSR **Q7**). The development process of Game Cloud with the approach presented in this thesis, part of which this part of the research is, is later detailed in this thesis.

7.2.3 A3: Design and develop, iteration 1

This is the first iteration within the *design cycle* (*3*) in which the scope of the artifact is detailed. Here, the new objectives for modifying the existing artifacts are applied.

The benefits of the previously developed artifacts, the abstract and functional models, were seen in the construction of the reference architecture from wide background information about the smart grid environment. The two environments share similarities in the sense that both are developed for collecting information that is later analyzed to offer users a better service. Also, in both, the collected information is also used for other purposes, such as load balancing of the electricity network in a smart grid and purchasing behavior analysis within the DGP. Furthermore, the basic task structure was observed to have similarities in both after doing some preliminary research with the abstraction and generalization principle in Game Cloud. Therefore, the existing artifacts (models) and the process that was previously established were selected as tools for the Game Cloud design.

The artifact: This research modifies the two artifacts, the abstract and functional models that were detailed in the previous research process (section 7.1 on page 111). The results of this research are improved artifacts (abstract and functional models) that can be used iteratively to support detection of information privacy risks during development and to help include the seven PbD principles in the design (answer to DSR **Q2**).

Process for research: The process is the same as previously. The principle of abstraction and generalization [55] is used as a research methodology (answer to **Q3**). This methodology helps to detect the underlying unique instances of Game Cloud for task and functionality-based analysis.

Evaluation: The following questions (some are the same as in the process for the *abstraction method*) are used as a checklist for evaluating the artifacts (answer to **Q5**):

1. Are all existing tasks applied in the approach?
2. Do the connections comply with the connections of Game Cloud between the tasks?
3. Does the information transferred between the tasks comply with the information transferred in Game Cloud?
4. Are all existing functions of Game Cloud platform included in the functional model?
5. Do all connections between functions comply with connections in Game Cloud?
6. Does the information transferred between the functions comply with the information transferred in Game Cloud?
7. Does the approach include the personal identifiable information (PII) transferred in Game Cloud environment in the process?
8. Is it possible to detect information usage in the application context with the approach?
9. Do the artifacts suit iterative development of Game Cloud?
10. Are the PbD principles included with the help of the artifacts in the design of Game Cloud? How?

7.2.4 A3: Design and develop, iteration 2

In the first iteration, the basics for artifact development and evaluation, as well as the process for conducting the research, was detailed. The first iteration in this part of the research is similar to the first iteration in the previous research process (described on page 115) as both concentrate on the same artifacts. The background information offered by the problem description in A1 (the *relevance* and *rigor cycles*), the requirements in A2 (the *relevance cycle*) and the criteria laid out in the first iteration of the *design cycle* are combined here to modify the previous artifact.

This second iteration of the *iterative framework* is regarded as an improvement iteration of the *abstraction method* devised in the earlier process. In this iteration, the fourth question, “Are the tasks generic enough to apply the abstract model to other similar real-world scenarios?," of the previous process is answered. Based on the analysis of Game Cloud, the abstract model is enhanced in this iteration.

First, the Game Cloud (eco-)system was researched for unique instances, the actors involved in the system operations. From the initial designs, the following actors were found: administrator, application programming interface (API), back end, database, developer, front end, game, ontology engine, player and service. They can be categorized as components and users:

- Components:
  - API: The interface through which all information from and to games and third-party services is transferred. This is a completely public component to which all games and services can connect, and this is the main component for transferring data outside the system to the connected components (games and services). Gets the raw data with identification from the games and services and forwards this to the back end. Delivers the processed data from the back end to the games and services per request.
  - Back end: The main unit of the Game Cloud that contains the database withholding all information about the players and their statistics in raw and processed form. This component dictates the information transfers within Game Cloud. The back end gets the information from and delivers it to the API, the front end and the ontology engine. The transferred information includes player, game and service identification, raw collected behavior data, processed behavior data and PII of the players. The Game Cloud administrator has direct external access to the back end to control the system and has limited access to the information.
  - Database: The storage facility of Game Cloud that contains all the data collected by the system and that is accessible via the system. The database is located within the back end that controls the information transfers.
  - Front end: The interface for the players and the developers to access the information within the system. The players input their credentials to access their PII and processed behavior data. The developers get the statistics of their games in processed form after inputting their separate credentials. The front end is a completely public interface, accessible via the Internet so the players and developers can access it without restrictions.
  - Game: A game that is connected to Game Cloud for collecting the data from the actions made by the player while playing the game. The player connects the game to Game Cloud by logging in through it or adding the game using the front end. The game can deliver the raw data to the API along the player identification and requests the processed

data through the API for offering immersion and continuity based on the processed data.

  - Ontology engine: The heart of Game Cloud. The ontology engine contains a specialized generic ontology and game-specific ontologies to process all actions, the raw data, made by the player within any connected game. The raw data is retrieved from the database through the back end among all possible identifications (game, player, service) in order to produce an analysis based on the ontology. The results of the processing are sent back to the database through the back end. The parameters and the ontologies of the ontology engine can be monitored and changed by the Game Cloud administrator.
  - Service: A third-party service that is connected to Game Cloud. This service gets some analysis data through the API for giving some real-world benefits for the players or to connect the real-world service actions to the data of a player. The real-world benefits can include, for example, getting some game-connected products cheaper if an achievement is met or adding a real-world item, such as a soda can, to the item list of a game character.

- Users:

  - Player (end user): The target group of Game Cloud and one of the most vital actors in the system. Creates the data by playing games that are connected to Game Cloud and can control the personal information and monitor own (processed) data collection through the front end. Logs in to Game Cloud through games, (third-party) services or the front end, each of which provides a different type of service for the player. In games, the added value comes from enhancements to the game-world in the form of achievements, new content, new items and personalization. In services, the benefits are in connecting the game and real-world environments. The front end offers monitoring of game progression, achievement collection, service uses, games played and the extent of the data collected.
  - Developer: The game developer who uses Game Cloud to connect the games made, to adjust the data collection of the games and to get the processed statistics of the games. All this is done through the front end by giving credentials and game identifications.
  - Administrator: The maintainer of the Game Cloud system. Can monitor and adjust the parameters of the back end, database and ontology engine. Has external access to the back end and the ontology engine. For both, the access to user data is limited.

This analysis of the actors within Game Cloud gave sufficient details about the information usage within the system. The information transferred within the system was classified with PII 2.0 categories [20] to help identify threats. The information and classifications are shown in Table 7.4.

Table 7.4: Information used in Game Cloud with PII 2.0 classification

Data	Description	PII 2.0 classification
P_{id}	Player identification, including the credentials.	identified
P_{PII}	Additional player information (e.g., email).	identified
P_{rdata}	Raw player data sent by the device.	identifiable
P_{pdata}	Processed player data returned for the player and utilized by the games.	identifiable / non-identifiable
G_{id}	Game identification.	non-identifiable
S_{id}	Service identification.	non-identifiable

The actors and the information that is transferred between help to map the whole (eco-)system. The layout of Game Cloud is portrayed in Figure 7.5.

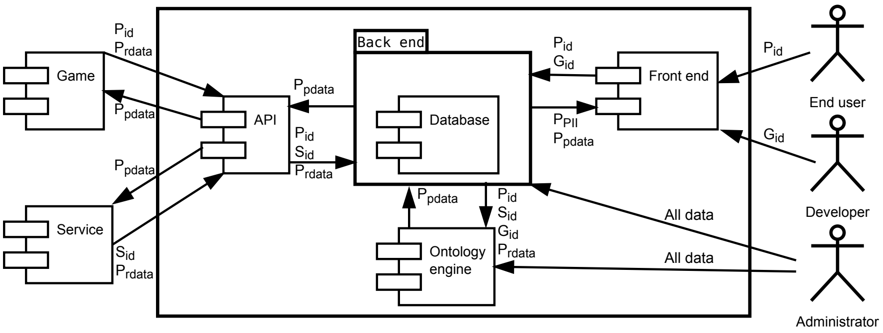

Game
Service
API
Back end
Database
Ontology engine
Front end
End user
Developer
Administrator
P_{id} P_{rdata}
P_{pdata}
P_{pdata}
S_{id} P_{rdata}
P_{pdata}
P_{id} S_{id} P_{rdata}
P_{id} G_{id}
P_{PII} P_{pdata}
P_{pdata}
P_{id} S_{id} G_{id} P_{rdata}
P_{id}
G_{id}
All data
All data

Figure 7.5: Layout of the Game Cloud (eco-)system

The details about the actors, the layout of the actors and the information transferred inside and outside the system make it possible to research the generic tasks of the system. First, the abstract tasks in the environment were researched with the abstraction and generalization principle [55]. The unique instances within the system were found to be similar to the abstract tasks defined in the previous research process of the *abstraction method*. However, because the architecture of Game Cloud involves different access levels, even at the abstract level it was decided to extend the existing abstract architecture by splitting the accessing task into two; high and low levels. The high-level accessing task is end-user API access to the data, whereas the low-level accessing task is access directly to the databases of the environment.

Furthermore, in Game Cloud the information transferred has three classifications as there are three separate instances found during the analysis: *player*, *game* and *service*. Each of these instances create data of different type, whereas in smart grid the data that was generated had only one type. All the three types of data (player data, game data and service data) could have been abstracted as *raw data* as it was defined in Table 7.4 but for further analysis needs regarding Game Cloud development it was seen necessary to show the multiplicity of data transferred even in the abstract model.

Moreover, by comparing the layouts of smart grid (the reference architecture in Figure 7.3 on page 125) and Game Cloud (Figure 7.5), it is evident that in Game Cloud the information flows between different actors are more bi-directional than in smart grid. For example, the ontology engine retrieves data from the database but also stores the results of the analysis in the database. The analysis of the tasks proved the point that many generic tasks have bi-directional information transfers. Using the previous example with the ontology engine and the database, the processing task exchanges information with the storing task by getting the *raw data* from the storing task and putting the *processed data* back to the storing task.

At the high abstract level, the tasks have different access levels to the information. The tasks and their descriptions are as follows:

T1. *Controlling* the information source, in here either by playing the game or using some third-party services. This is a one-to-many connection; one *controlling* task handles multiple *sources* (2).

T2. The *source* creating the data (actions, events) from the actions of the user. In Game Cloud, the sources that generate new data are the game and the third-party device/service. The created data (from multiple *sources*) in this case is forwarded (sent) to the *reading* (T3) task.

T3. *Reading* the data, in this case, the actions and events, from the information *source* (T2). In Game Cloud, the multiple *sources* connected to the *reader* use the push method instead of polling. One *reading* task handles multiple different *sources*. Thus, the connection to outside Game Cloud is many-to-one and inside Game Cloud, to the *storing* (T5) task is one-to-one.

T4. The information *processing* task is a bi-directional connection to the *storing* (T5) task, since the results of the processing are stored for future use. In Game Cloud, the results of the *processing* are forwarded to another *storing* task. There can be many different participants doing the *processing*, and therefore, the connection to *storing* (T5) is many-to-many.

T5. The *storing* task is the most connected task, and it is responsible for storing and delivering the information to the connected tasks based on the request and access type. The information is mainly inputted in the *storing* task by the *reading* (T3) task, but data can be pushed by the *processing* (T4) and the *low* (T6) and *high* (T7) *accessing* tasks (e.g., user information and administrative changes).

T6. *Low-level accessing* is a bi-directional connection to the *processing* (T4) and *storing* (T5) tasks using administrative privileges. Therefore, the access is to all the data both tasks control. There can be multiple administrators for each environment, and the connection to the *processing* (T4) and *storing* (T5) tasks is many-to-many.

T7. *High-level accessing* of the database contents defines the end-user access in the environment. The data received is always processed, and the connection to the *storer* (T5) is always many-to-one, since there is a certain data storage the multiple end-users are allowed to use.

The analysis and descriptions of the tasks help to connect them to the real-world actors of Game Cloud. The mapping of the abstract tasks to the actors of Game Cloud is shown in Table 7.5. This kind of mapping that is not tied to the functions offers more flexibility in the iterative assessment process as the designs can have big changes that affect to the mapping. This complies with the first and third goals set in A2 on page 137.

Table 7.5: Mapping of abstract tasks to the actors of Game Cloud

Component	T1	T2	T3	T4	T5	T6	T7
API			x				
Front end							x
Back end					x		
Database					x		
Ontology engine				x			
Game		x					x
Service		x					x
End user	x						x
Developer							
Administrator						x	

This resulted in the following improved abstract architecture, shown in Figure 7.6. The PII in the abstract model is kept by the components executing the *storing* (5) task. The PII is used to connect the end-user to the player data (player- and game-generated data) using an identification. The game and service data is set up by the game developers and third-party service maintainers, and it is not considered here as part of the PII.

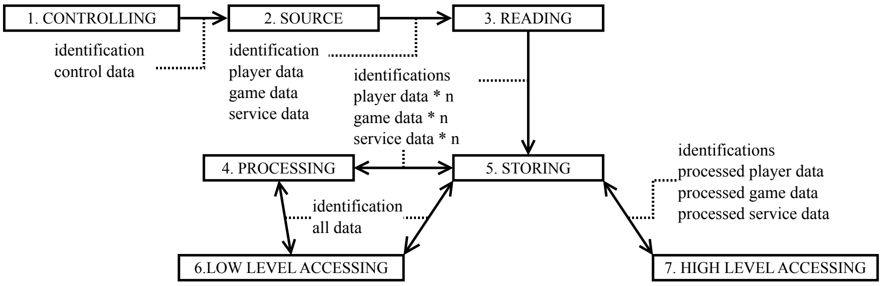


Figure 7.6: The improved abstract model for DGP development

The clear improvements in the previous version of the abstract model (Figure 7.1 on page 120) are (answer to the DSR **Q5** improvements part) the following:

- An additional task to support multiple levels of information access
- More information flows between the tasks dealing with raw data (access, process and maintenance).
- Bi-directionality of the information flows between the tasks dealing with raw data.

This version of the model was found to be suitable for the analysis but a bit confusing; thus, there is no separation in the data transferred in bi-directional connections. Therefore, another small development iteration is required for the abstract model.

However next, the functions within Game Cloud are determined. As in the previous process, the research on the generic tasks helped in finding out the basic functions in the system. Similarly to the previous process, the basic verbs occurring in the Game Cloud development documentation were researched with the principle of abstraction and generalization. The detected verbs are (in alphabetical order) *administrate, compile statistics*, *generate*, *manage*, *measure*, *monitor*, *process* and *serve.*

From these eight verbs, the functions for Game Cloud can be deduced. In Game Cloud, the functions and their descriptions are as follows:

F1. Player data measurement: The software component of Game Cloud used by the game, which measures player behavior in the game. The measurements are delivered for data generation functionality.

F2. Player data generation: Creates events from the actions of the player in the game. The generated data is forwarded to the player data management functionality.

F3. Player data management: Collecting, storing and managing the player data in Game Cloud. This data is given to processing functionality.

F4. Player data processing: Processes the raw events by request or for use in other operations of Game Cloud. The monitoring, statistics and third-party functionalities receive only the processed information.

F5. Player data monitoring: Using the processed data in the games and viewing them via games.

F6. Player statistics: Viewing the processed and analyzed events and other player statistics via the front end.

F7. Third-party player services: The additional services offered by third parties that utilize game events.

F8. Administration: Maintaining and configuring the components of Game Cloud.

The functional division enabled us to map the information exchanged in Game Cloud (Table 7.4) to the functionalities according to Table 7.6. The *x*es in the parentheses are not mandatory for the task. The mapping of tasks is excluded from this table since the development process more likely changes them, and another way of presenting the task mapping (Table 7.5 on page 144) was seen to be more suitable. This type of mapping supports better the changes occurring within the development of new systems. As mentioned with the abstract tasks, this also complies with the first and third goals, set in A2.

Table 7.6: Information required by different functionalities

F#	Functionality	P_{id}	P_{PII}	P_{rdata}	P_{pdata}	G_{id}	S_{id}
1.	Player data measurement	x		x		x	x
2.	Player data generation	x		x		x	x
3.	Player data management	x	x	x	x	x	x
4.	Player data processing	x		x	x	x	x
5.	Player data monitoring	x			x	x	x
6.	Player data statistics	x	x		x	x	x
7.	Third-party services	x			x	x	x
8.	Administration	(x)	(x)	(x)	(x)	(x)	(x)

The data in Table 7.6 is connected as follows:

- P_{id} is contained within P_{PII} and is linked to P_{rdata} and P_{pdata}.
- All the G_{id}s of the games the end-user has are contained within the P_{PII} and are linked to the P_{id}.

- All the S_{id}s of the services the player uses are also contained within P_{PII} and are linked to P_{id}.

This mapping of information to functions leads to the mapping of functions to the actors. The mapping is presented in Table 7.7.

Table 7.7: Mapping of functions to the actors of Game Cloud

Component	F1	F2	F3	F4	F5	F6	F7	F8
API	x							
Front end					x	x	x	
Back end			x					
Database			x	x				
Ontology engine				x				
Game	x	x						
Service							x	
End user					x	x		
Developer						x		
Administrator								x

With this information about the functions and their mapping, the functional model of Game Cloud is established. The functional model presented in Figure 7.7.

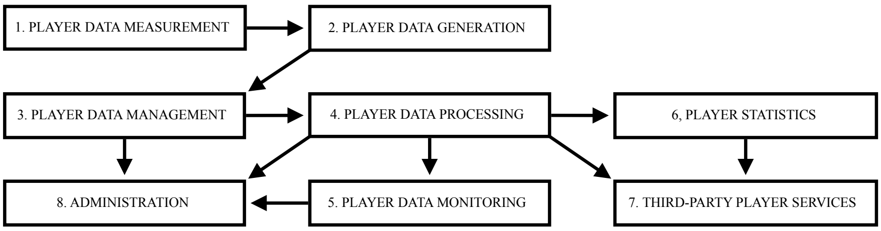

1. PLAYER DATA MEASUREMENT
2. PLAYER DATA GENERATION
3. PLAYER DATA MANAGEMENT
4. PLAYER DATA PROCESSING
6, PLAYER STATISTICS
8. ADMINISTRATION
5. PLAYER DATA MONITORING
7. THIRD-PARTY PLAYER SERVICES

Figure 7.7: Functional model of Game Cloud

The formation of the abstract and functional models, with some modifications, shows that the process developed in the earlier research process description of part I: *abstraction method* is suitable for other real-world scenarios, too. This answers the fourth question, “Are the tasks generic enough to apply the abstract model to other similar real-world scenarios?,” presented in the previous process to answer DSR **Q5**.

It is evident that the generic tasks and functions do not need to be sought out on each iteration. Instead, the mapping of both is more likely to change during the development. This is the issue that has to be noted in design iteration assessments. The mapping offers a good reference to the previous version to show which areas need improvement, and based on the information a new, more secure and privacy preserving layout can be designed. This way, the feedback loop is integrated into the process. It is, however, difficult to say when to stop making improvements and which is the last iteration. The available time and resources, and the time schedules of the project, dictate this.

7.2.5 A3: Design and develop, iteration 3

This is the third iteration in the *design cycle* (*3*) where the abstract model is improved based on the notions in the previous iteration. The functional model does not require changes as it is always *application domain* specific.

To address the problem of clarifying the bi-directional connection and to make the model more readable, the information flows were separated between the tasks under separate flows (arrows). This new development version is portrayed in Figure 7.8.

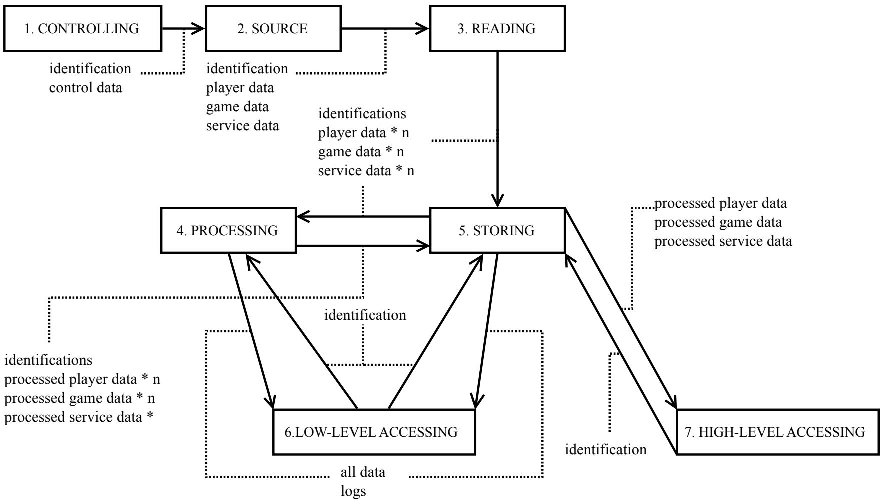


Figure 7.8: Second improvement in the abstract model for DGP development

This development version of the abstract model at first seems more complex and less readable than the previous version (Figure 7.6 on page 145). However, the details offered by this version (Figure 7.8) reveal a lot more about the environment. The added directional arrows to display the actual information transfers in each direction between the tasks offer a lot more value than the ambiguous presentation of the previous version. This answers DSR **Q5**.

7.2.6 A3: Evaluation of the artifact

This is part of the *design cycle* (*3*) and is executed after the artifacts are designed. The resulting process to create the artifacts for iterative development, the abstract and functional models, is first evaluated with the 10 questions presented earlier (on page 139) before conducting the field testing as a demonstration. The answers to the questions are the following:

1. After increasing the task number to seven by splitting the previous single accessing task into two, the tasks within Game Cloud are included in the approach.

2. The re-mapping of the task connections and creation of a new version of the abstract model the connections comply with those in Game Cloud.

3. With the added information flows and changing the bi-directional transfers to separate directional transfers in the second improvement for the abstract model, the information transferred between the tasks in Game Cloud is accounted for.

4. Since the functional model is case specific that is required to be established for each assessed environment and system, the model complies with the Game Cloud functions.

5. All connections between the functions in the established functional model comply with the connections of the Game Cloud functions (reason: see the previous answer).

6. According to the two previous answers, this is also fulfilled by the functional model.

7. The transfer of PII in different functions is shown in the functional model. The approach can include the usage in the process of detection.

8. The process in which the both models are to be created forces the person doing the analysis to include many details about the information transfers within the system. In Game Cloud, this forced the researcher to look deeper into the design and to discuss with the developers to get the required information. Thus, more information was acquired than it was needed to formulate the models.

9. This question can be answered only after the demonstration.

10. The PbD principles are not included in the models directly. However: the models help to fulfill them during the development, attempting to meet the second goal of this research. How the *iterative framework* can help in fulfilling is detailed as follows:

(a) The iterative development process with a continuous assessment of information privacy risks with the models can fulfill the first PbD principle.

(b) The second principle, privacy by default, can be fulfilled by enforcing it as a design principle, which also helps to fulfill the third principle.

(c) The utilization of the approach makes the system more safe in terms of information privacy, but it is not always guaranteed that the result is a positive sum; therefore, at this stage, it is too early to state whether the fourth principle is met.

(d) By detecting the problematic information usage in different components, the fifth principle can be met, which also supports fulfilling the seventh principle by suggesting problems in accessing private information.

(e) The sixth principle can be helped to be met if the design process is published with enough details that the users can see their private information protected by the design.

(f) The seventh principle is about giving access to the users for maintaining their data, which is completely beyond the scope of this *iterative framework* or its usage. This can be partially met with the usage of this framework by detecting where more privacy protection is required; thus, by employing appropriate means, this framework can be used in increasing end-user privacy, although indirectly.

7.2.7 A4: Demonstration of the new artifact

This is the field-testing part of the *relevance cycle* (*1*) in which the use of the artifacts, the abstract and functional models, is demonstrated. This is done in the *application domain* of the *environment* (*a*) by analyzing the information the process of constructing both models offers. This information is used to establish an improved layout for the Game Cloud (eco-)system (answer to DSR **Q6**).

Another round with Game Cloud development was done to demonstrate the use of the process. The task and functional distribution (Table 7.5 on page 144 and Table 7.7 on page 147) with the information use (Table 7.6 on page 146) offered showed that many types of information were accessed by many different actors through one front end and one back end. This includes access to the P_{PII}. The access rights management would have to be carefully designed to avoid possible unauthorized access from outside or inside. It was evident that access could not be restricted from the outside as it would make use of the system more difficult. However, the current solution with two external access (front end and administrator access) routes completely public was redesigned to be more privacy preserving and to be more secure. A hash-based solution was selected to hide the information retrieval under specific queries that are required to be known in order to get any piece of information. The result of the first development iteration is shown in Figure 7.9, where H stands for hash that matches a query to retrieve some data from the query database and Q stands for the specific query that is used to get the data (P_{pdata}) from the database.

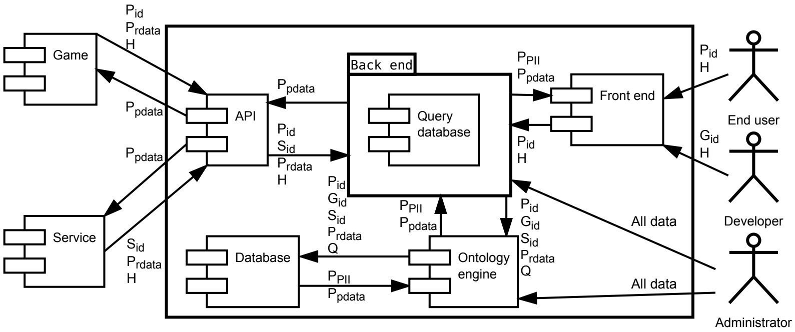


Figure 7.9: First improved version of the Game Cloud architecture

This is just one example of what was done during the iterations of Game Cloud development. More details about how this redesign was performed are described later in this thesis through the complete case example of Game Cloud development, starting on page 261.

The *abstraction method* was developed to establish a reference architecture from existing information. This new research step of the same process changed the scope to the *iterative framework* supporting multiple development iterations of a new system. Previously, it was straightforward to demonstrate the use by constructing something concrete for analysis. This new *iterative framework* would need a multiple-iteration demonstration of the development of a new system to fully grasp the benefits. Since the Game Cloud development is presented later in this thesis (also published in [46]), the demonstration of this *iterative framework* is continued there.

Finally, to answer the ninth evaluation question, the changes that were made in the first round strongly suggest that the process is suitable for iterative development. This is because changes and their information uses can be compared those of the previous version. The case example presented on page 261 shows this in full detail.

7.2.8 A5: Evaluation of the results of the Game Cloud demonstration

The abstract model remains the same during the development because the basic tasks are not going to change in this system. The functional model stays the same as well, but the mapping of the functions and tasks to the components keeps changing during development. The information used within the functions should remain the same, but changes are possible if the development changes are radical. In addition, if the design changes a lot, or new features are included, the functions might increase if the scope of the platform is changed as well. In the scope of DGPs, however, the basic functions should remain the same throughout the development.

All of these issues have to be accounted for in each iteration of the development process evaluation. The tasks and functions should be reevaluated on a component basis for each assessment iteration and re-mapping is required if changes are noticed.

Objective 1: Risks in the information use within the system were detected, and design changes can be made based on the details. But in order to fully map out the risks and threats to information privacy, another tool that goes deeper into the details of each component has to be employed. By employing such a tool or method, the DGP can be designed to be more privacy preserving, and the PbD principles can be better accommodated.

Objective 2: The existing artifacts required some changes in the new *application domain*, but the adaptation to iterative use required only small procedural changes. The mapping of the tasks and functions must be separate so they are mapped only to the actors in order to offer flexibility along the development process, thus the possible changes.

Objective 3: The answer to **objective 1** also applies here. The artifacts did not require numerous changes, and there has to be another tool that offers more detailed analysis of the risks on a component (actor) basis.

Objective 4: The seven PbD principles can be helped to be fulfilled with the process as the answer to the 10th evaluation question shows. But inclusion of the PbD principles requires an additional tool or method to evaluate the information privacy risks of each component in the system. The *iterative framework* can reveal only the information use within the system in different tasks and functions, and in components as well. In order to look inside the components and their attributes there needs to be another method to assess that. It is not feasible to incorporate such a method into the *iterative framework*.

New requirement: These answers to the four objectives clearly show that while some things were possible others require an additional tool to fully meet the objectives. It is not feasible to embed more properties in these artifacts as they are meant to offer a high-level view of the system. The additional tool for the *iterative* *framework* has to be designed as a separate artifact and the development of these artifacts, the process of the *iterative framework*.

Meeting the goals: The goals set in A2 are met for the most part. The first goal is met with the iterative approach adaptations. The second is partially met by including the PbD principles in the design, but this is more of a system design issue that can be solved with the help of an additional tool. The third and ultimate goal is met by devising the process for iterative development with the mentioned changes to the existing process. The later described case example of Game Cloud proves this point.

Decision: Since the process established here seems suit to the needs of the iterative process for the most part, it is reasonable to continue to the next activity. This is mainly because another tool must be developed for a more detailed assessment, and it is not feasible to incorporate them in the developed, or as they were modified here, artifacts.

7.2.9 A6: Communication of the results

This is part of the *rigor cycle* (2) in which new additions are contributed to the *knowledge base* (c). The designed artifacts were suitable for solving the problem laid out in A1. Adaptating the *abstraction method* to the *iterative framework* required only small changes. All goals could not be met with the current process, but with an additional, separate tool, the goals can be met. As in the previous research process (part I: *abstraction method*), the process of analyzing the DGP system with the *iterative framework* is the meta-artifact of this research, which is published in [46] (answer to DSR **Q7**).

This activity is not described here in full detail because the process and the results were published in [46]. The results were published as a journal article in the *International Journal on Information Technologies & Security* (number 4) in December 2014. This is the actual communication of this research to the proper audience. A summary of the publication [46] is detailed in Appendix B on page 252, and the highlights regarding this research process are as follows:

- Introduction of risks in game data use in DGPs.
- A detailed description of the process through a case example with multiple development iterations. This shows the *iterative framework* in action: how it is used and what it reveals.
- The development process of Game Cloud to be more privacy preserving

and more secure. With the level of detail provided, the transparency of the platform operations is increased and published.

- A strong claim about the adaptability of the *abstraction method* for the assessment of other environments or systems.

As in the previous process, the new information contributed to the *knowledge base* (*c*) was a description of a process to be used in iterative development as a framework for detecting information uses during design the process (answer to DSR **Q7**). **RQ1** is answered by analyzing the information flows inside the Game Cloud (eco-)system during the development (**objectives 2** and **3**) and the generic risks to information privacy that exist in DGPs and utilization of collected game data (**objective 1**). The first specific research question is answered by the modification of the *abstraction method* to support iterative use (**objective 2**). The second specific research question cannot be completely answered with the developed artifact and requires more research in the form of another process in which an additional tool is established. However, by partially meeting the aim of **objective 4**, the second specific research question can be also partially answered with the description on page 149.

These are the answers to DSR **Q8**. This concludes the research process on the *iterative framework*.

8 Description of research to create and evaluate contribution 2

This section presents the research to develop the second contribution of this thesis: the *assessment model*. The process of research is an instantiation of the DSR process described in section 6. As in the previous section, here the design of the artifacts is presented as the activity-driven DSR process depicted in Figure 6.2 on page 107.

Research on the *assessment model* development began in the MobiServ project [24] (see also Appendix C on page 257) as shown in the research process time line (Figure A.1 on page 247 in Appendix A) and is an ongoing process. Here, in the last subsection, the research up to the current state of research is presented. The model has had three design stages, and the development process has been research oriented from the beginning. The model was also used in the Game Cloud project as an analytical tool, which gave good feedback for the design but did not change the orientation of the development. The research still weighs more than the needs of the projects. Most parts of the second activity and the third activity descriptions in the process of developing the *assessment model* (section 8) are taken directly from the author's fifth unpublished manuscript [59] (see Appendix B).

The motivation for this part of the research emerged from the new needs and requirements introduced by EU [23]. The problem was the new definition of DPD in the proposed the EU regulation [23] as (1) it affects many, even smaller, companies, and (2) the proposed penalties for not assessing information privacy risks and threats are immense, not to mention (3) the penalties in case of a leak or theft.

The aim was to research how to help companies, corporations and organizations comply with the requirements. This question brought up another problem: how to measure information privacy, what kind of approach is suitable for the need. The resulting approach has to be easily understandable, and expert knowledge should not be required as the new regulation concerns many small companies, corporations and organizations, which can have very limited resources (answering this helps to answer **RQ3** and the third goal of the research). Therefore, the approach was decided to be developed as a mid-level tool [50].

As a summary of the research incentive, there is a growing need for a method to assess information privacy risks in any system that either stores or collects information about individuals. Use of the information can be excluded as the regulation has a strong impact on the withholding of information that can be linked to an individual [23]. Information privacy is a complex issue [5, 6, 7, 8, 18, 19, 20] that is affected by many different attributes ranging from security and legal aspects [20, 23, 48, 49, 144] to properties of data [51, 52, 53, 117, 118]. These attributes lead to the formation of a theoretical construct of information privacy (this aids in answering **RQ1**). In addition to the theory about information privacy, the research has to include legislation in the process. Because the approach is researched and devised as a need introduced by legislation, the legislative aspects and definitions of privacy have to be included (this offers answer to **RSQ3.1**).

The assessment in this case (to answer **RQ3**) is most suitable to conduct with a software tool. The tool has multiple benefits in comparison to a methodology or an approach that exists only on paper, diagrams or presentations:

1. First the tool can hide all the complexity behind the user interface. The user just needs to know how to operate the tool, and knowledge about the theoretical background is not required at all.

2. Second, the tool makes it straightforward to compare the results of the analysis after making changes to the system. The tool can also test what effects the proposed changes would have on the analysis results without making the actual changes. Additionally, during the development stages of a new system, the tool can be used as a design tool to map out the problems in the current version or to compare the different layouts.

3. Third, using the tool requires much less effort than a full-scale assessment of the system architecture. The tool can be also used to survey the system and to detect where more protection is needed, and the resources can be targeted to those areas. This may have significant economic benefits.

In this work, only the approach for assessing information privacy risk is developed through research. This part of the research describes the model development process, which is the key element in the approach for developing the tool for assessing the risk to information privacy. The software tool would be an ideal presentation of the complete approach presented in this thesis, but due to time limitations and the amount of work it would require to develop such a tool, it is left for future work. The previously detailed processes of the *abstraction method* and the *iterative framework* will be included in the tool later and are not discussed in this part of the research. Only a software prototype of the *assessment model* was developed for evaluation purposes. This software prototype is available at `https://github.org/lut-projects/iprat` and is referred to in this part of research as such.

8.1 A1: Problem

There is no exact *application context* (*a*) in which this research was conducted. It is more suitable to state that the context is more of a generic high-level representation of information-centric systems that collect or withhold identifiable information about individuals. Or that the *application context* is information privacy itself.

The background for this research comes from the projects in which other parts of the research presented in this thesis was performed, such as SGEM [57] and MobiServ [24], and they are regarded as part of the *knowledge base* (*c*). One part of the research artifact demonstration is done in such a system: the new DGP, Game Cloud. As previously, the research on the model is described as activity-driven research.

The problem in general is how to measure information privacy and how to generate useful and easy-to-read results. In addition to being a complex issue, privacy is a highly subjective issue with cultural ties that affect understanding and defining it. Therefore, measuring this issue and producing results that are not subjective is a problem. Money is also a question; it is problematic to assure companies, for instance, to conduct such an assessment of an issue with an undefined (or undefinable) value. As a part and origin of the problem, as well as a solution to the previously mentioned issue, the EU introduced a new regulation [23] with hefty fines to make the privacy assessment worthwhile for companies, so to speak.

First, it is required to understand how to define privacy and personal data and then to research the aspects and attributes of information privacy. The research on the theory of privacy and presented in section 2.2 on page 42 and information privacy risk presented in section 2.5.2 on page 58 is used as the background for this part of the research. Additionally, how the existing research or methods measure privacy was described in section 2.6 on page 59 is also applied here. These methods direct the research in a way that the resulting artifact can benefit from the positive aspects of existing solutions and aim to overcome the weaknesses detected in the existing solutions.

In addition to the research on existing systems, expert knowledge is applied to the *knowledge base* (c). The issues that were noted and things that were learned in previous projects (SGEM [57] and MobiServ [24]) are first-hand expert knowledge on the information-centric systems collecting information about users.

Value of the solution: The solution is of value if it (a) models information privacy in an understandable manner, (b) generates an understandable result for information privacy risk, (c) is usable in assessing different types of information-centric (eco-)systems or environments and (d) is useful for analysts responsible for private information risk management in enterprises. Furthermore, the resulting solution is to be used later as the theoretical background for a software tool that is capable of analyzing any system and the solution has to be research keeping this incentive in the process. (a) strongly suggests that a model would be of the most value, and since software is later built using the result of the research, it is reasonable to investigate whether the model can be based on an existing software modeling method, e.g., UML.

Research questions: This part of the research answers all the six research questions. This research will bring more in-depth knowledge to answer **RQ1** about the attributes of information privacy as they are the attributes that are used to establish the artifact. The resulting artifact itself acts as an answer to **RQ2** as the aim is to offer a way to assess the assets of the ecosystem under study. The artifact development involves many attributes that have to be connected somehow in order to produce the combined results of all the different values, which is an answer to **RSQ1.1**. Naturally, the resulting artifact is an answer to **RQ3,** and the development process introduces the answer to **RSQ3.1**. This part of the research involves a demonstration of the resulting artifact, the model, and gives some insight into **RSQ3.2** but it can be better answered by using the complete approach to assess the development process, in which multiple iterations of use are required. This description is an answer to DSR **Q1**.

8.2 A2: Objectives

The six research questions help to limit the objectives of the research. In the following, the requirements, foundations and objectives are detailed.

8.2.1 Requirements iteration 1

This is the first *relevance cycle* (*1*) iteration to go through the initial requirements for the artifact. This part details the scope, focus and goals, as well as highlights the objectives for the research.

The challenges inherent in quantification of the financial [53] or even the abstract [7] value of privacy mean many organizations might regard a privacy risk assessment as too expensive because of the costs of executing the process. Therefore, the model aspires to create a cost-effective and feasible method that is a usable and user-friendly way of assessing information privacy risks that enables the reutilization of the results (**objective 1**). However, owing to the fines the EU will set [23] for not even assessing the effect and the risk of operations to privacy (the lower limit, 2% or 1€ million of annual revenue), it can be said that the money spent on privacy assessment is not wasted.

From the evaluation and risk assessment viewpoint, information privacy can be seen through its loss. It is more reasonable to quantify information privacy through the attributes that cause the loss than through the ones that define it. The working definition of privacy loss contains the quantitative and qualitative nature of data and the people who have access to data. Quantitative data refers to the amount of data that is lost. Qualitative nature defines how significant the data is and what the data enables, including identifiability. The interests of unauthorized (e.g., attacker) and authorized users (e.g., insider attack) are to be included in the information privacy risk definition as additional parameters. They introduce elements of the security viewpoint into the definition through the evaluation of the likelihood of an attack or misuse. Additionally, the longer the data is available, the more likely it will interest potential attackers. Therefore, the time the data is stored is an important attribute in an information privacy risk assessment. In summary; (1) the resulting artifact must include and use qualitative and quantitative attributes mainly focusing on the potential loss of privacy (**objective 2**), and (2) the interests of the unauthorized user for possible misuse, which is affected by the storage times, have to be included in the artifact design (**objective 3**).

There are many emerging systems where the risks to privacy cannot be assessed with hard financial values. In these systems. the quality of the system operation is important for the user and the provider, the main emphasis being on the user. The damaging results of a successful attack do not necessarily affect the provider directly, but it is the user [145], whose private information is at stake. The maintainer, however, should be [77] and can be held responsible [22] if the protective measures are poor to begin with. In addition to the potential fines [23], companies can be affected by reputation loss in the eyes of potential customers. Fines can be easily dealt with (e.g., apply for a plead) but it is difficult to regain users' trust once it is lost. Therefore, in the model the quality of the service has to be included from the users' point of view, while keeping the companies in the background but still in the process (**objective 4**).

In the research, the main focus has to be on private information and the privacy requirements for such information (**objective 5**). In order to define the risk to privacy, the damage, or as defined in [120], injury, the attacker can cause to privacy and to the user has to be included (**objective 6**). The damaging effect of an attack or misuse plays a big part in defining the impact on privacy, but the probability of an attack (or misuse) and the benefits acquired by the attacker from the attack also have to be noted (**objective 7**). These, combined with the possibilities that the attacked asset opens up, lead to estimation of how probable an attack is.

The model is not aimed at analyzing single information systems, nor is it for users but for analysts conducting an assessment of a larger environment. Therefore, the model can be a useful tool, for example, in the PIA process in reducing analysts' workloads. Or the model can be utilized in the process of embedding PbD principles [9] in the design. The aim is not to be absolutely precise but indicative to reduce the resource consumption and to be an economically viable method by introducing a clear way to classify the assets (**objective 8**).

8.2.2 Foundations iteration 1

This is the first *rigor cycle* (*2*) iteration. The foundations were laid out earlier in the background research on privacy and information privacy, presented in section 2.5.2 on page 58. In addition, the details and insight the research on the existing risk assessment methods (in section 2.6 on page 59) gave are included. The following is a summary of the attributes found during the background research.

Summary of foundations: The attributes that define information privacy are the nature or the quality of the information, access to information or to the asset, the quantity of information, the storage time of the information, the likelihood of an attack, damage to the individual or to the asset, the identifiability of the information (linkability) and the purpose of use. These are the results of the first iteration on existing theories, systems and methods.

8.2.3 Foundations iteration 2

This is the second *rigor cycle* (*2*) iteration that continues directly after the first one summarizing the foundations from the background research. The purpose of this iteration is to map out and present details from the projects this research was involved in or in which the foundations were laid out. This brings the experience from the *knowledge base* (*c*) into the research process.

During the SGEM project it was noted that identifiability of consumption data plays a big role in privacy [45]. This can be also noted from the vast number of identity-hiding methods [32, 33, 36, 82, 72, 146], such as aggregation [34, 36, 83, 140]. Because of the potential the identified or identifiable consumption data has [12, 30, 31], the amount of consumption data stored in various assets poses a big risk to privacy, as does the access to these assets, which may open up access to the consumption data stored. In smart grids the storage times, often required by legislation, are long and are difficult to meet in terms of maintaining security, thus, the amount of data that is generated daily [80]. For example, in Finland the storage time of six years [79] puts a lot of pressure on the design of the storage system as the data encryption methods should withstand brute force attacks for the whole time period, unless the system is designed to be flexible enough that the data encryption can be changed from time to time. Therefore, the number of people who can access these assets withholding the information for long periods has a major effect on individuals' privacy in smart grids. Insider attacks may be most effective if the purpose is only to steal data for malicious purposes as such behavior has no direct effect on the functionality of the system. The only thing left behind is an entry in the access logs.

Moreover, the information transferred in smart grids has many different identifiability levels. It was most accurate when the data was retrieved from the smart meters, and the granularity was reduced after the electricity bill was calculated. The granularity of the consumption data was even further reduced when the data was passed to third parties for analysis. The aim of the attackers would naturally be assets that have the most accurate data, but as data mining methods have advanced [97, 98, 99, 101], attacks on information that is less granular might be of interest. This suggests that even if the collected information is now regarded as non-identifiable it might not be thus in the future. In information privacy, even the identifiable information should have a significance in defining the threat level.

In MobiServ, the number of different types of identifiable information is immense: video, audio, motion in various locations, health status with various instruments, appliance usage within the residence and nutrition data, which is an analysis of the resident's actions. This shows that the information collected about the user is gathered through various means and used for a wide range of purposes within the environment. The extent to which the information is collected certainly poses a major privacy risk since such information can help form a behavioral profile of the resident. Therefore, also in MobiServ, the various storage locations and the times they store the sensitive information posed a risk to an individual's privacy.

In order to gain the full benefits of PII 2.0 [20], a mapping of PII 2.0 categories to FIPs (OECD PPs) [77] is presented in Table 8.1. This table, among other issues, also introduces the issue how to deal with data that can be identified through data mining. These small steps toward a more exact definition of information privacy classification will someday result in definitive privacy legislation to protect people. But for now, this classification helps to define the information requirements for the model.

Table 8.1: Summary of requirements for information privacy

Category	PP1.	PP2.	PP3.	PP4.	PP5.	PP6.	PP7.	PP8.
Identified	x	x	x	x	x	x	x	x
Identifiable	x		x	x	x	x		
Non-identifiable			x					

These three categories, non-identifiable, identifiable and identified, and their connections to different PPs in Table 8.1 are justified as follows:

- The non-identifiable information has to fulfill only the relevance of use principle since information cannot be tied to an individual but should be used only for a specified purpose. Such information collection does not need to be exactly specified as it can be derived from various sources through aggregation and anonymization.
- Identifiable information does not need the individuals' consent for use, nor does the individual need to have access to it since the information is not tied to any particular individual, although, it can still be linked to an individual and, therefore, according to EU directives, is private information that the individual has the right to access. However, there has to be a *close link* between an object or an event and a person for information about the object or the event to fall under the private information jurisdiction [49].
- The identified information does, however, have to be used only for the specified purpose with clear collection specifications in addition to good protec-

tion since the information can be connected to an individual utilizing data from other sources (e.g., data mining). For this particular potential for the data, the quantity of information must also be limited. In addition, any infraction regarding identifiable data should be treated as an infraction of identified data, which has to fulfill all eight privacy principles.

Furthermore, as Figure C.1 on page 258 in Appendix C shows, there is a wide range of external users who access different parts of the system. This has a major impact on the privacy of the resident as the more people access the resources within the residence, the more the risk of human error is increased. For example, if the computer is unlocked while logged in into the nutrition data server and an unauthorized person can see (or even worse, access the information to manipulate the nutrition data), the status will impair the privacy of the resident. Unauthorized access to the asset itself may submit the resident to physical damage, e.g., by administering the wrong medication or turning off the lights just before the resident crosses a doorstep. Therefore, access to the assets may not just impair the resident's privacy; such access can be used to inflict physical damage on the resident and on the system.

Summary of foundations: These two cases introduce numerous attributes to be accounted for in assessing the risk to information privacy. The attributes found through background research were detected to be similar to those in these two cases (section 2.5.2 on page 58). The following list is a summary and generalization of the attributes affecting information privacy that were found from the background research and from the expertise gained from previous projects:

- Access to information
- Access to the asset withholding information
- Damage to the individual who can be identified with the information
- Damage to the reputation of an individual
- Damage to the asset or the system
- Identifiability of the information (according to PII 2.0 [20])
- Likelihood the asset withholding information is attacked
- Nature of the information or its significance to the user or to the system operation
- Misuse potential of the asset
- Quantity of information

- Quality of the information or what is the potential of misuse
- Purpose for which the information is used (this is excluded in the model, thus the definition of scope in EU regulation [23])
- Time the information is stored in the asset

The attributes for defining information privacy are, therefore, clear, but the mapping of them in order to produce a risk value is a question. An existing process of security risk assessment was considered promising in the MobiServ project. The experience gained by using the "root pattern of all enterprise concerns" [116] in the MobiServ risk analysis [43] brought up the need for a separate privacy risk analysis but also provided an insight into what kind of process the privacy risk analysis could be. The process that was described [116] was straightforward, but the details of how risk and all other affecting attributes were defined acted as a starting point for developing the artifact as a model. All attributes in [116] are defined with a qualitative scale from one to six shown in Table 8.2. This same qualitative scale was considered useful and is to be used during the development of the artifact throughout the whole process.

The dynamics presentation of the different attributes as a sequence, such as the

Table 8.2: Qualitative scale of attributes [116]

Value	Risk	Asset value	Likelihood	Vulnerability
6	Extreme	Vital asset for business and human health	The attack is bound to happen	Is a common, trivially exploited vulnerability
5	Very high	Asset is critical for business functions or for the human health.	The attack is very likely to happen	Is a fairly common, easily exploited vulnerability
4	High	Asset is highly valued	There exists a high risk of attack	Exploiting is a challenge but exists in many systems
3	Medium	Asset is of moderate value	There exists the risk of an attack	Is found only in a few systems and is difficult to exploit
2	Low	Asset is of minor financial value	An attack is not very likely	Is rare, offers no gain and is very difficult to exploit
1	Negligible	Asset is not significant for the enterprise	The attack will not happen	Can be exploited only in theory

"Sequence constraints of the asset valuation process" on page 106 [116], gave the idea that instead of describing a process the definition of each could be modeled utilizing connections between the attributes. Furthermore, the way the *risk* was calculated (Equation 8.1) supported this idea of establishing a model with specific connections between each attribute. In [116], *risk* comprises of the *asset value*, (*threat*) *likelihood* and *vulnerability:*

- *Asset value* is the quantitative value the asset has for the environment the asset resides in or to the organization to which it belongs to. An asset within the context of security assessment has multiple types: physical (e.g., building, vehicle), the type of information (e.g., employee data, research data), external business factor (e.g., laws, loans) or internal business factor (e.g., intellectual property, details of items of the business) [116]. In order to define the value of the asset, its type or role in the environment and security properties that are required to operate or access and the impact the asset has on the business of the context.
- *Likelihood* (or *threat*) comprises the frequency of an attack and the impact the attack has on the physical asset. In order to define *likelihood*, the events that could cause harm must be identified [116]. These events result in threats to the assets, and with a scale of the frequency of an attack, the *likelihood* value is established.
- *Vulnerability* is a combination of the frequency of attacks and the severity of the impact of a successful attack. It is a weakness in an asset, which may be exploited in order to affect the asset's security properties [116]. In order to define *vulnerability* the weaknesses within the context must be mapped out and then scaled with a vulnerability scale using the threat identification in the *likelihood* estimation.

Eventually, the *risk* is calculated from these three attributes with Equation 8.1 [116]:

$$Risk(asset) = \sum[Likelihood * Vulnerability] * Value(asset), \tag{8.1}$$

This is a valid starting point for artifact research because it (a) defines a risk as a value dependent on other attributes, (b) is qualitative with quantitative attributes, (c) offers a clear qualitative scale for attributes and (d) can be represented as a model. Furthermore, the familiar process properties can be modified to support the information privacy risk assessment.

This grounds the research in a wide range of concrete theories and details of existing systems, answering DSR **Q4**. The main contribution of this research is the artifact modeling information privacy in an understandable manner (answer to DSR **Q7**).

8.2.4 Requirements iteration 2

This is the second *relevance cycle* (*1*) iteration to more closely specify the requirements (R) as a continuum for the objectives defined in the first iteration. This part utilizes the knowledge obtained in the two *rigor cycle* (*2*) iterations from the *knowledge base* (*c*).

In general, privacy is a qualitative value. Losing one's privacy may result in reduced life quality, e.g., in the case of an identity theft, especially if creditworthiness is lost as a corollary. Additionally, the attributes indicate that the qualitative approach is suitable for assessing information privacy risk. Many of the attributes describe a qualitative measure, but there are some, such as the quantity of information, that are clearly quantitative. Whereas the approach is qualitative, it should also take into account quantitative attributes. The existing methods [53, 118] also use qualitative scales and measures.

The focus in this research is on the private information used in and collected by large systems, such as the emerging systems used to enhance life or service quality or energy efficiency. In these systems, the risk is not mainly the amount of information or to whom it belongs. The factors affecting user privacy in such systems can be regarded as user identification, information that is linkable to an identity, the number of information, access control, the amount of people or assets that have access to the information and the length of time the information is stored [45]. The user identification can contain more than just an identification number used in the database operations. It can be a full information package about the user: birth date, address and mobile phone number, to name a few. Some of the data can be given by the user (e.g., billing information for some constantly used service), and the rest can be gathered from the actions of the user.

In economic analyses conducted using personal data, the subject is aware that private information is collected and used by the service [18], but in modern systems, the use of the information might be ambiguous for the end-user. In these systems, there are usually multiple parties that either require or get access with users' consent to the data. This approach can increase the transparency of the company's operations, for instance, but the traditional "notice and choice" in getting the consent is said to have outlived its usefulness [37]. The data itself can be distributed and even duplicated in the different information systems comprising the environment. Duplicates of any personal data bring challenges with the manageability of data and can increase the risk of personal data disclosure [147].

The six privacy risks described in the PIAF [52] mostly concentrate on the identifiability of the individual, but the actual problem is the connection of even seemingly peripheral information and other information about an individual [8]. The different services can anonymize or aggregate the collected or gathered information and state that not all of it is private. This can be concluded from the PII 2.0 classification [20] and from the mapping of information privacy requirements to PII 2.0

in Table 8.1. How to draw a line between identified and identifiable information regarding privacy and ownership? Should the aggregated information be treated as private information, or is it only a block of bytes that in its current form cannot be linked to an individual? Companies might be willing to claim ownership and full control over such data, but still, if information is linkable to an individual, it falls under the jurisdiction of the EU legislation, but only if there is a *close link* between the identifiable information and the individual [49]. Therefore, the private information classification of identifiable information from a legislative stance is still ambiguous. There should be a definition of what is a *close link* and can the derived link, for example, with data mining be held as such. In light of current legislation, identifiable information cannot always be regarded as private information.

With identified and identifiable information, the potential (of misuse) and significance (to the individual) of information has a big impact on information privacy risk. The potential defines the level of usefulness of the information not only for an unauthorized user but also for a legitimate user misusing the information. The information significance (or the nature of the information) partially defines the privacy level of the information. The bigger effect the information has on the individual, the more private it is. The information can be a detailed personal background, as well as login credentials or just a scripture from an unfinished blog entry.

Access to data, both identified and identifiable data, is a broad aspect that must be accounted for when measuring privacy. Access control itself is not enough to restrict the usage of the data. The number of people or devices that can access that data has a major effect on privacy. Poorly protected access without sufficient restrictions of use opens up ways for attackers, or even personnel, to misuse the information. Access can be defined from two viewpoints. First, the access to the assets (devices) can be external, internal or completely public. And second, access to the data itself can be limited by access control or some other restrictive measures, such as the network used. Access control methods are regarded as security attributes and are not dealt with in detail in this study.

The attributes of information privacy that this study presents correspond to the goals of a privacy risk assessment [148] but do not directly follow the OECD [77] and EU DPD [23, 48] requirements of fair information practices. The reason is that here the focus is on information privacy, whereas OECD and EU DPD are about data protection. Therefore, the model does not take a stance on the purpose of the use of data as the model is related to data protection.

The OECD privacy principles [77] in a way aim to reduce the amount of information in information systems and recommend keeping only what is relevant. The goals here are similar in the sense that by detecting redundant usage of private information the amount can be reduced. This can be achieved by abstracting the environment into basic tasks in order to gain a deeper understanding of the relations between the assets and the information handling, including redundant usage [45], which helps when conducting an analysis with the model.

This discussion of the requirements results in a set of more specific requirements for the model. In the following sections, these requirements are summarized, and the requirements are used as the evaluation criteria later in the process of model development.

8.2.5 A summary of the requirements

The legislative perspective, scope, focus, goal of the model and the requirements sum up to a set of constraints and more specific requirements for the model, which are summarized in Tables 8.3 and 8.4. In the same tables, the effects of each requirement on the model design are detailed. Each requirement is labeled with an identification number, which is later used when referring to the requirements in the model evaluation section, where the implementation of each requirement is explained.

Table 8.3: Summary of the limitations and effects of each requirement on the model design and, requirements 1–6 (1 of 2)

Constraint	ID and Requirement
Legislation regarding information privacy is bound to change.	R1: The model must account for the current definition of information privacy and be able to adapt to possible future changes.
Private information and derived data exist in multiple forms.	R2: The model has to take account the various types of personal data used in different systems. Different data has different significance to the individual.
In large systems, there are multiple parties that have access to different assets.	R3: The model has to take into account the different parties and people who can access the assets. The misuse potential of each asset has to be included which is affected by the damage and the value of data.
In large systems, there are multiple parties that can access the data.	R4: The model has to take into account the different parties and people who access the data. Different parties and people have different access levels to the data.
Data can be from various sources, and the nature of it can vary.	R5: The model has to take into account the different capabilities and potential of the data. The capability and potential of the data have to be evaluated from the privacy point of view: What harm can be done with it.
Not all data is private. The identifiability level defines the legal compliance of the data.	R6: The model has to include a way to define the identifiability level of the data in order to able to define whether the information is considered private in the jurisdiction.

Table 8.4: Summary of the limitations and effects of each requirement on the model design, requirements 7–17 (2 of 2)

Constraint	ID and Requirement
Data can be valued from different viewpoints in different scenarios.	R7: The model has to be able to value the data based on the scenario requirements for the data. The value of the data is determined by its significance and access.
Data storage times differ between different systems and their assets.	R8: The model has to take into account the storage times for the data on an asset basis.
Different systems require and store different amounts of data.	R9: The model has to take into account the quantity of the data an asset withholds or requires in its operation.
Access to the assets can vary (external, internal, public).	R10: The model has to take into account the different access methods that are offered to the assets. The access type has an effect on the probability of an attack.
There are different types of assets in different systems.	R11: The model has to be able to differentiate the assets based on the asset functionality. The role of an asset is used for defining the value of the asset.
The damage an attack can cause to an individual can vary.	R12: The model has to take into account the varying levels and types of damage an attack causes to individuals' privacy.
Attack can benefit the attacker in different ways.	R13: Attackers benefit has to be able to be assessed with the model. With information-containing systems, the gain from a successful attack depends on the value of the data, which has to account for the significance of the data to the individual and the amount of data that the attacker can get.
All attacks are not of the same probability. Different ways exist to attack an asset.	R14: The model has to assess attacks based on the attack characteristics and attack paths. The attack path is largely defined by the access medium to the asset.
If a system containing personal data is breached by an attacker, the privacy of an individual is at stake.	R15: The model has to assess the information privacy regarding the individual whose information is kept. The model has to take into account the importance of the quality of the system operation for the individual.
There can be overlapping usage of personal data between assets.	R16: The model has to note the possible duplicate data or offer means for detecting redundancies in personal data usage.
Loss of reputation privacy is harmful for the individual.	R17: The model has to account for the possibility of losing reputation through the disclosure of information.

8.3 A3: Design and develop

The constraints and requirements presented earlier specifically define the limitations of the research and the resulting artifact. Here, the artifact is designed in multiple iterations by first starting from the definition of the artifact, its evaluation criteria and the process of conducting the research. On each iteration, the artifact and its related concepts are refined, resulting in a prototype of the *assessment model* ready for evaluation.

8.3.1 Iteration 1

In the first iteration of the *design cycle* (*3*), the scope of the artifact is detailed. This iteration combines the requirements researched in the *relevance cycle* (*1*) and the grounding researched in the *rigor cycle* (*2*) to define the basis for the artifact development in terms of the artifact type, the process used and the evaluation that is done for the artifact.

As a design decision, a qualitative model is being devised in this research as an artifact, thus, the number of attributes and the need to create an easy-to-use method. The model can encompass qualitative and quantitative attributes but the assessment is done on a qualitative basis. This is because the method, the risk assessment method titled a “root pattern for all enterprise concerns” described in [116], was chosen for use as the basis, and many characteristics are drawn from it. In addition, the same method was used to conduct the MobiServ risk analysis [43], in which the need for a separate privacy assessment was detected, and the method at that time was considered suitable for designing a privacy assessment on the same grounds.

The artifact: The artifact that is devised in this research is a modeling of information privacy risk from a qualitative viewpoint using qualitative and quantitative attributes on the asset level encompassing the requirements of the (European) legislation. The artifact is aimed for the needs of qualitative assessment procedures to act as a second part of the mid-level tool described in this thesis. This research produces an artifact in the form of **an *assessment model* for information privacy** (answer to DSR **Q2**).

Process for research: The grounds for this research are the vast amount of literature on privacy and the hands-on experience that was gained in the projects. It is necessary to have multiple iterations in the development of the model. Therefore, the prototyping approach is selected as a process for research (the answer to DSR **Q3**). It allows to try different combinations and connections in the attempt to model information privacy. In this way, the details from the *knowledge base* (*c*) can be refined and compared to the development steps of the model and the results it generates, thus, making the model more accurate in modeling information privacy.

Evaluation: Here, the evaluation checklist focuses on the correctness of the resulting artifact, the model (the answer to DSR **Q5**). The following issues must be verified from the model design:

1. Are all attributes that are included necessary?
2. Does the model emphasize the correct attributes?
3. Are all requirements met in the design?
4. How does the model overcome the three downsides of risk assessment: (1) the results might not be reusable [116], (2) the results are subjective [120] or (3) speculative [126]?
5. Is the resulting artifact, the model, usable in any information-centric environment or (eco-)system?
6. Does the model generate understandable results?

8.3.2 Iteration 2

The summary of the foundations, objectives and requirements laid out in the second activity during the artifact specification and the process of development presented in the first design iteration drew the outlines for specifying the artifact. In this second *design cycle* (3) iteration, the detailed specification for the artifact and the attributes from which it is formed are laid out. This is a result of combining the requirements from the *relevance cycle* (*1*) and the foundations from the *knowledge base* (*2*).

The first research prototype was developed to display the outlines in the form of a model portraying the initial assumption of various connections between the different attributes of information privacy. The initial idea was to utilize the definition of risk in the "root pattern for all enterprise concerns" [116] for defining information privacy risk as the basis in order to establish a model of all attributes. However, first, it was important to find out how these three attributes are defined with the attributes described as the foundations for information privacy.

From vulnerability to impact: In the context of information privacy, *vulnerability* is not seen an attribute as it traditionally describes a weakness in something, usually a system of some sort that is bound to be exploited. Instead, in the context of information privacy the individual can be regarded as corresponding to the system, and it is the individuals' privacy that can be exploited, harmed or directly damaged. Therefore, it is more reasonable to call this attribute in the context of information privacy as an *impact on privacy* instead of *vulnerability*. But what *impact* could an attack have on privacy? *Vulnerability* defines a weakness that causes damage to the business operation. In the context of information privacy, the damage is an impact on integrity of an individual. It may be a direct impact on the reputation, or the damage comes from enabling identity theft causing more harm to the individual if the attacker, for example, can utilize the identity to apply for loans or purchase goods.

Defining damage: The damage to the individual's privacy is a big factor, but the damage must be declared in a much wider manner in information privacy. This is because in MobiServ [43] it was possible to physically harm the person or the environment by gaining unauthorized access to the systems. Direct physical harm may be only a side effect of the workings of an attacker but is still a possibility. Therefore, in the damage definition more than the damage to reputation or integrity must be included. It would be reasonable to define damage through all possible damage that can be caused to all the elements; the individual, the information and the system withholding the information.

Defining impact: Additionally, as the *vulnerability* concerned a system weakness, and, although it was previously defined that the individual may be regarded as corresponding to the system, it seems more reasonable to include the asset withholding the information in the *impact* definition. This is because the asset is the one that opens up access to the sensitive information about an individual or to the information belonging to the individual and also because the researched artifact, the model, is intended to be used for analyzing information systems on an asset basis. Therefore, an individual cannot be included directly in the model. The value of the asset that is assessed is better suited as it introduces the impact of information disclosure into the assessment through the *impact on privacy*. This goes in a different direction from the previous risk definition in [116], but as the scope is changed from security to privacy, the grounds are also different. This way of assessing the *impact* or *vulnerability* still includes all the attributes but in a different way attempting to overcome the challenges inherent in assessing information privacy.

Valuing an asset: *Asset value* in information privacy is largely defined by the information the asset holds. However, it is not only the data but also the different aspects related to it. The amount of data and the length of time the data is stored in the asset have an effect on the value of the asset. The more data the asset holds, the bigger its value is for the system. If the data is personal data, it is of more value to the individual whose data it is. The longer that particular data is kept, the bigger the risk to the asset will be, and the value of the asset must also be higher. Additionally, in [118] the potential of the information is used in defining how exploitable the data is for the potential attacker. In addition to these attributes (quantity, time and the potential of the data) the properties and capabilities of the asset have to be accounted for in the value estimation. The misuse potential of the asset;, what type of access the asset can offer the attacker either to the data or to the system, is an attribute for estimating the properties of the asset from the attacker's perspective. Similarly, from the system perspective, the properties of the asset can be included through the role the asset has in the system. Furthermore, access to the asset itself must be included as an attribute because it can be used to estimate the publicity level of the asset in the network in which it resides. The more public the access is, the bigger the risk, and thus, the bigger potential for attacks.

Defining likelihood: The third attribute that defined security risk, the *likelihood* of an attack, is suitable for use in an information privacy assessment. It is used to describe the probability of an attack in both contexts. Here, in the context of information privacy the *asset value* is not seen as an attribute that directly affects *likelihood*, but some attributes that define *asset value* expand the valuation by including the necessary aspects of the asset. The potential of asset misuse introduced earlier is an apt attribute that introduce the damage that may be done with the particular asset and is usable in *likelihood* estimation. In addition, the gain of an attack for the attacker is a separate attribute that is to be included in the estimate. *Attack gain* is the estimation of what and how big the attackers' benefits are if the attack succeeds. The benefits may include the information, the quantity and the nature of the information withheld by the asset, but other incentives may tempt the attacker. It may be the personal satisfaction that the systems can be penetrated or modified that interests the attacker. To support **RSQ3.2** all possible characteristics must be incorporated in the assessment, and both aspects of *attack gain* are to be included as there are systems capable of harming the individual in many ways (e.g., MobiServ [24]). In addition to *misuse potential* and *attack gain*, which define the threat, the frequency of an attack needs to be included in the *likelihood* estimation as it was used in [116]. The frequency of attacks on an asset needs to be estimated by utilizing the probability of an attack, which is affected by the network the asset is in and the route by which the asset can be attacked. If the asset is in a completely private network, then the probability of an attack is low as it cannot be attacked from outside, whereas with the Internet, for example, this is completely different, and the probability of an attack is very high.

Valuing information: The value of the data the asset contains has a big impact on the risk value of the asset. The asset itself is of a different value and has properties defining the access to the asset. Access to data has to be separately defined because the access limitations of an asset include the network and the paths by which it can be accessed, but the limitations on data access in an information system are different. *Data access* is used to define the number of people who can access the data withheld by the asset, and this is used in valuing the data. The more people who can access the data, the bigger impact it should have on the *data value* and to the information privacy risk. The probability of unauthorized use rises as the number of people who have access to the data increases. In addition to *data access,* the nature of the data has a major impact on the *data value*. The significance of the data defines the level of importance for the individual or system operation. The *data significance* does not define the privacy level of the data but the nature of the data, what type of data it is and how important it is for the individual and for daily, regular operation of the system. If the data is important only for the system operation, then the data may not be important for the individual. However, it may indirectly affect the individual if it is the calibration data of a device of some sort that is used for measuring something closely related to the individual. The quantity of data does not affect the *data value* itself but affects the *asset value* because the more data the asset has the more valuable it is within the system, but the amount of valuable data does not have an increasing effect on the value. The more valuable the data is, the more the effect on the *attack gain* increases because then the attacker would benefit more from the data or could do more harm with the more valuable data.

Defining information privacy risk: In a security risk assessment [116], the value of the asset was also directly included in the calculation and the different specific vulnerabilities were combined with the likelihoods of an attack to establish a risk value. In this research, the goal is to establish an artifact, a model of information privacy and the specific threats including their likelihood of occurring have to be generalized. Therefore, by accompanying parts of the asset attributes, the information privacy risk is defined mainly through the *impact on privacy* and the *likelihood*, which are defined through other attributes that affect information privacy.

Connections between attributes: The attributes used for calculating information privacy risk are defined through various other attributes. By attempting to generalize all aspects of information privacy, it seems obvious that there is more than one type of connection between the attributes. *Information privacy risk* can be calculated from the two attributes as an average of the values. This calculation would also suit other attributes, for example, in the *asset value* calculation as it has a total of five attributes that affect the value directly: *asset role*, *asset network*, *data capabilities*, *data storage time* and *data quantity*. However, some attributes do not have an direct impact on other attributes. For example, the network the asset is in has a direct effect on the *asset value* but also affects the value of the attack frequency or how probable the *attack actualization* is. The impact on *attack actualization* is not seen as direct as both can be considered attributes that have to be estimated first. Therefore, another connection type is needed in the model of information privacy: indirect. The use of UML for developing the model then suits well since it contains two distinct types of connections between the classes: composition (direct, because a class is composed of other classes) and dependency (indirect, because the other class does not directly belong to the dependent class but affects it).

Iterative model: This connectivity expands the possibilities of the resulting model allowing to do it as a self-balancing model. Self-balancing here means that certain rules are to be devised between the indirect connections, which define how the values are changed. If there are changes in even one value that has dependencies, all the others have to be valued again according to the rules. This creates iterations within the model, which stops when there are no changes. However, in order to achieve this, there has to be a certain order in which the values of certain attributes are changed. This is important as many of the attributes have to be assessed by the analyst doing the assessment. Some attributes can be dependent on the values that are calculated only from the values of other attributes. This suggests that there will be two types of attributes: assessable and calculable.

Two types of attributes: The calculable attributes are calculated from the values of all directly affecting attributes as an average. Assessable attributes have an initial estimate from the analyst. This suggests that specific scales are to be devised for each attribute.

Scaling of attributes: Similar qualitative scaling, presented in Table 8.2 on page 163, was chosen for use in the model for valuing the attributes. The scaling is required to be constructed for each attribute that is to be defined by the analyst. This is part of the later iterations but also affects the research from the beginning. In order to be usable without an extensive, amount of expert knowledge, the model should not have too many attributes that require manual assessment. Therefore, in this research it is worthy to investigate how the number of manually assessed attributes can be reduced in the model.

8.3.3 Iteration 3

In the third iteration of the *design cycle* (3), the first version of the artifact (which is the first model prototype) is developed using the outlines and the detailed specification of the previous iteration. The previously detailed definitions of information privacy, foundations and requirements for this research and the attribute definitions and their connections result in the first prototype of a model for information privacy assessment. The first prototype is shown as Figure 8.1 that has the assessable attributes in yellow and the calculable attributes in blue.

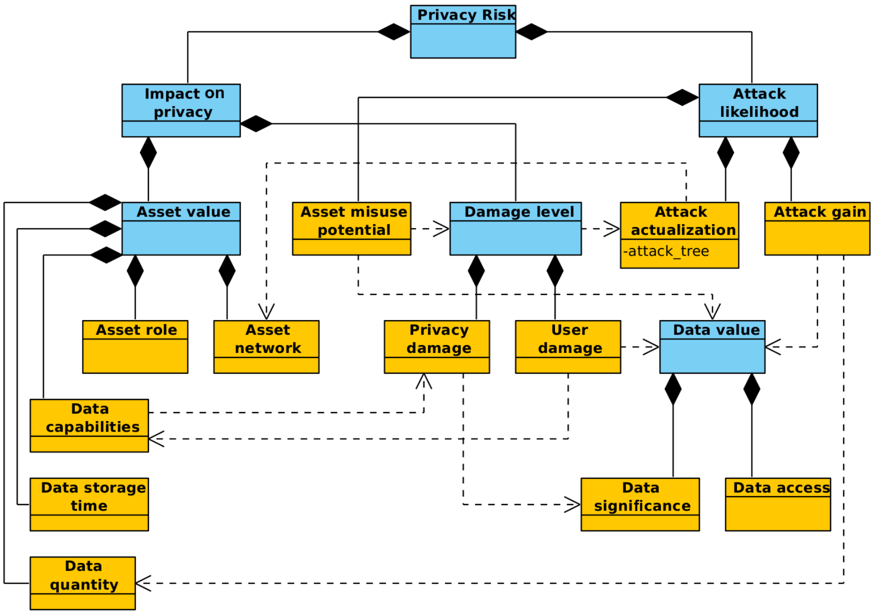


Figure 8.1: First prototype of a model for information privacy risk assessment

The attributes in the model (Figure 8.1) and their short descriptions are as follows (in alphabetical order):

- Asset misuse potential: The measure of the possibilities this asset opens up for an attacker.
- Asset network: The network type the asset is in that defines the basic level of asset protection from unauthorized users.
- Asset role: The role of the asset within the environment, measures the significance of the asset to the user and the system.
- Asset value: The calculable value of the asset formed of its composites.
- Attack actualization: The measure of probability and the frequency of an attack.
- Attack gain: The measure of the attacker's benefits in the case of a successful attack.
- Attack likelihood: The calculable value of the likelihood of an attack.
- Damage level: The calculable value of the damage that a successful attack can cause to the user and the user's privacy.
- Data access: The number of people who have access to the data.

- Data capabilities: The measure of the potential of the data for an attacker; how useful the data can be.
- Data quantity: The measure of the amount of data withheld by the asset.
- Data significance: The measure of the nature of the data. Defines the significance of the data for the user and system operation.
- Data storage time: The definition of the data storage time.
- Data value: The calculable value of the data formed of its composites.
- Impact on privacy: The calculable value of how big an impact a successful attack has on the user's privacy.
- Privacy damage: The measure of the extent of the potential impairment of individuals' integrity and reputation in case of an attack.
- Privacy risk: The result of the model on the scale similar to Table 8.2 on page 163.
- User damage: The measure of how an attack can degrade the life quality of the user and the effect on individual autonomy.

The connections in the figure are as they are used in UML and were derived from the research on foundations and iterating through requirements and from the two iterations of *design cycle* (*3*). Both two types of connections mentioned earlier are used in the model.

- Composition means that the value for an attribute is calculated from the composites. For example, the *attack likelihood* is calculated from the values of *asset misuse potential*, *attack actualization* and *attack gain*. If the values are 4, 5 and 6, the value for *attack likelihood* is 5.
- Dependency means that the attribute is dependent on the value of another attribute or values of multiple other attributes. For example, *attack gain* is affected by the values of the *data quantity* and the *data value*. These values were calculated with the dependencies presented in Table 8.5.

In this version, there are a total of 18 attributes. Six are calculable, and the remaining 12 are assessable. The scales for the attributes in yellow, the assessable types, are presented in Tables 8.6, 8.7 and 8.8. The number of attributes is one less than the ones that were summarized in the second iteration of the foundations. This is because excluding the purpose of use is more of a data protection attribute, which was previously discussed in the second requirements iteration on page 165. All other attributes are included in the model. However, the identifiability of the information is missing from the model and is included through *data capabilities*. This has to be included in the further development iterations as a separate attribute.

Table 8.5: Dependency calculations in the first model prototype

Client (C)	Supplier (S)	S_{value}	C_{value}
Asset misuse potential	Damage level	[5,6]	if $\mathit{diff}(S_{value},C_{value}) > 1$ then $C_{value} = S_{value} - 1$
		[2,4]	if $C_{value} > S_{value} + 1$ then C_{value} -= 1 else if $C_{value} < (S_{value} - 1)$ then C_{value} += 1
		1	if $C_{value} > S_{value}$ then C_{value} += 1
	Data value	[4,6]	if $C_{value} < S_{value}$ then C_{value} += 1
		[1,3]	if $C_{value} > S_{value}$ then C_{value} -= 1
Attack actualization	Asset network	[5,6]	if $C_{value} < 4$ then $C_{value} = 4$ else if $C_{value} < S_{value} - 1$ then C_{value} += 1
		[3,4]	if $C_{value} < 2$ then C_{value} += 1 else if $C_{value} > 5$ then C_{value} -= 1
		[1,2]	if $C_{value} > 3$ then $C_{value} = 3$
Attack gain	Data value	[4,6]	if $C_{value} < 3$ then C_{value} += 2 else if $C_{value} < S_{value}$ then C_{value} += 1
		[2,3]	if $C_{value} > 3$ then C_{value} -= 1
		1	if $C_{value} == 6$ then C_{value} -= 2 else if $C_{value} > 1$ then C_{value} -= 1
	Data quantity	[5,6]	if $C_{value} < 3$ then C_{value} += $S_{value} / 2$
		[3,4]	if $\mathit{diff}(S_{value},C_{value}) > 1$ then if $C_{value} < S_{value} - 1$ C_{value} += 1 else if $C_{value} > S_{value} + 1$ C_{value} -= 1
		[1,2]	if $C_{value} == 6$ then C_{value} -= 1
Damage level	Attack actualization	[4,6]	if $C_{value} < 2$ then C_{value} += $S_{value} / 2$ else if $C_{value} < 4$ then C_{value} += $S_{value} - 3$
		[1,3]	if $C_{value} == 6$ then C_{value} -= 1
Data capabilities	Privacy damage	[4,6]	if $C_{value} < 3$ then C_{value} += $S_{value} / 2$
		[2,3]	if $C_{value} > 4$ then C_{value} -= $\mathit{diff}(S_{value},C_{value}) - 1$
		1	if $C_{value} > 4$ then C_{value} -= 2
Privacy damage	Data significance	[4,6]	if $C_{value} < 3$ then C_{value} += $S_{value} / 2$ else if diff(C_{value},S_{value}) > 1 then C_{value} += 1
		[1,3]	if $C_{value} < S_{value}$ then C_{value} -= 1
User damage	Data value	[4,6]	if $C_{value} < 4$ then C_{value} += 1
		[1,3]	if $C_{value} > S_{value}$ then C_{value} -= 1
	Data capabilities	[5,6]	if $C_{value} < 3$ then C_{value} += $S_{value} / 2$ else if $C_{value} = 3$ then C_{value} += 1
		[3,4]	if $C_{value} < 2$ then C_{value} += 1 else if $C_{value} > 5$ then C_{value} -= 1
		[1,2]	if $C_{value} > 4$ then $C_{value} = 4$

Table 8.6: Scales for assessable attributes in the first model prototype, 1 of 3

Attribute	1	2	3	4	5	6
Asset misuse potential	The asset capabilities do not interest attackers.	Mildly interesting asset that has potential for user annoyance.	Mildly interesting asset that opens up ways for user harassment.	Interesting asset that can be used directly for small privacy violations.	Interesting asset that can be used directly for major privacy violations.	Asset can be used to do permanent harm to user privacy.
Asset network	No network access.	Private network with no external access to asset.	Private network with restricted external access.	Protected private network with external restricted access.	Public network with access restrictions.	Public network without access restrictions.
Asset role	Not important at all.	An extra appliance that gives some practical benefits.	Everyday usage appliance, but user can live without it.	Important but not vital asset. Some maintenance gaps are tolerated.	Almost vital, asset. Short maintenance gaps are tolerated.	Vital for the user.
Attack actualization	Attack is unlikely because the breach requires huge efforts.	Breach requires enormous effort, and attacks happen very rarely.	Asset is protected but because of the contained data attacks can happen infrequently.	Attack requires knowledge, and with reasonable efforts, an attack can be successful.	Asset has some vulnerabilities that are known and are tried often.	Asset is either open or very vulnerable, and attacks will happen.
Attack gain	Small or nonexistent reward regardless of the effort.	A notable reward with enormous effort.	A notable reward with fair amount of effort.	Maximum benefit with enormous effort.	Maximum benefit but requires fair amount of effort.	Maximum benefit with minimal effort.

Table 8.7: Scales for assessable attributes in the first model prototype, 2 of 3

Attribute	1	2	3	4	5	6
Data access	Only user can access the data.	Accessible to only a few persons with access control.	Accessible to only a handful of persons with access control.	Accessible by a large number of persons with access control.	Data is publicly shared with access restrictions.	Open access to shared data.
Data capabilities	No data or data of no interest.	Leaked data has meaning only inside the system.	Leak would increase curiosity but is no real threat.	Large amounts of data would threaten privacy.	Privacy is violated with leaked data if it is not properly anonymized.	Data can be used to permanently affect (decrease) user privacy.
Data quantity	No data.	Contains a copy of the transferred data (router).	Small amounts of personal data are kept at any time.	Contains personal information that the user can wipe out securely.	Contains lots of personal information (e.g., home computer).	Contains all user-related private information (database).
Data significance	Not significant, necessary for user or required in any operation. Leak has no impact.	The data has a small role in the user's life, and a leak causes only annoyance. In these systems, such data has to be recreated, and a leak causes some offline time.	Data is useful for the user, and a leak of large quantities of data can cause privacy issues. In these systems, such data has to be replaced, and maintenance is required.	Data is important for the user and is needed in system operations. Leak causes temporary harm to privacy or opens up access to the asset.	Data is important for the user and is needed in system operations. Leak causes harm to privacy or opens up parts of the system to the attacker.	Data is either vitally necessary for the user or crucial for the system operation. Leak causes severe privacy infractions or opens access to system.

Table 8.8: Scales for assessable attributes in the first model prototype, 3 of 3

Attribute	1	2	3	4	5	6
Data storage time	Does not store anything.	Stores for the time the data is being transferred.	Short-term storage (wiped out or overwritten now and then)	Medium-term storage (relatively short period of time).	Long-term storage (stored for a long period of time).	Permanent storage (data is kept for an indefinite period of time).
Privacy damage (loss)	No effect on privacy. No data leak/loss possibility.	No real effect on privacy. Minor personal data is lost.	User privacy or personal data is threatened.	User privacy and personal data are threatened.	User privacy is lost, and/or personal data is lost.	User loses privacy completely. Private data is lost.
User damage	No damage is possible.	No real damage is possible, at least not directly.	Can inflict damage in the long term if other assets depend on it.	In the long, term the damage keeps increasing.	Health is endangered if there is a emergency.	Health of the user would be in imminent danger.

With the designed scales and the dependencies, the model was first tested for the applicability of the dependency calculation. The initial version of the *software prototype* was developed to evaluate this. All possible state combinations were created, and the results were to be calculated, but the dependencies were problematic from the beginning. Because of the iterative approach used in the model to find a balance in the values in which there would be no changes, the calculations got into an never-ending loop (for this reason, the *software prototype* still contains a cut-off at 1,000 iterations). A handful of values kept changing continuously on every iteration; thus, a balance could not be found. It is irrelevant which dependencies caused this because the dependency calculation system of this first model prototype was deemed to be unsuitable for the need. The calculations can be stopped in the software by setting a maximum limit for the iterations, but a better way to calculate the dependencies was chosen to be searched. Furthermore, the dependencies shown in Table 8.5 were also hard to read and understand. Both reasons drove the research into finding a new, more definitive dependency calculation approach for the model.

This first version included almost all the attributes, but the connections between them were also a question. Another question arose: Are all the connections correct and necessary? Additionally, it seems that some attributes, such as *damage level*, are defined in two ways. The devised scales also need polishing in terms of readability, and ambiguous definitions must be removed, but this is not the core issue in this research. At this early stage of the research, it was more important to develop a better model than to adjust the definitions of the input value scales.

Therefore, in the next prototype of the model, the following issues must be researched:

1. A new dependency calculation system must be created.
2. The connections between the attributes need to be revised.
3. The multiplicity of attribute types needs to be assessed.

8.3.4 Iteration 4

This *design cycle* (*3*) iteration creates the second version of the artifact (the second prototype of the model) as a continuum for the first version. In this version, presented as Figure 8.2, the three issues found in the first version are researched to solve them. This version includes major changes compared to the first version. There are now three types of attributes on three separate levels, and the connections between the attributes have been revised. Although the layout is different from the first prototype version, the connections were not revised in this iteration as other big changes were made, including the process of calculating the attributes. This answers DSR **Q5** on design improvements.

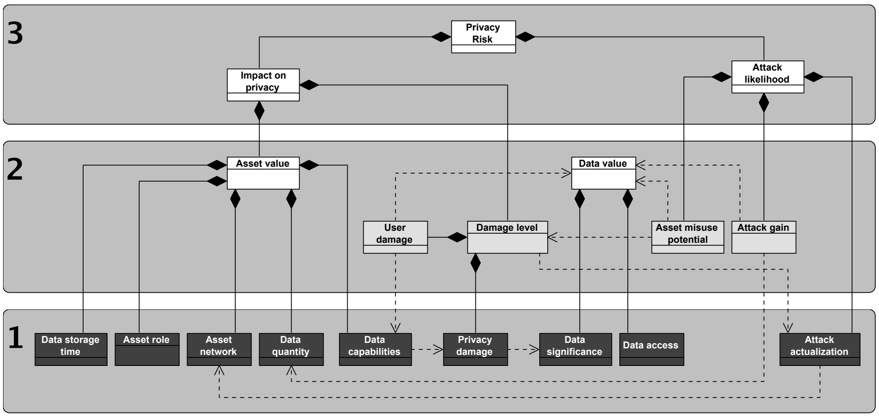


Figure 8.2: Second prototype of a model for information privacy risk assessment

It was clearly evident from the first version, that there will be more than two types of attributes. In this second version three types were seen to be appropriate. In addition to calculable (the attributes in white) and assessable (the dark gray attributes), a third one falls in between these two: definable (the light gray attributes). The definable attributes (*user damage, damage level, asset misuse potential* and *attack gain*) are not to be assessed by the analyst but are calculated from the values of other attributes indirectly using dependencies. Or in the case of the *damage level,* the value is defined by utilizing both direct (composition) and indirect (dependency) connections. Therefore, the *damage level* is called a hybrid attribute.

There is one main logical reason behind changing these four types into new definable type attributes. In the first version (shown in Figure 8.1 on page 175), it is clearly seen that these four attributes are highlighted: Each has two dependencies. This means that previously the initial given value is changed twice, resulting in many unnecessary changes without ever reaching a balance as it was a problem in the first version. It is also hard to define which dependency has a bigger effect (which of these two is dependencies is used first). This issue can be solved by introducing a third attribute type for such attributes.

Therefore, the values for these four attributes (*user damage, damage level, asset misuse potential* and *attack gain*) come from the results of the initial values of other attributes and their dependency calculations. This also brought up one benefit as some attributes, which previously were assessable, are now definable and thus, no longer needed to be manually assessed reducing the number of assessable attributes. This is a major development step in the model research. By reducing the number of assessable attributes from 12 to 9, the model is more user friendly and can be used with much less effort.

To calculate the values for the new attribute types, as well as the rest, a new way to calculate the dependencies was needed. It was not seen to be reasonable to change the calculation of the direct connections (compositions) as each with the current system utilizing averages each value (composite) has an equal weight for the value of the attribute in question, because the previous method of calculating the values of the dependent attributes was not clear or sound and had a multitude of problems during testing. Therefore, a more specific dependency calculation was selected that will also result in fewer iterations with the model. The new way to calculate the dependencies is a matrix-based approach. The values for each dependency matrix were analyzed separately estimating the effect of both affecting values on the resulting value using the foundations from the *rigor cycle* (*2*), the previous dependency calculation scheme of the previous *design cycle* (*3*) iteration and the scales laid out in that previous iteration (Tables 8.6, 8.7 and 8.8). As a result of this analysis, the matrices, such as Table 8.9, were devised for each dependency. The other dependency matrices, including the shown *asset misuse potential* matrix, are detailed in Appendix H on page 311.

Table 8.9: Asset misuse potential adjustment matrix

Damage level Data value	**1**	**2**	**3**	**4**	**5**	**6**
6	2	4	5	5	6	6
5	1	**3**	4	5	5	6
4	1	3	3	4	5	6
3	1	2	3	4	4	5
2	1	2	2	3	4	4
1	1	1	1	1	1	2

These matrices are used by inputting the values of the attributes on which the resulting value depends. The value of the attribute in question is determined by using the values of the two attributes inside the parentheses as (column, row). For example, the value of the *asset misuse potential* is defined by the values of the *damage level* and the *data value* using Equation 8.9, where the value of the *damage level* defines the column and the *data value* defines the row. With values of 2 for the *damage level* and 5 for the *data value*, the value of the *asset misuse potential* would be then set to 3 (the bold number in Equation 8.9). This dependency calculation scheme is more straightforward and clear to use. It is also much more easier to implement in the *software prototype* and reduces the numbers of iterations as now there are distinct rules about what value combination creates a change.

By analyzing the new dependency calculation scheme, the values for the matrices, it was noted that the scales for the initial estimates of the attributes needed more work. It was evident that the assessable attributes can be divided into different classes based on their focus. This resulted in a classification that divided the scales into two separate groups: asset- and data-related attributes. The data-related attributes are presented in Table 8.10, and the asset-related attributes are presented in Tables 8.11 and 8.12. This type of division seemed logical since it allows the analyst to focus on estimating two different aspects at once.

Table 8.10: Data-related attribute values in the third model version

Attribute	1	2	3	4	5	6
Data access	Only the user can access the data.	Accessible to only by a few persons with access control.	Accessible to only by a handful of persons with access control.	Accessible by a large number of persons with access control.	Data is publicly shared with access restrictions.	Open access to shared data.
Data capabilities	No data or data of no interest.	Leaked data has a meaning only inside the system.	Leak would increase curiosity but is no real threat.	Large amounts of data would threaten privacy.	Privacy is violated with leaked data if it is not properly anonymized.	Data can be used to permanently affect (decrease) user privacy.
Data quantity	No data.	Contains a copy of the transferred data (e.g., a router).	Small amounts of personal data are kept at any time.	Contains personal information that the user can wipe out securely (e.g., cache).	Contains lots of personal information (e.g., home computer).	Contains all user-related private information (e.g., database).
Data significance	Not significant, necessary for the user or required in any operation. Leak has no impact.	Data has a small role in the user's life and the leak causes only annoyance. In the systems the data has to be recreated, and a leak causes some offline time.	Data is useful for the user, and a leak in large quantities can cause privacy infractions. In the systems the data has to be replaced, and maintenance is required.	Data is important for the user and is needed in system operations. A leak causes temporary harm to privacy or opens up access to the asset.	Data is important for the user and is needed in system operations. A leak causes harm to privacy or opens up parts of the system to an attacker.	Data is vital for the user or crucial for the system operation. Leak causes severe privacy infractions or opens up access to the system.
Data storage time	Does not store anything.	Stores for the period of time the data is being transferred.	Short-term storage (wiped out or overwritten now and then).	Medium-term storage (a relatively short period of time).	Long-term storage (stored for a long period of time).	Permanent storage (data is kept for an indefinite period of time).

Table 8.11: Asset-related attribute values in the third model version, 1 of 2

Attribute	1	2	3	4	5	6
Asset misuse potential	The asset capabilities do not interest attackers.	Mildly interesting asset that has the potential for user annoyance.	Mildly interesting asset that opens up ways for user harassment.	Interesting asset that can be used directly for small privacy violations.	Interesting asset that can be used directly for major privacy violations.	Asset can be used to do permanent harm to user privacy.
Asset network	No network access.	Private network with no external access to the asset.	Private network with restricted external access.	Protected private network with external restricted access.	Public network with access restrictions.	Public network without access restrictions.
Asset role	Not important at all.	An extra appliance that gives some practical benefits.	Everyday usage appliance, but user can live without it.	Important but not vital asset. Maintenance gaps are tolerated.	Almost vital asset. Short maintenance gaps are tolerated.	Vital for the user.
Attack actualization	Attack is unlikely because the breach requires an enormous effort.	Breach requires an enormous effort and attacks happen very rarely.	Asset is protected but because of the contained data, attacks can happen infrequently	Attack requires knowledge, and with reasonable efforts, an attack can be successful.	Asset has some vulnerabilities that are known and are tried often.	Asset is either open or very vulnerable, and attacks will happen.
Attack gain	Small or nonexistent reward regardless of the effort.	A notable reward with enormous effort.	A notable reward with a fair amount of effort.	Maximum benefit with enormous effort.	Maximum benefit but requires a fair amount of effort.	Maximum benefit with minimal effort.

Table 8.12: Asset-related attribute values in the third model version, 2 of 2

Attribute	1	2	3	4	5	6
Privacy damage (loss)	No effect on privacy. No data leak/loss possibility.	No real effect on privacy. Minor personal data is lost.	User privacy or personal data is threatened.	User privacy and personal data are threatened.	User privacy is lost, and/or personal data is lost.	User loses privacy completely. Private data is lost.
User damage	No damage is possible.	No real damage is possible, at least not directly.	Can inflict damage in the long term if other assets depend on it.	In long-term the damage keeps increasing.	Health is endangered if there is a emergency.	Health of the user would be in imminent danger.

In order to further enhance the user friendliness a process for valuing the attributes and calculating the values of the calculable and definable attributes is required. For this reason, the model is now divided into three levels, which illustrate the direction of the process of assessment.

1. The first level at the bottom of the model consists of assessable attributes. It is required to first assess the values for the nine assessable attributes using the predefined scales (which were not changed in this iteration since it was not a priority) and then to adjust the values according to the dependency matrices. Here, the order is significant only in the *privacy damage* calculation as it is required to be done before calculating the value for *data capabilities*. The simplest way is to start from the rightmost attribute, *attack actualization*, and proceed to the attributes on the left.

2. The second level in the middle of the model consists of definable and calculable attributes. Here, the order is significant. The attributes formed of the composites, *asset value* and *data value,* are first calculated. Next, the *user damage* is defined, and after this, the *damage level* is first calculated from its composites. Next, the other definable attributes, including *damage level*, are defined using the appropriate equations (or matrices). In the case of the *damage level,* the composites establish the “initial estimate” for it before the attribute can be adjusted with the value of *attack actualization*.

3. The third level consists of only the calculable attributes, which are calculated last, producing the risk value. The order is here somewhat significant as it

can be seen from Figure 8.2: the *impact on privacy* and *attack likelihood* must be calculated before the *privacy risk* can be calculated.

This version removes the need for multiple iterations of model use with the new style of dependency calculation and the process in which the values are calculated. For manual use of the model, this is a very good thing as it would be laborious to conduct the analysis by hand and to have to go through multiple iterations with the model. After testing with this new prototype version, no never-ending loops were detected and the values for every possible state were created. Since there are 9 attributes each of which can have values between 1 and 6, there was a total of 10077696 states. These states generated many results that were difficult to interpret especially for detecting possible flaws or deficiencies in the model connections or dependency matrices. It would have required a lot of time to develop analytics software for displaying and analyzing the generated results, and it was not feasible to do within the time-frame of this research. However, this is an important issue worthy of research in the future.

The values generated and calculated by the prototype, however, seemed to be somewhat sound. High values generated high risk, medium values generated elevated risk values depending on how the values were spread to the attributes and low values generated low risk. The testing of this second model prototype would be more beneficial in a real scenario with real requirements to see how it operates and whether the calculated risk values correspond to the expected or analyzed ones. However, another revision of the model was required since the connections between the attributes were seen to lack some finesse. For example, it must be resolved how to include the *asset role* in the *user damage* calculation and how to adapt more than two dependencies in the calculation. The latter issue requires that the structure is analyzed: Can some indirect dependencies be transformed into direct ones? Therefore, it was decided that the model in its current state was not seen to be fit for real-world assessment, and another development iteration is required.

In this version, identifiability is not included, and this is being researched. In addition, the connections between the attributes were not changed during this iteration. This has to be addressed in future iteration(s). However, the hybrid attribute definition opened up a new door in the design. It is worthy to research whether there would be more hybrid attributes in which three connections can be easily used to define the value. This would create a more complex calculation, but the reward of being more accurate in assessing information privacy risk makes it worth the effort.

8.3.5 Iteration 5

This is the fifth iteration of the *design cycle* (*3*) in which the third artifact version (the third model prototype) is developed. As a direct continuum from the second model prototype, this version revises the connections between the attributes, introduces polished scales for the assessable attributes and introduces adjusted matrices for dependencies (this is an answer to DSR **Q5** on design improvements). This version, before demonstrating it to solve a real-world problem, was developed during the Game Cloud project [25]. Much feedback was received from attempting to assess the different components in the Game Cloud eco–system, presented in section 7.2 on page 131. This resulted in the following third model prototype, portrayed in Figure 8.3.

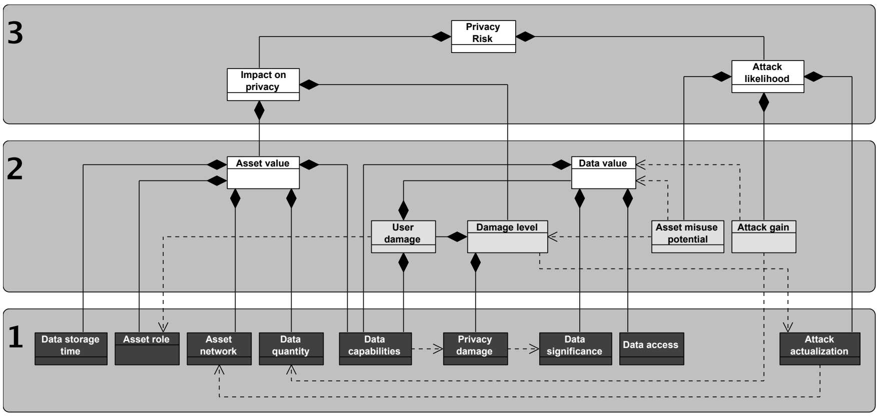


Figure 8.3: Third prototype of a model for information privacy risk assessment

The use in Game Cloud showed that the connections might not be correct in the second prototype. The initial use of the model for valuing the components and calculating the risk values gave the expected results, but there were some oddities in the *impact on privacy* calculations with some value combinations. With a thorough investigation into the model calculations, it seemed that the role of the asset had too little significance in the calculation and, the *damage level* had too big an emphasis on data through *user damage* and not on the damage on the asset itself. The idea presented in the previous iteration about hybrid attributes made it possible to make small adjustments to expand the significance of the *asset role*. The role defines how important the asset is in the environment, especially for the user. Therefore, the importance of the asset must be accounted for in calculating *user damage.*

To comply with this, the attribute *user damage* was changed from the regular definable type attribute to hybrid, and the *asset role* was included in the value calculation as a dependency. The *asset role* defines the task of the asset in the environment, including its importance to the user and to the system and, thus, can reduce the subjectivity of *user damage* when *asset role* is included in calculation. The previous connections of *user damage* were changed from dependencies to composites because the previous scaling shown in Table H.7 on page 312 was somewhat linear and calculating averages from the *data capabilities* and *data value* would produce similar results. The addition of *asset role* would then bring more adjustments based on the value the two attributes produce.

This resulted in redefinition and assessment the appropriate dependency calculation values for the *user* damage using the *user damage* and *asset role* values. In addition, based on the attempt to value the components of Game Cloud, the dependency calculations of the other attributes were adjusted as well. The updated dependency calculation matrices are shown as Tables 8.13, 8.14, 8.15, 8.16, 8.17, 8.18 and 8.19.

Table 8.13: Asset misuse potential adjustment matrix

Damage level Data value	1	2	3	4	5	6
6	2	4	5	5	6	6
5	1	**3**	4	5	5	6
4	1	3	3	4	5	6
3	1	2	3	4	4	5
2	1	2	2	3	4	4
1	1	1	1	1	1	2

Table 8.14: Attack actualization adjustment matrix

Attack actualization Asset network	1	2	3	4	5	6
6	5	5	5	5	6	6
5	4	4	4	5	5	6
4	2	3	3	4	5	5
3	2	2	3	4	5	5
2	1	2	3	3	3	4
1	1	1	1	2	2	3

Table 8.15: Attack gain adjustment matrix

Data quantity Data value	1	2	3	4	5	6
6	1	5	5	6	6	6
5	1	4	4	5	5	6
4	1	3	4	4	5	5
3	1	2	2	3	4	5
2	1	1	2	2	2	3
1	1	1	1	1	1	2

Table 8.16: Data capabilities adjustment matrix

Data capabilities Privacy damage	1	2	3	4	5	6
6	3	4	5	5	6	6
5	2	3	5	5	5	6
4	1	3	4	4	5	6
3	1	2	3	3	4	5
2	1	2	3	3	3	4
1	1	2	3	3	3	4

Table 8.17: Damage level adjustment matrix

Damage level Attack actualization	1	2	3	4	5	6
6	2	3	4	5	6	6
5	1	2	3	4	5	6
4	1	2	3	4	5	5
3	1	2	3	4	4	5
2	1	2	3	3	4	4
1	1	1	2	2	3	3

Table 8.18: Privacy damage adjustment matrix

Privacy damage Data significance	1	2	3	4	5	6
6	1	2	4	5	6	6
5	1	2	4	5	5	6
4	1	2	3	4	5	6
3	1	2	3	4	5	5
2	1	2	3	4	5	5
1	1	1	2	3	4	5

Table 8.19: User damage adjustment matrix

User damage Asset role	1	2	3	4	5	6
6	4	5	6	6	6	6
5	3	4	5	5	5	6
4	2	3	4	4	5	6
3	1	2	3	4	5	6
2	1	2	3	4	5	6
1	1	2	3	4	5	6

This change also requires a small change in the process for calculating the values for the second level of attributes. Because the *damage level* is formed of *privacy damage* and *user damage*, it is necessary to first calculate, after the *data value* and the *asset value,* the value for *user damage* using the composite attributes. Then the value for the *damage level* can be calculated using its composite attributes. Next, all values on the second level can be adjusted based on their dependencies. This approach makes the second-level calculations more clear: first the composites and then the dependencies. However, there is also a downside; this change requires that the model is used iteratively. A change in *user damage* will require that the *damage level* and all other attributes that are composed of it (*asset misuse potential*, *attack likelihood*, *impact on privacy* and *privacy risk*) are recalculated.

Another change in the model was the inclusion of PII 2.0 [20] in the model. This was not included as a separate attribute but as an preparative measure for evaluating the value for *data capabilities*. The value of *data capabilities* is first selected according to the predefined scales for it and then adjusted based on Table 8.20. This seems similar to the dependency calculation, and in future versions, it can be included in the model directly as an additional attribute. However, as a preparative measure, it is only required to be done once and was not considered important enough as an additional attribute. This way, the identifiability is included in the calculation of the information privacy risk value. Additionally, it was seen that the potential of the data (*data capabilities*) utilizing the identifiability of the data must be included in the *data value* calculation. This was because the value of the data should also include the misuse potential of the data and the identifiability, which has a major impact on valuing the data. Therefore, *data capabilities* was added as a composite in the *data value* calculation.

Table 8.20: Data capabilities identifiability classification

Data capabilities Data identifiability	1	2	3	4	5	6
1. Non-identifiable	1	1	2	3	4	4
2. Identifiable	1	3	4	4	5	6
3. Identified	3	4	5	6	6	6

The scales were also adjusted during the Game Cloud project development. This was done by attempting to value different components of Game Cloud and classifying them. The previous division, based on the scope of the attributes, into two classes, data and asset, was seen as too restrictive. It was more of a security approach, but in the information privacy assessment, the emphasis must be on the privacy aspects. Three categories were detected in the scope of Game Cloud: it contains (1) different assets that are used by the (2) users and the assets and the users access, generate and analyze the data stored in (3) the system. With this classification of the asset, user and system perspectives following the new initial assessment scales for assessable categories were designed. These new valuing scales are presented as Tables 8.21, 8.22 and 8.23.

Table 8.21: Attribute values from the asset perspective

Value	Asset network	Asset role	Attack actualization
6	Public network without access restrictions.	Vital for the user.	Asset is either open or very vulnerable, and attacks will happen.
5	Public network with access restrictions.	Almost vital, asset. Short maintenance gaps are tolerated.	Asset has some vulnerabilities that are known and are tried often.
4	Protected network. External restricted access.	Important but not vital asset. Maintenance gaps are tolerated.	Attack requires knowledge, and with reasonable efforts, an attack is successful.
3	Private network. Restricted external access.	Everyday usage appliance, but user can live without it.	Asset is protected, but because of the data, attacks can happen infrequently.
2	Private network. No external access to asset.	An extra appliance that gives some practical benefits.	Breach requires an enormous effort, and attacks happen very rarely.
1	No network access.	Not important at all.	Attack is unlikely because the breach requires enormous efforts.

This was the last prototype of the model for information privacy assessment. It seemed that now all attributes were included, the model gave reasonable results and the development could be stopped. Thus, this version of the model seemed to be suitable for the task it was designed for. But this has to be proved through evaluation.

The previous prototypes could have been evaluated more thoroughly using the six evaluation questions laid out in the first development iteration, but it was seen as more important to establish a working model that is reasonable enough to submit for evaluation, thus the strict time schedules. In addition, as Figure A.1 on page 247 shows, there were projects running at the same time, including the continued development of the *iterative framework*. The time left for evaluation was short, and it was spared to evaluate the working prototype version. In the next three sections, the third prototype of the model is evaluated on the attribute emphasis of the model (part 1), requirements fulfillment (part 2) and models' capability to answer the three challenges inherent in risk assessment (part 3).

Table 8.22: Attribute values from the user perspective

Value	Data capabilities	Data significance	Privacy damage
6	Data can be used to permanently affect user privacy.	Data is either vital for the user or crucial for the system operation. A leak causes severe privacy infractions or opens up access to the whole system.	User loses reputation privacy completely. Private data is lost.
5	Privacy is violated with leaked data if not properly anonymized.	Data is important for the user and is needed in system operations. A leak causes harm to privacy or opens up parts of the system to attacker.	User reputation privacy is lost, and/or personal data is lost.
4	Large amounts of data would threaten privacy.	Data is important for the user and is needed in system operations. A leak causes temporary harm to privacy or opens up access to the asset.	User reputation privacy and personal data is threatened.
3	A leak would increase curiosity but is no real threat. In the systems such data has to be recreated, and a leak causes some offline time.	Data is useful for the user, and a leak of a large amount of data causes privacy issues. In the systems such data has to be replaced, and maintenance is required.	User reputation privacy or personal data are threatened.
2	Leaked data has a meaning only inside the system.	Data has a small role in the user's life, and a leak causes only annoyance.	No real effect on privacy. Some data is lost.
1	No data or data of no interest.	Not significant, necessary for user or required in any operation. A leak has no impact.	No effect on privacy. No data leak/loss possibility.

Table 8.23: Attribute values from the system perspective

Value	Data access	Data quantity	Data storage time
6	Open access to shared data.	Contains all user-related private information (e.g., a large database).	Permanent storage for data, and there are backups.
5	Data is publicly shared with access restrictions.	Contains lots of information most of which is identifiable, and some is identified (e.g., a home computer or a small database).	Long-term storage (data is stored for years).
4	Accessible to a large number of persons (>10) with access control.	Contains information (some of it is identifiable) that can be wiped out securely (e.g., cache).	Medium-term storage (data is stored for months, less than a year).
3	Accessible to only a small number of persons (<10) with access control.	Small amounts of data (some of it is identifiable) are kept at any time.	Short-term storage (wiped out or overwritten now and then).
2	Accessible to only a few persons (<5) with access control.	Contains a copy of the transferred data (e.g., a router).	Stores for the period of time the data is being transferred
1	Only the user, system component(s) or system maintainer can access the data.	No data.	Does not store anything.

8.4 A3: Evaluation of the artifact

In order to demonstrate that the developed artifact, the *assessment model*, is usable, an evaluation needs to be performed before the model is applied in practice. Here, the artifact is evaluated on the emphasis of the attributes, how the requirements are met and how the artifact answers the challenges inherent in existing risk assessment methods. Last, a summary of how the evaluation criteria (six questions defined in section 8.3.1) are met is presented.

8.4.1 Attribute emphasis evaluation

This is the first evaluation part of the *design cycle* (*3*). This section answers the second evaluation question about the attribute emphasis.

Since the current version of the model does not yet take the inter-asset dependencies into account, the evaluation focuses on the attribute weights when defining the privacy risk to a single asset. In order to analyze the weights of the assessable attributes to the *privacy risk*, the model is presented as an Ishikawa diagram [149] in Figure 8.4, which enables calculation of the attribute weights as the model is divided into groups based on the relationships between the attributes. The weight calculation demonstrates that the model emphasizes the right attributes in privacy risk calculation.

In the Ishikawa diagram (Figure 8.4), the three topmost attributes in Figure 4.1 are split into calculable, definable and assessable attributes utilizing the relationships between attributes, but excluding the relationship type in the connections diagram connections. The connections are, however, reversed in the supplier–client relationship compared to Figure 4.1. Here the arrow points from the supplier to the client. The coloring of the attributes in Figure 8.4 follows the same scheme as in Figure 4.1. The percentage of the effect on *privacy risk* is located at the top of each attribute in Figure 8.4. The numbers in parentheses represent the value of the branch, and the bold numbers represent the weight of the (assessable) attribute. In Figure 8.4, all numbers are rounded, but the calculations are made with exact values, with a 0.01% margin of error.

From the Ishikawa diagram it can be noted that some attributes, such as *data significance*, affect the values of multiple other attributes indirectly through other attributes. This was not directly notable from the model in Figure 4.1. Therefore, presenting the model in Ishikawa diagram offers an improved understanding of the extent of the consequential effects of each attribute. This approach offers a clear way to represent the actual weight of each attribute as a percentage of the *privacy risk*.

It is reasonable to calculate the weights only for attributes that have an initial estimate, since other type attributes are defined solely by the assessable attributes, directly or indirectly, as Figure 8.4 shows. Therefore, attributes other than those of the assessable type have no weight in the *privacy risk* value. The results of the calculations are presented and analyzed in the next subsection. But first, in the following, the weight calculation is explained.

The value weighting process The process for calculating the weights for the branches and each attribute is simple. Each branch has a total weight that is equally divided among every sub-branch, that is, the weight of the branch is divided by the number of sub-branches:

$$weight = \frac{w}{b}, \tag{8.2}$$

Where w is the total weight of the branch and b is the number of sub-branches.

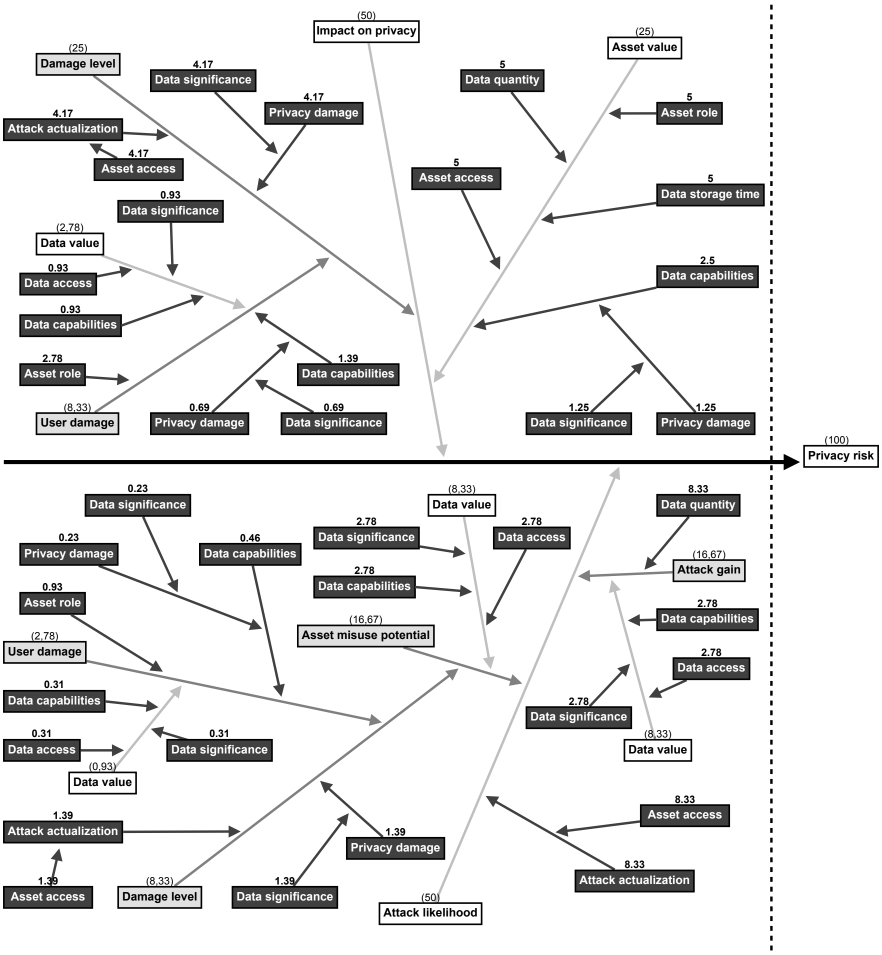


Figure 8.4: Ishikawa diagram presenting the effects of the attributes on the privacy risk

The division is continued until a value is calculated for each assessable attribute in the branch. The process is demonstrated with the following example.

An example calculation The calculation starts from the result of the model, the *privacy risk*, and is then continued toward the branches according to Figure 8.4. *Privacy risk* is calculated from two same type attributes, The *impact on privacy* and the *attack likelihood*; therefore, the weight is divided equally for both, which in this case has a 50% effect on *privacy risk*.

If the attribute has no other dependencies, the calculated weight is directly assigned for the attribute. For example, the *asset network* in the *asset value* branch (25% effect; thus, *impact on privacy* has two sub-branches) has a 5% weight in *privacy* *risk* whereas *data capabilities* is a separate branch that has a 5% effect as the total. This includes the attributes that affect to the value of *data capabilities*.

In order to calculate separate weights for the different type attributes of the *data capabilities* branch, it needs to be again divided into smaller branches. The weight for the supplier and the client in a branch is calculated with same equation as the composite branches (Equation 8.2). Since *data capabilities* is an assessable type attribute, half of the weight is assigned to it, and the other half is the total weight for the *privacy damage* branch, which, in turn, is divided equally among *privacy damage* and *data significance*. Therefore, *data capabilities* has 2.5% weight, and *privacy damage* and *data significance* both have 1.25% weight.

The data capabilities attribute in the example has to have a weight as it is an assessable attribute, but for example, *user damage*, a sub-branch of the *attack likelihood* branch, has no weight since it is of a definable type. In this case, that particular branch has a weight of 2.78% (*attack likelihood* defines half of the *privacy damage* and has three branches, of which *asset misuse potential* has two branches, of which *damage level* has three branches, of which *user damage* is one; therefore, the weight is $100/(2*3*2*3) = 100/36$), and its sub-branches, *asset role*, *data capabilities* and *data value*, have a third each (0.93%). The composites of *data value*, therefore, have a weight of 0.31%. Similarly, in the same branch *data capabilities* has a weight of 0.46%, and both sub-branches, *privacy damage* and *data significance* have a weight of 0.23% each.

The sums of the weights of the nine assessable attributes are shown in Table 8.24. The attributes in the table are ordered by weight.

Table 8.24: Assessable type attribute weights

Attribute	Weight (%)
Asset network	18.89
Data significance	14.52
Attack actualization	13.89
Data quantity	13.33
Data capabilities	11.14
Asset role	8.70
Privacy damage	7.73
Data access	6.79
Data storage time	5.00

The attributes can be grouped based on their definition and what areas the attributes are assessing. By doing so, the following groups and sum weights are established:

- Information based from the user view (*data significance*, *data quantity* and *privacy damage*): 35.58%

- Access based (*asset network* and *data access*): 25.68%
- Attacker based (*attack actualization* and *data capabilities*): 25.03%
- Asset based (*asset role* and *data storage time*): 13.70%

From the table and the list of attribute groups, it can be noted that in the model, the *privacy risk* value is largely defined by the characteristics of the information and how the information can be accessed. Since the model is targeted to assess information privacy risk, the emphasis has to be on the importance of the data (*data significance*) and its quantity (*data quantity*), in addition to *privacy damage*, which alone has lower weight.

Another thing the model emphasizes, according to the weights, is access in general. For information privacy, it is imperative to also evaluate the asset where the data is retained. This includes the access to the asset itself and the access the asset enables to the information. Therefore, the weight for the *asset network* has to be fairly high. But the access to data (*data access*) has a significantly lower effect because the publicity level of the data alone does not define the risk. Instead, the risk will be increased through other attributes that define the quantity and significance of the data.

In addition to access, *attack actualization* is also significant since the model focuses on assessing the *privacy risk* on an asset level. Therefore, the probability of an attack (to an asset) is a factor that has a big effect on the privacy risk. The number of occurrences of *privacy damage* in Figure 8.4 suggests a high effect on *privacy risk*, but the weight division clearly shows that the initial estimate of *privacy damage* does not have much weight for the *privacy risk*. The *privacy damage* introduces the connection to current information privacy regulation but defines only the loss of reputation privacy and what type of data is lost (see the definition in Table 8.22 on page 193) not taking into account the significance of the data. Therefore, the risk of losing individual autonomy comprises more than just damage to individuals' privacy (*privacy damage*) and, in the model, is assessed using the significance and the capabilities of the data.

The *data capabilities* attribute has an average effect on *privacy risk* since it is not the biggest factor in defining the information privacy risk as the value offers the level of usefulness of the information for the attacker and the legal compliance of the data in terms of identifiability. Therefore, the weight of approximately one ninth, being one of nine assessable attributes, is not over- or under-emphasized.

The asset-based attributes (*asset role* and *data storage time*) have the least effect when combined. The *asset role* as a separate attribute has a moderate effect on *privacy risk* since it partially also defines the damaging effect on the user in addition to the value of the asset (*asset value*). In future versions, the effect of *asset role* increases when dependencies on other assets are introduced. The length of time the data is available on the asset (the *data storage time*) has the least effect of all the assessable attributes as it affects only one attribute directly (the *data value*). The previous speculation about whether to apply the *data storage time* to the *data quantity* definition needs more research since it would have a significant effect on the weights.

Therefore, the emphasis of the research artifact, the model, is on correct attributes. This evaluation answers the second evaluation question presented in activity three on page 170.

8.4.2 Requirements evaluation

This is the second evaluation part of the *design cycle* (*3*). This section answers the third evaluation question about requirement fulfillment.

How the requirements, defined in Table 8.3 on page 167, are implemented in the model design are explained in the following subsections. Each subsection is labeled with the identification of the requirement. This answers the third evaluation question presented in activity three on page 170.

R1: The legislation is included by utilizing the European directive *close link* definition [49] between an object or an event and a person to define whether the information is regarded as private. Therefore, current legislation is included, and future changes can be adopted with ease without the need for changes in the model. It is also required to use the definitions in legislation about information privacy to guide the estimates for different data attributes (such as *privacy damage*).

R2: The data is valued from two viewpoints: how exploitable the data is (*data capabilities*) and how necessary the data is for the individual (*data significance*). The scales for both attributes are designed to account for the different forms of personal data. In these scales, subjectivity is reduced by emphasizing the level of the privacy violation, which has to be estimated using legislative definitions.

R3: Each asset can have different types of network access, and this is accounted for in the *asset network* attribute that defines the access to the asset in a non-subjective way using clear definitions for different network types (private, protected, public). The potential of the asset storing the data and offering access to the data is defined only by the *damage level* and the *data value*. The initial estimate has no effect on the *asset misuse potential* in the current model but based on the diagram (Figure 8.4 on page 196) is indirectly affected by the *data access* attribute.

R4: The *data access* attribute is used to define the level of access of the data, and this attribute directly affects the *data value*. The number of users is non-subjective, and specific limits for the initial estimates are given in Table 8.23 on page 194.

R5: The potential of the data is accounted for in the *data capabilities* attribute. The initial estimate values (in Table 8.22 on page 193) are designed to reduce subjectivity through identifiability, and the value is adjusted with the value of the *privacy damage* attribute that defines the effect on individuals' privacy.

R6 The level of identifiability is accommodated in the model through *data capability* using the PII 2.0 classification [20]. This makes it possible to include the stance of legislation on information privacy in the model.

R7: To accommodate this requirement, the *data value* is calculated directly from the values of *data significance* and *data access*. Therefore, changes in the scenarios are accounted for by using the significance of data and the number of people accessing data.

R8: The model accounts for the time the asset stores the data in the *data storage time* attribute. The definition of storage times is not feasible to define with hard values since the requirements, often determined by legislation, can differ greatly. Therefore, the attribute is partially subjective with quantifiable limits.

R9: The quantity of the data requirement is accommodated from the view of the individual, and the *data quantity* is valued using the amount of personal data that the asset contains. Some of the value definitions in Table 8.22 on page 193 are tied to the storage times of that data (e.g., the copy of transferred data; the storage time is short), and it is worth investigating whether adding dependency to *data storage times* would bring more value to the definition of the *data quantity*.

R10: In the model, the type of the network the asset is in is taken into account with the *asset network* attribute. This attribute is also used to adjust the value of the *attack actualization* that defines the probability of the attack. This approach makes it possible to give more weight to the network type in the calculation.

R11: This requirement is not completely fulfilled because the model in its current version does not utilize the dependencies between different assets. Only the role of the asset is accounted for using the importance of the asset. The role of the asset affects the *user damage* attribute, which introduces more weight for the role in the *privacy risk* calculation. This, therefore, increases the importance of the asset type and its functions in the model.

R12: The damage of an attack is taken into account through two separate attributes: *privacy damage* and *user damage*. In the former, the damage is the loss of reputation privacy and the loss of personal data. In the latter, the damage is defined by the value of the data (*data value*), the potential and the identifiability of the data (*data capabilities*) and the importance of the asset holding all the data (*asset role*). These three attributes are used to acquire the level of damage that can be inflicted on the user through the data or asset.

R13: The gain for the attacker (*attack gain*) is included through the quantity (*data quantity*) and the value of the data (*data value*), which is valued from the attackers' and individuals' perspective. When the data is necessary for the user (*data significance*), it is also useful for the attacker. This takes into account the benefit the attacker can get by targeting the particular asset. The full likelihood of the attack utilizes, in addition to *attack gain*, two more attributes, which include the level of usefulness of the asset (*asset misuse potential*) and the expenses of the attack paths (*attack actualization*) for the attacker.

R14: The use of an external method, such as attack trees [133], is recommended in determining the path of the attack in order to include it in the *attack actualization* attribute. This, however, requires a separate classification for each potential attack path and is left for the analyst since it is highly dependent on the environment in which the assessment is conducted. The results have to be scaled using the classification in Table 8.21 on page 192 and then adjusted based on the network the asset is in (with Table necessity of 8.14 on page 189). Using this process, the path and the access medium can be covered.

R15: The *privacy risk* in general is viewed from the individuals' point of view, focusing on the loss of information privacy that can be caused by an attack or other potential misuse or disclosure of private information. The *privacy damage* directly defines how big the effect of a successful attack would be on an individual's reputation and privacy. The importance of the data for the user and the system quality is defined using the *data significance* attribute for defining the necessity of the data, and the *data capability* attribute for defining the potential and identifiability of the data. The combined weights of these three attributes define a third of the *privacy risk* (Table 8.24 on page 197), which clearly shows that the privacy of individuals has a big emphasis.

R16: This requirement is not included in the model directly. Instead, use of an existing method for detecting the data redundancies in the environment is recommended. The first part of the method, the *abstraction method*, also presented in previous research [45, 46], is a suitable tool for the task.

R17: In the model, the risk of losing reputation privacy is defined through the *data significance* and the *data capability*. If the data is important and identifiable to an individual, then the risk of losing one's reputation is high. The effect of these two attributes on *privacy risk* is more than 22%, and therefore, the effect is significant.

8.4.3 How the existing challenges are met: an evaluation

This is the third evaluation part of the *design cycle* (*3*). This section answers the fourth evaluation question about the challenges of risk assessment.

As part of the method for evaluating the *assessment model,* in addition to attribute emphasis analysis and how the requirements are met, it is required to evaluate how the model can answer the challenges posed by existing methods and models. In the following, some of the methods found through the literature review are introduced and compared to the *assessment model.*

The three downsides of risk assessments: Quantitative enterprise-level risk assessment methods, such as CRAMM [119], INFOSEC Assessment Methodology [123] and OCTAVE [124], focus on protecting assets, including the information held, and mitigating the impact of potential attacks by enhancing security or applying countermeasures. Qualitative methods can also take into account the business impact of security risk. This is, for example, the case with the "root pattern for all enterprise concerns" approach [116]. Qualitative risk analysis methods, such as SQUARE [122] and OCTAVE-S [124], as well as the approach in [116], are used to estimate the need for security: what type of security properties should be applied and where. Most of the methods, both quantitative and qualitative, are aimed at larger enterprises. The methods do not solely concentrate on information systems and the information held but take into account every asset in the domain of the enterprise. The disadvantages of these methods can be summarized as (1) the results might not be reusable between consecutive assessments [116], or (2) the results are subjective [120] or (3) speculative [126].

Overcoming the challenges: The proposed model answers these three challenges as follows (and answers the fourth evaluation question presented in activity three on page 170):

1. To overcome the disadvantage of non-reusable results, the *assessment model* enables the comparison of different approaches and setups. This would, however, require further development. The method presented here opens up ways to create a software tool for mapping and analyzing the environment. It is imperative that the software tool presents the risky areas in the deployment of assets by their abstract task, data storing and sharing specifications, including the connections between the assets. Such a tool would provide a more reusable privacy risk assessment process that would ease the workload of the persons responsible for the security of the private information. The proposed EU regulation [22, 23] allowing the EU to penalize companies for failing to address the privacy measures adequately, can be a worrisome issue for smaller enterprises. The presented model and resulting software could help to ease the burden on small companies. Additionally, the resulting software tool can be used to demonstrate to customers that privacy issues are taken care of. This would increase transparency and result in increased customer trust.

2. Subjectivity was accounted for in the early model design phases, and this is also included in the values of the attributes. The attributes and the connections are designed in a way that attempts to reduce subjectivity. Defining a value for subjective attributes, such as *asset* and *data value*, *damage level* and *impact on privacy*, is tricky, and therefore, they are not given an initial estimate. Instead, they are defined by the values of other attributes of which only a few are bound to subjectivity. To further reduce the subjectivity, the scales for the initial estimates (Tables 8.21 on page 192, 8.22 on page 193 and 8.23 on page 194) were designed to be as non-subjective as reasonable. Subjectivity is hard to remove completely as the use of the model involves an analyst, whose opinions and expertise can affect the values allocated to the attributes.

3. Whereas subjectivity of the results is hard to remove completely, the ambiguousness of the results can be reduced. In the *assessment model* the ambiguousness of the results is reduced if not completely removed with predefined scales for each assessable attribute, and the results follow a certain consistent scale. The assessment of different assets does not leave room for speculation, not at the qualification step or when results are generated. Therefore, the *assessment model* does not suffer from this disadvantage.

8.4.4 A summary

This part summarizes the evaluation results of the *design cycle* (*3*). The three previous evaluations show that in the model the attributes are emphasized appropriately, all requirements are met and the challenges of risk assessment can be overcome.

The answers to the six evaluation questions are as follows:

1. The attributes listed in section 8.2.4 on page 165 are included as follows:

    - Access to information: covered by the *data access* attribute
    - Access to asset withholding information: covered by the *asset network* attribute
    - Damage to the individual that can be identified with the information: covered by *user damage* that is formed of *data value*, *data capabilities* and *asset role.*
    - Damage to the reputation of an individual: covered by the *privacy damage* attribute.
    - Damage to the asset or the system: included in the *damage level* calculation and *asset misuse potential* through the role of the asset and the significance of the data to system operation.
    - Identifiability of the information: included in the *data capability* attribute calculation.
    - Likelihood the asset withholding information is attacked: covered by *attack actualization* and the resulting calculated *attack likelihood* value with *attack gain* and *asset misuse potential.*
    - Nature of information or its significance to the user or to system operation: included in the *data significance* definition scales.
    - Misuse potential of the asset: covered by the *asset misuse potential* attribute that is defined through the value of the data and the level of damage.
    - Quantity of information: covered by the *data quantity* attribute.
    - Quality of information or what is the potential of misuse: covered through utilization of *data significance* that indirectly affects the *asset misuse calculation*.
    - Time the information is stored in the asset: covered by the *data storage time* attribute.

2. According to the first part of evaluation about attribute emphasis, the correct attributes are emphasized.

3. According to the second part of evaluation, the requirements are met with the third model prototype.

4. According to the third part of the evaluation, the model can (1) produce reusable and (3) definite results that are (2) reduced in subjectivity. However, the subjectivity can be further reduced by adjusting the scales for initial estimates. Therefore, the three downsides of risk assessment are answered for the most part. The model can be used in the future to further research this aspect.

5. Since all the attributes are accounted for and the aim was to develop the model as environment agnostic, it is usable to assess any information-centric ecosystem. There is no one thing that ties the model to any specific context.

6. The results, with a qualitative scale similar to Table 8.2 on page 163, leave no room for interpretation. The results are not meant to be fully descriptive but indicative to direct the resources into the areas that have the biggest risk in order to find out what aspects are causing the big risk value. This enhances the model's stance as a tool for assessing information privacy risk as a mid-level tool.

All evaluation questions, therefore, are answered. This is the last cycle of the *design cycle* (*3*), and next, the artifact, the model, is demonstrated through use of the Game Cloud ecosystem.

8.5 A4: Demonstration of the artifact

This is the field testing part of the *relevance cycle* (*1*) in which the use of the artifact, the model for information privacy assessment, is demonstrated. This is done in an example *application domain* of the *environment* (*a*) by utilizing the *software prototype* of the model to assess values for different components of an example of a DGP: Game Cloud. This answers DSR **Q6**.

Game Cloud has been used extensively as an example in this thesis, especially for describing the development of the *iterative framework*. Game Cloud was described earlier in section 7.2 on page 131, and its components, including their descriptions, were presented in section 7.2.4 on page 139. The Game Cloud development process is used as a case example later in this thesis to demonstrate how both parts of the research, the *iterative framework* and the *assessment model*, can be used together in the development process of a new system. Therefore, Game Cloud or the full process is not fully detailed in this part of the artifact demonstration. Here, only the first round of development iteration is shown, and the components present at that development stage are assessed with the *software prototype* of the model. The rest of the case example is the more extensive demonstration in which the model is used mainly as a tool.

The information use and the relations of the components that were detected during the development of the *iterative framework* were used as the basis for this demonstration as background information. The depth of knowledge obtained from the ecosystem with the help of the *iterative framework* offered enough information to select appropriate initial values for each component.

The overlay of the Game Cloud components is presented in Figure 8.5. The components that are to be assessed for their information privacy risk are the software components with identification numbers from 1 to 7. Human actors (8 to 10) are excluded in this assessment.

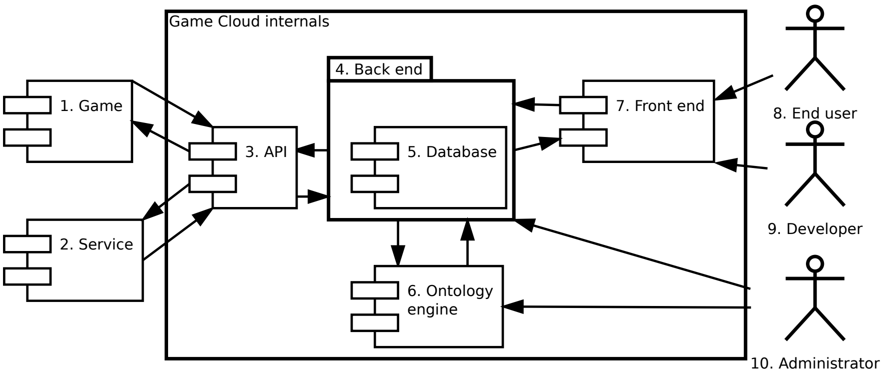


Figure 8.5: The overlay of the components of the Game Cloud ecosystem

Each component was valued separately using the predefined scales, and the attributes were assigned with the following values presented in Table 8.25. The results from each iteration, one calculation iteration per component, are presented in Appendix F on page 281.

Table 8.25: Selected attribute values for the Game Cloud ecosystem components

Component Attribute	1.	2.	3.	4.	5.	6.	7.
Data storage time	3	4	2	6	6	3	2
Asset role	5	2	5	6	6	6	5
Asset network	3	6	6	4	4	3	6
Data quantity	4	3	3	6	6	2	4
Data capabilities	6	4	5	6	6	3	5
Data identifiability	2	1	2	3	3	1	2
Privacy damage	4	3	4	6	6	2	5
Data significance	3	2	5	6	6	2	5
Data access	1	2	1	4	4	2	4
Attack actualization	2	6	6	4	4	2	6

The values were selected with the following criteria:

1. Game

    - Data storage time: 3 because the game stores data but it is not kept for a long time.

- Asset role: 5 because this is the asset that is used to generate the data from the actions of an user.
- Asset network: 3 because the game connects to a service and does not offer connectivity to others(therefore has restricted access).
- Data quantity: 4 because the data generated from the actions of an user is identifiable that can be fairly securely wiped out, but the amount is usually limited. It is the amount of data a playing session can generate.
- Data capabilities: 6 because the data generated is identifiable with the user.
- Data identifiability: 2 because the generated data is identifiable.
- Privacy damage: 4 because with the generated data some decisions about player psychology, for instance, could be made as the data describes the behavior within one game session.
- Data significance: 3 because the generated data can be useful in creating player statistics, and when leaked in large amounts, the player's privacy can be threatened. However, data from one game session is not vital for analysis.
- Data access: 1 because the data can be accessed by the Game Cloud components or the owner of the game system in which the game is played.
- Attack actualization: 2 because it is not probable that a specific game is attacked as the amount of data stored is fairly low.

2. Service

   - Data storage time: 4 because a service can store data, but it is not permanent storage for the data. The data may be stored for longer than a year, but it is more likely that after that it is stored in a processed format.
   - Asset role: 2 because the service is not an integral part of the system and is offering something extra for the users.
   - Asset network: 6 because the service is completely in the public Internet allowing access from anywhere.
   - Data quantity: 3 because the data from the service use might not be stored as it is but in an analyzed or otherwise processed format. The data that is stored about the service use is small in quantity.
   - Data capabilities: 4 because in large quantities this data can reveal something about behavior or physical location or details about the connections (IP address).
   - Data identifiability: 1 because, as mentioned, the details about service use are more likely to be stored in processed form, and the data is at most identifiable, but more likely it is non-identifiable.

- Privacy damage: 2 because this data can harm privacy only if large amounts of this data are obtained. It has no direct effect on privacy or the integrity of an individual.
- Data significance: 2 because the service data is not significant in Game Cloud use. It offers only some additional value.
- Data access: 3 because the service can have multiple maintainers and main users, each of which more likely has a separate access profile in the access control system.
- Attack actualization: 6 because the service is completely public and may be running on a vulnerable platform.

3. API

- Data storage time: 2 because the API has to store the data only for the period of time it is transferred to the back end for processing and storing.
- Asset role: 5 because the API plays an important role in Game Cloud as all end-user activities are sent through it. However, the system can function without it for short periods of time.
- Asset network: 6 because the API resides in a public network for easy access without access restrictions.
- Data quantity: 3 because the API contains a small amount of data at any time point and stores no user data. The data contained is identifiable with an individual.
- Data capabilities: 5 because gaming data can be used for multiple different purposes [37]; as some can harm the privacy of an individual, the data has to be protected. It might be possible to connect pseudonymized data to the identity of an individual.
- Data identifiability: 2 because the API contains information (gaming data and service data) that can be later connected to the identity of an individual. The data itself contains only a pseudo-identifier, and therefore, the data is identifiable.
- Privacy damage: 5 since if the API leaks the transferred data it might be possible to harm individuals' privacy as the data contains an identifier that can be connected to the identity of an individual.
- Data significance: 5 because gaming data is important for the Game cloud system as it generates information based on the end-users actions for third parties and developers. In addition, the gaming data is important for the users in order to gain more achievements and to be able to transfer content between games.
- Data access: 1 because the API delivers the data directly to and from the back end and stores none of it. No external user access is available to the API, and all data is transferred via software components (game, service and back end).

- Attack actualization: 6 since the API resides in a public network and is open for access, it is likely to be attacked or at least checked for vulnerabilities by unauthorized users.

4. Back end

   - Data storage time: 6 because the back end contains the database in which all data is kept for an indefinite period of time.
   - Asset role: 6 because this is one of the core components in Game Cloud and the system will not work without the back end.
   - Asset network: 4 because the back end resides in a protected network that can be accessed externally either by other components or by the system administrator.
   - Data quantity: 6 because of the database containing all data on all identifiability levels.
   - Data capabilities: 6 because the gaming data can be used for a multitude of purposes as was discussed in section 2.3.3 on page 46 and in the *iterative framework* research process in section 7.2 on page 131.
   - Data identifiability: 3 because the database contains data on all identifiability levels, also as identified.
   - Privacy damage: 6 because the gaming data can cause major harm to individual integrity and to the privacy of an individual. This was discussed in the same sections that were mentioned in the value selection discussion of data capabilities above.
   - Data significance: 6 because the data contained within the database is vital for system use from the players' point of view. In addition, the data in the back end is important for system operation in general.
   - Data access: 4 because the data can be accessed by a small number of personnel responsible for Game Cloud development and maintenance.
   - Attack actualization: 4 because the back end is in a protected network and the system has clear access restrictions. But with proper knowledge about exploits and 0-day vulnerabilities, attacks may succeed.

5. Database (same values and reasons as in back end because the database is contained within it in the initial designs of Game Cloud).

   - Data storage time: 6 because the database contains all data collected by the system.
   - Asset role: 6 because without the database Game Cloud would not operate.
   - Asset network: 4 because the database resides in the protected network that can be accessed externally either by other components or by the system administrator.

- Data quantity: 6 because all collected, processed and analyzed data is stored in the database.
- Data capabilities: 6 because of the same reasons the data capabilities of the back end are classified.
- Data identifiability: 3 because the database contains data on all identifiability levels, also as identified.
- Privacy damage: 6 because of the same reasons the privacy damage of the back end is classified.
- Data significance: 6 because the data contained within the database is vital for system use from the players' point of view.
- Data access: 4 because of the same reasons the data access of the back end is classified.
- Attack actualization: 4 for the same reasons the attack actualization of back end is classified.

6. Ontology engine

    - Data storage time: 3 because the data is kept only for the period of time it is being processed.
    - Asset role: 6 because this is the heart of Game Cloud, the system will not function without it.
    - Asset network: 3 because the ontology engine is within the internal private network of Game Cloud. This network has no direct external access but very restrictive access for maintenance.
    - Data quantity: 2 because only a copy of data is stored for processing.
    - Data capabilities: 3 because the amount of identifiable data is small and it is kept only for the time to be processed, the data causes no threat. In addition, the processed data is non-identifiable and is of no use to an attacker.
    - Data identifiability: 1 because the processed data is anonymized and only small amounts of identifiable data (only within the system) are used in processing at a time.
    - Privacy damage: 2 because the anonymized processed data cannot be used to harm the integrity of an individual. The data used for processing is also identifiable only within the system.
    - Data significance: 2 because the processed data can be generated again from the raw data it has a very low significance in the system and to the user as well.
    - Data access: 2 because the ontology engine is within the private network and the actual data within the engine is accessible by only a few persons who have maintenance privileges. Even in this case, they can access the parameters of the engine.

- Attack actualization: 2 because it is not likely that this component is attacked as it would require penetration of the defenses of the Game Cloud system first. In this case, there is a more lucrative target: the database.

7. Front end

    - Data storage time: 2 because the front end only keeps a copy of data that is requested by the player or the developer through it.
    - Asset role: 5 because for the players and developers the front end is important for getting own statistics and modifying preferences. However, brief downtime may be tolerated.
    - Asset network: 6 because the front end is the interface for the players and the developers, it has to be completely in the public without access restrictions.
    - Data quantity: 4 because the front end can be regarded as a cache for the requested data.
    - Data capabilities: 5 because the data retrieved through the front end contains personal data, identification and statistics, especially in the case of players. All of this information can be used for malicious purposes.
    - Data identifiability: 2 because the information retrieved is identifiable within the system, but if the session through which the information is viewed is hijacked, the information would be linked to the initiator of that particular session. However, it is unlikely, and the information that goes through the front end is in its core form treated as identifiable.
    - Privacy damage: 5 because the personal data, identification credentials, statistics and the other possibly accessible information can be used to harm the individuals' privacy or to steal or manipulate the personal data.
    - Data significance: 5 because the data that is obtained through the front end is important to the player as it contains identification details, as well as detailed statistics of the playing behavior, which may be prone to malicious use in harming privacy.
    - Data access: 4 because the particular requested data can be accessed by the system administrators in addition to the one requesting the data.
    - Attack actualization: 6 because the front end is completely in the public, running on some widely used web server that may have existing vulnerabilities or the vulnerabilities are not found yet, and it will be prone to 0-day vulnerability exploits.

These values were inputted in the *software prototype*, and the results of the calculations are shown in Table 8.26. The details of other attributes, such as the *damage level*, are presented in Appendix F on page 281.

Table 8.26: Result of the component-based Game Cloud information privacy assessment

Component Attribute	1.	2.	3.	4.	5.	6.	7.
Impact on privacy	4	5	5	6	6	3	5
Attack likelihood	3	4	5	5	5	2	6
Privacy risk	**4**	**5**	**5**	**6**	**6**	**3**	**6**

These values indicate that the biggest risk in information privacy lies within the three core components: the back end, database and front end. This was expected as the first two contain and control all the information that Game Cloud collects. For the same reason these two have the biggest *impact on privacy*, but the network restrictions on these components mean that they may not be tried as often as the front end, residing in a public network. The front end is the one that offers a public access to the information withheld by Game Cloud, and the risk value is as it should be, but the impact is less than with, for example, the database. This is because of the quantity and the identifiability level of the data that is handled.

The API has the next highest information privacy risk value because it is also in the public and is the hub for inputting all information from behavior in games and in services. Thus, the API handles many information transactions and deals with sensitive data. Therefore, the second highest values can be expected.

The game and the service have similar risk values. This was expected because they both deal with small quantities of personal data, which is sent to Game Cloud and is not meant to be stored within the asset. Games are less likely to be attacked as it is more useful to attack the place to which the information collected by these games is sent. The service, being public, is more prone to attacks, but if it has information of no or low interest, the probability of an attack is merely average. However, services have more information than games, and whereas the nature of the information might not be at the same level as the games collect, the information still can be used to harm the privacy of an individual through other means. Therefore, the one step higher risk value for service is justified.

The lowest risk is, as expected, assigned for the ontology engine. It processed data without storing it and, therefore, will have a less than medium risk, and the impact on privacy is low.

8.6 A5: Evaluation of the results of the demonstration

The *field testing* during the Game Cloud development was the first utilization of the model in the form of the created *software prototype* to detect information privacy risks in a real environment. This evaluation section summarizes the objectives based on the results of the demonstration results, attribute emphasis analysis, requirements fulfillment discussion and discussion about how the challenges of existing assessment methods are met.

The demonstration of the artifact showed a lot of promise as the resulting values were as expected. It proves that the model can be used as a mid-level tool in assessing information privacy risk in an information-centric system. The objectives laid out in section 8.2.1 on page 158 are met as follows.

Objective 1: During the iterations, the number of assessable attributes was reduced, and the scales were polished to be more readable and definite. This has a positive effect of being more user friendly, easier to use and cost-effective. This is, however, hard to measure without an evaluation of the actual use of the model in the hands of an analyst who was not involved in the design process. But being in its infancy, the model is already usable as a *software prototype* that reduces a lot of effort from the calculation of the values. In any case, the analyst would have to assess each component separately to gain some insight, and this presented model is no different. In addition, as the later full detailed case example of Game Cloud presents, the results the model produces are reusable between the development iterations.

Objective 2: The different attributes account for all aspects of information privacy as presented earlier in section 8.4.4 on page 203. Quantitative and qualitative attributes are included. The loss of privacy of an individual has a total of 35.58% weight in the risk value calculation (section 8.4.1), and therefore, it has the biggest significance in the model.

Objective 3: The interests of an attacker or unauthorized user are included in the model through the potential of the data (*data capabilities*) and *attack actualization*. They have a combined weight of 25% in the risk value calculation (section 8.4.1). They are indirectly used as the values for the *asset misuse potential* and *attack gain* as shown in 8.4 on page 196. The issue of the effect of *data storage time* on the interest of an attacker is not included in the model, and this is left for further research. In this research, the nature and the potential of the information were seen as attributes that may have increased in the attacker's interest.

Objective 4: The model is aimed to assess the risk for the information privacy of an individual in a system that is maintained by another party. The asset and all aspects that affect its value, as well as the attacker interests, are estimated by analyzing the system run by a company, corporation or organization. The model is not meant to be used by an individual to assess his or her own privacy risks but for companies. In this assessment, the quality of the service offered by another party is included by the loss of the quality of service if there is a breach. Therefore, individuals' privacy is assessed by utilizing parameters from within the company's information systems and services by an analyst working for the company or other organization or corporation conducting an assessment. Thus, this objective is met.

Objective 5: The research focus was on the privacy requirements of private information as the many iterations on objectives, requirements and foundations presented earlier shows. This can also be seen from the emphasis of the model attributes presented in Table 8.24 on page 197. The security and data protection principles were not directly included in the research process but were kept in the background in the process.

Objective 6: In the research artifact, the model, damage to individual autonomy (*user damage*) and damage to individual integrity (*privacy* damage*),* are accounted for. In addition, the damaging effect of data misuse is included through *data capabilities.*

Objective 7: The research artifact, the model, includes the benefits of an attack (*attack gain*) through the value of the data that can be obtained and the quantity. The data is valued using the *data access, data significance* and *data capabilities,* and the last two attributes are the ones that mainly affect the benefits of the attacker. *Data capabilities* define, the exploitability of the data from an attacker's perspective, but *data significance* introduces also the importance of the data to the user in the assessment. This way, the gains of an attack are even expanded to account for the harm that an attacker can cause to the user if the intent is just to irritate and cause annoyance to an individual.

Objective 8: The results the developed model generates are definite but not very descriptive. Because of the qualitative nature, the model is not absolutely precise but offers results with moderate resource consumption to create an overview of the ecosystem under study in order to focus more closely on the assets that have high risk values. The predefined scales for each assessable attribute, presented as Tables 8.21, 8.22 and 8.23 on page 194, introduce a clear way to first classify the attributes of the assets, and the results help to classify the asset itself based on the impact they have on privacy, the likelihood of an attack and the information privacy risk they have on an understandable qualitative scale (similar to the scaling of Table 8.2 on page 163).

Decision: From the three evaluations conducted in addition to the demonstration of the artifact, the model, it can be concluded that the model is what was required and answers the challenges well. In addition, correct attributes have the most weight in the calculation. Furthermore, since all of the objectives were met, the transition to the sixth activity was found to be suitable.

8.7 A6: Communication of the results

The designed artifact was suitable for solving a problem in an example *application domain* of information-centric systems for which the artifact was designed. This is part of the *rigor cycle* (*2*) in which new additions are contributed to the *knowledge base* (*c*). The model itself is the main artifact of this research, and there is no meta-artifact in this research (this partially answers DSR **Q7**).

This research has not yet been published, but the key points are included in the author's fifth publication (summarized in Appendix B) [59]. At the time of writing, this publication is under review in a journal focusing on software quality, which was seen as an appropriate audience for communicating this part of the research. In addition to the many sections presented in this part of research, the fifth publication [59] contains the discussion and overview of information privacy that was detailed in this thesis in section 2 on page 35.

The new information this research contributes is the following:

- A new way of viewing information privacy
- A unprecedented way of modeling information privacy
- A model to be used in a qualitative information privacy assessment
- A basis for software that can be used cost-effectively and easily for information privacy assessment

This research forced to search for the attributes of information privacy to answer **RQ1**. The attributes were presented in section 8.2.3 on page 160, and they are included in the model, except the purpose of use that falls under data protection. The model itself can be used as a tool for detecting the components that require more protection in terms of information privacy, which offers an answer to **RQ2**. The connections between the different attributes of information privacy within the model is a clear answer of how these characteristics relate to each other (answer to **RSQ1.1**). During the research process, it was noted that in order to enhance user friendliness, the initial estimate scales for assessable attributes must be clear, and the number of the attributes must be attempted to be reduced. This may not be the full answer to **RQ3** of how to model information privacy in a user-friendly way but is the first step toward it. The model shows the relations in a clear manner, understandable to any person involved in software development, thus the use of

UML, and, thus, may be regarded as a user-friendly presentation. However, many non-developers might disagree. Still, the model is a one step toward answering **RQ3**.

The legislative attributes are not directly included in the model, but the valuing of some attributes may benefit from the inclusion of the legal perspective. This is answered with the final version of the model that is presented later in this thesis as the second part of the research contribution. In that version, **RSQ3.1** is answered. In addition, **RSQ3.2** is fully answered in the case example that demonstrates the use of both parts of the research described in this thesis. However, the initial demonstration using the initial design of the Game Cloud ecosystem shows that the model is usable for assessing information privacy in information-centric system. This, however, can finally be answered only after multiple usages of the model and the resulting complete approach, as well in ecosystems that have varying details, scopes and purposes.

As a result of the research, an extensive model encompassing all attributes of information privacy was developed. This model utilizes many different connections between the attributes, which helps in understanding and further modeling information privacy through its attributes. The model is for assessing information privacy risks on the component level establishing a qualitative risk value based on selecting appropriate values from predefined scales for 10 attributes per component.

These answer DSR **Q8**. This concludes this part, as well the complete research part of this thesis.

Part IV

Concluding remarks

This fourth part draws together the results of this thesis. First, further development ideas regarding the *assessment model* and the complete approach are introduced. Then final remarks about this work and research conclude this thesis.

9 Future visions

The presented approach is usable for information privacy risk assessment as is; but some future research is needed to enhance it. Here, a discussion about future visions about the research around this approach is introduced.

9.1 The model

The current version of the model utilizes many dependencies between the attributes. Every value change in one attribute creates changes in some other attribute, and with some values, this causes a large update chain that is cumbersome to handle manually. With the presented model, the maximum number of update rounds for any possible combination of initial estimates is six, which was tested with the software prototype. However, in the Game Cloud case example, there was only one iteration with each calculation according to the detailed results presented in Appendix F. With a small number of assets, the calculations can be made manually but with multiple assets that have inter-asset dependencies, the process is too laborious, a software is required.

The *asset role* opens up an idea about connecting the assets within the system to others in the assessment to include the effects each asset has on them. The development may be directed to create dependencies to other assets based on their network connections to form a topology network, where the dependencies are included as scalar factors between one and zero [150]. This would result in a map of the assets, in which the value is formed of the value of the asset and the value of the parent, multiplied by the link weight scalar factor. Or alternatively, the assets may be connected by their relative necessity: how the asset affects the other functions of the system and what is the importance of the asset to the system operation [120]. This type of dependency would require connecting other attributes than just the *asset role* between the assets. As a result, the influence of the asset on the system would be better accounted for. This type of approach could be beneficial in mapping the attack paths as an additional measure or connected attribute. But it would be also possible to include both [120, 150] since both aspects are already included in the model. In addition to the *asset role*, the network type can be connected through the *asset network*, and the *asset misuse potential* and *attack actualization* could be affected by the importance of the asset.

Additionally, the dependencies between the attributes open up a way to tailor the model for a more specific purpose. The direct dependencies can be weighted to generate required values or have increased or reduced weight in the *privacy risk* calculation depending on the ecosystem and the assessment need. For example, *data access* can be weighted higher than the current 33% in the *data value* calculation, for example, at 50%, which, in turn, would reduce the weights of the *data capabilities* and *data significance* to 25%. With weighted dependencies, the values would have to be calculated with an attribute specific function that includes the weights of the dependencies. This will naturally affect the weights of the assessable attributes and increases subjectivity, since anyone can tailor the model to produce certain kinds of results. This is not seen as a downside but instead as a benefit. Since there is no one singular truth or definition of privacy, the weighting of the attributes extends the potential use of the model.

The current two-dimensional dependency approach has a clear limit on the number of dependencies each attribute can have. One big aspect in future work is to overcome this limitation by devising a way to increase the number of dependencies for each attribute, either by using intermediate results or by applying a more complex dependency calculation model. Currently, the three dependencies are utilized by using two as direct dependencies and the third as an indirect dependency (e.g., *damage level* attribute in Figure 4.1 on page 79). This approach will be expanded so the initial guesses can also be applied for definable attributes to support and guide the assessment when necessary. A more complex dependency calculation would also make it easier to include security attributes in the model and to add more dependencies between the attributes. With added dependencies and security attributes, the accuracy is increased, and the scope of the assessment is extended.

To get the full extent of the model's benefits, a complete software suite would be ideal. Such software would greatly benefit from the broader dependencies between assets, which would enable a clear graphical representation of the ecosystem and the areas of risk. The dependency weight adjustment would be feasible only with the help of software. The software could also present the actual weight factors for assessable attributes with the new, changed dependency weights. Or the assessable attribute weights could be directly changed with the software, and the weights of the dependencies changed accordingly, which would require the adoption or development of a suitable algorithm for the task.

The specifications for such software are beyond the scope of the current research but will be addressed in future research. As of yet, it is unclear whether such software is feasible as a stand-alone application or if it would be better to include the approach in existing software, such as business process engines, where the privacy risk assessment could be done alongside the business process design.

9.2 The approach

The discussion about developing software from the model could be extended to cover the complete approach. This way, the user-friendliness of the approach may be enhanced, and the results of the first part could be also easily compared in the case of the iterative development process. It is straightforward to implement the process presented in Figure E.1 on page 262 as software.

Such software would require a modeling tool for creating layouts of the system and to map the information flows between them. In addition, it would require specific tools to map out the abstract tasks and functions to the abstract and functional models. In addition, the information that is transferred within the system would have to be mapped out with the PII 2.0 classification, for example, as it was shown in Table 7.4 on page 142.

The software would require a heuristics tool to offer an analysis based on the the layout, information transfers and mapping of tasks and functions to the abstract and functional models, including the information transferred and required. This way, the software could suggest some initial estimates for the model attributes or to guide in selecting them, for example, noticing that such a low value may not be possible because of the handled information type. The calculation of the information privacy risk would then be done with the software implementation of the model.

As a result, the ecosystem that is assessed can be presented in graphic form in which the risk values of different components can be highlighted with different colors to draw attention. Furthermore, it would be also possible to generate different views from different viewpoints: one view for customers with fewer details, one for executives with only the necessary details, one for software developers with full details and one view for lawyers with legislative aspects. The changes and the effects they had on risk values could be also documented within the presentation, even in interactive form. This way, the customers, for example, could see that the company's efforts have improved the protection of their private information. In addition, such documentation may suffice for the EU requirements to answer the need to conduct an assessment of the system and to show what issues there were and how they have been solved.

10 Conclusion

This thesis stated that the presented approach addresses the problem of assessing information privacy in a system or ecosystems that collect, maintain and process private information. To validate this statement, the research processes of the two contributions comprising the approach were presented in detail, evaluated and demonstrated in real-world contexts.

The first part of this thesis (starting on page 18) offered an overview of the research context of this thesis and introduced the goals, statement and limitations of the research, as well as detailed the research questions. In the same part, in the second section the state of art of privacy and especially information privacy was examined in close detail through the literature, real-world contexts in the form of projects this research was involved in and legislative definitions.

The second part of this thesis (starting on page 65) presented the research contributions. The approach was described as two contributions: (1) the *abstraction method* and the *iterative framework* (starting on page 67) and (2), *assessment model* (starting on page 77). These representations excluded the details of the research processes of both, which were later described in the evaluation section. This second contribution was concluded with a summary of the approach use combining both contributions.

In the third part (starting on page 99), the research principles and paradigms, principle of abstraction and generalization and design science research methodology were described. The creation of the research contributions and the evaluation of them as an integral part of the design processes were detailed in this part. The DSR methodology includes a separate activity in which the resulting research artifacts (contributions) are to be evaluated against the criteria that are to be devised in earlier stages of the research process. The criteria were distinct for each artifact (*abstraction method, iterative framework* and *assessment model*), and each artifact met the evaluation criteria, for the most part. To fully answer some criteria more extensive use of the different artifacts is required in different types of ecosystems.

This fourth part of the thesis consists of a discussion section (10) about the future development regarding the approach and this concluding remarks section. In the following sections, the research contributions are summarized, and how the research goals and research questions are answered with the devised approach is explained. Last, final remarks about this research are given.

10.1 Result: an approach for assessing information privacy risk

As a result and as a contribution of this thesis, an approach to be used in information privacy risk assessment as a mid-level tool for detecting deficiencies and risks in handling sensitive information within an information-centric system is presented. The approach is aimed at analysts assessing a system that manages and stores individuals' personal data , collected through unspecified or specific means. This approach answers the need introduced by the EU [22, 23] to strengthen the privacy protection of various systems. However, the approach presented in this thesis does not offer the means to strengthen the protection but detects the problems with information privacy in any system. The approach offers clear but indicative results detailing the lack of privacy protection in the components of any system and, thus, allows to focus resources on the system components with the highest risk.

With the approach the assessment is performed on three levels: abstract, functional and component. The approach consists of two separate parts.

Contribution 1: The first contribution can be used with two different scopes for conducting the assessment on the first two, abstract and function, levels. First, it can be used as an *abstraction method* to detect information flows and connectivity between components within the system to establish, for example, a common representation of multiple similar architectures. Second, the first contribution can offer valuable information about the systems under development while used iteratively during the development process as the contribution enables comparison of the results of different iterations and the effects of the changes that were made on each iteration. The first contribution includes all generic tasks and connections between them that exist in information-centric systems, can be used to map out the specific functions, detects PII usage within any system and helps to include PbD principles when used as an *iterative framework* (more details on pages 123 and 149).

Contribution 2: The second contribution, the model for information privacy risk assessment, conducts a more specific component-based assessment of the system. The first contribution forces an analysis of the system specifics and generates a lot of information about it, which is then used as inputs for the model. The model establishes a qualitative risk value for each component utilizing all aspects that affect information privacy; qualitative and quantitative attributes of information privacy are used. The model emphasizes the attributes that define information privacy from the user view and access to the information (more details on page 194) and answers the three challenges (re-usability [116], subjectivity [120] and speculative [126] results) inherent in risk assessment (more details on page 202).

Although the approach is meant for analysts, both parts of the approach were designed to be usable without expert knowledge. The current processes, however, still require some amount of expertise, but the future directions regarding this approach include the development of software based on the approach. The software would reduce the need for expert knowledge but also can introduce many other beneficial aspects, such as a clear graphical comparison of the results of the assessment to previous iterations or to other systems. These representations in the software could be presented with varying details for different focus groups (customer, executives, engineers and lawyers, for example) that view the issues from different perspectives.

10.2 To achieve the goals

In the current form, the approach, demonstrated through the Game Cloud example in section E on page 261, answers the four goals laid out in introduction of this thesis (on page 22):

1. The results are

    (a) clear because the first part, the *abstraction method* and the *iterative framework* (described on page 67), presents the results of the analysis as understandable models of the system including only the components and their respective information flows utilizing mapping of information usage as readable tables.

    (b) clear because the second part, the model (described on page 77), generates qualitative risk values for each component with specific limits and scales set for each initial value assessment.

    (c) reusable because the results of the first part allow comparing, for example, the effects of changes in the previous development iterations when used as an *iterative framework*.

    (d) reusable because the results of the first part used as an *abstraction method* can be used to establish a generalized representation of the details of multiple systems.

    (e) reusable because the results of the second part are directly comparable to other results obtained from the system was shown in Table E.6 on page 277. This way, the previous results can be reused within the development cycles.

    (f) reusable because the results of the information privacy risk analysis of systems with a similar scope but different methods and layouts can be compared. For example, using the second part makes it possible to compare the risk values of databases in two or more different systems.

2. The approach allows comparison of the results of the assessment because

   (a) the results that are generated with both parts are definite and leave no room for speculation.
   (b) the results of the first part clearly show the layout, and from the layout, the changes can be easily compared.
   (c) the results of the second part are easily compared because from the beginning (the initial estimates using the predefined scales) to the end of the assessment (the calculated results for information privacy risk, impact on privacy and attack likelihood), all values are qualitative on a scale from one to six, such as in Table 8.2 on page 163. These values offer a clear representation of the risks of the system components and leave no room for speculation.

3. Both parts of the approach were designed to be used without the need for expert knowledge, but as mentioned, with the current approach some expertise is required.

   (a) The first part requires going into the details of the system and requires the ability to understand the structures and behaviors of an information-centric system.
   (b) The second part is straightforward to use because of the understandable scales designed for each attribute, but knowledge about different aspects of information privacy is still required.
   (c) To comply with this requirement and to reduce the need for expert knowledge, a software implementation of the approach with detailed explanations of the aspects that are required to conduct the assessment is required.

4. Use of the approach does not require interruptions to system operations because it operates as a mid-level tool by utilizing only the details of the system. However, in complex systems it might be of use to capture traffic between different components if the documentation lacks detail. But this can be done without interrupting the system.

10.3 To answer the research questions

The result of this thesis, the approach, and the research done alongside the development answers the six research questions (RQ), laid out in section 1.4.2 on page 22, as follows:

RQ1: What attributes define information privacy? In order to answer this question, this thesis described many issues regarding information privacy, including its definitions, differences in understanding, risks in private information use and legislative stances, to use as the background to prove that the author is aware of the state of the art of privacy. The attributes of information privacy were found through the literature research on definitions of information privacy, research on privacy in three projects operating in different contexts (SGEM [57], MobiServ [24] and Game Cloud [25]) and research on legislative perceptions of privacy. The literature and legislative reviews offered the background details for deriving the definition for information privacy used in this thesis. The three projects brought up issues about information privacy in real-world contexts, which further backed up the previous research findings on the definition of information privacy. In order to establish the first part of the approach, two of the projects (SGEM and Game Cloud) were analyzed in detail for their information use, which gave the understanding of what aspects to account for in information privacy risk assessment. This resulted in a strong background for the development of the second part. The second part of the approach, the model, in addition to the background knowledge obtained through the projects, drew many influences from existing risk assessment methods on how to classify risk. In addition, the legislative definitions regarding privacy had a significant impact on the design. This way, all aspects of information privacy could be accounted for, and as a result, the model utilizes qualitative and quantitative attributes of information privacy in the risk value calculation. The attributes defining information privacy are comprised of properties of security, legal and data, and in this thesis they are (1) presented as foundations for contribution 2; the model on page 162, (2) used as attributes for contribution 2; the model in section 8.3.2 on page 170 and (3) used for evaluating contribution 2 in section 8.4.4 on page 203, in addition to the details offered by the contribution 1 research in sections 7.1.4 on page 117 and 7.2.4 on page 139. The attributes of information privacy are listed as follows in a general form:

- How, through which asset(s) and how easily information can be accessed and how long information is retained in a certain asset
- How identifiable the information is; does it have a direct link to an individual, an indirect link, a link that can be data mined or connected otherwise or completely unidentifiable.
- The means the asset withholding information can offer toward harming an identified individual directly or indirectly by opening up access to another system(s)
- The nature, quality, and quantity of the information and the potential of the information in misuse

RSQ1.1: What is the relation between the different attributes of private information? After a coherent understanding of information privacy was established, the model was developed. In the development process (described on page 155), it was necessary to research how the different attributes can be connected and how they related. Therefore, the process of establishing the model, a description of which starts on page 155, and the presentation of the model (the final version is shown as Figure 4.1 on page 79) are the answers to this research question.

RQ2: How to gather information about where to apply privacy protection? Both parts of the approach respond to this question. The first part of the approach forces to find out details about the system that show where information is stored and what type of information there is. The process of establishing the ecosystem (described on page 67) abstracts the ecosystem into the basic, generic tasks and functions and allows further analysis to be conducted based on the details found during the process. This information is then used as the background information for classifying and valuing the different components within the system. The model also contributes to this research question because it can be used as a tool to detect the actual components in which more privacy protection would be needed. The sub-question of this research question is answered by the first part of the method as both models, shown in generalized form in section 3 on page 67, generalize the tasks and functions within any information-centric system, including their connections. However, further testing in other ecosystems may be required to fully answer this sub-question as the models were used in only two contexts (the smart grid environment in SGEM [57] and the DGP in Game Cloud [25]).

RQ3: How to model information privacy in a user-friendly way? The modeling of information privacy alone was a time-consuming task that required lots of focus and logical reasoning. The developed model (Figure 4.1 on page 79) might not seem as user-friendly a representation for a person who is not involved in information systems research, is not an software engineer or is not an information privacy analyst with a programming background, for instance. But the model is a clear representation of how information privacy risk is defined, and with the clear scales defined for the initial estimates of assessable categories of the model and clear, non-speculative qualitative results the model offers, it is user-friendly for the focus groups for whom the model was designed. User-friendliness can be enhanced by developing software that utilizes the approach as a theoretical background as it was introduced in the introduction of this thesis (starting on page 25). This way, the requirements of user expertise may be reduced by offering extensive and brief details of the aspects included in the assessment with the software. Extensive explanations are required in order to give a full description and reasoning behind an issue. Brief explanations act as mere reminders for experts, as well as guidance for other users. However, the software would not be for just anyone as some expertise will be required in order to conduct the assessment. Therefore, this question is answered by stating that this version is suitable for the target groups and may fulfill their easy-to-use requirements, which, however, requires more field testing of the model.

RSQ3.1: How to create a legislation-agnostic model for information privacy? In the development of the model, it was seen as more beneficial to use the legislative definitions as guidelines in selecting appropriate values for the attributes than to include them directly in the model. This was because then the changes in legislation would not cause changes in the model, even though the changes in legislation may take a long time to come into effect (e.g., the process of the new EU regulation on data protection has been ongoing since 2011 [22, 23, 151]). Some definitions regarding information privacy, however, were included indirectly in the model development as the definition of a *close link* between an object or an event and a person [49] is used in determining the privacy level of the information. This is used as an inclusion of the stance of the current legislation in the valuation of the attributes, not as an integral part of the model. Therefore, to answer this question, legislative requirements and definitions of information privacy should be used more as guidelines in modeling information privacy as was done here.

RSQ3.2: How to achieve an ecosystem-agnostic model for information privacy? The case example of the Game Cloud development process described in section E on page 261 is one proof of the suitability of the approach for conducting information privacy assessment. This expands this question to concern the whole approach instead of only the model. According to the results of the Game Cloud (section E.3 on page 276), it can be concluded that the approach helped detect the flaws in the information management of the system, and to solve the problems, other means were necessary. Therefore, the approach and especially the model, are of use in information privacy assessment as a tool to detect the deficiencies in information privacy protection. However, the approach needs to be used in other information-centric contexts with different scope in order to fully answer this question.

10.4 Final remarks

The major contribution of this thesis is the modeling of information privacy. The model is an unprecedented way to model the human made, complex and multidisciplinary issue called (information) privacy, which is ironically understood and defined differently by its creators: us. It is continuously evolving with us, and now in the digital era, information privacy is involved in our everyday lives. Many systems collect and analyze the information we create with our actions in the real world or on the Internet. Multiple different kinds of uses, both legitimate and unauthorized (illegal), exist for the data. The legitimate means can enhance our life quality, help to save money or offer additional information. The unauthorized use of private information can destroy the life of an individual, perhaps not literally, but it is possible to ruin one's creditworthiness, for instance.

Legislators attempt to control illegal and other unauthorized use of private information with new regulations [22, 23], which is a step in the correct direction. But in order to know what to protect, it is imperative to know what can be classified as private information. New definitions, such as PII 2.0 [20], can help achieve the goal if these classifications are adopted by legislation.

Whereas the approach does not solve the problem with information privacy, nor does this thesis offer an universal definition of information privacy, it is a step ahead toward a solution to the problem of information privacy. The approach is usable in detecting the deficiencies in private information management, and the attributes and their connections presented in the model design can help in understanding information privacy in a new light.

The lesson that was learned during this research process, the analysis of information-centric systems, such as MobiServ and during the involvement in the design process of Game Cloud, is that information privacy is not solely defined by the data. It is a combination of people's attitudes toward privacy [8], legislative definitions [23, 48, 49] of privacy and private information [20] and finally, the actual data that has to be closely inspected in view of access and potential use (as was done in this research), including economics.

To finally conclude this thesis, although there are 1,000 eyes watching our every move, the world should not stand still and wait for the eyes simultaneously blink. Instead, the information these eyes can obtain must be limited with a Venetian blind. Some information is public, or it is identifiable but necessary for the service to operate as it is designed, and some information should be kept private. Limiting the rights of the observers is one issue, but another one is protecting the information. However, first, it is required to know what to protect and where to employ measures. The research presented in this thesis used extensively the definition of "what" in order to offer an approach to detect the "where." As a result, the world is not a better place, but the problems of this extent in the context of information privacy cannot be solved overnight, or as a result of a workload of four years by a one person. These problems require multiple iterations, and even then, the solution might be far away. Here, an ecosystem-agnostic approach for detecting information privacy risk was presented as a result of four years of painstaking research as the author's contribution. This approach is one step toward an universal solution to the problematic context of information privacy assessment.

References

[1] G. Orwell, *1984*. San Diego: Harcourt Brace Jovanovich, 1984.

[2] C. G. Reddick, A. T. Chatfield, and P. A. Jaramillo, "Public opinion on national security agency surveillance programs: A multi-method approach," *Government Information Quarterly*, vol. 32, no. 2, pp. 129 – 141, 2015. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0740624X15000246

[3] C. Bowden and D. Bigo, "The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights," *European Parliament*, 2013. [Online]. Available: http://www.europarl.europa.eu/RegData/etudes/note/join/2013/474405/IPOL-LIBE_NT(2013)474405_EN.pdf

[4] M. Duggan, N. B. Ellison, C. Lampe, A. Lenhart, and M. Mary, "Social Media Update 2014 - While Facebook remains the most popular site, other platforms see higher rates of growth," *Pew Research Center*, Jan. 2015. [Online]. Available: http://www.pewinternet.org/2015/01/09/social-media-update-2014/

[5] L. Rainie and J. Anderson, "The Future of Privacy," *Pew Research Center*, 2014. [Online]. Available: http://www.pewinternet.org/2014/12/18/future-of-privacy/

[6] B. Schneier, "The eternal value of privacy," *Wired.com*, May 2006. [Online]. Available: http://archive.wired.com/politics/security/commentary/securitymatters/2006/05/70886

[7] D. J. Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy," *Social Science Research Network Working Paper Series*, Jul. 2007. [Online]. Available: http://ssrn.com/abstract=998565

[8] M. Ortlieb, "The anthropologist's view on privacy," *Security Privacy, IEEE*, vol. 12, no. 3, pp. 85–87, May 2014.

[9] A. Cavoukian *et al.*, "Privacy by design: The 7 foundational principles," *Information and Privacy Commissioner of Ontario, Canada*, 2009.

[10] S. D. Warren and L. D. Brandeis, "The Right to Privacy," *Harward Law Review*, vol. 4, no. 5, pp. 193–220, December 1890.

[11] C. Brewster and D. Hine, "Legibility, privacy and creativity: Linked data in a surveillance society," in *Proceedings of the Society, Privacy and the Semantic Web–Policy and Technology Workshop (PrivOn 2013)*, vol. 11, 2013, p. 2014.

[12] U. Greveler, B. Justus, and D. Loehr, "Multimedia Content Identification Through Smart Meter Power Usage Profiles," Jan. 2012, Presented at Computers, Privacy and Data Protection (CPDP) 2012.

[13] T. Steimer, "The biology of fear- and anxiety-related behaviors," *Dialogues in Clinical Neuroscience*, vol. 4, pp. 231–249, 2002.

[14] P. Silvia, *Exploring the Psychology of Interest*, ser. Psychology of Human Motivation. Oxford University Press, 2006. [Online]. Available: https://books.google.fi/books?id=39YJCAAAQBAJ

[15] T. B. Kashdan, J. D. Elhai, and W. E. Breen, "Social anxiety and disinhibition: An analysis of curiosity and social rank appraisals, approach-avoidance conflicts, and disruptive risk-taking behavior," *Journal of anxiety disorders*, vol. 22, pp. 925–939, 2015.

[16] The Ministry of Economic Affairs, Agriculture and Innovation in Netherlands, "Slimme meter kan snel ingevoerd (Smart meters can be quickly entered, in Dutch)," Feb. 2011. [Online]. Available: http://www.energiebusiness.nl/2011/02/22/eerste-kamer-stemt-in-met-wetsvoorstellen-slimme-meter/

[17] S. Renner, M. Albu, H. van Elburg, C. Heinemann, A. Lazicki, L. Penttinen, F. Puente, and H. Sæle, "European Smart Metering Landscape Report, SmartRegions Deliverable 2.1," *SmartRegions*, Feb. 2011. [Online]. Available: http://www.smartregions.net/_ACC/_Components/ATLANTIS-DigiStore/Download.asp?fileID=253415&basketID=1522

[18] K.-L. Hui and I. Png, "The Economics of Privacy," EconWPA, Industrial Organization 0505007, May 2005.

[19] D. J. Solove, *Nothing to hide: The false tradeoff between privacy and security*. Yale University Press, 2011.

[20] P. M. Schwartz and D. J. Solove, "Reconciling personal information in the united states and european union," *102 California Law Review (2014 Forthcoming)*, 2014.

[21] E. Neill, *Rites of Privacy and the Privacy Trade: On the Limits of Protection for the Self.* McGill-Queen's University Press, 2001. [Online]. Available: https://books.google.fi/books?id=coMT_ZD4hZgC

[22] European Commission, "Proposal for a Regulation of The European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)," *Council of Europe*, 2012. [Online]. Available: http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf

[23] European Commission, “European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 - C7-0025/2012 - 2012/0011(COD)),” *Council of Europe*, Mar. 2014. [Online]. Available: http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2014-0212&language=EN

[24] “Mobiserv - An Integrated Intelligent Home Environment for the Provision of Health, Nutrition and Well-Being Services to Older Adults,” *Mobiserv*, 2014. [Online]. Available: http://www.mobiserv.info/

[25] “Pelipilvi / Game Cloud,” *Lappeenranta University of Technology*, 2014. [Online]. Available: http://www.lut.fi/gamecloud

[26] U.S. NIST, “Guidelines for Smart Grid Cyber Security: Volume 2 - Privacy and the Smart Grid,” *U.S. NIST*, August 2010. [Online]. Available: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

[27] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber security and privacy issues in smart grids,” *Communications Surveys Tutorials, IEEE*, vol. 14, no. 4, pp. 981–997, 2012.

[28] A. Martinez-Balleste, P. Perez-Martinez, and A. Solanas, “The pursuit of citizens’ privacy: a privacy-aware smart city is possible,” *Communications Magazine, IEEE*, vol. 51, no. 6, pp. 136–141, 2013.

[29] E. Toch, Y. Wang, and L. F. Cranor, “Personalization and privacy: a survey of privacy risks and remedies in personalization-based systems,” *User Modeling and User-Adapted Interaction*, vol. 22, no. 1-2, pp. 203–220, 2012. [Online]. Available: http://dx.doi.org/10.1007/s11257-011-9110-z

[30] D. Carluccio and S. Brinkhaus, “Smart Hacking For Privacy,” in *28th Chaos Communication Congress*, Dec. 2011. [Online]. Available: http://events.ccc.de/congress/2011/Fahrplan/events/4754.en.html

[31] M. Lisovich, D. Mulligan, and S. Wicker, “Inferring personal information from demand-response systems,” *Security Privacy, IEEE*, vol. 8, no. 1, pp. 11–20, 2010.

[32] A. Cavoukian, J. Polonetsky, and C. Wolf, “Smartprivacy for the smart grid: embedding privacy into the design of electricity conservation,” *Identity in the Information Society*, vol. 3, no. 2, pp. 275–294, 2010. [Online]. Available: http://dx.doi.org/10.1007/s12394-010-0046-y

[33] C. Efthymiou and G. Kalogridis, “Smart grid privacy via anonymization of smart metering data,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 238–243.

[34] F. Li, B. Luo, and P. Liu, “Secure information aggregation for smart grids using homomorphic encryption,” in *SmartGridComm, 2010 First IEEE International Conference on*, 2010, pp. 327–332.

[35] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1621–1631, 2012.

[36] F. Mármol, C. Sorge, O. Ugus, and G. Pérez, “Do not snoop my habits: preserving privacy in the smart grid,” *Communications Magazine, IEEE*, vol. 50, no. 5, pp. 166–172, 2012.

[37] J. Newman and J. Jerome, “Press Start To Track: Privacy And The New Questions Posed By Modern Videogame Technology.” *American Intellectual Property Law Association’s Quarterly Journal*, vol. 42, no. 4, 2014.

[38] B. Bostan, “Player motivations: A psychological perspective,” *Computers in Entertainment (CIE)*, vol. 7, no. 2, p. 22, 2009.

[39] G. van Lankveld, P. Spronck, J. Van den Herik, and A. Arntz, “Games as personality profiling tools,” in *Computational Intelligence and Games (CIG), 2011 IEEE Conference on*, Aug 2011, pp. 197–202.

[40] M. Birk and R. L. Mandryk, “Control your game-self: Effects of controller type on enjoyment, motivation, and personality in game,” in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, ser. CHI ’13. New York, NY, USA: ACM, 2013, pp. 685–694. [Online]. Available: http://doi.acm.org/10.1145/2470654.2470752

[41] E. Boyle, T. M. Connolly, and T. Hainey, “The role of psychology in understanding the impact of computer games,” *Entertainment Computing*, vol. 2, no. 2, pp. 69–74, 2011.

[42] K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G. Voelker, and S. Savage, “Click trajectories: End-to-end analysis of the spam value chain,” in *Security and Privacy (SP), 2011 IEEE Symposium on*, May 2011, pp. 431–446.

[43] P. Jäppinen, J. Laakkonen, P. Heinilä, and H. van den Heuvel, “Mobiserv D6.2: Final Coordination and Communication system prototype,” 2013. [Online]. Available: http://www.mobiserv.info/wp-content/uploads/2013/01/MOBISERV_D6.2.pdf

[44] G. Bella, P. Jäppinen, and J. Laakkonen, “The Challenges behind Independent Living Support Systems,” in *Springer Lecture Notes in Computer Science*, August 2014, iSSN:1611-3349.

[45] J. Laakkonen, S. Annala, and P. Jäppinen, "Abstracted architecture for smart grid privacy analysis," in *Social Computing (SocialCom), 2013 International Conference on*, Sept 2013, pp. 637–646.

[46] J. Laakkonen, J. Parkkila, P. Jäppinen, and J. Ikonen, "Continuous development of gamecloud with privacy by design." *International Journal on Information Technologies & Security*, vol. 6, no. 4, pp. 51–64, Nov. 2014, ISSN:1313-8251.

[47] A. Guadamuz and D. Cabell, "Analysis of UK/EU Law on Data Mining in Higher Education Institutions," *EU Law on Data Mining in Higher Education Institutions (January 15, 2013)*, 2013.

[48] The European Parliament and Council, "Directive 95/46/EC. Directive on protection of individuals with regard to the processing of personal data and on the free movement of such data," 1995.

[49] European Union Agency for Fundamental Rights, "Handbook on European data protection law," *Council of Europe*, 2014. [Online]. Available: http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law

[50] P. L. Campbell, *A classification scheme for risk assessment methods.* USDOE, Aug 2004. [Online]. Available: http://www.osti.gov/scitech/servlets/purl/925643

[51] P. De Hert, D. Kloza, D. Wright, K. Wadhwa, G. Hosein, and S. Davies, "Recommendations for a privacy impact assessment framework for the European Union," European Commission - Directorate General Justice, Tech. Rep., 2012.

[52] D. Wright, K. Wadhwa, P. De Hert, and D. Kloza, "A Privacy Impact Assessment Framework for data protection and privacy rights Deliverable D1," European Commission - Directorate General Justice, Tech. Rep., 2011.

[53] J. I. Hong, J. D. Ng, S. Lederer, and J. A. Landay, "Privacy risk models for designing privacy-sensitive ubiquitous computing systems," in *Proceedings of the 5th Conference on Designing Interactive Systems: Processes, Practices, Methods, and Techniques*, ser. DIS '04. New York, NY, USA: ACM, 2004, pp. 91–100. [Online]. Available: http://doi.acm.org/10.1145/1013115.1013129

[54] A. Hevner and S. Chatterjee, *Design Research in Information Systems: Theory and Practice*, 1st ed. Springer Publishing Company, Incorporated, 2010.

[55] Klein, Heinz K. and Myers, Michael D., "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems." *MIS Quarterly*, vol. 23, no. 1, pp. 67–93, March 1999.

[56] F. Gilbert, “Privacy v. Data Protection. What is the Difference?” Oct 2014. [Online]. Available: http://www.francoisegilbert.com/2014/10/privacy-v-data-protection-what-is-the-difference/

[57] CLEEN Oy, “The final report of the Smart Grids and Energy Markets (SGEM) research program,” 2014, http://www.cleen.fi/en/sgem. [Online]. Available: http://www.cleen.fi/en/sgem

[58] J. Laakkonen, J. Parkkila, P. Jäppinen, J. Ikonen, and A. Seffah, “Incorporating Privacy into Digital Game Platform Design: The What, Why, and How,” *IEEE Security & Privacy*, vol. 14, no. 4, pp. 22–32, July-Aug 2016. [Online]. Available: http://dx.doi.org/10.1109/MSP.2016.87

[59] J. Laakkonen, P. Jäppinen, and A. Seffah, “An Assessment Model for Information Privacy Risk,” vol. 0, no. 0, pp. 0–0, - 2015, unpublished/Research report.

[60] United Nations, “The Universal Declaration of Human Rights,” *United Nations*, 2015. [Online]. Available: http://www.un.org/en/documents/udhr/index.shtml

[61] J. D. Moss, “Galileo’s letter to christina: Some rhetorical considerations,” *Renaissance Quarterly*, vol. 36, no. 4, pp. pp. 547–576, 1983. [Online]. Available: http://www.jstor.org/stable/2860733

[62] C. M. Graney, “The Inquisition’s Semicolon, Punctuation, Translation, and Science in the 1616. Condemnation of the Copernican System,” 2014. [Online]. Available: http://arxiv.org/ftp/arxiv/papers/1402/1402.6168.pdf

[63] S. Sutherland, *Irrationality: The enemy within.* Constable and Company, 1992.

[64] D. David, J. Schnur, and A. Belloiu, “Another search for the ḧotc̈ognitions: Appraisal, irrational beliefs, attributions, and their relation to emotion,” *Journal of Rational-Emotive and Cognitive-Behavior Therapy*, vol. 20, no. 2, pp. 93–131, 2002. [Online]. Available: http://dx.doi.org/10.1023/A%3A1019876601693

[65] A. Maslow, *Motivation and personality.* New York: Harper and Row, 1987.

[66] E. J. Bloustein, “Privacy as an aspect of human dignity: An answer to dean prosser,” *NYUL Rev.*, vol. 39, p. 962, 1964.

[67] J. Rule and G. Greenleaf, *Global Privacy Protection: The First Generation.* Edward Elgar, 2010. [Online]. Available: https://books.google.fi/books?id=L2I2Lrf1BeYC

[68] *OECD e-Government Studies OECD e-Government Studies: Finland 2003*, ser. OECD e-Government Studies. OECD Publishing, 2003. [Online]. Available: https://books.google.fi/books?id=sl7_d4_3kOwC

[69] M. Berry, “Communicating the Cultural Richness of Finnish Hiljaisuus (Silence),” in *11th International CercleS Conference*, 2010. [Online]. Available: https://www.utu.fi/en/units/tse/units/unit-for-languages-and-business-communications/Development_projects/Documents/communicating_finnish_silence.pdf

[70] P. Stahlberg, G. Miklau, and B. N. Levine, “Threats to privacy in the forensic analysis of database systems,” in *Proceedings of the 2007 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD ’07. New York, NY, USA: ACM, 2007, pp. 91–102. [Online]. Available: http://doi.acm.org/10.1145/1247480.1247492

[71] S. Afroz, A. Islam, J. Santell, A. Chapin, and R. Greenstadt, “How privacy flaws affect consumer perception,” in *Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on*, June 2013, pp. 10–17.

[72] F. Siddiqui, S. Zeadally, C. Alcaraz, and S. Galvao, “Smart grid privacy: Issues and solutions,” in *Computer Communications and Networks (ICCCN), 2012 21st International Conference on*, 2012, pp. 1–5.

[73] S. Sullivan. (2011, Sept.) Trends: From Phishing to "Man-in-the-Middle" Phishing. F-Secure. [Online]. Available: http://www.f-secure.com/weblog/archives/00002245.html

[74] H. Gao, J. Hu, T. Huang, J. Wang, and Y. Chen, “Security issues in online social networks,” *Internet Computing, IEEE*, vol. 15, no. 4, pp. 56–63, July 2011.

[75] M. Lisovich and S. Wicker, “Privacy concerns in upcoming residential and commercial demand-response systems,” in *2008 Clemson University Power Systems Conference*. Clemson University, Mar. 2008. [Online]. Available: http://www.truststc.org/pubs/332.html

[76] B. J. Murrill, E. C. Liu, and R. M. Thompson, “Smart meter data: Privacy and cybersecurity,” 2012, CSR (Corporate Social Responsibility) Report for Congress.

[77] Organization for Economic Cooperation and Development, “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,” 2010. [Online]. Available: http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[78] European Parliament and Council, “Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC,” 2009.

[79] Finnish Council of State, “Valtioneuvoston asetus 66/2009 sähköntoimitusten selvityksestä ja mittauksesta (Government decree 66/2009 on settlement and metering of electricity deliveries, in Finnish),” 2009.

[80] R. Anderson and S. Fuloria, “On the security economics of electricity metering,” in *WEIS 2010, The Ninth Workshop on the Economics of Information Security*, Jun. 2010.

[81] A. Bleicher, “Privacy on the Smart Grid,” *IEEE Spectrum*, Oct. 2010. [Online]. Available: http://spectrum.ieee.org/energy/the-smarter-grid/privacy-on-the-smart-grid

[82] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda, “Privacy for smart meters: Towards undetectable appliance load signatures,” in *SmartGridComm, 2010 First IEEE International Conference on*, 2010, pp. 232–237.

[83] Z. Erkin, J. Troncoso-pastoriza, R. Lagendijk, and F. Perez-Gonzalez, “Privacy-preserving data aggregation in smart metering systems: an overview,” *Signal Processing Magazine, IEEE*, vol. 30, no. 2, pp. 75–86, 2013.

[84] X. Fang, S. Misra, G. Xue, and D. Yang, “Managing smart grid information in the cloud: opportunities, model, and applications,” *Network, IEEE*, vol. 26, no. 4, pp. 32–38, 2012.

[85] F. Luo, Z. Y. Dong, Y. Chen, Y. Xu, K. Meng, and K. P. Wong, “Hybrid cloud computing platform: The next generation it backbone for smart grid,” in *Power and Energy Society General Meeting, 2012 IEEE*, 2012, pp. 1–7.

[86] A.-H. Mohsenian-Rad and A. Leon-Garcia, “Coordination of cloud computing and smart power grids,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 368–372.

[87] S. Rusitschka, K. Eger, and C. Gerdes, “Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain,” in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*, 2010, pp. 483–488.

[88] A. Frey, J. Hartig, A. Ketzel, A. Zinkernagel, and H. Moosbrugger, “The use of virtual environments based on a modification of the computer game Quake III Arena® in psychological experimenting,” *Computers in Human Behavior*, vol. 23, no. 4, pp. 2026 – 2039, 2007. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0747563206000112

[89] C. A. Anderson, N. Ihori, B. J. Bushman, H. R. Rothstein, A. Shibuya, E. L. Swing, A. Sakamoto, and M. Saleem, “Violent video game effects on aggression, empathy, and prosocial behavior in eastern and western countries: A meta-analytic review,” *Psychological Bulletin*, 2010.

[90] C. A. Anderson and B. J. Bushman, “Effects of violent video games on aggressive behavior, aggressive cognition, aggressive affect, physiological arousal, and prosocial behavior: A meta-analytic review of the scientific

literature," *Psychological science*, vol. 12, no. 5, pp. 353–359, 2001. [Online]. Available: http://pss.sagepub.com/content/12/5/353.abstract

[91] S. M. Grüsser, R. Thalemann, and M. D. Griffiths, "Excessive computer game playing: Evidence for addiction and aggression?" *Cyberpsy., Behavior, and Soc. Networking*, vol. 10, no. 2, pp. 290–292, 2007. [Online]. Available: http://dblp.uni-trier.de/db/journals/cbsn/cbsn10.html#GrusserTG07

[92] N. L. Carnagey, C. A. Anderson, and B. J. Bushman, "The effect of video game violence on physiological desensitization to real-life violence," *Journal of Experimental Social Psychology*, vol. 43, no. 3, pp. 489–496, 2007.

[93] B. D. Bartholow, B. J. Bushman, and M. A. Sestir, "Chronic violent video game exposure and desensitization to violence: Behavioral and event-related brain potential data," *Journal of Experimental Social Psychology*, vol. 42, no. 4, pp. 532–539, 2006.

[94] A. K. Przybylski, E. L. Deci, C. S. Rigby, and R. M. Ryan, "Competence-impeding electronic games and players' aggressive feelings, thoughts, and behaviors." *Journal of Personality and Social Psychology*, vol. 106(3), pp. 441–457, Mar 2014.

[95] L. T. Graham and S. D. Gosling, "Personality Profiles Associated with Different Motivations for Playing World of Warcraft," *Cyberpsychology, Behavior, and Social Networking*, vol. 16, no. 3, pp. 189 – 193, March 2013.

[96] G. Chittaranjan, J. Blom, and D. Gatica-Perez, "Mining large-scale smartphone data for personality studies," *Personal and Ubiquitous Computing*, vol. 17, no. 3, pp. 433–450, 2013. [Online]. Available: http://dx.doi.org/10.1007/s00779-011-0490-1

[97] M. Herland, T. M. Khoshgoftaar, and R. Wald, "A review of data mining using big data in health informatics," *Journal of Big Data*, vol. 1, no. 1, pp. 1–35, 2014.

[98] S. Fernando, S. Perera *et al.*, "Empirical analysis of data mining techniques for social network websites," *Compusoft*, vol. 3, no. 2, p. 582, 2014.

[99] M. A. Russell, *Mining the Social Web: Data Mining Facebook, Twitter, LinkedIn, Google+, GitHub, and More*. " O'Reilly Media, Inc.", 2013.

[100] H. Saarijärvi, C. Grönroos, and H. Kuusela, "Reverse use of customer data: implications for service-based business models," *Journal of Services Marketing*, vol. 28, no. 7, pp. 529–537, 2014.

[101] C. McCue, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*. Elsevier Science, 2014. [Online]. Available: https://books.google.fi/books?id=re1MBAAAQBAJ

[102] E. McCallister, T. Grance, and K. Scarfone, *Guide to protecting the confidentiality of personally identifiable information*. National Institute of Standards and Technology, U.S. Department of Commerce, Apr. 2010, nIST Special Publication 800-122.

[103] S. Lohiya and L. Ragha, "Privacy preserving in data mining using hybrid approach," in *Computational Intelligence and Communication Networks (CICN), 2012 Fourth International Conference on*. IEEE, 2012, pp. 743–746.

[104] A. Sachan, D. Roy, and P. Arun, "An analysis of privacy preservation techniques in data mining." in *ACITY (3)*. Springer, 2012, pp. 119–128.

[105] J. Chopra and S. Satav, "Privacy preservation techniques in data mining," *9th April*, 2013.

[106] N. I. Hussain, B. Choudhury, and S. Rakshit, "A novel method for preserving privacy in big-data mining," *International Journal of Computer Applications*, vol. 103, no. 16, 2014.

[107] J. Adebayo and L. Kagal, "A privacy protection procedure for large scale individual level data," in *Intelligence and Security Informatics (ISI), 2015 IEEE International Conference on*. IEEE, 2015, pp. 120–125.

[108] E. Emam, "Risk-based de-identification of health data," *IEEE Security & Privacy*, vol. 8, no. 3, pp. 64–67, 2010.

[109] Y.-A. de Montjoye, L. Radaelli, V. K. Singh *et al.*, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science*, vol. 347, no. 6221, pp. 536–539, 2015.

[110] S. E. Coull, F. Monrose, M. K. Reiter, and M. Bailey, "The challenges of effectively anonymizing network data," in *Conference For Homeland Security, 2009. CATCH'09. Cybersecurity Applications & Technology*. IEEE, 2009, pp. 230–236.

[111] L. F. Pau, "Privacy Management Contracts And Economics, Using Service Level Agreements (Sla)," Erasmus Research Institute of Management (ERIM), ERIM is the joint research institute of the Rotterdam School of Management, Erasmus University and the Erasmus School of Economics (ESE) at Erasmus University Rotterdam, ERIM Report Series Research in Management ERS-2005-014-LIS, 2005.

[112] C-SIG SLA subgroup, "Cloud Service Level Agreement Standardisation Guidelines," *European Commission*, 2014. [Online]. Available: http://ec.europa.eu/digital-agenda/en/news/cloud-service-level-agreement-standardisation-guidelines

[113] The European Parliament and Council, "Directive 2009/72/EC concerning common rules for the internal market in electricity and repealing Directive 2003/54/EC," 2009.

[114] U.S. NIST, "Guidelines for Smart Grid Cyber Security: Volume 1 - Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements," *U.S. NIST*, August 2010. [Online]. Available: http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-7628

[115] CEN-CENELEC-ETSI Smart Grid Coordination Group, "Smart grid reference architecture," November 2012. [Online]. Available: http://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf

[116] M. Schumacher, *Security patterns: integrating security and systems engineering*, ser. Wiley series in software design patterns. John Wiley & Sons, 2006.

[117] M. Sajko, K. Rabuzin, and M. Bača, "How to calculate information value for effective security risk assessment," *Journal of Information and Organizational Sciences*, vol. 30, no. 2, pp. 263–278, 2006.

[118] U. Hahn, K. Askelson, and R. Stiles, "Global technology audit guide 5: Managing and auditing privacy risk," The Institute of Internal Auditors, Tech. Rep., 2006.

[119] SIEMENS Insight Consulting, "The Logic behind CRAMM's Assessment of Measures of Risk and Determination of Appropriate Countermeasures," Oct. 2005, whitepaper. [Online]. Available: http://www.cramm.com/files/techpapers/CRAMM%20Countermeasure%20Determination%20and%20Calculation.pdf

[120] B. Suh and I. Han, "The IS risk analysis based on a business model," *Information & Management*, vol. 41, no. 2, pp. 149 – 158, 2003. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0378720603000442

[121] S. Hariri, G. Qu, T. Dharmagadda, M. Ramkishore, and C. Raghavendra, "Impact analysis of faults and attacks in large-scale networks," *Security Privacy, IEEE*, vol. 1, no. 5, pp. 49–54, Sept.-Oct. 2003.

[122] N. R. Mead and T. Stehney, "Security quality requirements engineering (SQUARE) methodology," Carnegie Mellon, Tech. Rep. 4, 2005.

[123] B. C. Johnson, "National Security Agency (NSA) INFOSEC Assessment Methodology (IAM)," SystemExperts Corporation, Tech. Rep., 2004. [Online]. Available: www.systemexperts.com/assets/tutors/NSAIAM.pdf

[124] C. Alberts, A. Dorofee, J. Stevens, and C. Woody, "Introduction to the octave approach," Tech. Rep., 2003.

[125] E. Paintsil, "A model for privacy and security risks analysis," in *New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on*, may 2012, pp. 1–8.

[126] S. C. Payne, “A guide to security metrics,” *SANS Institute Information Security Reading Room*, 2006.

[127] G. Iachello and G. D. Abowd, “From privacy methods to a privacy toolbox: Evaluation shows that heuristics are complementary,” *ACM Trans. Comput.-Hum. Interact.*, vol. 15, no. 2, pp. 8:1–8:30, Jul. 2008. [Online]. Available: http://doi.acm.org/10.1145/1375761.1375763

[128] A. Cavoukian, *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act*. Information and Privacy officier Ontario, 2005.

[129] S. La and B. Choi, “The role of customer affection and trust in loyalty rebuilding after service failure and recovery,” *The Service Industries Journal*, vol. 32, no. 1, pp. 105–125, 2012.

[130] T. Kuosmanen, “Helsingissä panostetaan etäluentaan (Helsinki invests in smart metering, in Finnish),” *Lukema, MITOX OY:n Sidosryhmälehti*, vol. 1, Jan. 2008, www.mitox.fi/pdf/Lukema0801.pdf.

[131] A. Sievi, “Vattenfallin automaattinen sähkönmittaus Suomessa (Automatic electricity metering of Vattenfall in Finland, in Finnish),” in *Adato energy seminar*, 2008.

[132] K. Fakhroutdinov, “Dependency in UML,” 2013. [Online]. Available: http://www.uml-diagrams.org/dependency.html

[133] K. Reddy, H. Venter, M. Olivier, and I. Currie, “Towards privacy taxonomy-based attack tree analysis for the protection of consumer information privacy,” in *Privacy, Security and Trust, 2008. PST ’08. Sixth Annual Conference on*, 2008, pp. 56–64.

[134] I. Loloei, H. Shahriari, and A. Sadeghi, “A model for asset valuation in security risk analysis regarding assets’ dependencies,” in *Electrical Engineering (ICEE), 2012 20th Iranian Conference on*, May 2012, pp. 763–768.

[135] J. Iivari, “A paradigmatic analysis of information systems as a design science,” *Scandinavian Journal of Information Systems*, vol. 19, no. 2, p. 5, 2007.

[136] K. Peffers, T. Tuunanen, M. Rothenberger, and S. Chatterjee, “A design science research methodology for information systems research,” *J. Manage. Inf. Syst.*, vol. 24, no. 3, pp. 45–77, Dec. 2007. [Online]. Available: http://dx.doi.org/10.2753/MIS0742-1222240302

[137] G. Walsham, *Interpreting Information Systems in Organizations*, 1st ed. New York, NY, USA: John Wiley & Sons, Inc., 1993.

[138] E. Monteiro and O. Hanseth, “Social shaping of information infrastructure: on being specific about the technology,” *Information technology and changes in organizational work*, pp. 325–343, 1996.

[139] B. Latour, “On actor-network theory: a few clarifications,” *Soziale welt*, pp. 369–381, 1996.

[140] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, “Eppa: An efficient and privacy-preserving aggregation scheme for secure smart grid communications,” *Parallel and Distributed Systems, IEEE Transactions on*, vol. 23, no. 9, pp. 1621–1631, 2012.

[141] D. Fry, “Circumventing access controls under the digital millennium copyright act: Analyzing the securom debate,” *Duke L. & Tech. Rev.*, p. 1, 2009.

[142] L. Renkema, “TOP 10 MOST PIRATED GAMES OF 2008,” *Torrentfreak.com*, Dec. 2008. [Online]. Available: https://torrentfreak.com/top-10-most-pirated-games-of-2008-081204/

[143] R. Ritchie, “The true cost of free-to-play games,” *imore.com*, Mar. 2013. [Online]. Available: http://www.imore.com/true-cost-free-play

[144] V. Panusuwan and P. Batlagundu, “Privacy risk assessment case studies in support of SQUARE,” Tech. Rep., 2009. [Online]. Available: www.sei.cmu.edu/reports/09sr017.pdf

[145] Z. Tang, Y. J. Hu, and M. D. Smith, “Protecting online privacy: Self-regulation, mandatory standards, or caveat emptor zhulei tang,” in *Proceedings of the Fourth Annual Workshop on Economics and Information Security*, 2005.

[146] Y. Bi and A. Jamalipour, “Two-phase demand response based on privacy-preserving billing for smart grid,” in *Wireless Communications Signal Processing (WCSP), 2012 International Conference on*, 2012, pp. 1–6.

[147] P. Jäppinen and J. Porras, “Analyzing the attributes of personalization information affecting storage location,” in *International Conference on E-Society*. IADIS, Jun 2003.

[148] S. Abu-Nimeh and N. Mead, “Privacy risk assessment in privacy requirements engineering,” in *Requirements Engineering and Law (RELAW), 2009 Second International Workshop on*, Sept. 2009, pp. 17–18.

[149] J. Defeo and J. Juran, *Juran’s Quality Handbook: The Complete Guide to Performance Excellence 6/e*. McGraw-Hill Education, 2010.

[150] L. Beaudoin and P. Eng, “Asset valuation technique for network management and security,” in *Data Mining Workshops, 2006. ICDM Workshops 2006. Sixth IEEE International Conference on*, Dec. 2006, pp. 718–721.

[151] European Commission, “Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals withregard to the processing of personal data and on the free movement of such data (General Data Protection Regulation),” *Council of Europe*, Nov.

2013. [Online]. Available: http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&mode=XML&reference=A7-2013-0402&language=EN

[152] SGEM, “Smart Grids and Energy Markets, Work Package 4; Active Customer, Customer Interface and ICT,” 2011.

[153] J. Laakkonen, T. Kallonen, K. Heikkinen, and J. Porras, *Implementation of UMSIC Group Management Service*, ser. Acta Universitatis Lappeenrantaensis 440: Selected Papers from FRUCT 8. Lappeenranta University of Technology, Lappeenranta, Acta Universitatis Lappeenrantaensis, Finland, 2011, pp. 55–65.

[154] J. Laakkonen, T. Kallonen, K. Heikkinen, and J. Porras, “Introducing UMSIC Middleware Services,” in *Proceedings of the 6th Seminar of Finnish-Russian University Cooperation in Telecommunications (FRUCT)*, November 2009, pp. 53–60.

[155] J. Laakkonen, T. Kallonen, K. Heikkinen, and J. Porras, “Implementation of UMSIC Group Management Service,” in *Proceedings of the 8th Seminar of Finnish-Russian University Cooperation in Telecommunications (FRUCT)*, April 2010, pp. 87–96.

[156] J. Laakkonen, T. Kallonen, K. Heikkinen, and J. Porras, “Usability of Music for Social Inclusion of Children,” *Vehicular Technology Magazine, IEEE*, vol. 5, no. 1, pp. 55 –61, March 2010.

[157] J. Laakkonen, T. Kallonen, K. Heikkinen, and J. Porras, “System and Architecture requirements for UMSIC middleware,” in *Wireless World Research Forum 23rd Meeting*, October 2009, pp. 516–519.

[158] T. Kallonen, J. Laakkonen, J. Porras, K. Heikkinen, M. Myllykoski, P. Paananen, J. C. Read, A. Rantalainen, and H. Hedberg, “Introducing UMSIC scenarios,” in *Wireless World Research Forum 23rd Meeting*, October 2009, pp. 511–515.

Part V

Appendices

This part contains all appendixes of this thesis. Appendix A presents the time line of the research. Appendix B presents a summarization of the publications related to this thesis. Appendix C presents the layout of the environment developed in MobiServ project. Appendix D presents the seven guidelines of design science research. In Appendix E a case study is presented detailing and presenting the use of the two components of the contribution as a complete approach in development of a new DGP system. Appendix F presents detailed results of Game Cloud assessment with the *assessment model.* Appendix G presents a questionnaire and its results about Smart Meter implementations sent to the Finnish distribution system operators. Appendix H lists the dependency matrices of the second *assessment model* prototype.

A Research process time line

How this research is set on a time line from the beginning of the studies (fall 2011) until the finishing of this thesis, is portrayed in Figure A.1. The figure displays the involvement in three projects, the writing process of the five publications and the milestones of the two parts of the research. Each publication in Figure A.1 is summarized in Appendix B.

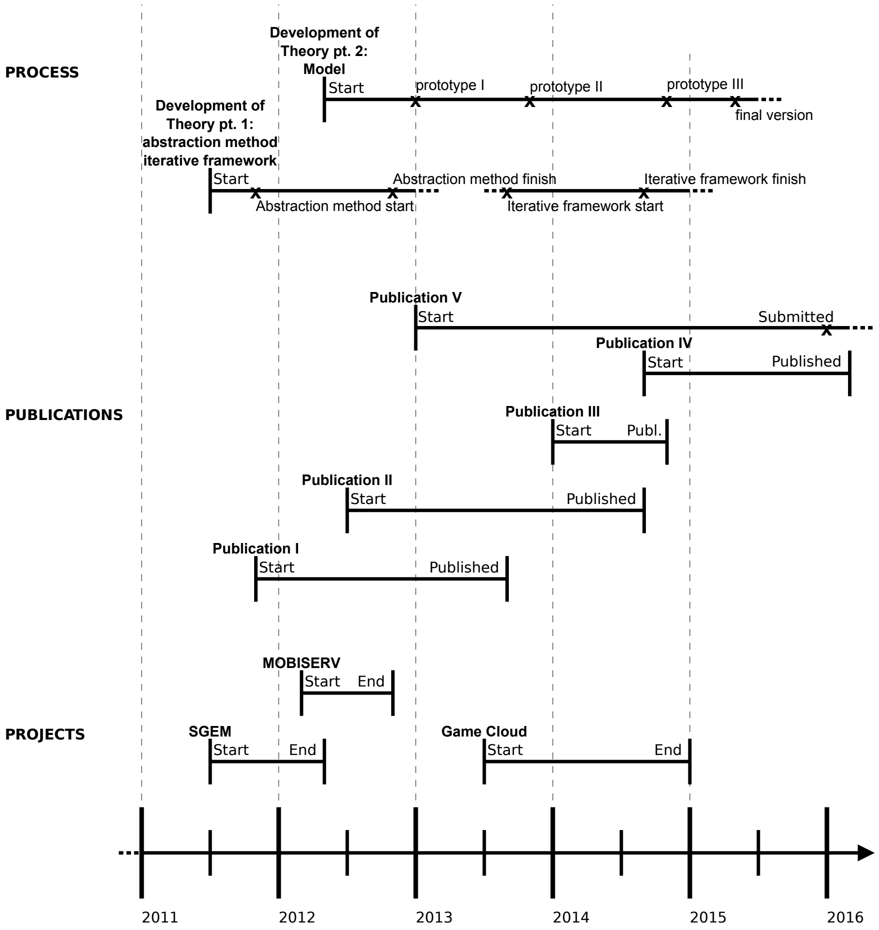


Figure A.1: Time line of projects, publications and research process

Descriptions of the three projects, SGEM [57], MobiServ [24] and Game Cloud [25], are presented on the time-line and the involvement of the author are described as follows:

- SGEM project aimed to develop international practices for smart grid solutions which can be demonstrated using Finnish R&D infrastructure. The project consisted of following areas: developing architectures and distribution infrastructures, management and operation practices, understanding of active resources and market integration and new business models. The author of this thesis was involved in mapping out and research of generic privacy issues in existing Finnish smart grid implementations. The research was done in SGEM WP4 [152]. The project was funded by Cleen Oy[55].

- MobiServ project aimed to develop a platform for supporting independent living of elderly utilizing various devices, middleware and services. The platform consists of a social companion robot, wearable smart clothes and a smart home environment. The author of this thesis was involved in WP6 [43] to conduct a risk assessment on the smart home environment and its external components. MobiServ was an EU funded project (Seventh framework programme).
- Game Cloud project aimed to establish a new type of DGP that enables content transfers among different games that increases marketplace visibility, immersion and promotion of different games. All of this is established with a specialized ontology that requires a lot of data collected from the games and the end-user's actions which in turn is beneficial not only for the players but for the game developers and marketing as well. The author of this thesis was involved in the layout design and development process of the platform as an information privacy analyst to assess risks to privacy of the end-users in order to enable more privacy preserving platform. Game Cloud was funded by TEKES[56], the Finnish Funding Agency for Innovation.

This research originated to address the needs of the SGEM project [57, 152] for assessing privacy issues in various smart grid implementations. During the project the first part of the theory was devised and it was the basis for **Publication I** [45].

Next, in the MobiServ project [24, 43] the need for more in-depth privacy assessment was noted as the existing risk assessment method [116] was found to be inadequate. This, in addition to the proposed EU regulation [22] introduced the need as well as offered motivation for devising a new way to assess privacy. As a result, the development and research process for the model was started. Also, **Publication II** [44] that presents one aspect of the project, the difficulty of requirements elicitation, was written. After this, the writing process of **Publication V** [59] was started. In this publication the model is described in full detail.

After these two projects focus was shifted to the model and in the beginning of Game Cloud project [25], contribution 1 (the *abstraction method* and the *iterative framework*) was included into the process. Both contributions were used in the development of Game Cloud DGP as tools for detecting flaws in privacy protection and personal data use. The development and analysis process of Game Cloud

[55] http://www.cleen.fi

[56] http://www.tekes.fi

provided feedback also to the development of both contributions. As a result, **Publication III** [46] was written and the experience gained in the project was used to improve **Publication V** [59]. Furthermore, **Publication IV** [58] was started at the end of the Game Cloud project. **Publication IV** [58] is the first publication to describe the utilization of both contributions, the complete approach.

B Summaries of own publications

Some of the research presented in this thesis has been published and at the time of writing one article is waiting to be published. The author of this thesis is the main author in all publications, except in **Publication II** [44], to which the author contributed the summarized findings of the project's security and privacy analysis.

Here the content, scope and contribution of each publication is described. Some of the text in this thesis is taken from these publications, with small or large modifications. Each section, in which the text from a publication is used, is mentioned at the beginning of the section detailing from which publication the text is taken from.

B.1 Published

Four articles have been published; two conference articles (**Publications I** [45] and **II** [44]) and two journal articles (**Publications III** [46] and **IV** [58]). First part of the theoretical background (contribution 1), the *abstraction method* (**Publication I** [45]) and the *iterative framework* (**Publication III** [46]), is published and demonstrated through two project examples. **Publication II** [44] describes the challenges of ILS system development and requirements engineering with notes about security and privacy, involving a brief introduction about the groundwork for this thesis: the MobiServ security analysis [43]. The fourth article (**Publication IV**) [58] presents the complete approach that is the combined use of **Publication III** [46] (contribution 1) and **Publication V** [59] (contribution 2) in a development project.

Publication I: Abstracted architecture for smart grid privacy analysis

> *Jussi Laakkonen, Salla Annala, and Pekka Jäppinen. Abstracted architecture for smart grid privacy analysis. In Social Computing (SocialCom), 2013 International Conference on, pages 637–646, Sept 2013.*

This publication describes the process of establishing an architecture offering a clear, information-centered overview into an existing environment by applying methods of abstraction and generalization principle. This process is the first step of the *abstraction method* presented in this thesis. In this publication, a reference architecture of smart grid layouts in Finland is established from the results of a questionnaire that was sent to electricity distributors in Finland by utilizing the *abstraction method*. The analysis is done by establishing specific abstract task layout that includes the information flows between tasks. This is then continued with an analysis of the environment's functions and information usage and tasks are mapped to the defined functions. The information this analysis offered and forced to gather from the environment enabled a creation of a reference architecture of smart grid layouts in Finland. The reference architecture is applicable for privacy analysis at high level as it clearly portrays the information transferred between different actors of the environment. The description of the process and the *abstraction method* is the main contribution of this publication. The secondary contribution is the analysis done on the basis of the established reference architecture.

Publication II: The Challenges behind Independent Living Support Systems

> *Giampaolo Bella, Pekka Jäppinen, and Jussi Laakkonen. The challenges behind independent living support systems. In Active Media Technology, volume 8610 of Lecture Notes in Computer Science, pages 464–474. Springer International Publishing, 2014.*

This publication is built on the requirements elicitation of MobiServ project [24] postulating the challenges of gathering requirements for ILS systems. The main contribution is the discussion about ILS system requirements and the difficulties in deploying such system. In addition, some specific socio-technical issues in ILS systems, such as multiple participants in the system and their roles, are analyzed and discussed in this paper. But more importantly, this publication briefly presents the highlights of the MobiServ security (and partially privacy) analysis. This paper and the detailed analysis [43] presented the need for a separate privacy analysis method in systems similar to ILS collecting vast amounts of data from the user's activities to guarantee that security is built to protect not only the system but the system's users, too.

Publication III: Continuous development of Game Cloud with Privacy by Design

> *Jussi Laakkonen, Janne Parkkila, Pekka Jäppinen and Jouni Ikonen. Continuous Development of Game Cloud with Privacy by Design. International Journal on Information Technologies and Security, November, 2014, vol. 6, no. 4, p. 51-64, ISSN 1313-8251.*

In this publication the process presented in the **Publication I** [45] is used as an *iterative framework* in the development of a new system, a digital game platform. With this adaptation of the *abstraction method*, privacy by design principles were incorporated into the design in the early stages to ensure that privacy of the users, the players, is guaranteed. This publication presents the analysis that was conducted by using multiple iterations of the *iterative framework* in the development of the Game Cloud layout. Next, based on the analysis results, the changes that were made to the ecosystem are presented. The effects of the changes are demonstrated with another analysis iteration using the *iterative framework*. As an *iterative framework* the *abstraction method* proved to be very useful in the development process as it offered details about the interactions of different ecosystem components. In addition, the *iterative framework* brought up details about information usage that was not visible from the design documents. This information forced the developers to seek out more safe ways to handle the information collected by the Game Cloud. This publication shows that the task-based layout used in **Publication I** [45] is applicable in analyzing information-centric environments. The main contribution of this publication regarding the work presented in this thesis is that the *abstraction method* can be used as a versatile *iterative framework* in development of a new system without adding overhead to the development process. This publication proves that the *abstraction method* is valid for performing the initial information-centric assessment for environments and ecosystems, where the information is collected from the end-users or from their devices. As a secondary contribution, this publication details the process of using the *abstraction method* as an *iterative framework* in incorporating privacy by design into a new system design.

Publication IV: Incorporating privacy into digital games platform design. The What, Why and How?

> *Jussi Laakkonen, Janne Parkkila, Pekka Jäppinen, Jouni Ikonen and Ahmed Seffah. Incorporating privacy into digital games platform design. The What, Why and How? IEEE Security & Privacy, August, 2016, vol. 14, no. 4, p. 22-32, ISSN 1540-7993*

This publication is direct continuum for the result presented in **Publication III** [46] and offers supplementary details of the design process. As a main contribution this publication portrays the steps of the design process with the approach presented in this thesis. In this publication the combined process of *iterative framework* (**Publication III** [46]) and model (**Publication V** [59]) use is presented through the example of Game Cloud development. First in this paper the opportunities and possibilities opened by the gaming data are discussed, introducing also the reasons for collecting gaming data. This is continued by a postulation of the potential privacy risks in using gaming data also presenting the potential difficulties in gaming data privacy definitions. These benefits, both positive and negative, are then summarized and the impacts of each are presented. Next the two components of the approach, abstraction framework [46] and the model [59], are briefly explained and the approach is put into practice. The process of Game Cloud development is used to demonstrate the use of the approach and the publication is concluded with a discussion about the benefits of the approach and how it affected the Game Cloud design. In the conclusion it is also discussed about how the use of the approach can benefit the digital game platform design in general.

Other publications: In addition to these there is one closely related publication not included in this thesis. The publication presents and analyzes three different cloud computing approaches for smart grid invoice calculation from customer privacy point of view.

> *Jussi Laakkonen, Pekka Jäppinen and Jari Porras. Smart Grid invoice privacy in the Cloud, Wireless World Research Forum 31th meeting, 21-24 October 2013 in Vancouver, Canada, 2013.*

Also, there is a wide number of publications [153, 154, 155, 156, 157, 158] related to previous work among UMSIC (Usability of Music for the Social Inclusion of Children) project[57] (funded by EU 7th framework programme). These publications describe the different aspects of the UMSIC project development and are not related to this research. There is a total of seven publications (one journal, one book chapter and five conference articles).

B.2 Waiting to be published

One manuscript is awaiting for publication, which is submitted to appropriate journal in 2017/2018. The article (**Publication V** [59]) that presents the model in full detail.

Publication V: An Assessment Model for Information Privacy Risk

> *Jussi Laakkonen, Pekka Jäppinen and Ahmed Seffah. An Assessment Model for Information Privacy Risk, waiting for submission.*

This manuscript introduces and describes the model in full detail. The difficulty of measuring and even defining privacy or information privacy is introduced in this paper through many examples from real world systems and academic papers. In this publication the background for the model development and design is presented leading to specific requirements, constraints and attributes for the model. The presented model (contribution 2 in this thesis) establishes a qualitative value for information privacy risk utilizing many different quantitative and qualitative attributes of information privacy. The model and all of its information privacy attributes and connections between these attributes are detailed in this manuscript, including the detailed description about how to use the model to calculate information privacy risk with a three step approach. In addition to presenting the model, the model is evaluated by (1) calculating the weight emphasis of each attribute

[57] http://www.netsoundsproject.eu/know-how/good-practices/umsic-usability-music-social-inclusion-children

with an Ishikawa diagram, (2) analyzing the requirements laid for the model, (3) comparing the model to the existing approaches and (4) presenting the economic and development process related benefits (privacy by design). In addition to these a case study of Game Cloud is presented to demonstrate the model use. This case study is the first iteration round of the *iterative framework* process presented in **Publication III** [46]. In this publication the layout of Game Cloud is analyzed in more detail and the information privacy risk value is calculated for each component of the Game Cloud ecosystem. The sole contribution of this publication is the introduction of the model, its foundations and use.

C MobiServ environment layout

The layout of the environment that was developed in MobiServ (EU FP7) project (see Appendix A) is shown in Figure C.1. The main components of the MobiServ system, labeled with roman numerals in Figure C.1 are:

I. PRU (Physical Robotic Unit) is a robot unit operating on battery power and offering the main user interface to the systems inside the residence. PRU offers assistance for the user as well as notifies about certain triggered events (e.g., eating, drinking and sleeping). PRU is the main place for storing user information and information is transferred over Wireless Local Area Network (WLAN). PRU is a combination of a tablet computer for notifications and control, database for health data storage and a web camera for visual interaction via, e.g., Skype.

II. SHACU (Smarthome Automation and Communication Unit) shares the Internet connection over WLAN to other devices and, therefore, has a WLAN Access Point. SHACU acts as a gateway for controlling home automation (IV) as it is a permanent element in the residence with fixed power supply and should be on at all times. The nutrition detection computer ORU (Optical Recognition Unit) is contained in SHACU and detection is done with the help of a video camera in the residence. The video itself is not stored into SHACU but the analyzed and anonymized result of each detected action is.

III. WHSU (Wearable Health Status Unit) is the wearable health detection unit that constantly monitors the health status of the user. WHSU contains sensors and data loggers which collect valuable information about the health status that is used to generate health alarms for doctors and caretakers. The collected data is stored into the PRU (I.) using either a wired connection or Bluetooth. The sensors communicate with loggers by using Body Area Network connections.

IV. Home automation system is responsible of managing of the generic household devices (locks, lights, temperature, etc.) and is controlled by other devices in the residence. The connection is going via SHACU (II.) and the home automation is mainly controlled by the user through PRU (I.).

V. Sensors in the residence comprises of temperature and motion sensors. The sensors are connected to the home automation system (IV.) and they provide state information about various parts of the residence.

VI. Internet access point handles all communication between the residence and outer world. Access to the device is restricted and all access from outside is rejected, only maintenance access within residence via LAN (Local Area Network) or VPN (Virtual Private Network) is allowed.

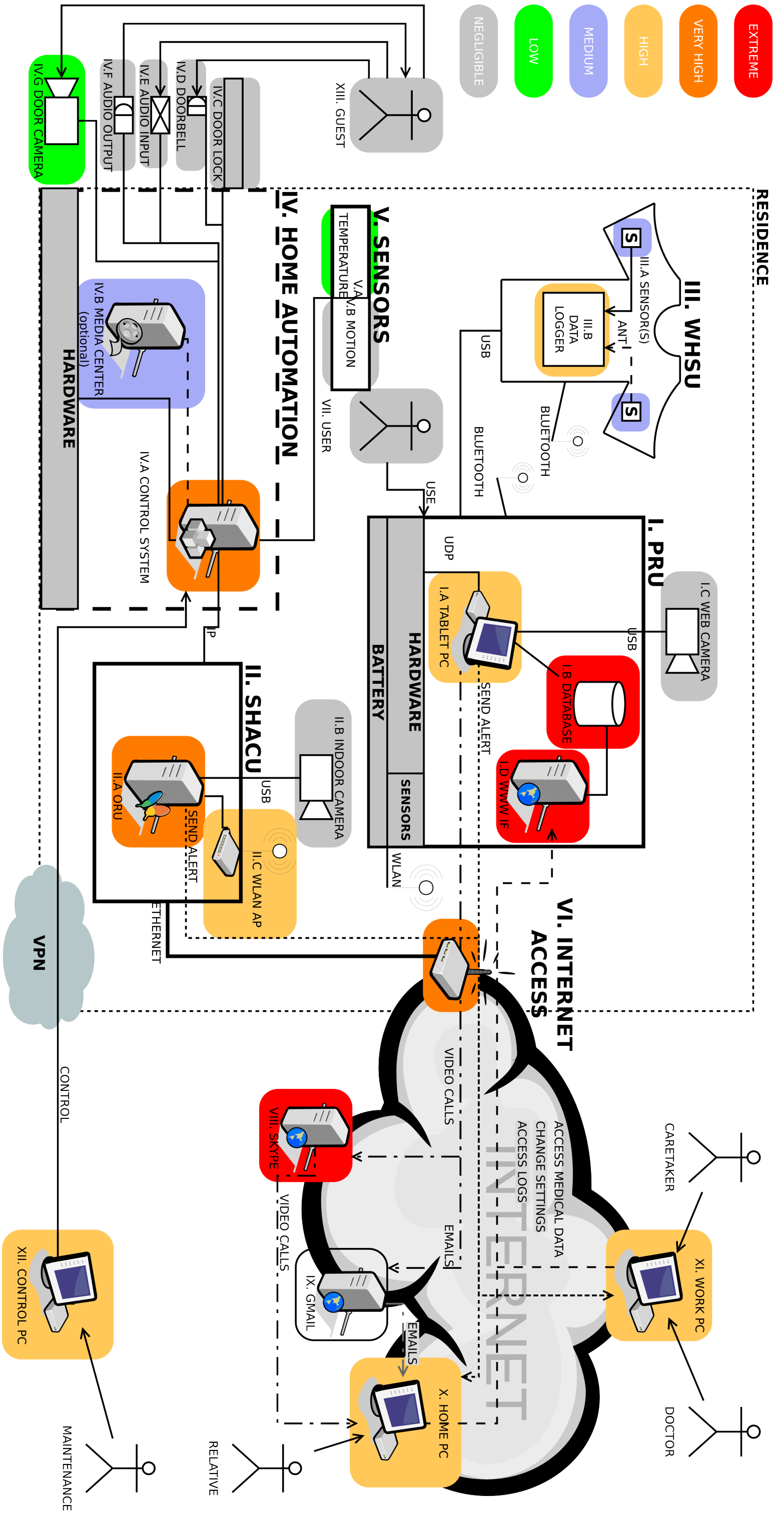


Figure C.1: MobiServ system layout and the results of component based security analysis

D Guidelines for design science research

Guidelines for conducting design science research [54] are described as a set of seven points presented in Table D.1.

Table D.1: The seven guidelines for design science research [54]

Guidelines (G)	Description
G1: Design as an Artifact	Design science research must produce a viable artifact in the form of a construct, a model, a method, or an instantiation.
G2: Problem relevance	The objective of design science research is to develop technology-based solutions to important and relevant business problems.
G3: Design evaluation	The utility, quality, and efficacy of a design artifact must be rigorously demonstrated via well-executed evaluation methods.
G4: Research contributions	Effective design science research must provide clear and verifiable contributions in the areas of the design artifact, design foundations, and/or design methodologies.
G5: Research rigor	Design science research relies upon the application of rigorous methods in both the construction and evaluation of the design artifact.
G6: Design as a search process	The search for an effective artifact requires utilizing available means to reach desired ends while satisfying laws in the problem environment.
G7: Communication of research	Design science research must be presented effectively to both technology-oriented and management-oriented audiences.

E Contribution use: the approach presented through a case study

In this section a case study with the approach is demonstrated through Game Cloud example. The basic iterative process with the abstraction has been presented in previous research [46] and here the full process is presented in full detail. **Publication IV** [58] also presents the highlights of this process. First, the complete approach is presented using Game Cloud development process as an example and then the detailed description of the process is presented.

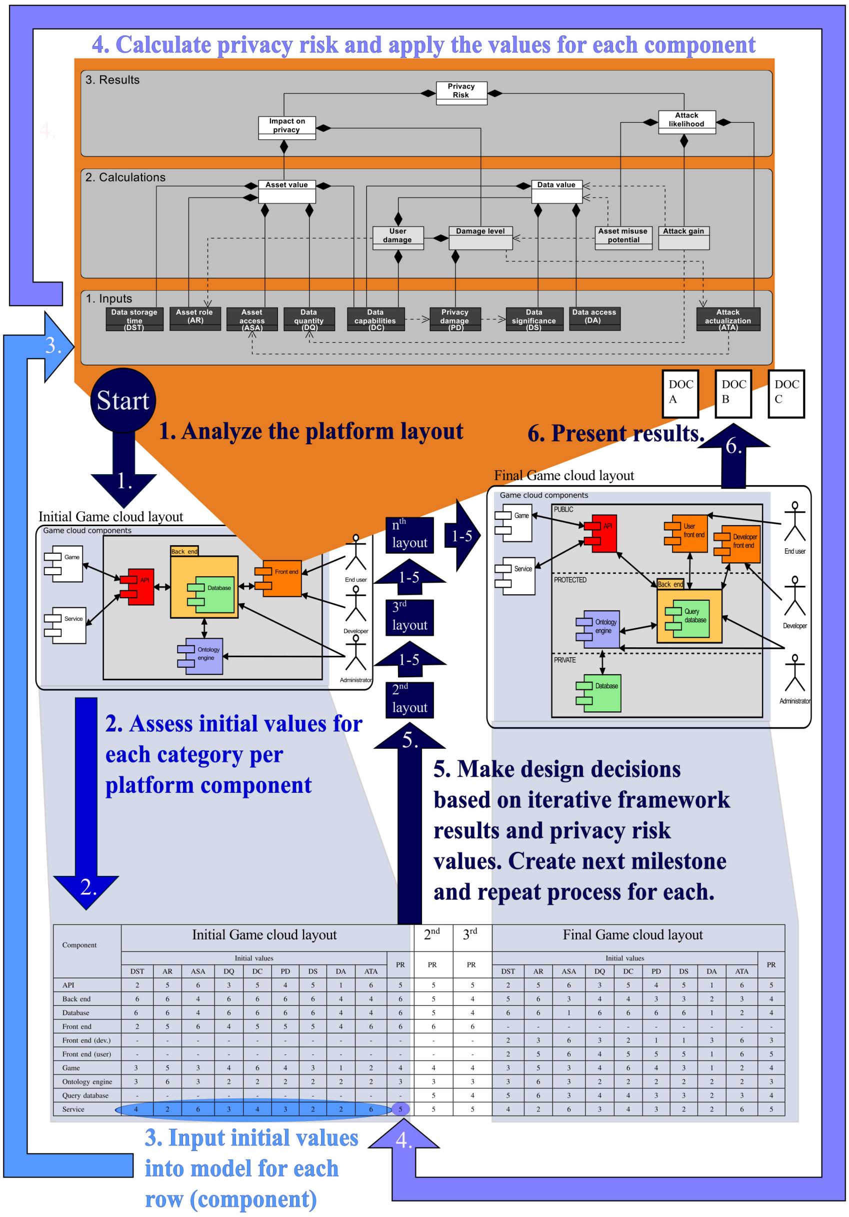
Most parts of the descriptions and tables of the development process (section E.2) are taken from **Publication III** [46]. Here these descriptions are extended since due to article length limitations, privacy risk calculation was excluded from the publication. Parts of the overview (section E.1) and the view on economical impacts (section E.3) are taken from author's fourth publication [58].

E.1 The process overview

In sections 3 and 4 the both parts of the contribution of this thesis were presented. The first part, the *abstraction method* and the *iterative framework* is a tool for detecting information flows within the system at abstract and functional level. The first part can be used for establishing an overview of the system and a mapping of system's information usage from two perspectives. This tool forces to analyze the system thoroughly and the information obtained during the process is useful for the second part of the the approach: the model for information privacy assessment. The model has a more specific scope: it is developed for assessing each component within the system separately by utilizing all attributes affecting information privacy. As a result of,the model produces qualitative risk values for each component that enable focusing of resources to high risk components.

The complete approach offers details of the system on three different levels. The approach is a mid-level tool that does not force to go through all small details but it does not give a mere approximate either. Instead, the approach operates in the middle and does not solve the problem but helps in solving problems that are found during the process of use. This was the case with Game Cloud development process in which the results of the approach were used to support design decisions to build a more privacy preserving DGP.

The process of using the complete approach in Game Cloud development process is illustrated in Figure E.1 on the next page. The topmost part of the figure illustrates the model and its attributes, the middle part details the first and last milestone of the Game Cloud development and the lowest part of the figure presents the selected initial and resulting risk values for each component in the platform.



Component	Initial Game cloud layout										2nd	3rd	Final Game cloud layout									
	Initial values									PR	PR	PR	Initial values									PR
	DST	AR	ASA	DQ	DC	PD	DS	DA	ATA				DST	AR	ASA	DQ	DC	PD	DS	DA	ATA	
API	2	5	6	3	5	4	5	1	6	5	5	5	2	5	6	3	5	4	5	1	6	5
Back end	6	6	4	6	6	6	6	4	4	6	5	4	5	6	3	4	4	3	3	2	3	4
Database	6	6	4	6	6	6	6	4	4	6	5	4	6	6	1	6	6	6	6	1	2	4
Front end	2	5	6	4	5	5	5	4	6	6	6	6	-	-	-	-	-	-	-	-	-	-
Front end (dev.)	-	-	-	-	-	-	-	-	-	-	-	-	2	3	6	3	2	1	1	3	6	3
Front end (user)	-	-	-	-	-	-	-	-	-	-	-	-	2	5	6	4	5	5	5	1	6	5
Game	3	5	3	4	6	4	3	1	2	4	4	4	3	5	3	4	6	4	3	1	2	4
Ontology engine	3	6	3	2	2	2	2	2	2	3	3	3	3	6	3	2	2	2	2	2	2	3
Query database	-	-	-	-	-	-	-	-	-	-	5	4	5	6	3	4	4	3	3	2	3	4
Service	4	2	6	3	4	3	2	2	6	5	5	5	4	2	6	3	4	3	2	2	6	5

Figure E.1: Illustration of the process of using the approach. Inputs for the model are dark gray color. Front ends in Game Cloud layout are orange color, databases with green color, API with red color, Back end with yellow color and Ontology engine with blue color.

The six steps of the approach: The six steps illustrated in Figure E.1 are a part of one iteration of use. The steps are:

1. Analyze the platform for information flows between components and map the abstract tasks and functionalities of the components utilizing a single iteration of the *iterative framework* [46].
2. Assess each component in the platform utilizing information from the first step to select appropriate initial values for the nine model input (assessable) attributes using predefined value-matrices detailed in section 4 (also in [59]).
3. Input the selected initial values for privacy risk calculation. Input the values separately for each component.
4. Use the model to calculate privacy risk separately for each component. The process for calculating privacy risk is detailed in section 4 of this thesis (also in [59]). Apply and document the risk value for each component.
5. Analyze the results and make design decisions based on the information privacy risk value and the information gained from utilizing the *iterative framework*. Create next milestone, an improved version of the platform layout and repeat the process starting from step one. If the results are satisfactory and significant improvements are made, proceed to step six.
6. Present the results by establishing a layout with information transfers, mapping of tasks, functions and components including their calculated information privacy risk values. Create a documentation of the development process, changes, improvements and establish a final analysis of the last layout.

E.2 Game Cloud development process

Here the process of Game Cloud development using the approach is detailed. Because Game Cloud has been extensively used as a basis for many parts of research in this thesis as well as demonstration of the research artifacts, some parts of the following descriptions simply refer to these previous results and descriptions. This process consists of an initial assessment (i.e., round zero) of the ecosystem and five separate rounds of development: two first rounds detail the establishment of abstract and functional models from the initial layout of Game Cloud and the last three rounds present the actual development rounds.

E.2.1 Round zero: Initial assessment

The analysis of Game Cloud ecosystem began by researching the components belonging to system and the information they transfer and withhold.

Components: The assets (software components) in the initial layout of the Game Cloud ecosystem, portrayed in Figure 8.5 on page 206, are: (1) a game linked to the system, (2) a third party service, (3) one API for the games and services, (4) one back end containing the database (5) of all game data, (6) an ontology engine for processing game data and (7) a front end for end users (players) and developers. The human actors are: (8) end users, (9) developers and (10) administrator of the Game Cloud system. All of these were further detailed in section 7.1.4 on page 117 describing the second iteration of *iterative framework* development process.

Information used and transferred: Using the three levels of the PII 2.0 [20] the information usage can be analyzed in much more detail. The information that is used and exchanged in the Game Cloud is presented in Table E.1 with the PII 2.0 classification. The table categorizes the data types for the analysis and these data types are used later in functional model construction and in each system illustration. The hashes (H) and queries (Q) did not exist in the previously presented Table 7.4 on page 142 of the *iterative framework* research process description as they were absent from the initial designs of Game Cloud. The complete query based information retrieval was added in the later versions of Game Cloud design. In this initial assessment these are not accounted for, but because these are used widely in the following development rounds, all information that is transferred in Game Cloud is presented in this one table to avoid further confusion.

Table E.1: Full details of data exchanged in Game Cloud

Data	Description	Category
P_{id}	Player identification, including the credentials.	identified
P_{PII}	The additional player information (e.g., email).	identified
P_{rdata}	Raw player data sent by the device.	identifiable
P_{pdata}	Processed player data returned for the player and utilized by the games.	identifiable / non-identifiable
G_{id}	Game identification.	non-identifiable
S_{id}	Service identification.	non-identifiable
H	Hash matching a query to retrieve player/game/service data.	non-identifiable
Q	A specific query to get player/game/service data.	identifiable

A layout of the Game Cloud ecosystem: This information was enough to add the information presented in Table E.1 to the flows of Figure 8.5 on page 206. As a result the layout is shown as Figure 7.5 on page 142.

E.2.2 Round one: establishment of abstract model

The abstraction of the ecosystem was done along the DSR development process of the contribution 1, *the iterative framework* in 7.2.4 on page 139. The more detailed process of establishing the abstract model was presented earlier in the same section.

The information obtained through previous initial assessment resulted in creation of an abstract model, shown in Figure 7.8 on page 148. The tasks within Game Cloud, detailed on page 143, were mapped to the components according to Table on page 144.

E.2.3 Round two: establishment of functional model

As a continuum for the abstract model creation the functional model of the real-world operations within Game Cloud was established. This was described earlier as a part of the research process description of the contribution 1, *iterative framework* in Game Cloud application context in section 7.2.4 on page 139.

The functional model was presented in Figure 7.7 on page 147. The model presents the connections between the real-world operations, which are presented from information flow perspective. The functions that were found were described on page 145 and mapping of them to the components of Game Cloud was presented in Table 7.7 on page 147.

The functional division enabled to map the information exchanged in the Game Cloud (Table E.1) to the functionalities according to Table 7.6 on page 146. P_{id} is contained within P_{PII} and is linked to both P_{rdata} and P_{pdata}. All the G_{id}s of the games the end-user has and the S_{id}s of the services the player uses are also contained within P_{PII} and are linked to the P_{id}. Hashes (H) are used for retrieving the correct identifiable queries (Q) for returning the requested information. Therefore, Q is connected to H but the connection to H cannot be extracted from any Q.

Using these details information privacy risk of the software components could be assessed with the model. Only the assets (from 1 to 7 in Figure 8.5 on page 206) were assessed since human actors (from 8 to 10 in Figure 8.5 on page 206) are not considered as part of the *assessment model*. In Table 8.25 on page 206 the initial values for level one attributes of the model (presented in Figure 4.1 on page 79) and the resulting values of the third level attributes as well as the result of assessment, the privacy risk, are shown.

This initial layout was already assessed in the demonstration of the *assessment model* and the results are shown in section 8.5 on page 205. The assessment was conducted with the *software prototype*. The values for the attributes as well as the results of the calculation iterations for each asset are detailed in Appendix F. The initial values for all the 9 assessable attributes were selected according to the tables 4.2 (on 87), 4.3 (on 88) and 4.4 (on 89) for each asset and are shown in Table 8.25 on page 206. The rest of the assessment was conducted with the *software prototype* which follows the three steps of model use and calculates the values using the dependency matrices detailed in section 4.3.1 on page 86.

The initial values for the attributes were estimated along the privacy assessment process detailed in earlier research [46], in which the existing *abstraction method* [45] proved to be useful. Also, the depth of knowledge obtained from the ecosystem with the help of the *abstraction method* offered enough information to select appropriate initial values for each component.

To demonstrate the initial value selection, the values for API (3 in Figure 8.5 on page 206) were selected using following criteria (selection of values for all components was previously detailed on page 206):

- Data storage time: API has to store the data only for the time it is transferred to the back end for processing and storing. Therefore, the initial value is 2 according to Table on page 89.
- Asset role: API plays an important role in Game cloud as all end user activities are sent through it. However, the system can function without API for short periods of time. Therefore, the initial value is 5 according to Table 4.2 on page 87.
- Asset network: API resides in public network for easy access without access restrictions. Therefore, the initial value is 6 according to Table 4.2 on page 87.
- Data quantity: API contains small amount of data at any time and stores no user data. The data contained is identifiable to an individual. Therefore, the initial value is 3 according to Table 4.4 on page 89.
- Data capabilities: Since the gaming data can be used for multiple different purposes [37], some of which can harm individual's privacy the data has to be protected. It might be possible to connect pseudonymized data to an identity of an individual. Therefore, the initial value is 5 according to Table 4.3 on page 88.
- Data identifiability: API contains information (gaming data and service data) that can be later connected to an identity of an individual. The data itself contains only an pseudo identifier and, therefore, the data is identifiable and the value is 2.
- Privacy damage: If API leaks the transferred data it might be possible to harm individuals' privacy as the data contains an identifier that can be connected to an identity of an individual. Therefore, the initial value is 5 according to Table 4.3 on page 88.

- Data significance: Gaming data is important for Game cloud system as it generates information based on the end users actions for third parties and developers [46]. Also, gaming data is important for the users in order to gain more achievements and to be able to transfer content between different games. Therefore, the initial value is 5 according to Table 4.3 on page 88.
- Data access: API delivers the data directly to and from the Back end and stores none of it. No external user access is available to API and all data is transferred via software components (game, service and back end). Therefore, the initial value is 1 according to Table 4.2 on page 87.
- Attack actualization: Since API resides in public network and is open for access it is bound to be attacked or at least tried for vulnerabilities by unauthorized users. Therefore, the initial value is 6 according to Table 4.4 on page 89.

These values resulted a information privacy risk value of 5 for the API. Since the gaming data that is transferred through API is pseudonymized the value is justified. API poses a high risk to privacy of an individual as it is publicly accessible but is not with the highest risk. The risk values as well as likelihood and impact values of the components of Game Cloud were presented in Table 8.26 on page 212 and were discussed on page 212.

From these results it is evident that the components which either maintain and withhold private information or offer an access to that information had the biggest risk values. The level of identifiability has a big impact on privacy and likelihood is largely affected by the accessing possibilities and the nature and the accuracy of information that may be accessed through that particular component. Therefore, it was important to improve the back end (4) and database (6) in order to reduce their risk values. In addition, the extent of information (player and developer) that could be accessed through the front end (7) was problematic because of two separate user groups. The risk value of API might be hard to reduce as it should stay public and it is built for transferring the collected and analyzed information in both ways, in and out of the system. The risk values of games (1) and services (2) is impossible to affect, hence they are out of control of the Game Cloud development team, and the risks of these can be only noted. Also, it seems that the processing engine of Game Cloud is designed well as the risk is low to begin with. The modification of the system might, however, pose changes to its risk value.

E.2.4 Round three: introducing query database

The initial version was simple and elegant but was found out to be highly problematic since many types of information, including P_{PII}, was accessed by many different actors through one front end from the back end as shown in Figure 7.5.

It would need rigorous rights management from both the front and back end to secure this version.

In the first round of the analysis it was noticed that the database in the back end contained all information about the users (PII) resulting in high impact value. Also, the access was not fully restricted from the public networks, resulting in attack likelihood of 5. The possibility to access the back end (4) externally was kept mainly because the administrator has to have an access to the internal functions for maintenance purposes. This approach was decided to be unsafe from both security and privacy perspective. The attacker breaking through the administrator backdoor would be able to collect all information about the players by attacking just one component through an existing access route.

To make the administrator access more ineffective and to allow separation of the identities from the actual data the combined component of back end (4) and database (5) was re-designed and split it into two. This involved using a query database that can be securely accessed by every component inside Game Cloud. The query database contains only the hashes (H), which are used to access the actual information through the ontology engine. No end-user related information is stored in the query database, nor can it be accessed directly. The hash-based approach was also beneficial for the game and the service developers; the only thing the developers had to know and to pass to the API (5) calls of the Game Cloud is the correct hash (H). No other query (Q) has to be made. Also, the front end (7) design is more straightforward as the calls to information are plain hashes. This was seen also as a measure to help to reduce the risk value of the front end (7).

Each hash (H) corresponds to a single event inside one particular game or an personal item or information piece. The result also depends on the identification (player, game and/or service) that is used with the query (Q). Without knowing the hash (H) no information can be retrieved through the back end (4) in which the query database is contained in. With random hashes (H) the results are just bits and pieces of information from some player, game or service, depending on the access type. Or, more likely, nothing will be returned if the hash (H) does not match to any query (Q).

This approach made it possible to anonymize the information using the hashes. All the raw and personal information of the players, games and services is stored in another database, which is accessible only via the ontology engine using the aforementioned hashing approach. The first analysis resulted in a revised layout and changes in information exchange that was presented in Figure 7.9 on page 151.

The only changes this layout modification introduced to tasks (Table 7.5 on page 144) and functionalities (Table 7.7 on page 147) were the added processing (4) and storing (5) tasks and player data processing functionality (4) for the query database. Therefore, the tasks or the functionalities are almost the same as previously.

Next, the new layout was analyzed for information privacy risk. In following the query database, being inside back end (4) has exactly the same initial values as well as the results as the back end. Query database is not, therefore, treated as an additional component but as a part of back end (4). The results of assessment are shown in Table E.2 and the complete detailed results, including the initial values are shown in Appendix F on page 284.

Table E.2: The results of the third round information privacy risk assessment on the second Game Cloud ecosystem layout

Component Attribute	1.	2.	3.	4.	5.	6.	7.
Impact on privacy	4	5	5	5	5	3	5
Attack likelihood	3	4	5	4	4	2	6
Privacy risk	**4**	**5**	**5**	**5**	**5**	**3**	**6**

These results show that the query based solution had a positive impact in reducing the risk values of back end (4) and database (5). The changes that were made to the back end (4) resulted in lower likelihood of an attack because the route was now more challenging and not as rewarding. In addition, because of the information was hidden behind the hashes, the impact of an attack to players' privacy is also reduced. But still, the problems with external access and the access to the components in general was not addressed. This kept the values of back end (4) and database (5) still fairly high and further work on them is required. The initial estimates changed were:

- Back end
  - *2. Privacy damage* was reduced from 6 to 3 because the queries and hashes have no identifiable information. They can be only used to retrieve information.
  - *3. Data capabilities* was reduced from 6 to 4 because only large amounts of queries and hashes can be used to harm privacy if they can be used to get data from the database.
  - *7. Data quantity* was reduced from 6 to 4 because the database is not within back end and the query database does not keep data but the hashes and corresponding queries.
  - *8. Data significance* was reduced from 6 to 3 because the hashes and queries are important but do not threaten privacy of a player unless large quantities of them are leaked.
  - *9. Data storage time* was reduced from permanent storage (6) to long term storage (5) because back end contains only the query database.
  - *10. Data identifiability* was reduced from 3 to 2 because back end no longer has the database which has the information in identified form.

- Database
  - *1. Attack actualization* was reduced from 4 to 2 because database can no longer accessed directly through back end and only way to access it is through ontology engine. Therefore, it requires a lot of effort to attack database.
  - *4. Asset network* was reduced from 4 to 3 because of the big change of access to database. Now, database is in private network but still there was an restricted access for administrator.
  - *6. Data access* was reduced from 4 to 2 because the access to data was restricted further as well.

Because the other components were not improved in any the values of them did not change. The highest value was calculated for front end (7) and it must be reduced by a proper design decision later.

E.2.5 Round four: more restrictions to access

In the previous analysis another deficiency was detected about accessing the information which was not solved by the query database. The different components had no strict access layer definition but it was noted that some components were accessible publicly and most of them were meant for internal use. With proper implementation of security measures this problem can be avoided but the layering of the design makes the implementation more clear.

Having the separate components (front end, API, back end, ontology engine and database and query database) made it possible to build separate access layers for the Game Cloud, since each component now has a specific role in the ecosystem.

- Front end (7) should only access the processed information through hashes (H) with addition to PII and it is more of public level access because it offers access in public Internet for players and developers.
- API (3) is also in the public because the games and services push raw data with identifications through for Game Cloud to process and store. But it also requests processed information via hashes (H) that is utilized in games and services.
- Back end (4) and query database are located inside the Game Cloud and are accessed only through API and Front end. Also, administrator has access to them for maintenance purposes. Through these the raw information is delivered to the database (5) with identifications to whom the data is connected to. The processed data is retrieved directly from the ontology engine (6), which requests it from the database (5) using queries (Q).

- Ontology engine (6), as mentioned above, processes the information retrieved from the database (5) to be forwarded for the back end (4). It would seem that both back end and ontology engine do not directly deal with raw data and, as they continuously request services of others, they are on the same access level within Game Cloud.

- Database (5) has all data the Game Cloud has collected from the players. It is the component that must be most guarded within the system as all other components rely on it and the database must be available at all times. Therefore, it is reasonable to restrict the access to it.

Therefore, access in Game Cloud is either public, protected or highly restricted (private), using the approach used by object-oriented languages, we decided to use three level approach: public, protected and private:

- Public layer can be accessed from anywhere.

- Protected layer can be accessed from the public layer but an external administrative access is offered too.

- Private level components cannot be accessed from any other than protected layer.

A strict access restriction between the database and the publicly accessible components using the back end and the ontology engine was built. The database was set to the private access layer, where access can come only from the protected layer. The protected level consists of the back end and the ontology engine, both of which offer access to the lower layer and can be accessed from the public level. Additionally, the administrator has a highly protected access to the components at the protected level. The API and the front end were put to public layer, since both need to be accessed by the games, end-users, game developers and third party applications. This layout is depicted in Figure E.2, in which the exchange of information through different layers is defined, thus helping the development of such interfaces.

This was a big change in the development and the risk values of back end (4) and database (5) were reduced because this change mainly concerned these two components. The resulting values are shown in Table E.3 and the detailed results are shown in Appendix F on page 285.

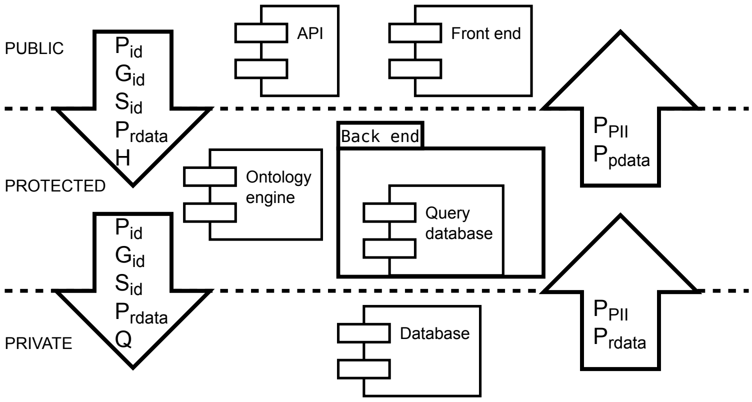


Figure E.2: Layer-based interface of data exchange in Game Cloud

Table E.3: The results of the fourth round information privacy risk assessment on the second Game Cloud ecosystem layout

Component / Attribute	1.	2.	3.	4.	5.	6.	7.
Impact on privacy	4	5	5	4	5	3	5
Attack likelihood	3	4	5	3	4	2	6
Privacy risk	**4**	**5**	**5**	**4**	**5**	**3**	**6**

The access layer makes it possible to enforce more security between the components and this resulted in lowered value for the back end (4.). It was assumed that the value of database (5) would also decrease but because it still controls all the data on all identifiability levels within Game Cloud the risk value remains high. The change that was made had the following changes on the initial estimates:

- Back end
  - *1. Attack actualization* was changed from 4 to 3 because with the new access restrictions it requires even more knowledge and the component is better protected.
  - *4. Asset network* was changed from 4 to 3 because it is now within a network access to which is happening through other components. The network is somewhere in between protected and private network but because of the added layers that can be used to enforce more security the value was reduced by one because external access for the administrator still exists.
  - *6. Data access* was changed from 4 to 2 because the new access layers mean that even less people can manipulate back end directly. The hashes and queries are not accessible for users or developers through the front end.

- Database

    - *4. Asset network* was changed from 3 to 2 because the external direct access to the database was removed and it can be accessed only through ontology engine.

    - *6. Data access* was changed from 2 to 1 because information is only accessed by a component of Game Cloud; ontology engine.

E.2.6 Round five: final development step

The previously shown layout brought up another big increase in privacy with the layering approach but the access to the personal data was still through one big front end, used by the game and service developers. This approach could create a possible situation, where with privilege escalation by a programming error or by a malicious intent, could grant unauthorized access to the personal data of the players for any developer. The access control, therefore, was not clear enough.

In order to make the access right control easier and more clear, the front end was split into two. The first front end is dedicated for the end-users only for viewing their statistics and setting up account details. The second front end is for the developers (game and third party service) and meant only for setting up game or service ontologies and other setup data. This enables a clear separation between player data and game data access and, therefore, increases the privacy of the end-users by reducing the possibility of personal data disclosure. The back end can easily differentiate what kind of data to retrieve via the ontology engine by checking from which front end the request came from. Since hashes are used for information retrieval, PII and other end-user data is hidden but with this approach of splitting the front end, we can make a clear access restriction. No end-user data is returned to the developer front end, all such requests are discarded by the back end.

The third round resulted in the current version of Game Cloud that is presented in Figure E.3, from which it can be seen that the P_{PII} is not delivered to any other but user front end and P_{rdata} is not delivered outside protected layer beyond the ontology engine. This layout was again analyzed for tasks and functionalitiesthat are shown in Table E.4.

This change with the front end by dividing it into two; user front end (7) and developer front end (8) had an positive effect in reducing the risk value of the front end. The separate front ends were, therefore, assessed separately. The results of the calculations are presented in Table E.5 and the detailed results are shown in Appendix F on page 286.

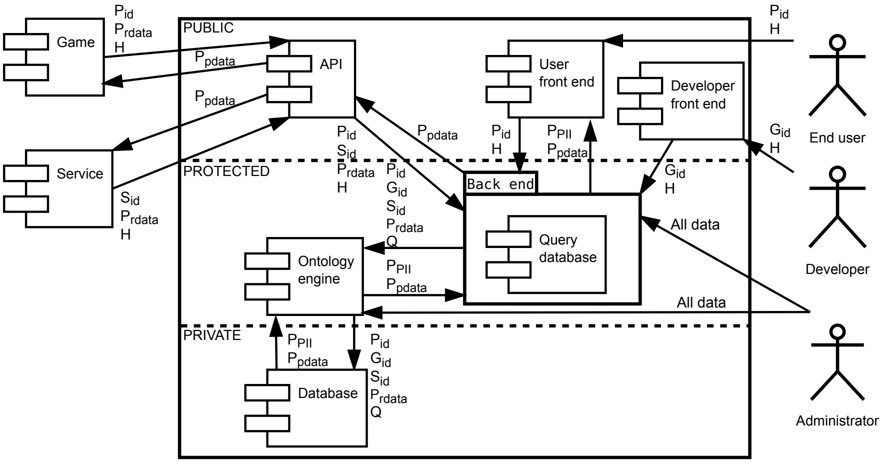


Figure E.3: Final version of Game Cloud

Table E.4: Tasks (T) and functions (F) in the final design

Component	T	T	T	T	T	T	T	F	F	F	F	F	F	F
	1	2	3	4	5	6	7	1	2	3	4	5	6	7
API			x					x						
User front end							x					x	x	
Developer front end							x							x
Back end			x							x				
Query database				x	x						x			
Ontology engine				x							x			
Database					x					x				
Game		x						x	x					
Service		x												x
End user	x						x					x	x	
Developer							x							x
Administrator							x							

Table E.5: The results of the fifth round information privacy risk assessment on the second Game Cloud ecosystem layout

Component / Attribute	1.	2.	3.	4.	5.	6.	7.	8.
Impact on privacy	4	5	5	4	5	3	5	3
Attack likelihood	3	4	5	3	4	2	5	3
Privacy risk	**4**	**5**	**5**	**4**	**5**	**3**	**5**	**3**

Because the user front end (7) deals still with private information the impact is not reduced. But the likelihood was reduced with one step, since now there are fewer persons using the front end and each user has equal level of access rights. The developer front end (8) can be used only for maintaining and retrieving game statistics, and contains no identifiable or identified information that can harm players' privacy. The developer front end, however, may have some vulnerabilities which can be exploited to gain access to the system and, therefore, it does not have an insignificant risk, impact or likelihood value.

This modification of the front end changed the initial assessment values when compared to the initial values of the previous combined front end as follows:

- *2. Privacy damage*
  - User front end: No change because the same data is still accessible.
  - Developer front end: Was dropped from 6 to 1 because no identifiable player information can be accessed.
- *3. Data capabilities*
  - User front end: No change because the same data is still accessible.
  - Developer front end: Was reduced from 6 to 3 because the game statistics can be of use only for some other than privacy violating purposes.
- *5. Asset role*
  - User front end: No change as it has the same purpose as previously.
  - Developer front end: Was reduced from 5 to 3 because it is not really needed for Game Cloud operation. Downtime in developer front end does not have an effect to the players' experience. It is important only for the developers for maintaining their data in which downtime might not be of problem as the front end might not be needed on daily basis.
- *6. Data access*
  - User front end: Was reduced from 4 to 2 because only the player can access his/her own data with the credentials through the user front end.
  - Developer front end: Was reduced from 4 to 3 because there are fewer persons accessing the data but still there can be multiple game developers maintaining the details and requesting statistics of one game.
- *7. Data quantity*
  - User front end: No change as the same amount of data is still accessible.
  - Developer front end: Was reduced from 4 to 3 because identified or identifiable information is not stored. Only the statistics are kept within the developer front end for the time the session lasts.

- *8. Data significance*
  - User front end: No change as the same data is still accessible.
  - Developer front end: Was dropped from 5 to 1 because the game statistics are not private data. It cannot harm the player's privacy and because it is in processed form it can be always re-created using the raw data. Therefore, it has no real impact on privacy.
- *10. Data identifiability*
  - User front end: No change as the same identifiable data is still accessible.
  - Developer front end: Was reduced from 2 to 1 because the game statistics contains no identifications.

E.3 Concluding remarks of the process

First at the design level, one key benefit is that Game Cloud can not only gain the players' trust but to maintain it. Using the model for assessing information privacy risk the effects of the changes were demonstrated, which also backed up the need for the changes and the actual changes as well.

E.3.1 The overview of the results of the development process

By looking the values in Table E.6 it is evident that the development process reduced the risks of the components which were possible to affect. For example, back end and database had their risk reduced from six to four and five. Now, there is not a component that has the highest risk value. However, the risk value of API remained high mainly because of the sensitive data that is used in the Game Cloud, including authentication data, is handled by the API. This information was very valuable, because now it is known which components need to be protected with strong security measures. The utilization of the approach improved Game Cloud design from privacy perspective and now privacy is included as default into the design.

But these benefits were not gained without a cost. The approach increased the development time and required more resources because of the changes to design resulting in more changes in the prototype implementation. However, this was justified because of the benefits the approach gave. Also in the long run because the approach is also beneficial in post-mortem since the documentation of the design process details well the internal information use as well as external access.

Table E.6: Privacy risk values of the Game Cloud system components

Component	Initial layout	2nd layout	3rd layout	Final layout
	Privacy risk	Privacy risk	Privacy risk	Privacy risk
API	5	5	5	5
Back end	6	**5**	**4**	4
Database	6	**5**	5	5
Front end	6	6	6	-
Front end (dev.)	-	-	-	3
Front end (user)	-	-	-	5
Game	4	4	4	4
Ontology engine	3	3	3	3
Query database	-	**5**	**4**	4
Service	5	5	5	5

E.3.2 Economical view of model use in context of DGPs

The economical issues on DGPs were earlier discussed in section 7.2.1 on page 132. The complete approach is not aimed to have direct economic benefits for a specific business area but in the case of DGP, some economic benefits were noted during the design process of Game Cloud. At the business level the benefits of the approach from economical point of view are presented in the light of cost mitigation after information disclosure. From the presented positive and negative impacts of game data use (Figure 7.4 on page 136) the following short- and long-term negative impacts on a company were drawn. The short-term impacts are:

- Legal sanctions from governmental institutions.
- Re-evaluation of the platform and assessment of security.
- Downtime of the platform that is a possible side conduit of re-evaluation.

And the long-term impacts are:

- Loss of customers' trust, which is difficult to re-gain but with transparency the symptoms can be alleviated.
- By losing the trust the brand and product values can and more likely will suffer too.

Short-term impacts: The short-term impacts on a company can be alleviated if not completely prevented with good design. In EU, for example, evaluation of the privacy risks and effects of business operations is required [23]. The approach used here forces to create a documentation, in which the information privacy risks are presented and also how these risks are mitigated is detailed. This can help to reduce the fines since in case of a disclosure negligence was not the reason. Re-evaluation of the systems is time- and money-consuming operation. With the approach presented in this thesis the risks of the components are mapped. This enables targeting of resources to correct areas in the security assessment, for instance. In addition, the information flows provide valuable insight for the analysts about which components have failed and why. When the time for re-evaluation and security assessment is reduced, it will also reduce the downtime and, therefore, mitigates potential losses caused by it.

Long-term impacts: The long-term effects are harder to mitigate as they are more of a reputation loss that can lead to financial losses. The impacts of these can only be alleviated. This approach can alleviate both: first by reducing the trust loss and after reducing the impact on brand and product values. The approach makes it possible to demonstrate for the customers that why the breach happened and how the new mechanisms will protect their privacy in the form of changed information privacy risk levels, for instance. By implementing privacy by default and the rest of the PbD principles into design, the extent of the breach can be reduced and, therefore, the approach helps in convincing the customers that without these measures, things would have been much worse. This will have a mitigating effect to the brand and product values.

E.3.3 Benefits of the approach

Game Cloud shows that one of the main benefits gained from using the approach is the forced generation of the documentation of the DGP design process. This documentation can be used for technical and economical purposes.

1. First, the approach helps in increasing as well as maintaining customer trust as the customer feels more secure and the customers' privacy is protected.
2. Second, the approach will reduce the sanctions, for example, in EU since the documentation can be used as a proof that privacy of the customers is taken into account. Furthermore, the potential sanctions due to a privacy or security breach are reduced for the same reason.
3. Third, the documentation will also help in continued development and, therefore, reduces the further development costs of privacy-centric platforms.

In the new DGPs like Game Cloud information privacy is essential in gaining trust which in turn has a direct impact on economics. Trust, and especially privacy, must be maintained but maybe not at all costs as the service quality might suffer but to a reasonable extent. According to the previous discussions about game behavior data on pages 46 and 132 it can be concluded that gaming data should receive the same treatment as any other user generated data. With proper security, the data can be kept safe and the trust of the players can be gained and maintained.

With these results the model for information privacy risk assessment clearly shows its benefits as it helps to classify different components based on their risk, impact and likelihood values to enable focusing of the resources into the problematic areas. This was the case with Game Cloud. During the development of Game Cloud, the design of the components and the design of the Game Cloud internals were improved based on the result of the analysis and the result of the information privacy risk calculated with the model.

F The detailed results of Game Cloud assessment

Here all Game Cloud assessment results are presented. In the following subsections assessment of each Game Cloud component is detailed. All components are assessed with the *software prototype* available at *http://github.com/lut-projects/iprat* and the following results are the output of the *software prototype*.

In the following results the attributes are labeled with a number. The order of the attributes used in the results are detailed in Table F.1.

Table F.1: Order of the attributes in the results

Nth. value	Attribute
1	Attack actualization
2	Privacy damage
3	Data capabilities
4	Asset network
5	Asset role
6	Data access
7	Data quantity
8	Data significance
9	Data storage time
10	Data identifiability
11	Data value
12	User damage
13	Damage level
14	Asset misuse potential
15	Attack gain
16	Asset value
17	Impact on privacy
18	Attack likelihood

All values were calculated with following script:

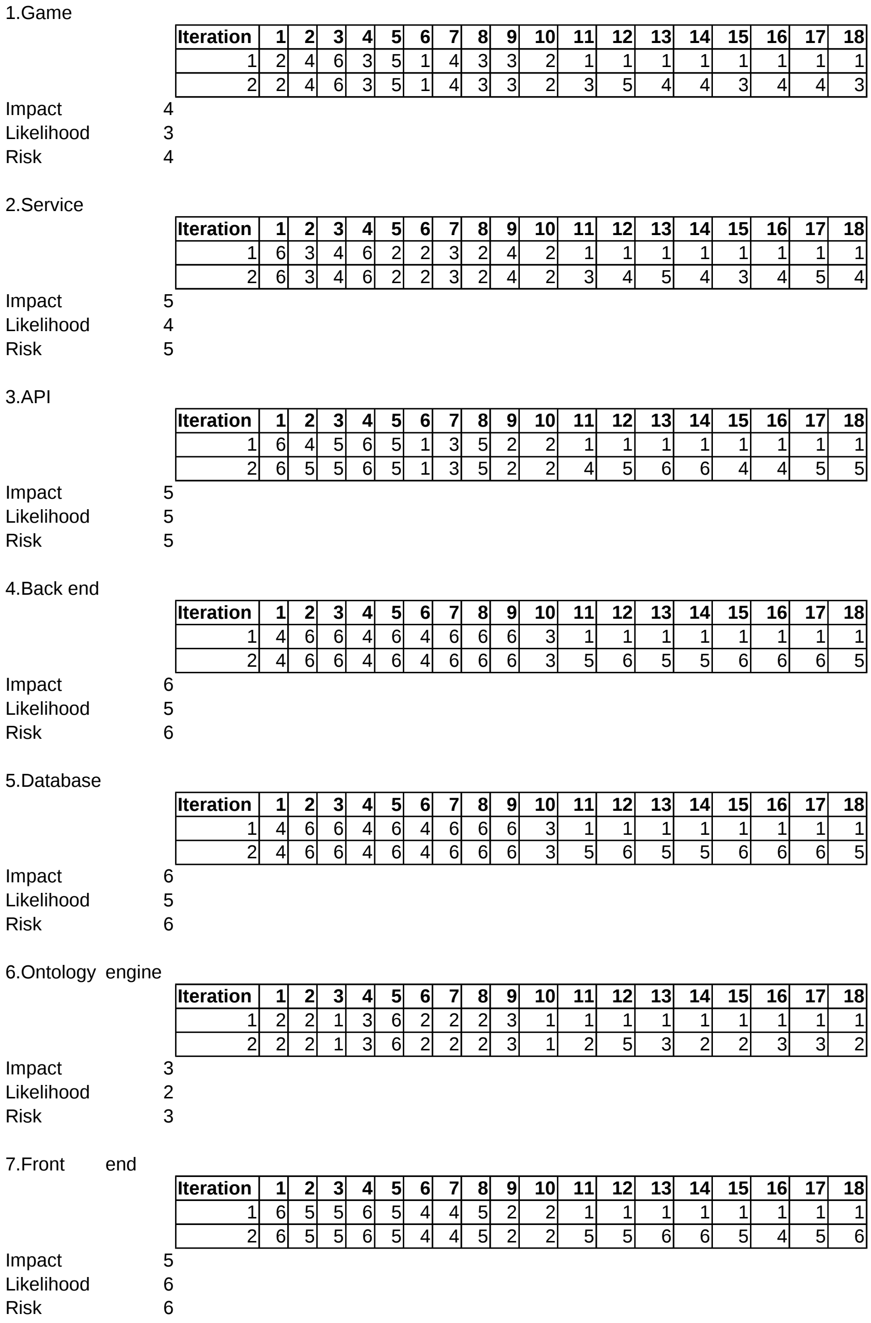
```
#!/bin/bash
cat gc_states.list |while read line; do
    if [ ${#line} -eq 4 ] ; then

        FILE="ROUND"$(echo $line|sed 's/---//g')".csv"
        if [ -f $FILE ] ; then rm $FILE ; fi
    else
        ID=$(echo $line|cut -d':' -f1)
        NAME=$(echo $line|cut -d':' -f2)
```

```
       VALUES=$(echo $line|cut -d’:’ -f3)
       echo "$ID.$NAME" >> $FILE
       echo -n " Iteration 1 2 3 4 5 6 7 8 9 10” >> $FILE
       echo “11 12 13 14 15 16 17 18" >> $FILE
       ./validator -v $VALUES >> $FILE
       echo "" >> $FILE
    fi
done
```

The following file content was used as input for the script above. These are the initial estimates for each component in Game Cloud.

```
---1
1:Game:2463514332
2:Service:6346223242
3:API:6456513522
4:Back end:4664646663
5:Database:4664646663
6:Ontology engine:2223622231
7:Front end:6556544522
---2
1:Game:2463514332
2:Service:6346223242
3:API:6456513522
4:Back end (QDB):4344644352
5:Database:2663626663
6:Ontology engine:2223622231
7:Front end:6556544522
---3
1:Game:2463514332
2:Service:6346223242
3:API:6456513522
4:Back end (QDB):3343624352
5:Database:2662616663
6:Ontology engine:2223622231
7:Front end:6556544522
---4
1:Game:2463514332
2:Service:6346223242
3:API:6456513522
4:Back end (QDB):3343624352
5:Database:2662616663
6:Ontology engine:2223622231
7:Front end:6556514522
8:Developer front end:6126333121
```

F.1 Round two



1.Game

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	4	6	3	5	1	4	3	3	2	1	1	1	1	1	1	1	1
2	2	4	6	3	5	1	4	3	3	2	3	5	4	4	3	4	4	3

Impact	4
Likelihood	3
Risk	4

2.Service

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	3	4	6	2	2	3	2	4	2	1	1	1	1	1	1	1	1
2	6	3	4	6	2	2	3	2	4	2	3	4	5	4	3	4	5	4

Impact	5
Likelihood	4
Risk	5

3.API

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	4	5	6	5	1	3	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	1	3	5	2	2	4	5	6	6	4	4	5	5

Impact	5
Likelihood	5
Risk	5

4.Back end

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	6	6	4	6	4	6	6	6	3	1	1	1	1	1	1	1	1
2	4	6	6	4	6	4	6	6	6	3	5	6	5	5	6	6	6	5

Impact	6
Likelihood	5
Risk	6

5.Database

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	6	6	4	6	4	6	6	6	3	1	1	1	1	1	1	1	1
2	4	6	6	4	6	4	6	6	6	3	5	6	5	5	6	6	6	5

Impact	6
Likelihood	5
Risk	6

6.Ontology engine

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	2	1	3	6	2	2	2	3	1	1	1	1	1	1	1	1	1
2	2	2	1	3	6	2	2	2	3	1	2	5	3	2	2	3	3	2

Impact	3
Likelihood	2
Risk	3

7.Front end

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	5	5	6	5	4	4	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	4	4	5	2	2	5	5	6	6	5	4	5	6

Impact	5
Likelihood	6
Risk	6

F.2 Round three

1.Game

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	4	6	3	5	1	4	3	3	2	1	1	1	1	1	1	1	1
2	2	4	6	3	5	1	4	3	3	2	3	5	4	4	3	4	4	3

Impact	4
Likelihood	3
Risk	4

2.Service

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	3	4	6	2	2	3	2	4	2	1	1	1	1	1	1	1	1
2	6	3	4	6	2	2	3	2	4	2	3	4	5	4	3	4	5	4

Impact	5
Likelihood	4
Risk	5

3.API

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	4	5	6	5	1	3	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	1	3	5	2	2	4	5	6	6	4	4	5	5

Impact	5
Likelihood	5
Risk	5

4.Back end (Query database)

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	3	4	4	6	4	4	3	5	2	1	1	1	1	1	1	1	1
2	4	3	4	4	6	4	4	3	5	2	4	6	5	5	4	5	5	4

Impact	5
Likelihood	4
Risk	5

5.Database

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	6	6	3	6	2	6	6	6	3	1	1	1	1	1	1	1	1
2	2	6	6	3	6	2	6	6	6	3	5	6	4	5	6	5	5	4

Impact	5
Likelihood	4
Risk	5

6.Ontology engine

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	2	1	3	6	2	2	2	3	1	1	1	1	1	1	1	1	1
2	2	2	1	3	6	2	2	2	3	1	2	5	3	2	2	3	3	2

Impact	3
Likelihood	2
Risk	3

7.Front end

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	5	4	6	5	4	4	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	4	4	5	2	2	5	5	6	6	5	4	5	6

Impact	5
Likelihood	6
Risk	6

F.3 Round four

1.Game

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	4	6	3	5	1	4	3	3	2	1	1	1	1	1	1	1	1
2	2	4	6	3	5	1	4	3	3	2	3	5	4	4	3	4	4	3

Impact	4
Likelihood	3
Risk	4

2.Service

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	3	4	6	2	2	3	2	4	2	1	1	1	1	1	1	1	1
2	6	3	4	6	2	2	3	2	4	2	3	4	5	4	3	4	5	4

Impact	5
Likelihood	4
Risk	5

3.API

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	4	5	6	5	1	3	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	1	3	5	2	2	4	5	6	6	4	4	5	5

Impact	5
Likelihood	5
Risk	5

4.Back end (Query database)

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	3	3	4	3	6	2	4	3	5	2	1	1	1	1	1	1	1	1
2	3	3	4	3	6	2	4	3	5	2	3	6	4	4	3	4	4	3

Impact	4
Likelihood	3
Risk	4

5.Database

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	6	6	2	6	1	6	6	6	3	1	1	1	1	1	1	1	1
2	2	6	6	2	6	1	6	6	6	3	4	6	4	4	6	5	5	3

Impact	5
Likelihood	4
Risk	5

6.Ontology engine

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	2	3	3	6	2	2	2	3	1	1	1	1	1	1	1	1	1
2	2	2	3	3	6	2	2	2	3	1	2	6	3	2	2	3	3	2

Impact	3
Likelihood	2
Risk	3

7.Front end

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	5	5	6	5	4	4	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	4	4	5	2	2	5	5	6	6	5	4	5	6

Impact	5
Likelihood	6
Risk	6

F.4 Round five

1.Game

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	4	6	3	5	1	4	3	3	2	1	1	1	1	1	1	1	1
2	2	4	6	3	5	1	4	3	3	2	3	5	4	4	3	4	4	3

Impact	4
Likelihood	3
Risk	4

2.Service

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	3	4	6	2	2	3	2	4	2	1	1	1	1	1	1	1	1
2	6	3	4	6	2	2	3	2	4	2	3	4	5	4	3	4	5	4

Impact	5
Likelihood	4
Risk	5

3.API

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	4	5	6	5	1	3	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	1	3	5	2	2	4	5	6	6	4	4	5	5

Impact	5
Likelihood	5
Risk	5

4.Back end (Query database)

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	3	3	4	3	6	2	4	3	5	2	1	1	1	1	1	1	1	1
2	3	3	4	3	6	2	4	3	5	2	3	6	4	4	3	4	4	3

Impact	4
Likelihood	3
Risk	4

5.Database

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	6	6	2	6	1	6	6	6	3	1	1	1	1	1	1	1	1
2	2	6	6	2	6	1	6	6	6	3	4	6	4	4	6	5	5	3

Impact	5
Likelihood	4
Risk	5

6.Ontology engine

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	2	2	1	3	6	2	2	2	3	1	1	1	1	1	1	1	1	1
2	2	2	1	3	6	2	2	2	3	1	2	5	3	2	2	3	3	2

Impact	3
Likelihood	2
Risk	3

7.User front end

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	5	5	6	5	2	4	5	2	2	1	1	1	1	1	1	1	1
2	6	5	5	6	5	2	4	5	2	2	4	5	6	6	4	4	5	5

Impact	5
Likelihood	5
Risk	5

8.Developer front end

Iteration	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	6	1	3	6	3	3	3	1	2	1	1	1	1	1	1	1	1	1
2	6	1	3	6	3	3	3	1	2	1	2	3	3	2	2	3	3	3

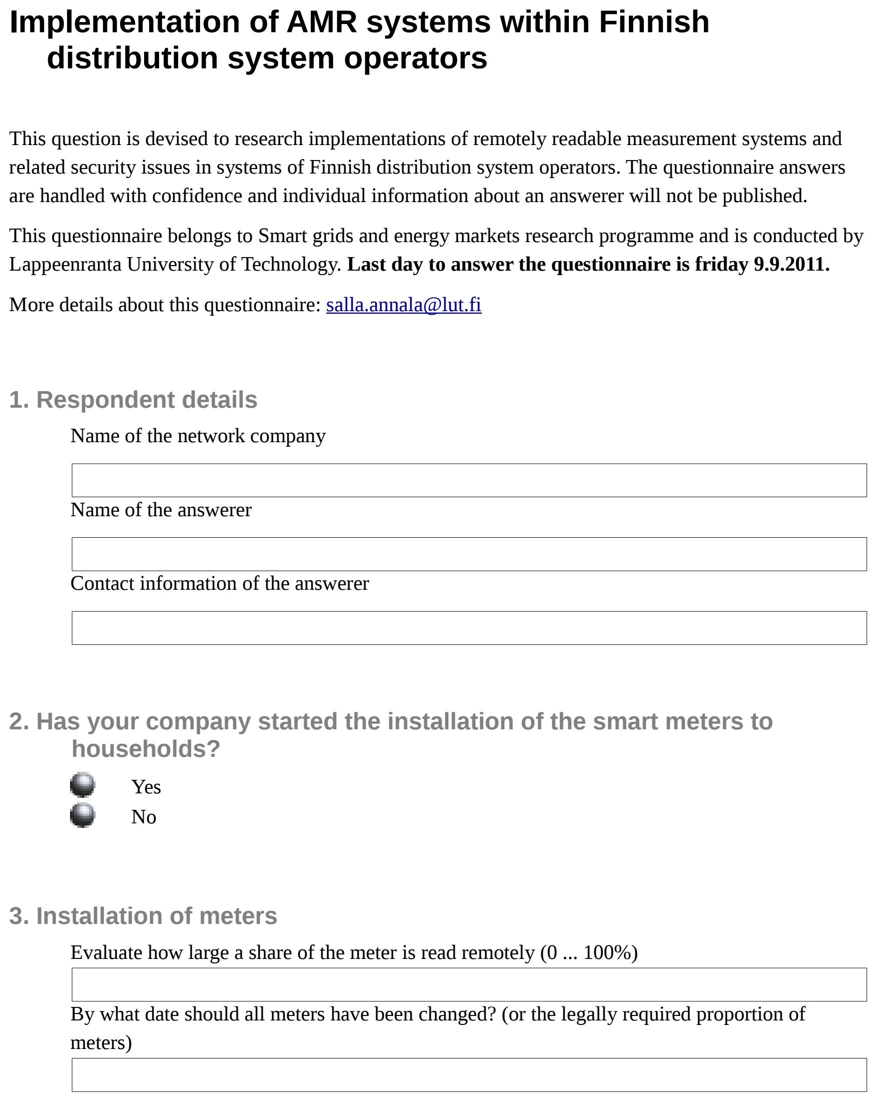
Impact	3
Likelihood	3
Risk	3

G SGEM questionnaire and answers

In the following pages the questions Salla Annala and Prof. Satu Viljainen of Electricity Markets and Power Systems laboratory of School of Energy Systems of Lappeenranta University of Technology devised for finding out the status of smart grid implementations are presented. After the questions the answers to the questions are presented. This survey was conducted in Finland and all questions and answers were in Finnish. Here the questions and the answers are translated into English. It must be noted that the answers were in some cases poorly articulated and the English equivalents are following the same trend in order to demonstrate the difficulty of interpreting the answers.

The survey was sent to all distribution system operators (DSO) in Finland via email in 2011. The survey was answered by 30 (out of 85) DSOs. The customer base of the questionnaire respondents covers 49% of all electricity customers in Finland.

G.1 Questionnaire



Implementation of AMR systems within Finnish distribution system operators

This question is devised to research implementations of remotely readable measurement systems and related security issues in systems of Finnish distribution system operators. The questionnaire answers are handled with confidence and individual information about an answerer will not be published.

This questionnaire belongs to Smart grids and energy markets research programme and is conducted by Lappeenranta University of Technology. **Last day to answer the questionnaire is friday 9.9.2011.**

More details about this questionnaire: salla.annala@lut.fi

1. Respondent details

Name of the network company

Name of the answerer

Contact information of the answerer

2. Has your company started the installation of the smart meters to households?

○ Yes
○ No

3. Installation of meters

Evaluate how large a share of the meter is read remotely (0 ... 100%)

By what date should all meters have been changed? (or the legally required proportion of meters)

METER

Evaluate the most common meter type if there are multiple meter types used

4. What information does the meter measure in addition to hourly energy?

● Instantaneous active power
● Instantaneous reactive power
● Power
● Phase voltage
● Interrupts
● 0-faults
● Else, what?

5. What meter data is read and how often?

	More than once a day	Once a day	Many times in a week	No more than once a week	If necessary
Hourly energies	●	●	●	●	●
Instantaneous power	●	●	●	●	●
Instantaneous voltages	●	●	●	●	●
Interrupts	●	●	●	●	●

6. What other information is read from meter and how often?

7. What identification information the meter contains? (How the meter is identified when doing upgrades, controlling as well as reading)

8. Is there a standardized interface to the meter?

○ Yes, which standard?

○ No

9. Does the meter have an adjustable a fuse?

○ Yes

○ No

OPERATING

10. Which of the following functions belong to the network company and which to the service provider?

	Network company	Service provider
Meter ownership	○	○
Meter reading	○	○
Meter updates	○	○
Meter maintenance (maintenance, repairs)	○	○
Ownership of reading system	○	○
Measuring Database Maintenance	○	○

11. Estimate the possibilities of network company and service provider to execute meter related functions. (You can select both options)

	Network company	Service provider
Who can make updates remotely?	○	○
Who can do controls remotely?	○	○
Who can perform upgrades on the spot?	○	○
Who can carry out controls on the spot?	○	○
Who can read the meter remotely?	○	○

12. Does the meter send reading data necessary for billing automatically without separate request?

○ Yes
○ No

13. How to ensure that the request is from authorized party?

14. What updates, or controls can be done remotely to the meter ?

○ Changes in tariff

○ Switch off / on

○ Else, what?

15. What updates, or controls the meter can be made on the spot?

○ Changes in tariff

○ Switch off / on

○ Else, what?

16. What are the communication methods used to monitor updates and controls?

- ○ Electricity network
- ○ GSM/GPRS (public Internet)
- ○ GSM/GPRS (private network)
- ○ Else. What?

17. Does the meter send an acknowledgment to the updates and the controls carried out remotely?

- ○ Yes
- ○ No

MEASUREMENT DATABASE

18. What data is stored in measurement database?

- ○ Hourly energies
- ○ Dead times
- ○ Else. What?

19. Who will be able to

	Network company	Service provider
To write the measurement database	○	○
To read the measurement database	○	○

21. If the maintenance of a measurement database belongs to network company, does the service provider have a copy of it (database)?

○ Yes
○ No

METER LOG INFORMATION

21. What information is stored in the meter and for how long?

	Less than week	1-4 weeks	4 weeks – half years	More than half years
Hourly energies	○	○	○	○
Instantaneous power	○	○	○	○
Instantaneous voltages	○	○	○	○
Interrupts	○	○	○	○

22. What other information is stored in the meter and for how long?

23. Will the meter log data entry of

	Yes	No
Remotely made updates	○	○
Remotely made operational controlling	○	○
Carried out on-site updates	○	○
Carried out on-site operational controlling	○	○
Remote reading of meter	○	○

24. Who will be able to read the log data?

○ Network company

○ Service provider

○ End user

25. Is there a copy of the meter log

○ Network company

○ Service provider

26. Here you can type more details on certain answers and also give feedback on the questionnaire

G.2 Questionnaire answers

AMR

1. Involved network companies

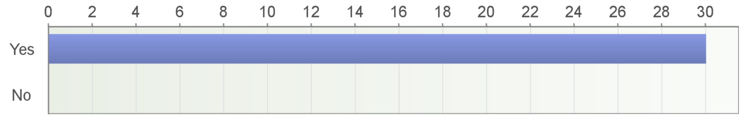
Number of respondents: 30

The Network company's name

- Lappeenrannan Energiaverkot Oy
- Kronoby Elverk
- Muonion Sähköosuuskunta
- Koillis-Satakunnan Sähkö Oy
- Seiverkot Oy
- Porvoon Sähköverkko Oy
- Tunturiverkko Oy
- Vimpelin Voima Oy
- E.ON Kainuun Sähköverkko Oy
- Vatajankosken Sähkö Oy
- Kemin Energia Oy
- Jeppo Kraft Andelslag
- Lehtimäen Sähkö Oy
- Parikkalan Valo Oy
- Savon Voima Verkko Oy
- Jylhän Sähköosuuskunta
- Yli-Iin Sähkö Oy
- Kuopion Energia Liikelaitos
- Järvi-Suomen Energia Oy
- Oulun Energia Siirto ja Jakelu Oy
- Vattenfall Verkko Oy
- Lammaisten Energia Oy
- LE-Sähköverkko Oy
- Sallila Sähkönsiirto Oy
- Iin Energia Oy
- Helen Sähköverkko Oy
- PKS Sähkönsiirto Oy
- Pietarsaaren Energialaitos
- JE-Siirto
- Keuruun Sähkö Oy

2. Has your company started the installation of the smart meters to households?

Number of respondents: 30



3. Installation of meters

Number of respondents: 30

Evaluate how large a share of the meter is read remotely (0 ... 100%)

- 8%
- 8%
- 5%
- 87%
- 94
- 14%
- 12
- 100
- 99
- 65%
- 56
- 60%
- 90%
- 48
- 60%
- 99%
- 100
- 20%
- 47%
- 32
- 99.6%
- 99.8
- 70%

- 60
- 100%
- 45
- 4
- 88%
- 42%
- 68

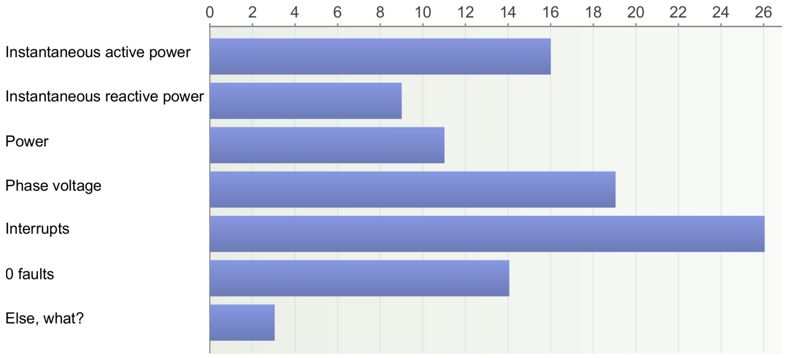
By what date should all meters have been changed? (or the legally required proportion of meters)

- The objective is by the end of 2012. No later than the end of 2013.
- Q3 / 2013
- 31.12.2013
- 6/2012
- 2012
- According to legally required schedule
- 80% by the end of 2013
- 2010
- 12/2011
- At the end of 2012
- 31.12.2013
- 2013
- 31.12.2012
- 2014
- 2013
- 2011
- 2008
- 2013
- 31.12.2013
- 28.2.2013
- 2008
- 2012
- mass exchange at the end of the year, few items mainly next year
- 2014
- 2007
- By the end of 2012,
- 06/30/2014
- in 2012
- 31.12.2012

- 12/2013

4. What information does the meter measure in addition to hourly energy?

Number of respondents: 29

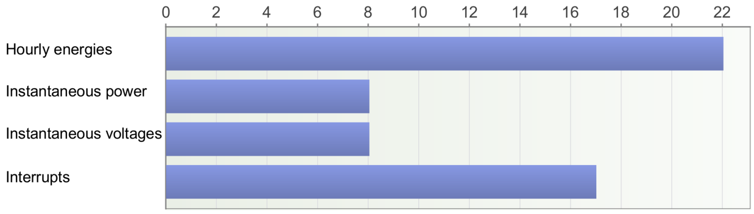


Open replies: Other, what?

- Overruns and shortfalls in the voltage levels by two limit values
- Over-voltage and under-voltage
- The yard information is collected with AIDON and each connection has one meter installed. Some come as active alarms during the context of reading.

5. What meter data is read and how often?

Number of respondents: 22



	More than once a day	Once a day	Many times in a week	No more than once a week	If necessary	In total	Average
Hourly energies	2	26	0	0	2	30	2.13
Instantaneous power	0	2	0	0	13	15	4.6
Instantaneous voltages	0	1	0	1	14	16	4.75
Interrupts	2	7	0	3	15	27	3.81
Total	4	36	0	4	44	88	3.82

6. What other information about the meter is read and how often?

Number of respondents: 17

- Period registers once a month,
- Natural gas and district heating consumption data once a month
- Power quality data once a month
- Reactive power
- cumulative reading once a month
- registry values
- Status information (eg. Electricity connections and cleavages, alarms), if necessary.
- Network monitoring information (whether the customer has electricity?), if necessary.
- Event information, if necessary.
- Temperature, if necessary.
- Energy used once a month.
- Monthly readings once a month
- Generally, only cumulative registers about once a month
- The hourly meter readings are read once a day
- The information listed in section 4 in “Else, what?” is read once a day
- Daily readings are read every day
- no other
- Voltage quality information on the SFS-EN 50160.
- Power quality data once a day
- Refer to section 4
- We will utilize fault information from AIDON
- Phase / zero defects

7. What identification information the meter contains? (How the meter is identified when doing upgrades, controlling as well as reading)

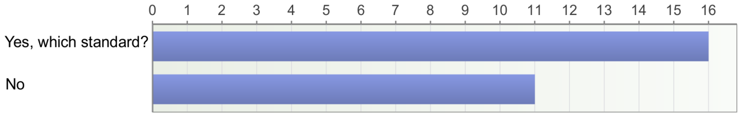
Number of respondents: 28

- Meter has a unique number identifier.
- (we are able to have functions as a service, so this question is for the service provider to respond)
- serial number
- Each meter has a meter-specific ID number, which identifies the meter.
- Fixed IP or Neuron ID or phone number
- Serial number
- The identification number must match the IP address
- The meter number is connected to the place of use.
- Serial number
- The meter number, address.
- id number
- IP address
- Neuron-ID
- Automatic detection during installation.
- The meter type, serial number, in addition to modems meters equipped with telephone number and a fixed IP address
- measuring point number, meter number
- unique ip address
- The meter ID as well as the company's meter ID
- Measuring point number / meter number
- Own ID.
- Based on L+G AIM properties
- Service provider takes care of this.
- SIM Number
- Number of place of use.
- Meter number
- Device number
- Program number
- IP address
- meter number
- With the meter ownership number of HSV and the meters own serial number.
- The meter identifier is a serial number of the meter when it is contacted remotely. The manual controls of reading system or queries can be made at location, but the command will go to meter, which is connected to the place of use in a database.

- The meter, the module and the IDs of SIMs must match in order to install the meter to the system
- The meter serial number, either through a hub (Landis & Gyr) or GSM (AIDON) connection.

8. Is there a standardized interface to the meter?

Number of respondents: 27

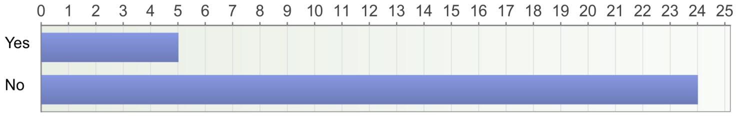


Open answers: Yes, which standard?

- DLMS / COSEM
- Aidon's meter and TeliaSonera consumption measurement service.
- Probably some "standard", the query needs to be directed to manufacturer
- PLC
- dlc
- COSEM / DLMS
- DLMS / COSEM
- L+G's LON, Plan and GRPS
- AIMIA?
- DLMS / COSEM
- IEC 62053-21, IEC 62053-22
- With the softwre of Landis & Gyr and AIDON.

10. Does the meter have an adjustable a fuse?

Number of respondents: 29



10. Which of the following functions belong to the network company and which to the service provider?

Number of respondents: 30

	Network company	Service provider	In total	Average
Meter ownership	29	1	30	1.03
Meter reading	12	18	30	1.6
Meter updates	7	23	30	1.77
Meter maintenance (maintenance, repairs)	17	13	30	1.43
Ownership of reading system	10	20	30	1.67
Measuring Database Maintenance	16	14	30	1.47
Total	91	89	180	1.49

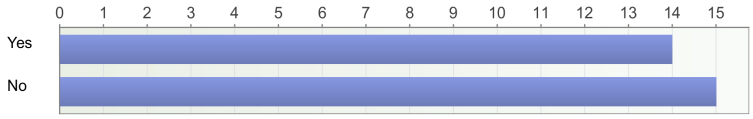
11. Estimate the possibilities of network company and service provider to execute meter related functions. (You can select both options)

Number of respondents: 30

	Network company	Service provider	In total	Average
Who can make updates remotely?	13	24	37	1.65
Who can do controls remotely?	28	20	48	1.42
Who can perform upgrades on the spot?	16	16	32	1.5
Who can carry out controls on the spot?	23	13	36	1.36
Who can read the meter remotely?	29	23	52	1.44
Total	109	96	205	1.47

12. Does the meter send reading data necessary for billing automatically without separate request?

Number of respondents: 29



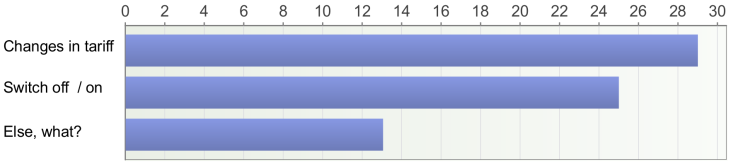
13. How to ensure that the request is from authorized party?

Number of respondents: 23

- It is the responsibility of the service provider.
- Meter can only be read by the service provider and the network company.
- Requests will be made only by own personnel / billing.
- Measuring Database requests
- Encrypted tunnel connection
- Message traffic is protected.
- By verification of the meter number and address.
- Untranslatable: “varmennetieto on” in finnish
- VPN
- Cannot tell
- I do not know
- Closed IP network
- Meter id is required for reading, as well as communication between the devices should work as requested.
- The service provider knows (Sonera)
- VPN secure connection
- Based on L+G AIM properties
- Service Provider takes care of this.
- Internal network of service provider.
- Passwords and SIMs are secret
- TeliaSonera can tell
- The meter identification details are only in their own (= service provider) reading system.
- Traffic encryption, the use of encryption keys
- Data transfers to meter are encrypted and various network companies have different encryption keys. And the keys of reading system and meter must match.
- The only remote link to meters is via the service provider's servers. This service provider is approved in Finland data centers safety rating. In addition, telecommunications service security description is available, which is implemented on our site.

14. What updates, or controls can be done remotely to the meter ?

Number of respondents: 30

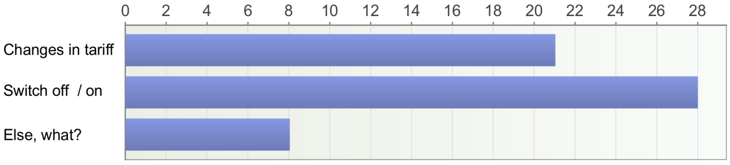


Open replies: Else, what?

- Configuration changes
- Cutting / switching part of the meter
- Program Changes / Updates
- Enables new features eg. Adjustable fuse
- Control times among others
- Cut Action section of the meters
- Software upgrade
- Change program
- Software
- Program updates
- Software update
- calendar setting
- The meter parameter changes, the time settings, current and voltage limits changes

15. What updates, or controls the meter can be made on the spot?

Number of respondents: 29

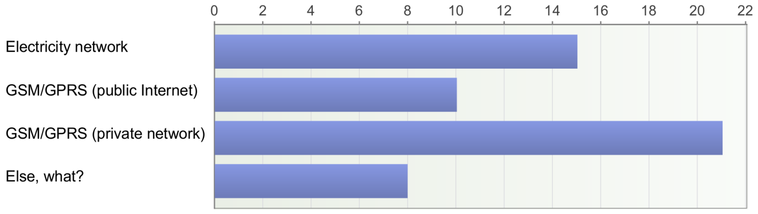


Open replies: Other, what?

- Enables new features e.g. adjustable fuse
- Control times among others
- Cut Action section of the meters
- Change Programme
- Software
- Program updates
- Software update
- The meter parameter changes, the time settings, current and voltage limits changes

16. What are the communication methods used to monitor updates and controls?

Number of respondents: 30

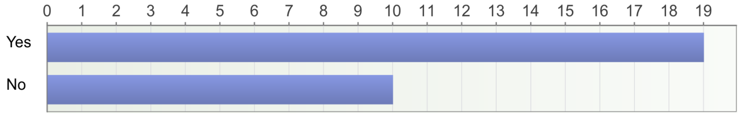


Open replies: Else, what?

- Radio network
- LAN
- Radio network
- Public Switched Telephone Network (PSTN)
- DSL (enterprise network, private network)
- Wimax, Kuopion Energia's own network
- PS: personal phone numbers
- The radio network of Kamsstrup

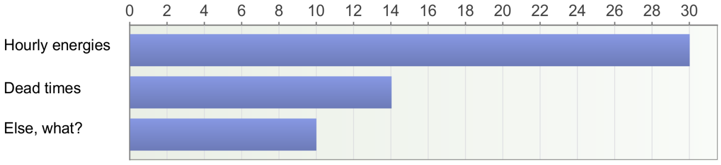
17. Does the meter send an acknowledgment to the updates and the controls carried out remotely?

Number of respondents: 29



18. What data is stored in measurement database?

Number of respondents: 30



Open replies: Else, what?

- All quality information
- Cumulative figures
- Billing records (section registers) data, status information, for instance
- Period register readings
- readings of the transfer
- Cumulative registers
- The other information in section 4
- Daily readings
- in the future; dashed information
- Voltage quality information

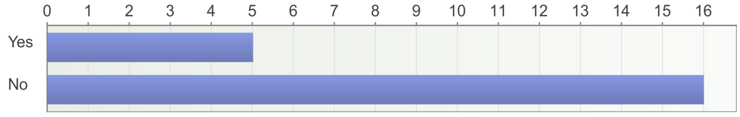
19. Who will be able to

Number of respondents: 30

	Network company	Service provider	In total	Average
To write the measurement database	23	15	38	1.39
To read the measurement database	28	15	43	1.35
Total	51	30	81	1.37

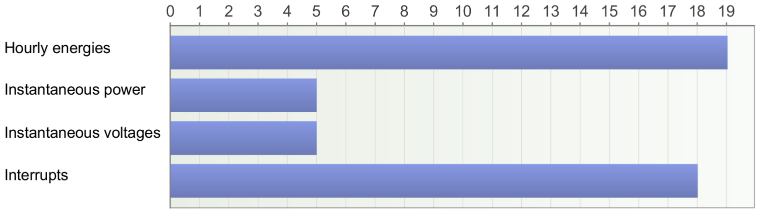
21. If the maintenance of a measurement database belongs to network company, does the service provider have a copy of it (database)?

Number of respondents: 21



21. What information is stored in the meter and for how long?

Number of respondents: 19



	Less than week	1-4 weeks	4 weeks – half years	More than half years	In total	Average
Hourly energies	0	3	18	9	30	3.2
Instantaneous power	2	2	6	2	12	2.67
Instantaneous voltages	2	2	6	2	12	2.67
Interrupts	0	3	15	9	27	3.22
Total	4	10	45	22	81	2.94

22. What other information is stored in the meter and for how long?

Number of respondents: 9

- Period registries, 0-faults
- Monthly readings (over six months)
- Cumulative figures
- E.g. the meter casing control
- Not known, the meter is from AIDON
- Status information, alarms
- The other information listed in section 4 and the retention period is the same
- Voltage Levels of the entire life cycle. Min / max values for 2 days
- 200 last power quality events is stored according to the manual of the L-Series meter

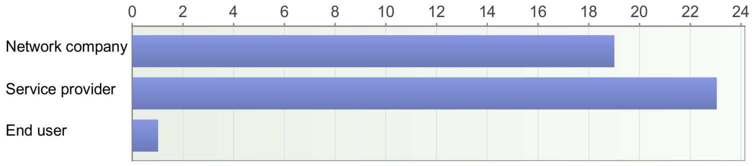
23. Will the meter log data entry of

Number of respondents: 24

	Yes	No	In total	Average
Remotely made updates	21	3	24	1.13
Remotely made operational controlling	20	4	24	1.17
Carried out on-site updates	17	4	21	1.19
Carried out on-site operational controlling	15	7	22	1.32
Remote reading of meter	12	11	23	1.48
Total	85	29	114	1.26

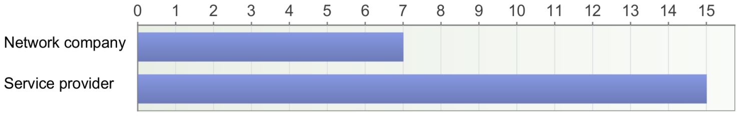
24. Who will be able to read the log data?

Number of respondents: 30



25. Is there a copy of the meter log

Number of respondents: 19



26. Here you can type more details on certain answers and also give feedback on the questionnaire

Number of respondents: 10

- There are some differences between Landis + Gyr and Aidon in information that is stored on the meters. There is an adjustable fuse but currently it is only informative, not triggering.
- According to the law dead times must be recorded / registered, this is not working on the service provider yet, but will work according to legislation. It may be that data is stored, but utilization of it or printing method has not yet been processed.
  The meter features can be further detailed by the equipment supplier AIDON, all existing features are not initially intended to be introduced, only to the extent that can be hourly readings and dead times can be retrieved.
  Meter can be connected to see whether it has voltage or is the 0 wire cut and so on.
  The meter storage capacity is short, important information, or the question is where measurement data is stored and for how long time, is already defined by the legislator.
  AIDON meter can not be read or programmed on-site, that is, it must be done at the system level. The question that whether the meter allows to make adjustments on the spot, i.e. remote cut device can cut the electricity, but all controls are made from within the system.
  What identifying information meter has? I do not remember exactly, but the meter number is connected to the service providers TeliaSonera's GPRS TCP / IP identification information used in communication, and the place of use number of the DSO. That is, three number sequences must match so that the information is directed to the right place.
  The log records, i.e. the consumption data from the meter must be usable by the user / our customer. but law did not quite require it, but is becoming.
- The responses deal specifically with precisely the most common meter.
  Everything is usually possible for the network operator through service provider (fee), so it is difficult to respond to these the network operator / service provider's questions, but the answers contain the most common method.
  In our case service provider is a group of companies.
- 19) via a software interface

23) No information on this issue

- The system of Landis + Gyr AIM
- In data security we have relied on the service provider, hopefully it is ok. Section 23: log data is likely to remain from all of those, no better information.
- When we buy services, many asked issues are not significant for us / known to us.
- I replied only to the extent that I thought to knew things. Our busy AMR project manager might have responded separately, so if there are, the answers are more informed. The case Lahti reminds cases of Vattenfall and Tampere, however so that we have Aidon meters and GSM reading (not PLC).
- The service provider for us is Satapirkka Sähkö Oy, which owns the reading system, and from whom we buy reading service.
- The answers are given on measuring devices below 63A.
  The reading and recording of the readings takes place in network company.

H Adjustment matrices for the second assessment model prototype

In the following Tables H.1, H.2, H.3, H.4, H.5, H.6 and H.7 the adjustment matrices created for the second assessment model are presented. These tables include also the example matrix for assess misuse potential presented earlier.

Table H.1: Asset misuse potential adjustment matrix

Damage level Data value	**1**	**2**	**3**	**4**	**5**	**6**
6	2	4	5	5	6	6
5	1	**3**	4	5	5	6
4	1	3	3	4	5	6
3	1	2	3	4	4	5
2	1	2	2	3	4	4
1	1	1	1	1	1	2

Table H.2: Attack actualization adjustment matrix

Attack actualization Asset network	**1**	**2**	**3**	**4**	**5**	**6**
6	4	4	4	5	5	6
5	4	4	4	4	5	6
4	2	3	3	4	5	5
3	2	2	3	4	5	5
2	1	2	3	3	3	3
1	1	2	3	3	3	3

Table H.3: Attack gain adjustment matrix

Data quantity Data value	**1**	**2**	**3**	**4**	**5**	**6**
6	1	5	5	6	6	6
5	1	4	4	5	5	6
4	1	3	4	4	5	5
3	1	2	2	3	4	5
2	1	1	2	2	2	3
1	1	1	1	1	1	2

Table H.4: Data capabilities adjustment matrix

Data capabilities Privacy damage	**1**	**2**	**3**	**4**	**5**	**6**
6	4	5	5	5	6	6
5	4	5	5	5	5	6
4	3	4	4	4	5	6
3	1	2	3	4	4	4
2	1	2	3	3	3	3
1	1	2	3	3	3	3

Table H.5: Damage level adjustment matrix

Damage level Attack actualization	**1**	**2**	**3**	**4**	**5**	**6**
6	4	5	6	6	6	6
5	4	4	5	5	5	6
4	3	3	4	4	5	6
3	1	2	3	4	5	5
2	1	2	3	4	5	5
1	1	2	3	4	5	5

Table H.6: Privacy damage adjustment matrix

Privacy damage Data significance	**1**	**2**	**3**	**4**	**5**	**6**
6	4	5	5	5	6	6
5	4	5	5	5	5	6
4	3	4	4	4	5	6
3	1	2	3	4	4	4
2	1	2	3	3	3	3
1	1	2	3	3	3	3

Table H.7: User damage adjustment matrix

Data capabilities Data value	1	2	3	4	5	6
6	3	4	5	5	6	6
5	2	3	4	5	5	6
4	1	2	3	4	5	5
3	1	2	2	3	4	5
2	1	1	2	2	3	3
1	1	1	2	2	2	3

ACTA UNIVERSITATIS LAPPEENRANTAENSIS

728. RINKINEN, SATU. Clusters, innovation systems and ecosystems: Studies on innovation policy's concept evolution and approaches for regional renewal. 2016. Diss.

729. VANADZINA, EVGENIA. Capacity market in Russia: addressing the energy trilemma. 2016. Diss.

730. KUOKKANEN, ANNA. Understanding complex system change for a sustainable food system. 2016. Diss.

731. SAVOLAINEN, JYRKI. Analyzing the profitability of metal mining investments with system dynamic modeling and real option analysis. 2016. Diss.

732. LAMPINEN, MATTI. Development of hydrometallurgical reactor leaching for recovery of zinc and gold. 2016. Diss.

733. SUHOLA, TIMO. Asiakaslähtöisyys ja monialainen yhteistyö oppilashuollossa: oppilashuoltoprosessi systeemisenä palvelukokonaisuutena. 2017. Diss.

734. SPODNIAK, PETR. Long-term transmission rights in the Nordic electricity markets: An empirical appraisal of transmission risk management and hedging. 2017. Diss.

735. MONTONEN, JUHO. Integrated hub gear motor for heavy-duty off-road working machines – Interdisciplinary design. 2017. Diss.

736. ALMANASRAH, MOHAMMAD. Hot water extraction and membrane filtration processes in fractionation and recovery of value-added compounds from wood and plant residues. 2017. Diss.

737. TOIVANEN, JENNI. Systematic complaint data analysis in a supply chain network context to recognise the quality targets of welding production. 2017. Diss.

738. PATEL, GITESHKUMAR. Computational fluid dynamics analysis of steam condensation in nuclear power plant applications. 2017. Diss.

739. MATTHEWS, SAMI. Novel process development in post-forming of an extruded wood plastic composite sheet. 2017. Diss.

740. KÄHKÖNEN, TOMMI. Understanding and managing enterprise systems integration. 2017. Diss.

741. YLI-HUUMO, JESSE. The role of technical dept in software development. 2017. Diss.

742. LAYUS, PAVEL. Usability of the submerged arc welding (SAW) process for thick high strength steel plates for Arctic shipbuilding applications. 2017. Diss.

743. KHAN, RAKHSHANDA. The contribution of socially driven businesses and innovations to social sustainability. 2017. Diss.

744. BIBOV, ALEKSANDER. Low-memory filtering for large-scale data assimilation. 2017. Diss.

745. ROTICH, NICOLUS KIBET. Development and application of coupled discrete and continuum models in solid particles classification. 2017. Diss.

746. GAST, JOHANNA. The coopetition-innovation nexus: Investigating the role of coopetition for innovation in SMEs. 2017. Diss.

747. KAPOOR, RAHUL. Competition and disputes in the patent life cycle. 2017. Diss.

748. ALI-MARTTILA, MAAREN. Towards successful maintenance service networks – capturing different value creation strategies. 2017. Diss.

749. KASHANI, HAMED TASALLOTI. On dissimilar welding: a new approach for enhanced decision-making. 2017. Diss.

750. MVOLA BELINGA, ERIC MARTIAL. Effects of adaptive GMAW processes: performance and dissimilar weld quality. 2017. Diss.

751. KARTTUNEN, JUSSI. Current harmonic compensation in dual three-phase permanent magnet synchronous machines. 2017. Diss.

752. SHI, SHANSHUANG. Development of the EAST articulated maintenance arm and an algorithm study of deflection prediction and error compensation. 2017. Diss.

753. CHEN, JIE. Institutions, social entrepreneurship, and internationalization. 2017. Diss.

754. HUOTARI, PONTUS. Strategic interaction in platform-based markets: An agent-based simulation approach. 2017. Diss.

755. QU, BIN. Water chemistry and greenhouse gases emissions in the rivers of the "Third Pole" / Water Tower of Asia". 2017. Diss.

756. KARHU, PÄIVI. Cognitive ambidexterity: Examination of the cognitive dimension in decision-making dualities. 2017. Diss.

757. AGAFONOVA, OXANA. A numerical study of forest influences on the atmospheric boundary layer and wind turbines. 2017. Diss.

758. AZAM, RAHAMATHUNNISA MUHAMMAD. The study of chromium nitride coating by asymmetric bipolar pulsed DC reactive magnetron sputtering. 2017. Diss.

759. AHI, MOHAMADALI. Foreign market entry mode decision-making: Insights from real options reasoning. 2017. Diss.

760. AL HAMDI, ABDULLAH. Synthesis and comparison of the photocatalytic activities of antimony, iodide and rare earth metals on SnO2 for the photodegradation of phenol and its intermediates under UV, solar and visible light irradiations. 2017. Diss.

761. KAUTTO, JESSE. Evaluation of two pulping-based biorefinery concepts. 2017. Diss.

762. AFZALIFAR, ALI. Modelling nucleating flows of steam. 2017. Diss.

763. VANNINEN, HEINI. Micromultinationals - antecedents, processes and outcomes of the multinationalization of small- and medium-sized firms. 2017. Diss.

764. DEVIATKIN, IVAN. The role of waste pretreatment on the environmental sustainability of waste management. 2017. Diss.

765. TOGHYANI, AMIR. Effect of temperature on the shaping process of an extruded wood-plastic composite (WPC) profile in a novel post-production process. 2017. Diss.