Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Imtiaz Uddin Ahmed

Smartphone Authentication: User experience, expectation and satisfaction

Master's Thesis

2017

Examiners:	Professor Ahmed Seffah Ossi Taipale
Supervisor:	Professor Ahmed Seffah

ABSTRACT

Lappeenranta University of Technology
School of Business and Management
Degree Program in Computer Science

Imtiaz Uddin Ahmed

Smartphone Authentication: User experience, expectation and satisfaction

Master's Thesis

86 pages, 19 figures, 16 tables, 2 appendices

Examiners: Professor Ahmed Seffah
Ossi Taipale

Keywords: Smartphone authentication, smartphone authentication method, mobile authentication, usability, security.

Context: Millions of smartphone users are using internet, storing important data, making transactions by their mobile phones. Smartphone authentication has become an unavoidable part of most of the people these days and numerous number of times users need to go through the authentication process to use their phones. In such a circumstance, users need a convenient authentication system to use their smartphones effectively with possible less amount of time spent and obviously with ensured security for protecting their important data and files. **Goal:** The aim of this thesis is to study the existing authentication methods in practice and their pros and cons from usability and security perspective, authentication methods under current research and what users prefer mostly and why they prefer it for their smartphone authentication. **Method**: A quantitative study was conducted by collecting 67 answers from smartphone users of the community of Lappeenranta University of

Technology, Finland. 43% of them were employee and 57% of them were student. **Results:** Mostly preferred authentication method is fingerprint based authentication and least preferred is PIN based authentication and ‘no authentication’. In general, 69% answers were convenience related and 31% answers were security concerned from all the participants, regardless of which authentication method they prefer. **Conclusion:** Fingerprint, a biometric authentication process has the best impact in users’ preference, mainly because it saves time for authentication and users do not need to memorize any secret, though it has some limitations regarding usability and security. Again, pattern based authentication system earned most user satisfaction.

ACKNOWLEDGEMENTS

I would like to express my heartiest gratitude to my supervisor Prof. Ahmed Seffah for providing me with good perception on my thesis work. He is always a source of factual inspiration for me not only for this thesis work but also for other course works and activities which is a substantial part of my career and personal life.

I want to say a big thanks to Syed Bilal Naqvi, a PhD candidate, who was very helpful to me throughout my whole period of thesis work. His valuable suggestions made me to focus on improving the quality of work.

I would also like to thank my wife, Syeda Fayeka Begum and my only daughter Zahraa Ahmed Inayaa for their understanding throughout my thesis work. I want to thank my only sister Dr. Bilkis Sultana who is a continuous well-wisher for me even from a long distance.

Lastly, all my good friends in LUT deserve appreciation, especially Shola Ola, Fakhrul Islam Farhad, Ahmed Yusuf and Maria Palacin Silva are mentionable for their open minds and helpful hands towards me.

Author
Imtiaz Uddin Ahmed
03.08.2017

TABLE OF CONTENTS

1 INTRODUCTION 6

1.1 BACKGROUND.. 6
1.2 GOALS AND DELIMITATIONS 7
1.3 STRUCTURE OF THE THESIS 8

2 STATE OF ART 10

2.1 USER AUTHENTICATION: DESKTOP VS MOBILE ENVIRONMENT 10
2.2 CLASSIFICATION OF MOBILE AUTHENTICATION METHODS............................... 11
2.2.1 Knowledge based Authentication...12

2.2.2 Ownership based authentication 12

2.2.3 Inherence based authentication 13

2.3 SEVERAL TYPES OF ATTACKS IN SMARTPHONES 13
2.3.1 Capturing Attacks 14

2.3.2 Cracking Attack 14

2.3.3 False Identity Attack 15

2.3.4 Physical Attacks 15

2.4 USER STUDIES 16
2.5 DETAILS OF AUTHENTICATION METHODS 18
2.6 A BRIEF DISCUSSION ON SECURITY AND USABILITY.................................... 24
2.6.1 Usability factors for mobile authentication 27

2.6.2 Security factors for mobile authentication......................................28

3 METHODOLOGY 33

3.1 RESEARCH PROBLEM AND QUESTIONS.. 33
3.2 RESEARCH METHODS.. 36
3.3 QUANTITATIVE STUDY 36
3.4 DESIGN METHODS.. 37
3.5 SAMPLING AND DATA COLLECTION 39
3.6 DATA ANALYSIS 40
3.7 DATA OVERVIEW:.. 40

4 RESULTS 43

4.1 RQ.1: WHICH AUTHENTICATION METHOD IS THE MOST PREFERRED ONE BY USERS? 43
4.2 RQ.2: WHICH AUTHENTICATION METHOD SHOWS THE HIGHEST USER SATISFACTION? 49
4.3 RQ3: WHICH ONE IS THE LEAST PREFERRED AUTHENTICATION METHOD? 51
4.4 RQ.4: WHAT IS THE CONCERN FOR PREFERRING AN AUTHENTICATION METHOD, IN GENERAL? (IS IT SECURITY OR CONVENIENCE? 55
RQ4.2 WHICH AUTHENTICATION METHOD IS MOSTLY SECURED FOUND BY USERS?.......... 57

5 DISCUSSION AND CONCLUSION 59

6 SUMMARY AND FUTURE WORK 66

REFERENCES 67

APPENDICES

APPENDIX 1

APPENDIX 2

LIST OF TABLES

Table 1. Research Questions (RQs) 8

Table 2: Survey results - Mobile User Security (Roy et al. 2015) 17

Table 3: Summary of Authentication methods 31

Table 4: Survey Research questions, goals and sections 34

Table 5: Survey Design and question design detail 38

Table 6: Survey methods 39

Table 7: Role of respondents 41

Table 8: Gender of respondents 41

Table 9: Age distribution of respondents 41

Table 10: Mobile OS used by respondents 42

Table 11: Users rating on convenience and security of fingerprint authentication method 45

Table 12: Difficulties in using fingerprint 48

Table 13: Answers given in free text fields for difficulties in using fingerprint 48

Table 14: Calculations of satisfaction rating level for different authentication methods 49

Table 15:Rating of users for the convenience and security of using PIN 54

Table 16: Rating of users for the convenience and security of using password 57

LIST OF FIGURES

Figure 1: Classification of authentication methods (Walailak J Sci & Tech 2015; 12(1)) (Vongsingthong & Boonkrong 2015) 13
Figure 2: Global users of desktop and mobile devices (Chaffey 2016)........ 17
Figure 3: Time spent in Internet by different device users (Chaffey 2016) 18
Figure 4: The relation between security and usability based on negotiation (Braz,Christina;Seffah,Ahmed and MRaihi 2007) 25
Figure 5: Preference of choosing different authentication methods 43
Figure 6: Demographics of fingerprint authentication method 44
Figure 7: Answers of multiple selection questions based on convenience and security 45
Figure 8: Users rating on convenience and security for fingerprint authentication method 46
Figure 9: Users satisfaction level for fingerprint authentication method 47
Figure 10: Problems faced by participants in using fingerprint authentication method 48
Figure 11: Average user satisfaction in using different authentication methods 50
Figure 12: Answers of multiple selection questions based on convenience and security ... 51
Figure 13: Demographics of PIN as an authentication method 52
Figure 14: Reasons for using PIN 53
Figure 15: Users rating on convenience and security for using PIN 54
Figure 16: Problems faced by users in using PIN as an authentication method 55
Figure 17: Usability and security related issues regarding all authentication methods 55
Figure 18: Users preference for increased satisfaction 56
Figure 19: Users rating on convenience and security for fingerprint authentication method 58

LIST OF SYMBOLS AND ABBREVIATIONS

PIN	Personal Identification Number
OS	Operating System
OTP	One-Time Password
SIM	Subscriber Identification Module
RFID	Radio-Frequency-IDentification
NFC	Near Field Communication
RQ	Research Question
MFA	MultiFactor Authentication

1 INTRODUCTION

1.1 Background

Smartphone, the highly popular device of the current era is a frequent storage medium of many sensitive information i.e confidential documents, trade secrets, credentials and many other personal data. One of the supreme importance is to provide security for user data and to control unauthorized access, as mobile devices can be easily lost or stolen. As a result, user authentication is quite essential for protecting the system which can be considered as a first defensive step. However, there is compromise between the usability and security for authentication of mobile devices. For example, one-shot authentication solutions are easy to use but vulnerable to theft and loss. On the other side, periodic authentication or automatic logouts after a certain period of inactivity are likely to be inappropriate from user's perspective (Feng et al. 2013a). The clumsy input methodology of smartphones and different user expectations still contradict with the need for strong authentication, especially if it is compared to the standard authentication solutions. As shown in a study of over 6,000,000 passwords, 91% of all user passwords belong to a list of just 1000 common passwords (e.g., 8.5% users use either "password" or "123456" as their passwords) (Feng et al. 2013a). Moreover, the standard biometric authentication techniques are not massively available to be adopted on mobile devices due to the additional cost. (Feng et al. 2013b)

Besides holding the sensitive data mobile devices provide access to even more data and services through Internet. Privacy falls at a substantial risk even if only temporarily a mobile device gets into non-entitled persons. Authentication protects devices from such unauthorized usage. Various authentication mechanisms are offered nowadays by operating systems of different smartphone. Nevertheless, either they are not enough user friendly to be broadly implemented or vulnerable in some situations. (Schlöglhofer & Sametinger n.d.)
The goal of the authentication is to ensure secure access to systems and services. Whereas different attacks against authentication may result mimicking genuine users by illegitimate users. Thus, attackers can take control of systems and services to continue different activities in the name of the legitimate users which is a great threat against confidentiality, availability and integrity. (Schlöglhofer & Sametinger n.d.)

Most of the smartphone users depend on a feature (authentication method) that lets them to ‘lock’ their smartphones using either PINs, swipe patterns or passwords (Ali et al. 2016a). These widely used authentication methods have some constraints. At first, these are single factor authentication methods where it is assumed that only legitimate users will have the knowledge of the PIN, password and swipe pattern. However, it is easily possible to conduct a social engineering attack by attackers. Shoulder surfing is an example of this kind of attack to steal authentication codes. Most of the mobile phone users do not have many options for authentication outside of these methods. Again, these methods are “annoying” to almost half of the users (Ali et al. 2016b). It is also can be a cause of frustration for having to authenticate device many times a day even after a relatively short time interval of using the feature of phone. Because of this, only 36% of users lock their smartphones (Ali et al. 2016b). Furthermore, those even who lock their phone use PINs or pattern to lock their devices whereas passwords are more secure option for authentication. This is expected because it takes less time to authenticate by using PINs or patterns comparing to passwords, as it is hard to type alphanumeric keys in small screen of mobile phones. This emphasizes on the importance of authentication methods to be personalized which will reduce the frustration of users. (Ali et al. 2016a)

1.2 Goals and delimitations

The foremost challenge faced by the system designers of smartphones is to make the authentication methods both secure and usable. It could be easily possible to make authentication much more secure by ignoring user needs. Where average users unlock their phones 50 times per day, authentication process must be fast and convenient for operators to use otherwise most of the users will not be able to operate it (Luca & München 2015).

The aim of this research is to investigate various smartphone authentication methods from usability and security perspective and identifying the most prevalent authentication methods and practices used in smartphones.

Table 1. Research Questions (RQs)

Research Question (RQ)		Goal	Action
Q.1. What are the diverse types of authentication methods?		Identifying the growth of existing and upcoming authentication methods.	By literature review
Q.2. What are the difference in user authentication for desktop/laptop and mobile phone environment?		Understanding the area of focus for smartphone authentications.	By literature review
Q.3. What are the user experiences in smartphone authentication	Q3.1. What mobile OS do users prefer mostly to use?	Identifying the most leading authentication methods and user preferences	By conducting a survey
	Q3.2 Which authentication method is used mostly? When and why they are used?		
	Q.3.3. What are the satisfaction level of different authentication methods?		

However, the focus of the research will be for smartphones only, not for laptops or any other handheld devices. The research will not cover the technical development details of smartphone authentication methods, rather it will emphasis on usability and security issues.

1.3 Structure of the thesis

This research work is divided into 6 chapters. The breakdown of each chapter is given below:

Chapter 1 titled: Introduction that provides information about the research background, the goals and delimitation of this research work.

Chapter 2 titled: State of the Art explores different research work relating to smartphone authentication methods.

Chapter 3 titled: Methodology presents procedure of carrying out this research using literature review and by conducting a survey using mostly close ended questionnaires under quantitative research method. This chapter presents the research organization and categorization of participants in the survey and the theme of the survey.

Chapter 4 titled: Results shows the result from the survey. The result from this chapter provides information about why users use the preferred authentication methods and under what circumstances.

Chapter 5 titled: Discussion and Conclusion demonstrates the arguments from the findings of research.

Chapter 6 titled: Summery and Future work concludes the research work and deliberates future activities of research.

2 STATE OF ART

2.1 User authentication: Desktop Vs Mobile environment

From the initial period of smartphones, the nature of user authentication has remained mostly unchanged. A Personal Identification Number (PIN) is used vastly as a point-of-entry protection in mobile devices. Similar situation is also seen in desktops where authentication approaches mainly relies on secret knowledge. However, users of mobile devices may use multiple mechanisms to lock various aspects of functionality. For example, Windows Mobile handsets support two distinct authentication mechanisms, such as, one to protect mobile device and other to protect user's SIM (Subscriber Identification Module). The frontline protection of the handset is ensured by device-level authentication, particularly when the device is switched on. Therefor device-level authentication guards access to applications and user's stored data in the phone. Whereas SIM-level authentication provides the safety of the contents of SIM and cellular network account. Otherwise, SIM card can be removed from authorized device and can be used in any unauthorized device. Thus, SIM level authentication effectively governs the use of cellular data and restricts from making voice calls. One of the unique difference between smartphones and desktop computers is that smartphones are solely personal device, typically used by one user. Whereas desktop computers are often shared by different users. The small sized smartphones are vulnerable to unauthorized use by loss and theft. Consequently, smartphone authentication and identification is different than desktop authentication methods. (Botha et al. 2009)

Potential attackers receive a powered and operational device in case of loss or theft as smartphones are typically always-on devices. User needs to be authenticated to the phone before usage to prevent unauthorized usage and to ensure the protection of stored data. The phone should be locked after user completes his/her tasks, for this reason smartphone operating systems usually provide short but frequent sessions. As a result, a significant impact on the usability of smartphones relies on the chosen authentication method by user. The speed and comfort of use are the key two factors for most of the users while deciding about the authentication methods whether to enable or not according to D¨orflinger et al., 2010 (Luca & München 2015).

As smartphones are very flexible for movements, these are often used in doubtful places with a vast number of potential observers. A user friendly and easy approach of authentication needs the independence of the environment the phone is used in, besides ensuring security. For the authentication on smartphones few requirements are listed below from (Luca & München 2015):

- A user needs to authenticate before each and every session
- A passing observer should not learn anything about the secret used for authentication
- Authentication should be secure and fast with minimum user effort

Authentication methods available in practice nowadays are not able to fulfil all these requirements. PIN/Password authentication is mostly common method which requires time consuming user interactions (typing again and again for each time while unlocking the phone). Therefore, most of the users prefer to use easy to type, short Password/PIN and eventually less secured especially when used in crowded public places. Graphical pattern is one of the alternatives of PIN/Password based authentication which has a benefit of faster input but comparatively easier to learn by casual observers and it is a security threat. Biometric based authentications, such as fingerprint or facial recognition are still not widely installed due to the additional cost and can be dodged by using a fake fingerprint or a simple photograph. (Luca & München 2015)

2.2 Classification of mobile authentication methods

“Authentication is the process of determining whether a particular person or device should be allowed to access a system, an application, or specific data on a device” (Sametinger et al. 2012). Authentication method is a process which is a vital security mechanism. There are three basic categories in which authentication methods can be broadly classified. Such as, knowledge based authentication (what we know), ownership based authentication (what we have) and inherence based authentication (what we are). These types are briefly discussed below: (Sametinger et al. 2012)

2.2.1 Knowledge based Authentication

PIN/Password based authentication is an example of knowledge based authentication or "what we know". Graphical patterns/passwords besides questions and answers are another example of this type of authentication. The device is being authenticated by the use of knowledge. Here, there is a possibility that secret knowledge passes to unauthorized hands. Anyone who has the knowledge of secret for the device authentication is capable to use it for authentication. Challenge-response authentication depends on knowledge too. Password authentication is a simplest example of challenge-response authentication where asking for the password is the challenge and the only valid response is the password itself.

Graphical passwords are a way to avoid numerical/alphanumerical passwords which are hard to remember as human brain is more capable of remembering visible images rather than complex strings of characters. There are recall based and recognition based graphical passwords. User needs to remember images in recall based systems. Recognition based systems requires users to identify images whether they have seen an image before. In this system images that are seen already has to be recognized rather than generating from memory. (Sametinger et al. 2012)

2.2.2 Ownership based authentication

Ownership based authentication ('what we have') includes the example of smartcards and electronic tokens. A key which opens a door is an example of real life ownership based authentication. Anyone can enter the door who has the proprietorship of the key. It is also possible to have copies of the key to allow multiple people to enter the door. Radio-Frequency-Identification (RFID) tags or magnetic strip cards are digital example of this type of authentication. For short distance communication, up to 10 cm Near Field Communication (NFC) is a standard for radio communication. Ownership authentication based NFC tags need to be hold closely to the NFC tag reading device. The identification number of the NFC tag can be used for comparison. Generation of secure passwords is an advantage of ownership based authentication but to remain in the ownership of the item a safe care has to be taken. If the item is lost or stolen then another person can successfully authenticate himself/herself. If copies of the item created and left unnoticed then it becomes a great threat.

Ownership based authentication is not yet in practice for smartphone authentications. (Sametinger et al. 2012).

2.2.3 Inherence based authentication

‘What we are’ type of authentication or inherence based authentication includes biometric based authentication methods. Fingerprints, the iris, faces, handwriting, voices, the gait, gesture and so on are the example of biometric characteristics. These characteristics can be classified as static and dynamic. Static methods focus on what a person is and dynamic methods emphasis on how a person acts or does something. Fingerprints are widely used for many decades to verify personally as a biological recognition technique. Recently automatic fingerprint recognition has been introduced in smartphones by few manufacturers which is still not widely available due to the additional cost. Face recognition was the only mechanism by inherence earlier provided by android. (Sametinger et al. 2012)

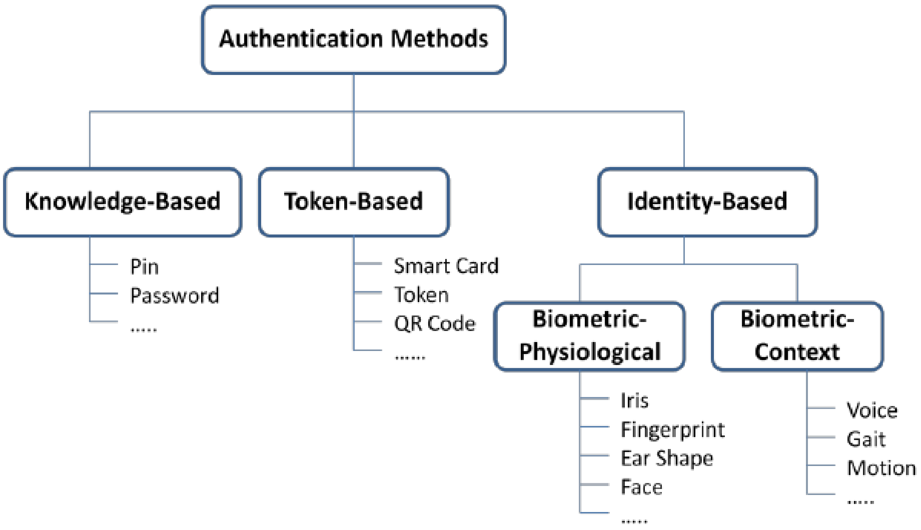


Figure 1: Classification of authentication methods (Walailak J Sci & Tech 2015; 12(1)) (Vongsingthong & Boonkrong 2015)

2.3 Several types of Attacks in smartphones

Systems and services needs to be secured using authentications. Unauthorized users may take control of the authorized users due to attacks against authentication. In the name of legitimate users, attackers can perform activities by using systems and services. Confidentiality, integrity and availability fall into great threat for this (Sametinger et al. 2012). Thus, several types of attacks are briefly discussed below as they are an issue in our context:

2.3.1 Capturing Attacks

Things that may be captured are involved in capturing attacks. Shoulder surfing, eavesdropping, social engineering are the examples of this type of attacks. The art through which people are manipulated for performing certain actions or for disclosing confidential information is known as social engineering. In enterprise level, usually people do not know personally all the staff members of technical support team and social engineering is commonly seen in this environment. Sometimes only a phone call is enough to receive essential information. Watching someone entering secret information, is defined as shoulder surfing. For example, gesture is used often on a smartphone for authentication and it can be guessed quite easily. Spyware is another method of capturing, i.e., malware which accumulates users' information without their concern. Information about authentication also may be included in this knowledge of malware. Authentication on mobile devices is inclined to these capturing attacks, such as, social engineering, shoulder surfing and spyware. Eavesdropping could become a factor if authenticating wirelessly, for example, by NFC tag, yet it is not an issue. (Sametinger et al. 2012)

2.3.2 Cracking Attack

In cracking attacks, interactions with authentic users is not required which is opposite of capturing type attacks. Cracking encompasses systematic approaches which try to find out successful authentication that a system accepts. If users fail to create a strong password then guessing may be successful. Password which is weak and insecure usually easy to remember but it is also easy to guess. Guessing attacks are typically mutually connected with social engineering where attackers want and try to get information about users, as much as possible. Attacker first try weak and commonly used passwords and therefore, weak password users are more prone to attack. In the time of creating passwords, avoiding use of personal data is recommended which may include date of birth, residential place, spouse name or child name etc. A list of commonly used passwords is used by dictionary attacks whereas Brute-force attacks use any combination of possible characters. Brute-force attacks and dictionary attacks are combinedly form hybrid attacks. Systematic modifications like appending few characters or switching upper and lower-case characters in passwords are made from a probable list of passwords. Typically, dictionary and brute-force attacks are done automatically. In principle, they can be performed in our context, but without automation they still remain in the category of guessing. (Sametinger et al. 2012)

2.3.3 False Identity Attack

Attackers may mislead authentic users by pretending using false identities. In spoofing attacks, someone can coverup as genuine user by falsifying data. Email spoofing, IP spoofing, website spoofing and referrer spoofing are the example of some forms of spoofing. (Sametinger et al. 2012)

For example, the creation of a hoax website which seems alike to the original website is known as website spoofing. The objective of website spoofing usually is to acquire sensitive information, e.g., credit card details. A special form of spoofing attack is the man-in-the-middle attack. In this type of attack, an independent connection between users and servers is made by attackers. Attackers can control whole conversation between two interconnected parties if they are able to interrupt all messages between these parties. Thus, they can get access to sensitive information of these parties even if it is encrypted. In this context of thesis, phishing can be considered as an issue while a rogue application perhaps gives a fake authentication screen and trap a user for revealing his/her credentials. In the context of mobile devices, man-in-the-middle attack and spoofing is not appropriate. (Sametinger et al. 2012)

2.3.4 Physical Attacks

Theft and duplicates are the examples of physical attacks. Things that we own can be taken from us or a duplication is possible. Attackers cab not steal something like password that is in our head but a smart card or a smartphone can be stolen. A password can be stolen only if we write it down somewhere, for example in a sheet of paper and the incident can be happened even without our concern. This is also true for duplicates. Dumpster diving also falls into this category as attacker may find the sheet of paper with written password from the garbage. Another form of physical attack is hardware manipulation. It may be observed in duplication. ATM skimmer is a common example where attackers make a copy of the ATM card by adding hardware to the regular ATM and keeping an eye on the legitimate user while entering PIN. In case of mobile device, hardware manipulation can hardly be unnoticed but theft, duplicates and dumpster diving can be considered as threat in our context. (Sametinger et al. 2012)

2.4 User studies

The need for continuous authentication can be observed by means of two user surveys (Roy et al. 2015). In the surveys, it has been demonstrated that participants are worried about the stored data on their phones and most of the participants observed someone else’s PIN in previous which indicates that most of the existing authentication mechanisms are not robust enough. Thus, the surveys showed the necessity for the development of alternatives to PIN based or pattern based authentication methods. Among two surveys, 47 participants of a northeastern university filled the first survey and 267 participants participated in the second survey which was conducted online (Roy et al. 2015). Both the surveys were designed keeping focus on the usage of mobile and usage of authentication mechanisms by participants. It has been seen by the studies that most of the participants keep their phones locked by means of any authentication mechanism. The number was 87% in first study and 82% in the second study. In both surveys, most of the participants were concerned about someone else would access their data in their absence (55% in the first survey and 71% in the second survey). In addition, 73% of participants in the second survey observed the PIN of a friend or a family member and 79% said that they knew the current PIN of someone else. This can raise a question about the safety of current locking mechanisms or authentication methods. The summery is presented below in Table 2 (Roy et al. 2015):

Table 2: Survey results - Mobile User Security (Roy et al. 2015)

	Study 1	Study 2
No of Participants	47	267
Lock the phone	87%	82%
Use PIN or Pattern lock	87%	81%
Worried about data privacy	55%	71%
Observed someone else's PIN	___	73%

It has been observed that most of the users are concerned about data privacy and are using any mechanism to lock their mobile devices. Interestingly, in second study it has been seen that most of the users looked at someone else's PIN in any earlier time. **(Roy et al. 2015)**

The following graph shows that how the number of mobile users increased since 2007. The graph gives a clear indication of rising mobile users over the world and eventually it crossed the number of desktop users after 2014 and going upwards.

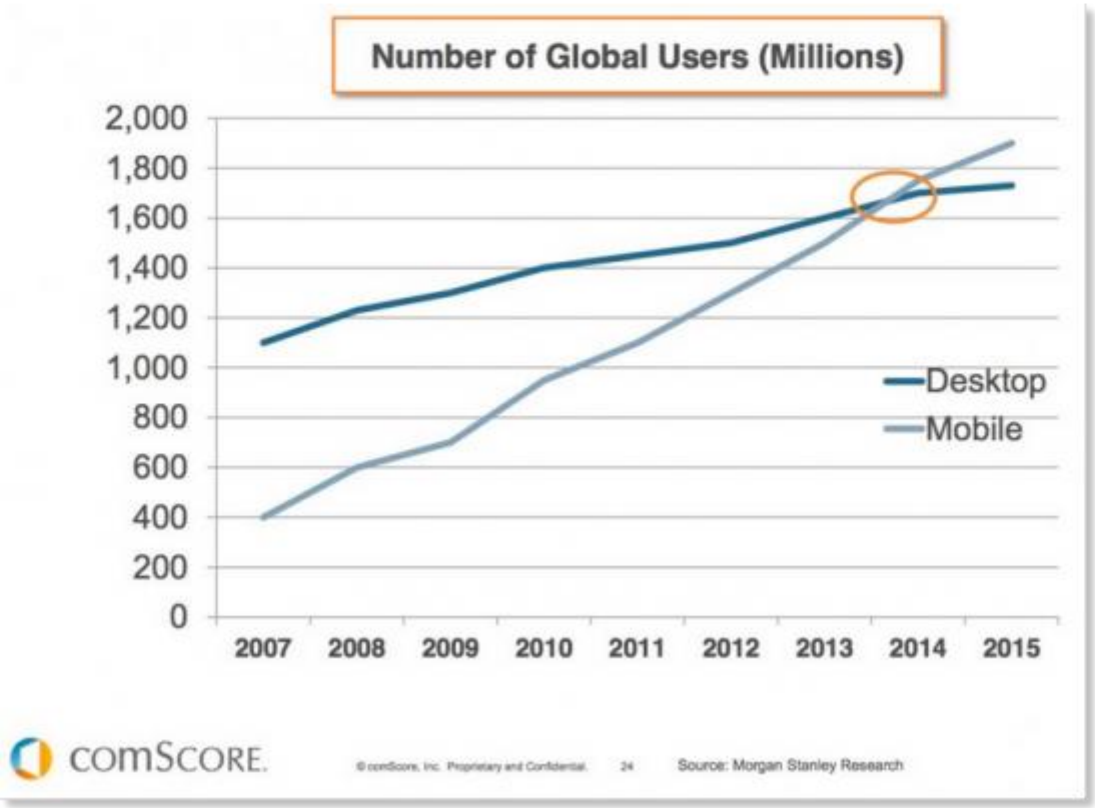
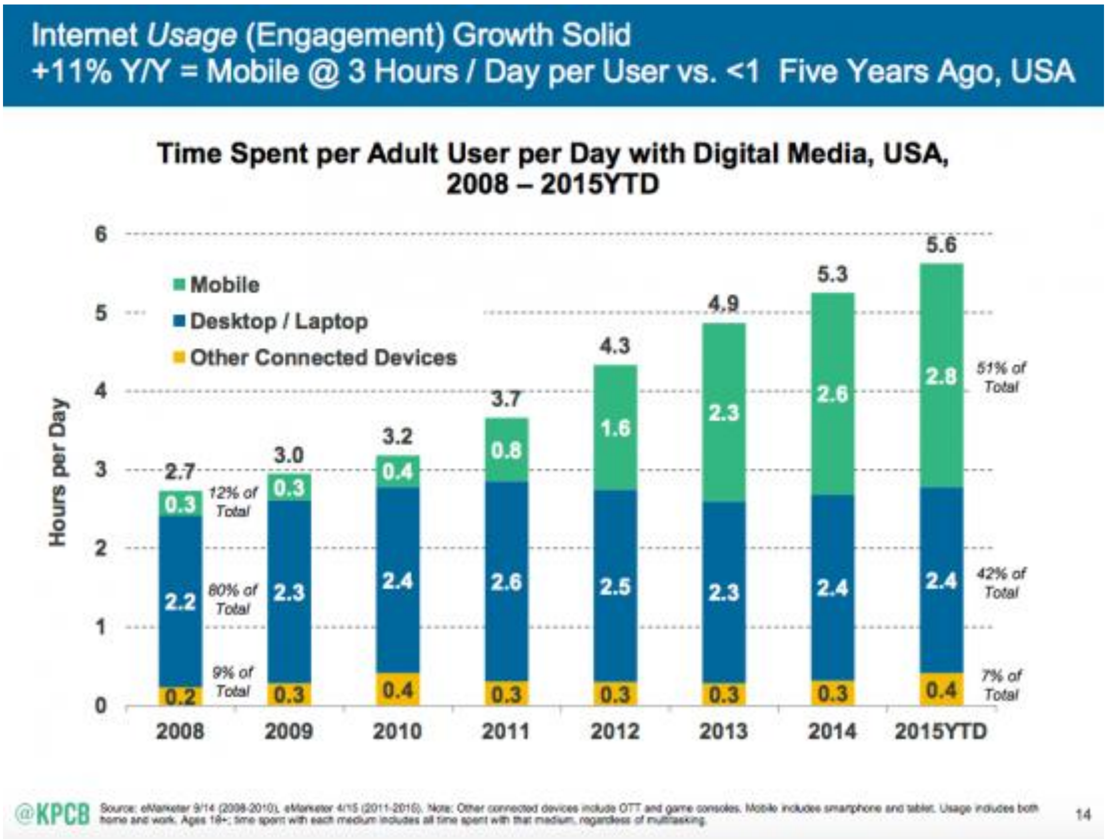


Figure 2: Global users of desktop and mobile devices (Chaffey 2016)

From the graph below, it is seen that mobile digital media time spent in the USA pointedly advanced which is 51% compared to desktop (42%). Users are spending much time with mobile phones in their daily life than any other devices.



Internet *Usage* (Engagement) Growth Solid
+11% Y/Y = Mobile @ 3 Hours / Day per User vs. <1 Five Years Ago, USA

Source: eMarketer 9/14 (2008-2010), eMarketer 4/15 (2011-2015). Note: Other connected devices include OTT and game consoles. Mobile includes smartphone and tablet. Usage includes both home and work. Ages 18+; time spent with each medium includes all time spent with that medium, regardless of multitasking.

Figure 3: Time spent in Internet by different device users (Chaffey 2016)

2.5 Details of authentication methods

This section represents the authentication methods under review in this article. All of them are not well practiced for mobile authentication though. Despite of not being a comprehensive list, the authentication methods in this section are an extended set of those presented in NIST Special Publication (SP) 800-63-2 (Burr et al. 2013) and NISTIR 8014, *Considerations for Identity Management in Public Safety Mobile Networks*, Identity management, authentication factors, and user and device identity, these types of topics are all addressed in NISTIR 8014, and act as a basis for the present effort. (Choong et al. 2016)

Knowledge-Based Authentication:

Preregistered knowledge tokens, which are predetermined information and/or questions with answers embedded with a system, are used for authentication in Knowledge-based authentication (KBA) system. Sometimes for identity proofing purposes these this type of authentication is used, but this usage is excluded from the scope of the thesis as it is not related with mobile authentication yet. Additionally, it is widely considered as a weak form of authentication and hence it is not recommended. (Choong et al. 2016)

Password and PIN:

These are referred as memorized secret tokens by NIST SP 800-63-2. Generally, PINs are numeric and short whereas passwords can permit a series of alphanumeric keys, special characters, different lengths, supporting pass phrases by including spaces. (Choong et al. 2016). Nowadays, graphical passwords are also under research as a means of authentication.

Gesture:

A gesture is a pattern for connecting a set of points or shapes drawn on a touchscreen. Though gestures are not clearly referenced within NIST SP 800-63-2 (Burr et al. 2013), still they appropriately matched with the definition of memorized secret tokens (Choong et al. 2016). More advanced behavioral measurements like speed, pressure, trajectory of gesture entry is excluded from this thesis for the analysis of gesture/pattern based authentication mechanism.

Ownership Based Authentication

One-Time Password Device:

The devices used for generating one-time password with a short lifespan are known as One-time password (OTP) devices. Usually, with the combination of memorized secret tokens like a password, OTPs are used. A valid OTP (something a person has) and the password/PIN (what a person knows) are presented as a proof of possession of the device, which results a multifactor authentication solution. Typically, a small electronic display is used for presenting passwords by OTP devices which are often key fobs and after some prespecified time (for example, one minute) these passwords change. This password is also known by the backend entity for performing authentication. A software based OTP like mobile application for generating new OTPs continuously, is a sub-classification for OTP devices. (Choong et al. 2016)

Embedded Cryptographic Token:

A user or a device can be authenticated by hardware and/or software components containing a cryptographic key know as embedded cryptographic tokens. A cryptographic protocol is used to identify possession of the key to accomplish the authentication. If anyone is in ownership of the token can use it for the authentication to a system or service then embedded cryptographic tokens considered as a method of single-factor authentication. Often multifactor authentication is possible by cryptographic tokens by making users to authenticate to tokens, for example, by using a PIN, and thus get the secret or private key. (Choong et al. 2016)

Removable Hardware Cryptographic Token:

The physical devices which provide reliable storage and other cryptographic processes like reliable key storage, for example, smartcards, Universal Serial Bus (USB), and MicroSD security tokens are the example of removable hardware cryptographic token and these types of tokens can possess a processor like a smart card for providing capabilities. Some hardware cryptographic tokens such as the Universal Integrated Circuit Card (UICC) and informally Subscriber Identity Module (SIM) card that exists in a mobile device require much effort to remove while others are easily removable. (Choong et al. 2016)

Smartcard with External Reader:

Multi-factor smartcards incorporate a processor capable of executing complicated cryptographic operations and may be used to save identification secret like digital certificates which is possible to unlock by a knowledge based secret token, i,e a PIN. Smartcards used in this way are referred as multifactor cryptographic tokens by NIST SP 800-63-2 (Burr et al. 2013). The size of smartcard readers is generally very large and it is not feasible to be built in mobile devices. For this it needs an eternal smartcard reader for accessing saved credentials. Integrated smartcard readers are uncommon for mobile devices, specifically for smartphones though it is usual for desktop environment. (Choong et al. 2016)

Near Field Communication (NFC) Enabled Smartcard:

Without a large external card reader, multifactor authentication (MFA) can be accomplished by this approach. A mobile device can access stored credentials in a smartcard by wireless communication if a smartcard is placed very close to an NFC-enabled device. For this, users need to keep the card very close to the mobile device because smartcard holds the protecting credentials. (Choong et al. 2016)

Proximity Token:

Based on the intimacy of the token to the system, a proximity token permits a user to have access to the system. Usually these tokens stay connected to a system and it revoke access when the connection is lost. Users can wear proximity tokens in their body which can be a subcategory as a wearable proximity token. These wearable tokens can be used as rings, on sleeves, or any other suitable part of the body or equipment. Memorized secret tokens or other software tokens can be used with wearable tokens as a combination to establish a multifactor solution. These wearable proximity tokens, probably using NFC, radio-frequency identification (RFID), Bluetooth Low Energy (LE), or other wireless technologies may be supported by the Universal 2nd Factor (U2F) open authentication standards from the FIDO (Fast IDentity Online) Alliance. (Choong et al. 2016)

Inherence Based Authentication

For the following four **biometric** authentication methods, sample of users has to be stored in the system for authentication, means they require initial enrollments. Samples can be stored locally (on the device storage) or remotely (in a central repository). For the identification of individuals these biometric modalities are commonly used. (Choong et al. 2016)

Fingerprints:

In modern mobile devices, the most commonly used biometric is fingerprint. Optical, capacitive, ultrasonic are the example of multiple types of fingerprint sensors. Each of them has unique styles of assessing features of a biometric sample. Usually, fingerprint scanners on mobile devices may have impact on accuracy due to the smaller surface area (may affect resolution) comparing to the traditional scanners. (Choong et al. 2016)

Facial Recognition:

In facial recognition, a picture of user’s face is captured by phone’s camera and it is compared with the previously captured and stored picture of the same user during registration/enrollment. This authentication scheme is available in several mobile device platforms but not widely practiced by users. (Choong et al. 2016)

Iris Recognition:

Patterns of an individual’s iris is identified in iris recognition. AS a COTS video camera is not sufficient enough always for iris scanning, so this method is not offered by many modern generation mobile devices. (Choong et al. 2016)

Speaker Recognition:

In speaker recognition, a user’s voice sample is taken by the microphone of a mobile device for the authentication of a user. In most of the recent mobile phones sensors for voice recognition are available. (Choong et al. 2016)

Focus of new research area

According to new studies, (Choong et al. 2016) the key focus area of authentication methods is on passive and continuous authentication of users as users have the control over their devices whereas in traditional methods discussed above, authentication is generally performed at the beginning of system usage. For example, number of different characteristics of users such as, a user's distinct typing pattern, usage of cursor, cognitive processing time can be used to monitor users continuously and to authenticate them, which can be referred as continuous authentication. It is required that users establish a profile first by interacting with the system they want to use in continuous authentication systems and then activities during the usage of phone are compared with user's known profile. Few examples of continuous authentication methods are briefly discussed below which are actually not to be used like or replace a traditional authentication scheme, instead to support other authentication mechanisms:

Keystroke Dynamics:

It is possible to identify a user for authentication by using his/her time intervals and pressure of keyboard presses. It can be used in mobile devices though typically it is applied to traditional keyboards. (Choong et al. 2016)

On-Body Detection:

If accelerometer of a mobile device is active then this mechanism keeps the device unlocked (when the device is attached with a moving user) and when the accelerometer is inactive the device is locked (movement is not detecting). (Choong et al. 2016)

Location-Based Awareness:

A user's location can be identified through device's Global Positioning System (GPS) location, IP address or proximity to a specific wireless network and this location can be used for the support of authentication of a user. (Choong et al. 2016)

2.6 A brief discussion on security and usability

One of the primary issues of current IT world is to make systems or services as easy as possible for the end users ensuring the security as well. For example, at the 2003 Computing Research Association's conference "Grand Challenges in Information Security & Assurance" (Anon 2003), the need to create better end-user security controls was identified as one of four "grand challenges" facing computer security researchers. In 2005, the President's Information Technology Advisory Committee identified improved techniques for end-user security as one of nation's foremost priorities for cyber security research. (Anon 2005)

A general concept for the systems development is that security is highly associated with functionality and usability is whereas mainly connected with user interface. Both usability and security can differ depending on the circumstance of use that consists of user profiles, job uniqueness, hardware (including network equipment), software, and physical or organizational environments. Following figure represents a key correlation between security and usability.

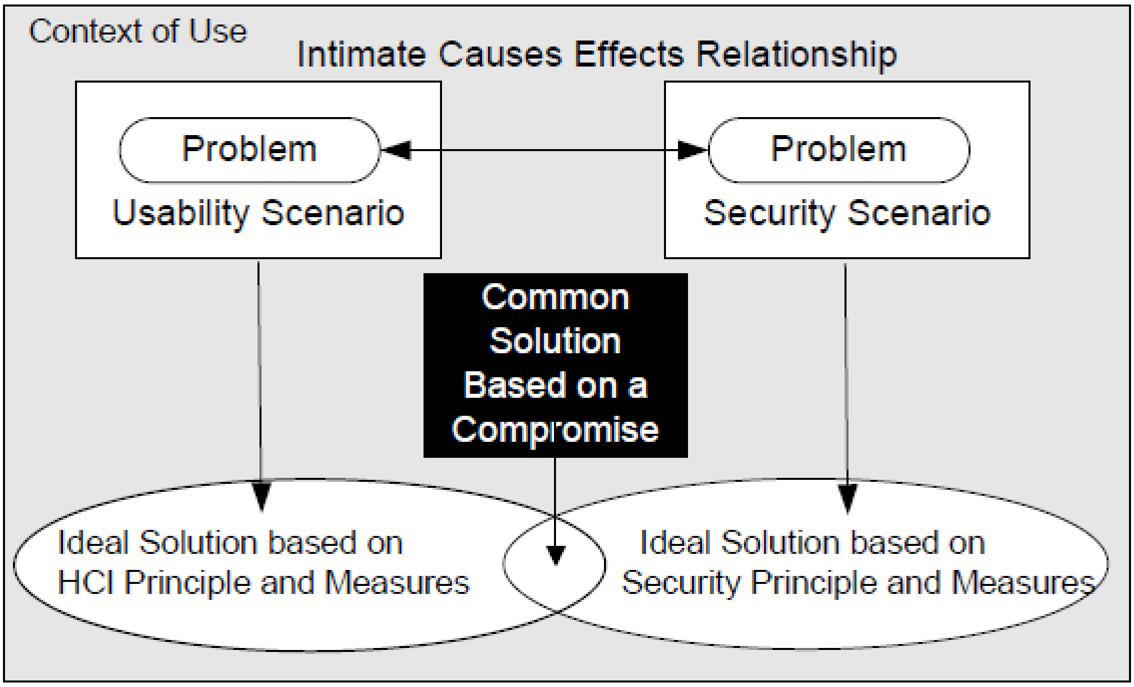

Context of Use
Intimate Causes Effects Relationship
Problem
Usability Scenario
Problem
Security Scenario
Common Solution Based on a Compromise
Ideal Solution based on HCI Principle and Measures
Ideal Solution based on Security Principle and Measures

Figure 4: The relation between security and usability based on negotiation (Braz,Christina;Seffah,Ahmed and MRaihi 2007)

Few reasons for which security specialists failed to deal with usability

One reason for the failure of security specialists to address usability issues is that traditionally security and usability are not mutually friendly enough during the development of a system. From (Garfinkel 2005), there are few possible reasons stated below:

The importance on cryptography

For the development of operating systems and encryption technologies with high security and was very challenging that there was less highlighting to work on usability issues. It is possible that serious importance on cryptographic practices to protect information is one of the main reasons for limited attention to the issues of usability. (Garfinkel 2005)

Focusing on bug fixing, rather than secure design

Bug fixing and antivirus systems are short term solutions to the considered long term problems. They are like first aid treatment without focusing on the basic reason of diseases. For hard-to-use software usually people are provided training instead of redesigning the software to make it easy-to-use. However, it is a cost-effective prospect which also helps not to fix the underling facts. (Garfinkel 2005)

Highlighting on new tools, rather than secure operations

For most of the institution's management it is trouble-free to plan for purchasing new tools hoping that these tools will improve the overall security and the organization will be benefitted instantly for short term. Whereas it is really a challenging decision for an organization to change the internal practices and processes to an approach which will definitely increase short-term expenses even though it will reduce long term expenses considerably. (Garfinkel 2005)

Few reasons for which usability specialists failed to deal with security

Usability is "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use." (ISO 9241-11) Sometimes technologists implement security systems that meet necessities but do not imitate the way people really work. For example, to protect patient information, access control and traceability usually are applied as individual health personnel accounts which are protected by passwords. However, this type of access management can actually hinder the immediate release of care (Nielsen 1993). Following reasons are stated from the work of (Garfinkel 2005):

Historical apathy in security

Many early works on usability just overlooked the issues related with security though it was a significant part of the general problem. Nielsen presents in his paper "Iterative User-

Interface Design," (Nielsen 1993) the results of four usability studies, three of which have security functions in a vital role.

Usability researchers were busy

The field of usability came into sight in the 1980s and 1990s and on that time researchers were more active to look at the basic issues of usability, such as to find out feasible use of graphical input and output devices, the prospective of handheld computing and to determine the effective way of accessing the huge information which could be stored in optical disks. This is another reason of usability researchers for not paying much attention on security issues. (Garfinkel 2005)

2.6.1 Usability factors for mobile authentication

The usability of today's mobile devices is inclined by two features: 1) the usage of touch screen and 2) the time of exposing to the device. Moreover, the complexity is evaluated in terms of how much users need to recall for an effective authentication, and the dependability of the system (Sametinger et al. 2012).

Touch screen:

In case of PINs and passwords, the usability is inadequate in the case of mobile devices because mobile devices do not have keyboard like computers, rather they are typically equipped with a touch screen. Variation of uppercase and lowercase letters, digits and special characters are available in virtual keyboards, are unsuitable for security whereas gesture puzzle, unlock pattern, secure lock is more suited for authentication in android phone by touchscreen. NFC tags are not dependent on screen and keyboard (Sametinger et al. 2012)

Duration:

For user acceptance, it is crucial to consider the duration of the authentication process. It is estimated unevenly that it takes 4 seconds to enter a PIN and 10 seconds to enter a standard-length password. The time required for unlock pattern and face unlock is less than a PIN. It is necessary to mention that the unlock pattern in Android devices is secured only if it uses a long path. But the longer the pattern, the more time it takes to authenticate which reduces the usability. Therefore, to reduce the time required, most users prefer short patterns. In case of Gesture Puzzle, it takes a little longer as the users have to analyze the images in the relevant area unlike the unlock pattern. In case of NFC, it takes 2-5 sec to authenticate, based on where the tag is carried and how easy it is to access. As Secure Lock combines both Gesture Puzzle and NFC tags, it will take a little longer time to authenticate. The time estimated for Secure Lock is 5-8 sec, which is less than the input of a standard-length password. (Sametinger et al. 2012)

Complexity:

From human perspective, it is easier to remember images compared to text except a text which is short like a four-digit PIN. Unlock patterns can be quite multifaceted if it is not a simple geometric shape like square or circle. It is same in case of Gesture Puzzle with the additional burden of remembering more than one pattern in addition to sets of images. (Sametinger et al. 2012)

Reliability:

Reliability of Android's Face Unlock is promising but it still requires substantial improvement as it has usability problems. For example, it is hard to recognize the faces of people in lower light or in darkness. As the front camera of the mobile devices is used for authentication, it is hard to correctly recognize the faces in low light because the front camera has no flash light. (Sametinger et al. 2012)

2.6.2 Security factors for mobile authentication

Security is one of the biggest issues which is needed to be considered while authenticating on a mobile device. Some of common security factors for mobile authentication are described below:

Social engineering:

It is a very well-known security factor which takes in the manipulation of people to disclose private evidence like PIN or password. Social engineering may also result in the revelation of a picture in possible uses of Face Unlock. NFC tags are also accessible if the attacker can come adjacent sufficiently to read the tag. Gesture Puzzle is assumed to be tough to social engineering as numerous passwords are used and a sequence of images plus the matching gesture would have to be exposed for each password. (Sametinger et al. 2012)

Shoulder surfing:

It is easier to identify a PIN or an unlock pattern for someone who is watching a user. A long password is fairly tougher to recognize because of its length while unlock patterns are susceptible to shoulder surfing as they are drawn on the screen and can be recognized even from a distance. All the other mechanisms do not post threat while being watched by others. (Sametinger et al. 2012)

Malware:

Malware is the oldest and most common security threat. It can appear in various forms. For instance, spyware or fake applications can run in the background, log user input and send it to a server controlled by the invader. The attacker may try to get physical access of the device if the authentication data goes to server and when a user is entering a PIN or a password it is easy to log a user’s input. In case of NFC, the only information needed is an image or the identification number of the NFC. It is also easy to create a user interface similar to the screen dialog to take the PIN or password from the user by a malware. Gesture Puzzle ensures some protection because the input depends on images shown to users. (Sametinger et al. 2012)

Guessing:

It is possible to generate random PINs or passwords using an application by an attacker, which can be tried after certain interval. If the interval is short, the device might deactivate itself due to the increased number of unsuccessful tries. As fingers leave greasy remainder on the touch screen, it is possible to trace the pattern used for Unlock pattern. Face Unlock, NFC tags and Secure Lock do not permit any form of guessing. (Sametinger et al. 2012)

Duplicates:

It is possible to duplicate the Face Unlock images and NFC tags. It is also possible to bypass Face Unlock using a photo of the legitimate user. In case of theft, it is possible to access the device owners photo which can be later used to authenticate on the device. (Sametinger et al. 2012)

Dumpster diving:

Dumpster diving is an issue if a user writes down his/her authentication credentials on paper and dispose them later. An attacker can get hold of the paper and hence, the information and can enter into the device. This can be possible in case of PIN or password while NFC tags are spared from such attacks as it is unlikely that users will throw away their tags. (Sametinger et al. 2012)

Unawareness:

Unawareness of a user is a security hazard in many cases. Many users do not think it necessary to guard their devices with a lock screen. They think their device is secure as they always carry it with them. Unawareness is also a problem in case of choosing proper PIN or password for authentication. They may use a weak PIN or password which are very easy to guess or to shoulder surf. Unlock patterns and Gesture Puzzle may also suffer patterns that are not carefully chosen and easy to figure out. Face Unlock, NFC tags and Secure Lock have fewer problems with unaware users as well. (Sametinger et al. 2012)

Summary:

Answer of the research question 2 from section 1.2, table 1 has been discussed in section 2.1. The goal of the research question was to identify key factors of smartphone authentication and it has been identified as speed, comfort of use/convenience and security. In section 2.2, several basic categories of authentication methods were introduced and in section 2.5 the types are discussed in detail and thus the understanding research question 1 was answered. In section 2.3 possible attacks are discussed which is important to know from security perspective of smartphone. In section 2.4 study on users carried to understand the significance of using mobile authentication and understanding the impact of mobile phones in users' lives these days.

A brief realization about several smartphone authentication methods (not practiced methods are excluded from consideration) are presented below in table 2:

Table 3: Summary of Authentication methods

Authentication method	**Usage**	**Problems**
PIN	Usually a 4-digit secret number is entered for smartphone authentication.	- Need to memorize - Easy to guess by attackers
Password	Generally, 6 to 12 characters alphanumeric secret for smartphone authentication	- Harder to memorize than PIN - Difficult to type - Takes more time to type comparing to PIN
Gesture puzzle/pattern	A pattern needs to be drawn connecting few points for smartphone authentication	- Need to memorize - Easy to guess - Leaves spot on screen usually which can be guessed by users
Fingerprints	A scanner reads the fingerprint and let the user authenticate in smartphone	- Dirty scanner/finger leads to failure of authentication - Wet hand, gloves are barrier for this authentication
Facial Recognition	An image of user is captured by the mobile camera and compares with a pre-captured image of the user is. Matching of both images gives a successful authentication.	- Authentication is not possible in dark places - A still picture of the user can be used by attackers and may lead to unauthorized authentication

Iris Recognition	Iris of a user needs to be scanned by a powerful camera to compare it with preregistered iris pattern of a user, for authentication.	- Users with glasses face problem - Bright sunlight can cause problem - Expensive technology yet and rarely introduced
Speaker Recognition	User’s voice and a prerecorded sample is compared for authentication	- Not appropriate in an environment where user needs to be remain quiet - Similarly, external noise can affect authentication

3 METHODOLOGY

In this section, the research methodology and data collection processes are discussed along with the description of research questions. A brief discussion and perspective of the selection of applied research approaches are detained. (Silva 2015) and (Kasurinen et al. 2017) were helpful to me for designing the outline of this section and acted as a source of some good references for studying in detail.

3.1 Research Problem and Questions

Convenience and security are two factors for which mobile users often need to go through compromises. Either users use 'lock' for security purpose but go through embarrassing authentication every time they use their phones, or they prefer not to use any security lock and put their data and other stuffs in threat.

Usability plays often as a barricade with the security on smartphones. If users give priority to the convenience of use for interacting with different applications in phones without typing a password for security every time then the users deteriorate the security. In this consequence, from a study it has been observed that more than 30% of mobile phone users do not use PIN to lock their phone whereas internet payment, money transfer and other data transfer and storage by mobile phones are increasing rapidly day by day. (Riva et al. 2011)

By replacing PIN, password, gesture/pattern based authentication by more appropriate authentication method can be an approach for increasing security. For example, token based authentication approach usually have better security than passwords in terms of preventing from attacks, but it will spoil the desire of carrying few devices from user's perspective. Recently, in the mobile community biometric authentication method has achieved high interest, nevertheless high price, good performance and acceptability are still a challenge. (Riva et al. 2011)

In this work, smartphone authentication problem has been observed from a different point of view. The focus of the study is identifying user needs, satisfaction factors, limitations and advantages of existing methods for the goal of developments of patterns for smartphone authentication in future; rather than exploring a new authentication scheme. This thesis studies the intersection between usability and security of smartphone authentication schemes in practice and how the users approach usability and security issues for their smartphone authentication through literature review and by a quantitative survey.

To deal with the above-mentioned research problems, the explorative approach by Kitchenham, (Kitchenham et al. 2002) was preferred. The problem was divided into a group of research questions (RQs) to achieve this approach, which were addressed through a quantitative survey study. Table 4 represents the research questions:

Table 4: Survey Research questions, goals and sections

Research Question (RQ)		Goal	Survey Section
RQ1: Which authentication method is the most preferred one by users?	RQ.1.1 Is there any significant impact of role, gender or used mobile OS?	Identifying contemporary trends of preferring authentication methods	Section 1, 2, 3 and 4: Basic Information, Selection of preferred authentication method, quaternaries based on selected method and user satisfaction
	RQ.1.2 What do users prioritize more between convenience		
	RQ.1.3 To what level the method serves the concern for security or convenience?		
	RQ.1.4 What is the level of user satisfaction for the most preferred method?		

	RQ.1.5 What difficulties users do experience in this		
RQ.2: Which authentication method shows the highest user satisfaction?	RQ2.1: Does the level of satisfaction varies due to role, gender or mobile OS?	Identifying the factors of user satisfaction for authentication method	Section 4: User satisfaction
RQ3: Which one is the least preferred authentication method?	RQ3.1 Is there any significant impact of role, gender or used mobile OS?	Identifying the reasons for less preferring an authentication method	Section 1, 2, 3 and 4: Basic Information, Selection of preferred authentication method, questionnaires based on selected method and user satisfaction
	RQ.3.2 What users do prioritize more between convenience of use and security?		
	RQ.3.3 To what level the method serves the concern for security or convenience?		

	RQ.3.4 What difficulties are expressed by users in the least preferred method?		
RQ.4: What is the concern for preferring an authentication method, in general? (Is it	RQ.4.1: What does user suggests for increasing satisfaction	Identifying the impact of security and usability from the user perspective	Section 3 and 4: Questionnaires based on selected methods and user satisfaction

3.2 Research Methods

Empirical guidelines from Kitchenham, (Kitchenham et al. 2002) and quantitative survey methods according to Fink (Fink 2013) were applied in order to approach the RQs. The main key facts are the following three:

i) general information overviews

ii) most preferred authentication methods in practice and

iii) users' concerns and recommendations regarding their preferred method

3.3 Quantitative Study

Gathering numerical data and simplifying it over diverse groups of people is the key focus of a quantitative study. Numerical analysis of data gathered through polls, questionnaires or surveys and objective measurements are the main emphasize of it methods (University of Southern California, 2013). The survey method is an appropriate method to assemble data as a part of an empirical research from a standardized sample of entities to receive information, according to Kitchenham. (Kitchenham et al. 2002)

To label, compare, or describe individual and social knowledge, feelings, values, preferences, and behavior, surveys are methods for information gathering. Self-administered (mailed or online) and Interview (By phone or in person) are the two types of surveys (Fink 2013). A **self-administered structured and online survey** was applied for this research. Using any internet connected device, the survey was opened and accomplished online without any personal help and the participants were responsible themselves for this activity.

Fink (Fink 2013) confirms that respondents choose online surveys to participate and they are getting more familiar with it. Additionally, Fink mentioned about some advantages and disadvantages about online surveys. For example, advantages: 1. Worldwide information can be attained instantly ("real time"). 2. It can deliver the respondent with clarifications of unaccustomed words to help them understand difficult questions. 3. Many reminders can be sent easily. 4. Data processing is easy as the response can repeatedly be taken to a spreadsheet data, analysis package or database. The disadvantages are: 1. A reliable internet connection is needed for surveyors 2. Respondents should have reliable email address 3. Questionnaires of the survey may look dissimilar in different browsers. 4. No method suggests for picking random samples from overall e-mail addresses.

Furthermore, to obey the morals of **privacy and confidentiality** (Fink 2013), a introductory section was added to the survey which confined: 1) Clarification of data storing actions and 2) A request to answer the investigations.

3.4 Design Methods

As the data was composed only at a single point of time, the selected design method was the **cross-sectional** according to the definition of Fink (Fink 2013). All the participants are considered as **unit of observation** (UO) since the survey permitted getting numerous participants in an organization (Kitchenham et al. 2002). For approaching the RQs detailed in table (number of table), the survey design followed a structured organization. The detail of **questions design** (Fink 2013) included in each section of the survey is given additionally in the following Table 5:

Table 5: Survey Design and question design detail

Survey sections	**Number of Questions**	**Question type**
Section 1: Basic Information	4	Nominal closed ended
Section 2: Preferred authentication methods	1	Closed ended question
Section 3: Different questionnaires based on the selection in section 2	Varies on selection	Rating scale Checklists Closed ended question. Optional open question.
Section 4: About user satisfaction	3	Rank order scale question. Multiple selection Closed question.
Section 5: Feedback about survey	2	Closed question - Semi open question
Section 4: About user satisfaction	3	Rank order scale question. Multiple selection Closed question
Section 5: Feedback about survey	2	Closed question Semi open question

3.5 Sampling and Data Collection

Probabilistic random sampling methods described by (Fink 2013) were used. Table 6 resumes all the methods and details used for the data collection:

Table 6: Survey methods

Method	**Detail**
Survey method	Online
Design method	Cross-sectional
Number of sample groups	1
Number of survey sections	5
Time duration	1 month (From 8 May 2017 to 7 June 2017)
Selection method	Random Sampling
Sample requirements	Employees and students of Lappeenranta University of Technology
Survey administration	Via webropol tool from Lappeenranta University of Technology (LUT)
Processing the data	Data is automatically entered from survey to database via webropol.
Survey distribution	Invitations to fill the survey to a random sample: 1) Via Emails, 2) Via Facebook.
UOs Answers collected	67
UOs contacted (times form opened)	250 (approx)
Amount of survey visitors	113

3.6 Data Analysis

In section 4, the results are presented after data analysis and descriptive statistics with averages, summaries, cross tabulations, and correlations are performed by following the method described by Fink (Fink 2013). Excel 2013 was used to analyze reponses.

The independent variables of the study were: respondents' role, gender, age, used mobile operating system and selected authentication method. **The dependent variables** of the study were: opinion about preferred authentication method, difficulties faced for the preference, reasons for preference, level of satisfaction, and suggestions for increasing satisfaction.

3.7 Data Overview:

The population of the survey was the community of Lappenranta University of Technology (LUT), including the employees and students. Invitations were sent to fill the survey to a random sample: 1) Via Emails, 2) Via Facebook. Total 67 respondents participated in the survey. Thesis supervisor, Professor Ahmed Seffah contacted with the employees of LUT School of Business Management via email. Author, Imtiaz Ahmed, contacted mainly with his known personnel of LUT via Facebook messenger. A request for participating in the survey was posted in one of the Facebook pages for international students of LUT. The survey was published on 8 May 2017 and was remained open until 7 June 2017. Most of the students completed the academic activities of the semester by this time and for this physical meeting with students in university was not fruitful significantly to gather more number of respondents. 2 answers were not considered for analysis in detail. One selected other as authentication method and wrote 'what is this' as used method and other wrote face recognition as preference. As face recognition was preferred by only one user so it has been excluded from analysis.

Role of respondents:

Among 67 respondents 38 were students and 29 employees.

Table 7: Role of respondents

Role	N	Percent
Student	38	56.72%
Employee	29	43.28%

Gender of respondents:

Among 67 respondents 45 were males and 22 females:

Table 8: Gender of respondents

Gender	N	Percent
Male	45	67.16%
Female	22	32.84%

Age group of the respondents:

Table 9: Age distribution of respondents

Age	N	Percent
21 and below	3	4.48%
22-34	48	71.64%
35-44	11	16.42%
45-54	4	5.97%
55-64	1	1.49%
65 and above	0	0%

Mobile OS used by respondents:

Most of the respondents were the android users.

Table 10: Mobile OS used by respondents

OS	N	Percent
Android	45	67.16%
Apple iOS	16	23.88%
Windows	4	5.97%
Other	2	2.99%

Two other users were the Symbian and sailfish OS users.

4 RESULTS

In this chapter, the cross-section survey results in which 67 UOs participated are described, organized by the research questions order. No respondent's answer found ambiguous, so all the data has been taken into consideration, no answer has been rejected.

4.1 RQ.1: Which authentication method is the most preferred one by users?

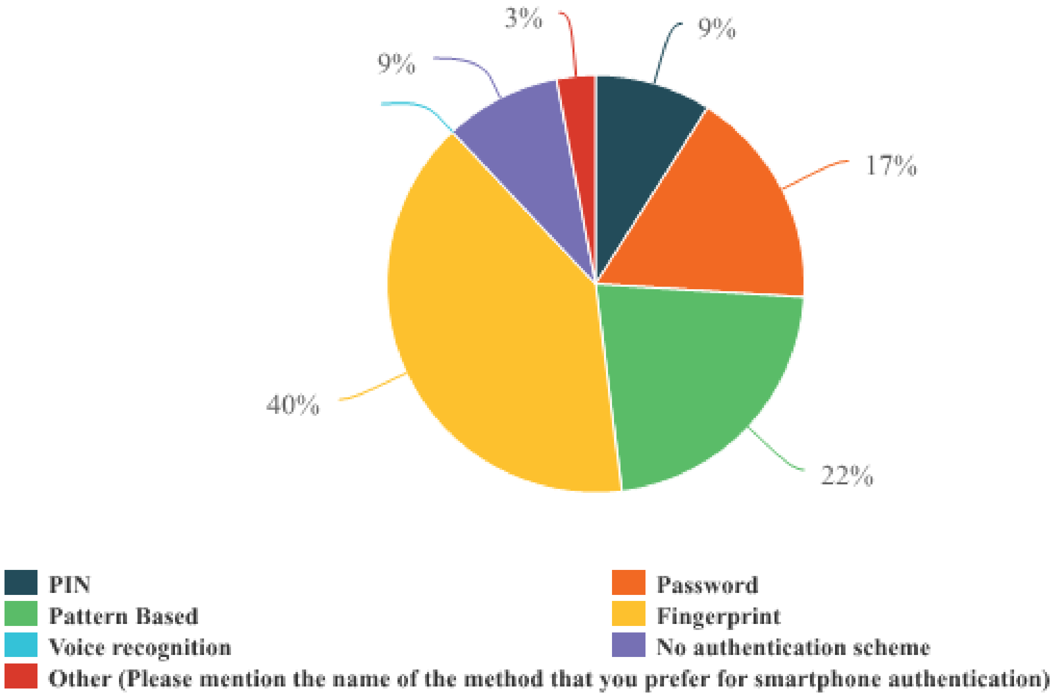


Figure 5: Preference of choosing different authentication methods

From the above pie chart, it is clearly visible that most of surveyors preferred fingerprint authentication method over any other methods. Out of 67 participants 27 selected fingerprint as their preferred authentication method.

RQ1.1. Is there any significant impact of role, gender or used mobile OS?

Number of male participants were maximum who preferred fingerprint authentication method and it is the double of female users. Android and iOS users are not significantly different here though it has been observed that the number of iOS users are more than android users only in this authentication method. And as other OS user, only one Sailfish OS user preferred fingerprint as an authentication method. Graph below represents the demographics of fingerprint authentication method:

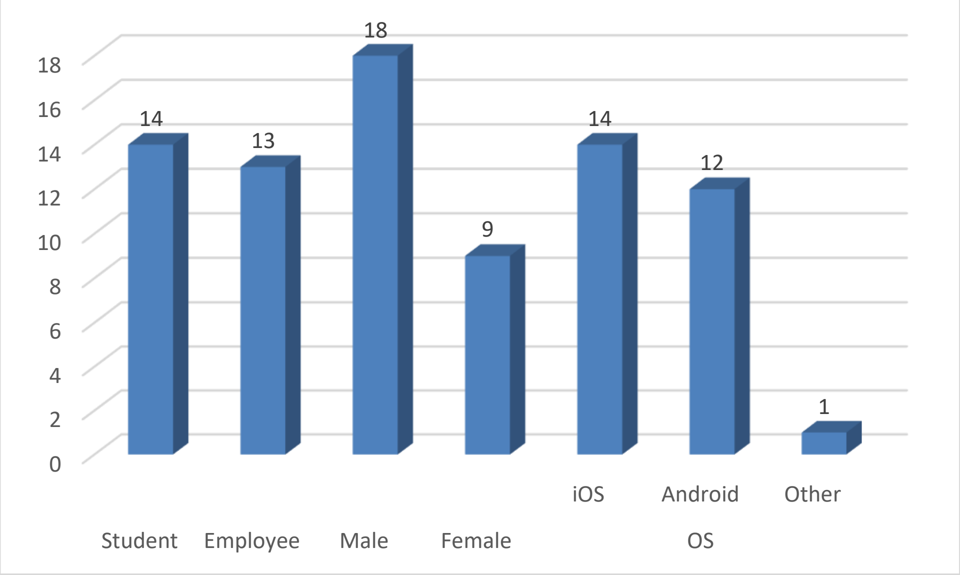


Figure 6: Demographics of fingerprint authentication method

RQ.1.2 What do users prioritize more between convenience of use and security?

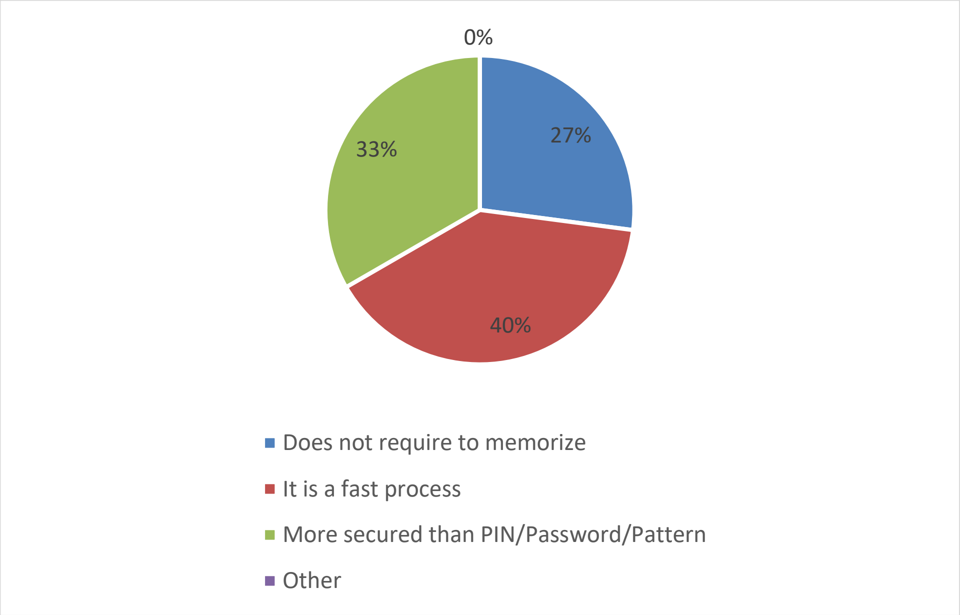


Figure 7: Answers of multiple selection questions based on convenience and security

In the survey, participants were asked few questions about the reasons of preferring their chosen method, here the above figure representing the reasons of choosing fingerprint as an authentication method. Here, two questions are basically related to convenience. 67% of participants said that they have chosen the method because it does not require to memorize any secrets for authentication and mostly because it is a fast process for authentication. Only 33% participants said that they consider this method is more secured than other methods and therefore they have preferred fingerprint.

RQ.1.3 To what level the method serves the concern for security or convenience?

Table 11: Users rating on convenience and security of fingerprint authentication method

Rating criteria	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree	Total	Average
Using fingerprint is a convenient	1	1	1	5	19	27	4.48
	3.71%	3.7%	3.7%	18.52%	70.37%		

way to authenticate							
Using fingerprint is a secured way to authenticate	0	2	4	7	14	27	4.22
	0%	7.41%	14.81%	25.93%	51.85%		

The table represents the rating of users on two statements about convenience and security of fingerprint authentication method in different scales. The highest average value expresses the most convenient perspective according to the surveyors. It is noticeable that the average value of “Using fingerprint is a convenient way to authenticate’’ is 4.48, which is higher than the value of “Using fingerprint is a secured way to authenticate”, which is 4.22.

The graphical representation of this outcome is depicted in the following figure:

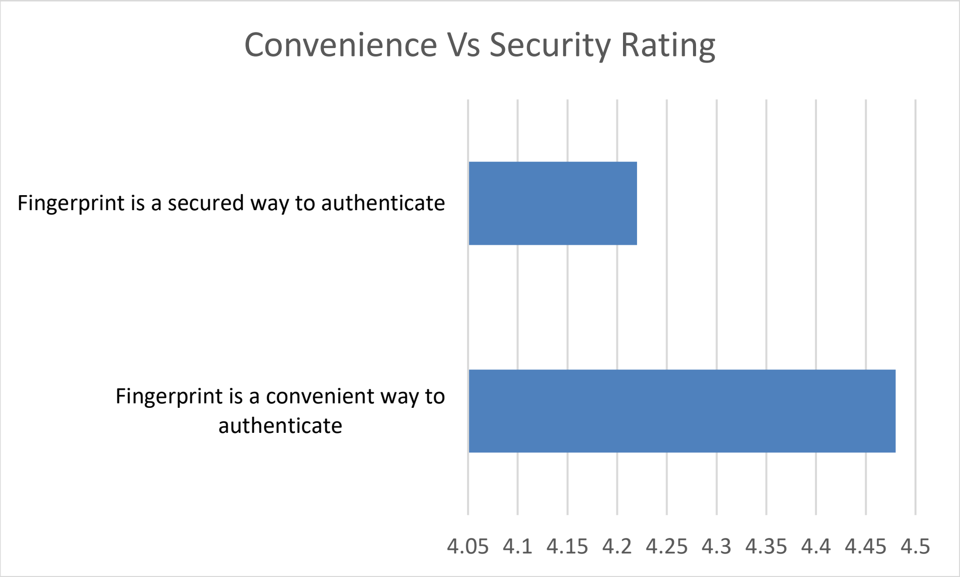


Figure 8: Users rating on convenience and security for fingerprint authentication method

RQ.1.4 What is the level of user satisfaction for the most preferred method?

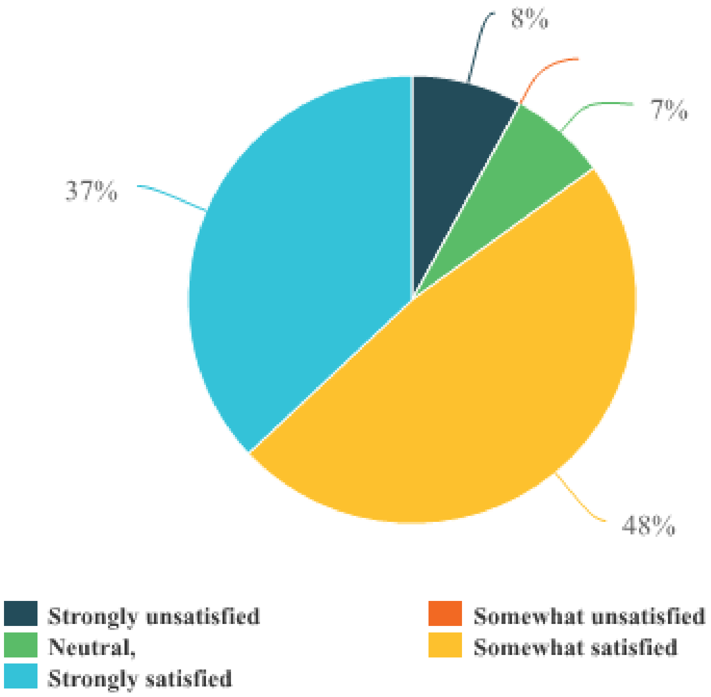


Figure 9: Users satisfaction level for fingerprint authentication method

Most of the users (13 users) were somewhat satisfied and a very good number (10 users) is strongly satisfied too. The number of strongly unsatisfied and neutrally satisfied were almost same. There was no surveyor who said somewhat unsatisfied.

RQ1.5 What difficulties users do experience in this mostly preferred method?

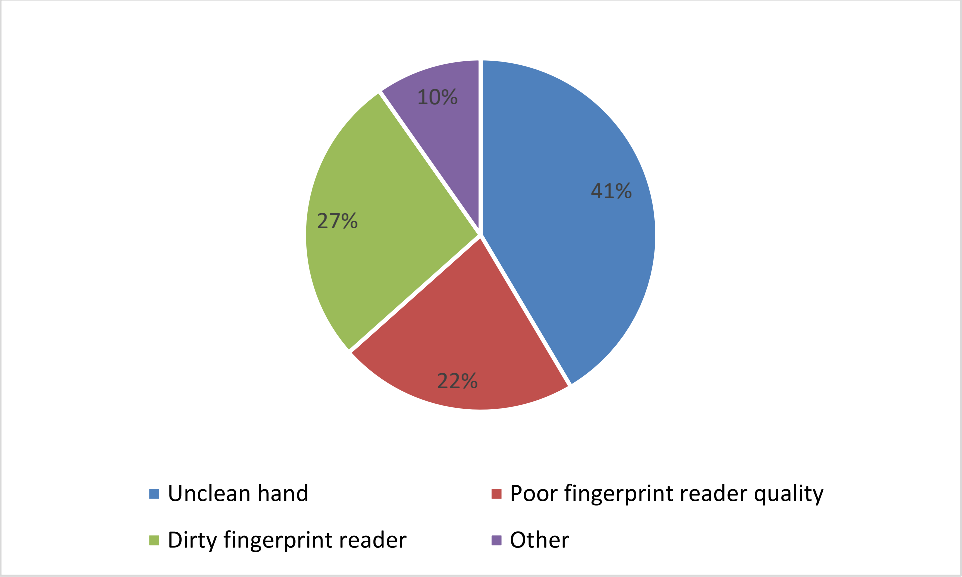


Figure 10: Problems faced by participants in using fingerprint authentication method

Most of the users (17) said that their unclean hand is the main reason of difficulties in using fingerprint. 11 participants said that dirty fingerprint reader is a problem and 9 of them said fingerprint reader's quality is poor.

Table 12: Difficulties in using fingerprint

Reasons of difficulties	Number of participants
Unclean hand	17
Poor fingerprint reader quality	9
Dirty fingerprint reader	11
Other	4

Table 13: Answers given in free text fields for difficulties in using fingerprint

Option names	Text in the given field
Other	wet hand
Other	in winter, one has gloves
Other	Have to position in weird way
Other	Moisture in fingers / reader

4.2 RQ.2: Which authentication method shows the highest user satisfaction?

All the participants were asked to rate their satisfaction level about their preferred method in a scale of strongly unsatisfied to somewhat unsatisfied, neutral, somewhat satisfied and strongly satisfied. It has been analyzed in the following table and average satisfaction level is calculated:

Table 14: Calculations of satisfaction rating level for different authentication methods

	PIN	**Password**	**Pattern**	**Fingerprint**
Strongly unsatisfied (1) * No of participant	1*0 = 0	1*0 = 0	1*0 = 0	1*2 = 2
Somewhat unsatisfied (2) * No of participant	2*0 = 0	2*0 = 0	2*0 = 0	2*0 = 0
Neutral (3) * No of participant	3*2 = 6	3*3 = 9	3*1 = 3	3*2 = 6
Somewhat satisfied (4) * No of participant	4*4 = 16	4*4 = 16	4*9 = 36	4*13 = 52
Strongly Satisfied (5) * No of participant	5*0 = 0	5*4 = 20	5*5 = 25	5*10 = 50
Total	22	45	64	110

Average satisfaction of each method	22/6 = 3.66	45/11 = 4.09	64/15 = 4.26	110/27 = 4.07

From the calculated average of satisfaction for different authentication methods the following graph is drawn:

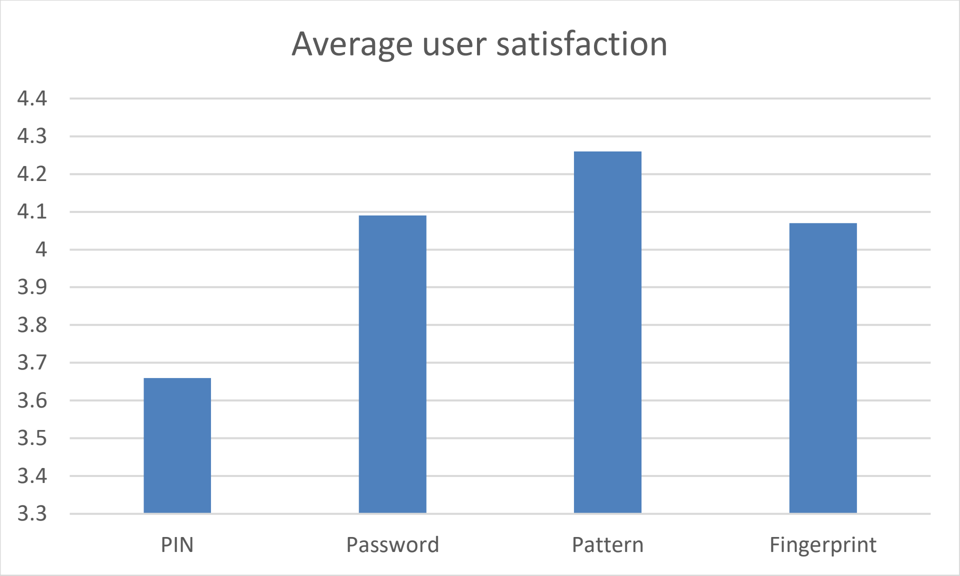


Figure 11: Average user satisfaction in using different authentication methods

It is clearly visible from the graph that the satisfaction level of pattern based authentication users is highest and for PIN it is the minimum. Whereas, both password and fingerprint based authentication method users have very close level of satisfaction.

RQ 2.1: What are the reasons of choosing the most satisfactory method (Pattern based)?

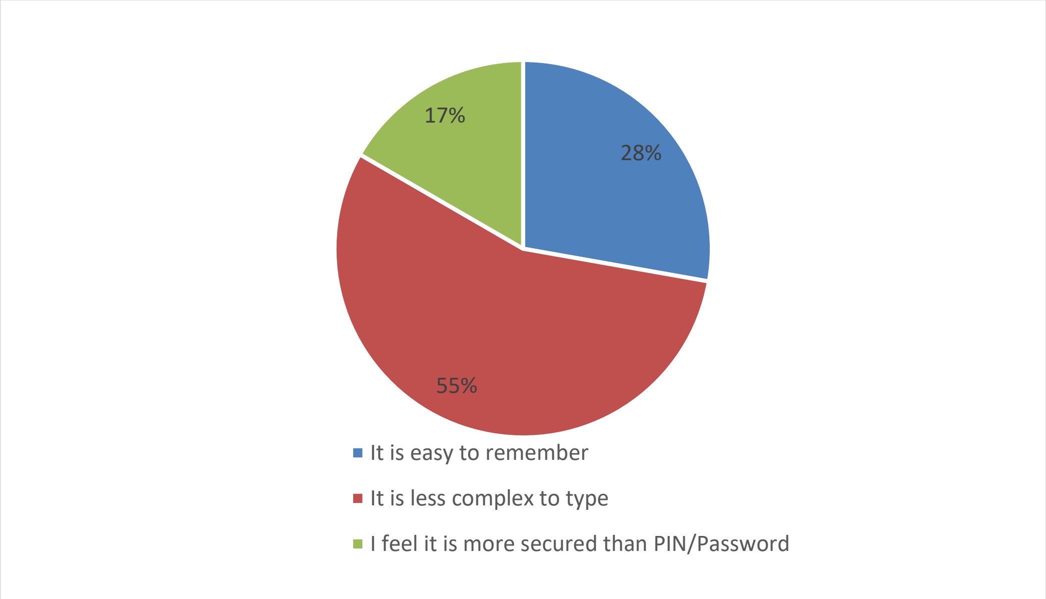


Figure 12: Answers of multiple selection questions based on convenience and security

It is clearly visible from the above pie chart that the main reason of choosing pattern based authentication is the less complexity of typing. Second reason is ease of remembrance and lastly, they consider it secured.

4.3 RQ3: Which one is the least preferred authentication method?

According to results that has been shown in **Figure 5**, there were no participants who selected voice recognition as a preferred authentication method. 6 participants selected PIN as their preferred authentication and 6 other participants selected 'no authentication' method as their preference. 'No authentication method' has been excluded from analysis as this segment of users do not feel that they need any authentication scheme for their smartphones. Therefore, PIN has been considered as the least preferred authentication method.

RQ3.1 Is there any significant impact of role, gender or used mobile OS?

It is clearly observed from the graph below that 5 out of 6 participants were employee in using PIN as an authentication method and only one was student. Same number of male and female preferred PIN. There is no significance variance in different mobile operating system users.

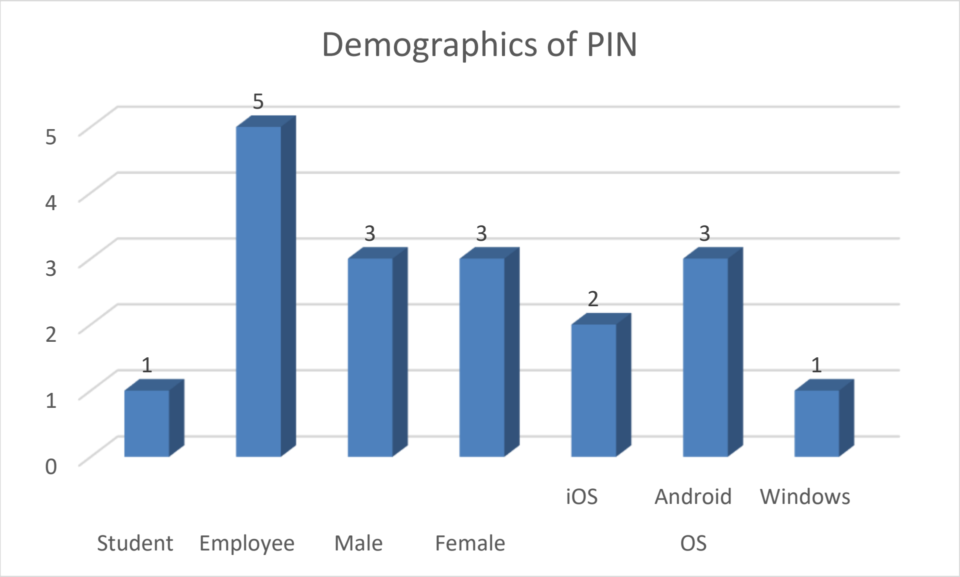


Figure 13: Demographics of PIN as an authentication method

RQ.3.2 What users do prioritize more between convenience of use and security in the least preferred method?

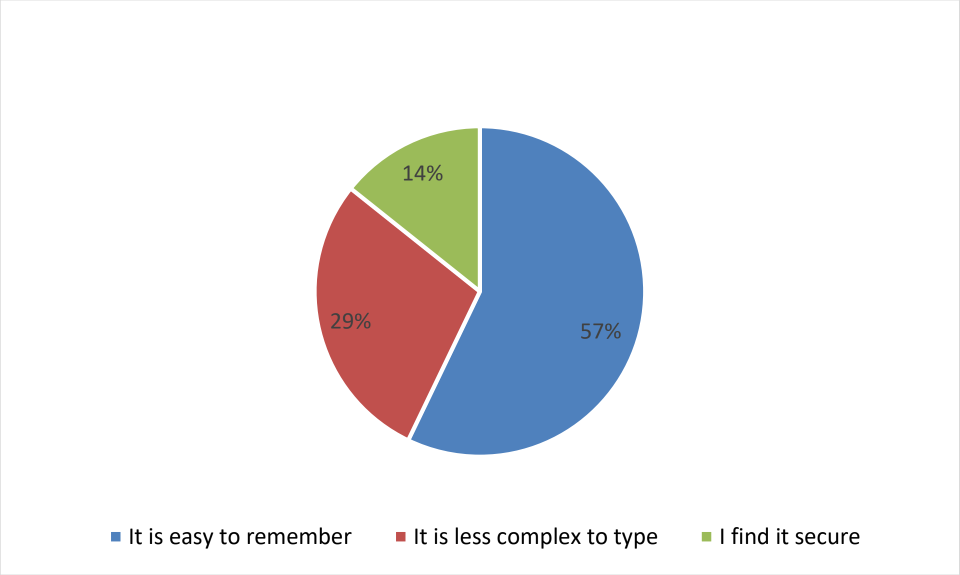


Figure 14: Reasons for using PIN

In the survey, participants were asked few questions about the reasons of preferring their chosen method, here the above figure representing the reasons of choosing PIN as an authentication method. Here, two questions are basically related to convenience. 86% of participants said that they have chosen the method because it is easy to remember and less complex to type. Only 14% participants said that they consider this method is secured and therefore they have preferred PIN as an authentication method.

RQ.3.3 To what level the method serves the concern for security or convenience?

The table represents the rating of users on two statements about convenience and security of PIN authentication method in different scales. The highest average value expresses the most convenient perspective according to the surveyor. It is noticeable that the average value of ‘’ Using PIN is a convenient way to authenticate’’ is 3.67, which is higher than the value of “Using PIN is a secured way to authenticate”, which is 3.17.

Table 15:Rating of users for the convenience and security of using PIN

Rating criteria	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree	Total	Average
Using PIN is a convenient way to authenticate	0	0	2	4	0	6	3.67
	0%	0%	33.33%	66.67%	0%		
Using PIN is a secured way to authenticate	0	1	3	2	0	6	3.17
	0%	16.67%	50%	33.33%	0%		

The graphical representation of this outcome is depicted in the following figure:

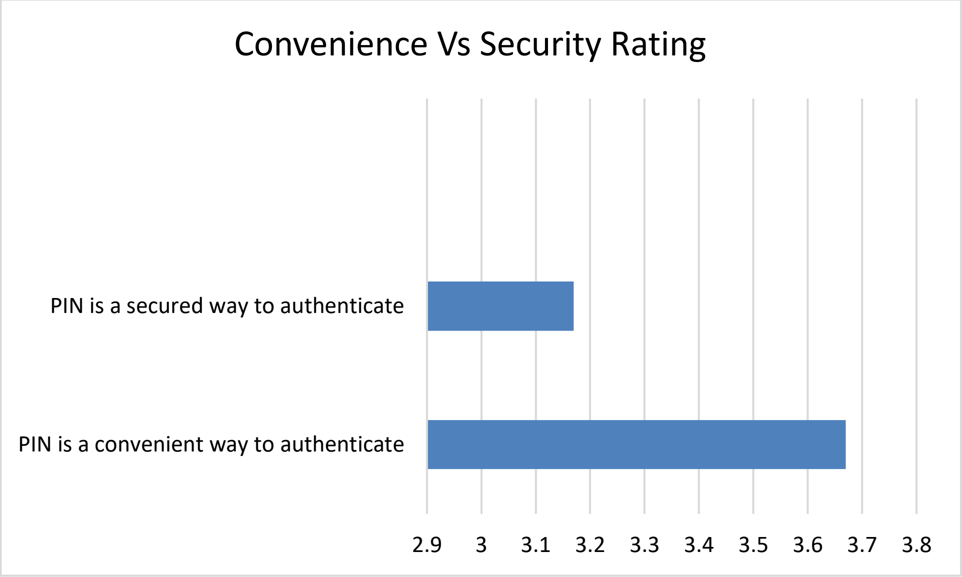


Figure 15: Users rating on convenience and security for using PIN

RQ.3.4 What difficulties are expressed by users in the least preferred method?

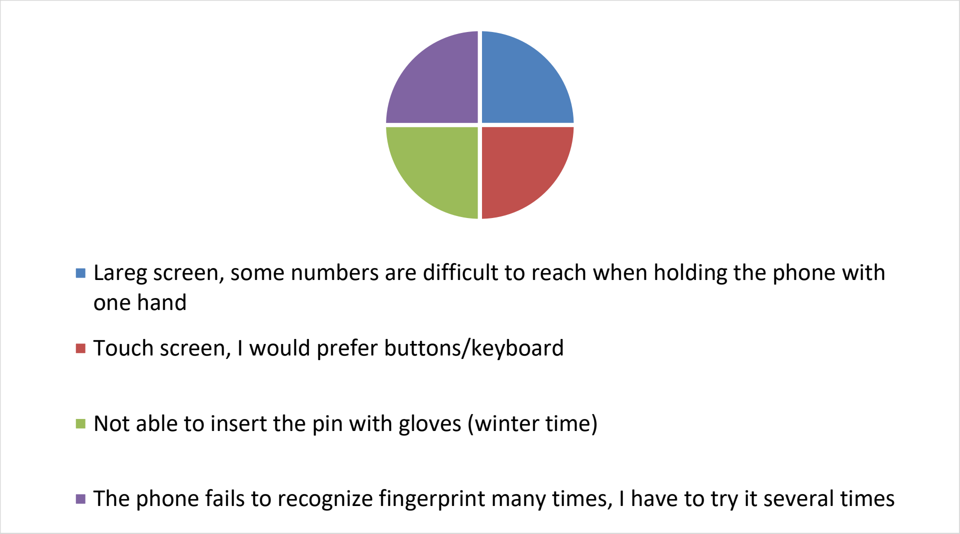


Figure 16: Problems faced by users in using PIN as an authentication method

These are basically the user’s responses collected from free text fields. 4 out of 6 users expressed their complaints against PIN which is shown in the above diagram.

4.4 RQ.4: What is the concern for preferring an authentication method, in general? (Is it security or convenience?

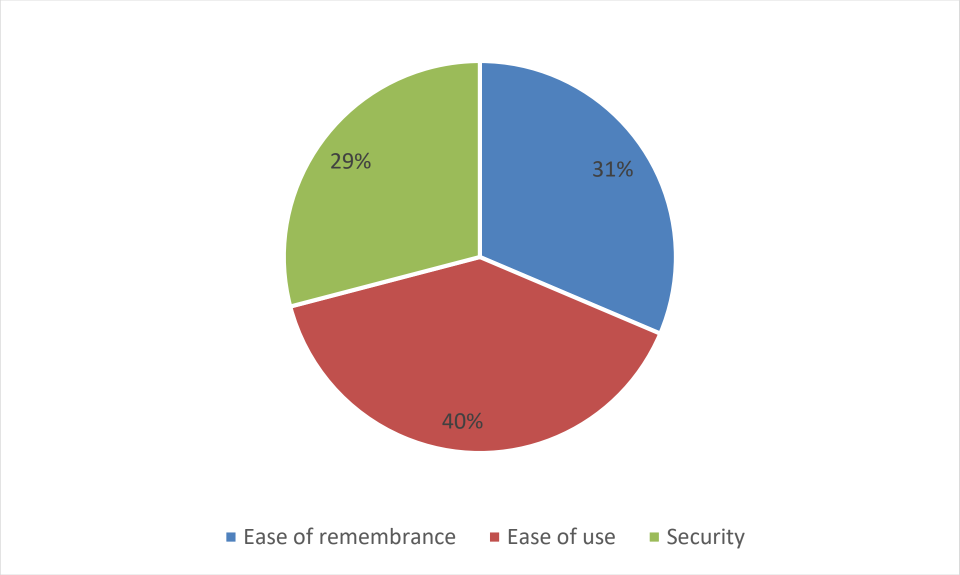


Figure 17: Usability and security related issues regarding all authentication methods

All the surveyors, those who selected any authentication method as their preference, were asked questions about the reasons of using the selected method. All questions were asked from usability and security perspective. Those questions can be generalized into ease of remembrance of authentication secrets, ease of use for the preferred method and about security of the selected method. Users, who selected PIN, password, pattern and fingerprint based authentication, answered all those questions. About figure is showing that almost 71% users said they use their preferred method because of convenience and 29% answers were for the security reasons.

RQ.4.1: What does user suggests for increasing their satisfaction for authentication methods?

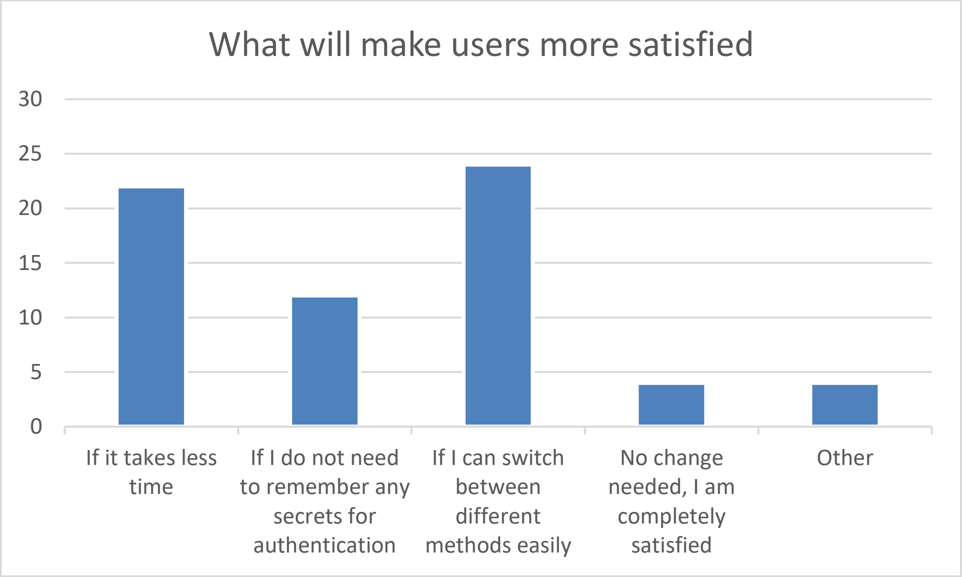


Figure 18: Users preference for increased satisfaction

In the end of the survey, there was question of multiple choices to understand what will increase user satisfaction for authentication method. The above graph is showing that most of the users like to be able to switch between different authentication methods easily, based on necessity. A very considerable number of users want authentication process faster. More than 10 persons said they do not like to memorize any secrets for authentication.

RQ4.2 Which authentication method is mostly secured found by users?

The following table represents the rating of users on two statements about convenience and security of password authentication method in different scales. It is noticeable that the average value of ‘’ Using password is a convenient way to authenticate’’ is 4.27, which is lower than the value of “Using password is a secured way to authenticate”, which is 4.55

Table 16: Rating of users for the convenience and security of using password

Rating criteria	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree	Total	Average
Using password is a convenient way to authenticate	0	0	3	2	6	11	4.27
	0%	0%	27.27%	18.18%	54.55%		
Using password is a secured way to authenticate	0	0	1	3	7	11	4.55
	0%	0%	9.09%	27.27%	63.64%		

The graphical representation of this outcome is depicted in the following figure:

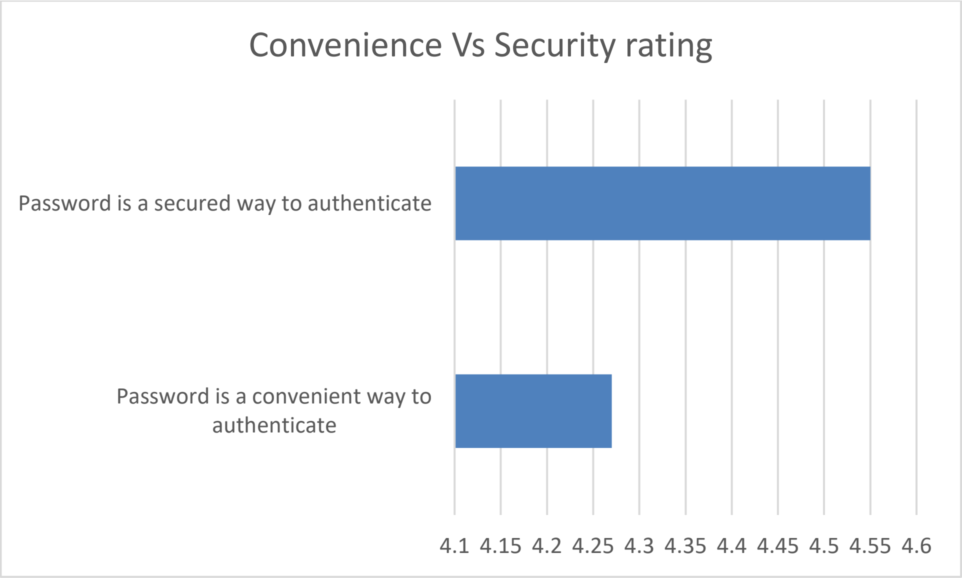


Figure 19: Users rating on convenience and security for fingerprint authentication method

5 DISCUSSION AND CONCLUSION

In this work, different authentication methods are studied and main focus area for smartphone authentication is identified and existing authentication methods have been observed from user's perspective; by literature review and by conducting a survey. The difficulties faced by users in using their selected authentication method, reasons for preferring an authentication method, rating on convenience and security related issues of chosen method, rating on their satisfaction level for the preferred method and users' recommendations about improving their satisfaction has been collected from a survey. The key focus of the study was in investigating the usability factors of the existing methods from the users' point of view and how they feel about security; rather than exploring a new authentication method. Besides this, the possible attacks have been studied to identify the threats against smartphone to understand security perspective. Furthermore, smartphone attributes that are related to usability and security has been studied.

Throughout the study, research objectives are studied and analyzed to achieve the goals of research. Research questions of table 1 from section 1.2 and the goals achieved from the research are briefly discussed below:

RQ.1: What are the diverse type of authentication methods?

The goal of the research question was to understand different types of authentication methods that are existing in practice widely, authentication methods that can be used for authentication but not widely accepted and authentication methods those are under current research for possible future development. The objective of the research question has been achieved from literature review of section 2.2 and 2.5.

The basic classification of authentication methods can be divided into three types, such as **knowledge based** (what we know), **ownership based** (what we are) and **inherence based** (what we are). PIN, password, gesture pattern these are the main examples of knowledge based authentication in smartphones. Ownership based authentication is not practiced for smartphone authentication as it is not feasible from usability perspective. Suppose, carrying another device always and using it several times a day for smartphone authentication, makes the authentication process clumsy. Examples of inherence based authentication are fingerprint, face recognition, voice recognition, iris recognition and possible other biometric identifications of an individual. Among all types, fingerprint based authentication is mostly available and popular nowadays in recent smartphones. The current research of smartphone authentication methods focuses on developing a continuous and passive authentication where users' movement, key pressing, touching behavior, location etc. are identified and recorded for **continuous authentication**. Users need to establish a profile at first by interacting with the device for such authentication. However, these mechanisms will not replace the existing authentication methods, yet can bring ease in a user's life by minimizing number of authentication needed for using one's smartphone.

RQ.2: What are the difference in user authentication for desktop/laptop and mobile phone environment?

The goal of the research question was to identify the key focus area for smartphone authentication methods. In section 2.1, the research question is analyzed and the key areas are identified.

Smartphone is a small device what users carry with their body mostly and is used numerous times a day. Usually, it is being used for shorter but several sessions and every new session of use needs authentication each time. Most identically the device is solely personal, commonly not shared by more than one users. It is more exposed to the outer world and hence it has increased chance of theft or lost. On the other hand, desktops/laptops mostly show the opposite of these characteristics unlike smartphones. Therefore, the focus areas of smartphone authentication are **speed** (fast authentication process), **convenience** (comfort of use) and **security**.

RQ.3: What are the user experiences in smartphone authentication?

The goal of the research question was to identify the most leading authentication methods and users' preference. Key focus was on what users like mostly, what they dislike, what is their satisfaction level and what is their recommendations. There were three subparts of this question. i. Which mobile OS is mostly used? ii. Which is the mostly preferred method iii.

What is the satisfaction level of different authentication methods? The answers of all these research questions were collected from the survey and presented in detail in section 4, titled result.

A brief discussion of findings **from the survey** is carried out below based on the research question:

Most used mobile OS:

67% of total respondents were **android** users and most of the android users preferred pattern based authentication. In the survey, iOS users are in the second position and more than 80% of iOS users chose fingerprint authentication method. No iOS users preferred password or pattern based authentication and typically these two types authentication are not available in iPhones. A lot of android phones do not have fingerprint technology for authentication except few recent phones which are comparatively expensive than older android phones. Both pattern and fingerprint are more convenient to use than PIN/password based authentication and preferred by both android and iOS user groups.

Most preferred authentication method:

We have seen in section 4.1 that fingerprint is the mostly preferred method for mobile authentication chosen by 40% of total respondents. A noticeable fact is that 52% of those respondents were iOS users. The main reason of preferring fingerprint is ‘it is a fast process’, answered by almost 40% respondents of fingerprint authentication method. 33% answers were for ‘it is secured’ and 27% were for ‘it does not need to memorize authentication secret’. 41% answers said that unclean hand is the main problem of this method and 22% stated the quality of fingerprint scanner is poor.

Findings:

- Users mostly prefer a fast process for authentication.
- Security is a crucial factor for users
- Users do not like to memorize secrets for authentication

- Most of the iOS device users prefer to use fingerprint authentication scheme
- Still there is a need for the improvement of fingerprint scanner quality
- Dirty fingers, wet hand, winter gloves are barrier for fingerprint authentication

Method which have highest user satisfaction:

From section 4.2 it has been observed that pattern based authentication method has the highest user satisfaction and this method was chosen by 22% of total respondents which is the second highest preferred method. The main reason choosing the method is the less complexity of typing, seems drawing is much easier then typing PIN/password. Almost 55% answers said that it is less complex to type. 28% answers stated that it is easy to remember and 17% feel it is more secured than PIN/Password. There was nothing significant about demographics for this method and hence excluded from showing in result section. Only mentionable fact is that no iOS users preferred this method.

Findings:

- Users main priority is the ease of use
- Users do not like to type, at least during authentication
- Users do not prefer to memorize something hard even though it is more secured
- Pattern based authentication is more preferred than PIN/password based authentication due to its ease of use

Least preferred authentication method:

From the diagram of section 4.3, it is visible that the least preferred authentication method is PIN which was selected by only 6 respondents out of 67 participants. Most of the users of least preferred method use it because of convenience. They feel, PIN is easy to remember and less complex to type.

Findings:

- PIN is less preferred method than password and pattern based authentication
- PIN is less convenient than pattern based authentication as the number of participants and rating point for convenience is less than pattern based authentication
- PIN is less secured than password based authentication as password has received the highest rating for security and more respondents said password is more secured

The priority: Security or Convenience?

Regardless of any types of authentication method, most of the answers collected from users were convenience concerned. Even though password received maximum rating for security, 45% of password users think that it is easy to remember and 27% do not find it hard to type. 82% of password users identified the main problem of using password is that typing both alphabet and numbers is hard during authentication. Thus, it can be said that those who are using password for mobile authentication they do not think password is inconvenient to use and they are highly concerned about security. For all other methods we analyzed, it is clearly seen that users' main reason of preference is convenience of use. Their preference was mainly for a fast authentication mechanism with minimum typing difficulties and with ease of memorizing secret or no memorizing at all.

Findings:

- Users' preference is mainly for a fast authentication mechanism with minimum or no typing difficulties and with ease of memorizing secret or no memorizing at all.
- Security comes after convenience as a priority to most of the users
- Some users are more security concerned and they compromise the difficulties they face during authentication to ensure better security.

Typically, mobile phones are not used for long continuous period like desktops or laptops. Users need to have access to their phone for periodical events, mostly many times in a day. Every time users use their device they need to authenticate them to the device, even when they keep it attached to them (e.g., in pocket). For this, authentication process should be fast and should offer maximum possible usability for users besides ensuring the safety of their data and device oriented features

Future work:

The overall goal of the thesis work was to improvise the knowledge of smartphone authentication which can help both academic researchers and industries to identify their significant target area for the development of smartphone authentication mechanisms. Academic researchers can investigate more about users' behavior in specific segment based on geographical area, role, different OS users and collect more patterns of smartphone authentication. The research might lead to a standardized definition of developing authentication methods by establishing a well balance between convenience and security.

On the other hand, in industrial level, various mobile companies can focus on how to improve their existing authentication methods to increase users' satisfaction. Furthermore, industries can emphasis on the difficulties that users face during authentication to minimize the hardship faced by users and can analyze users' recommendations to improve user satisfaction.

Limitation of research

1. **Researcher's Constraint:** The author had neither an earlier profound thoughtful knowledge about mobile authentication methods, nor an understanding of evaluating authentication methods from usability and security perspective. By data analysis and literature review this problem has been reduced.

2. **Sample limitation:** The number of respondents were not very good as expected before. The publication of the survey was at the end of the spring semester in LUT and most of the students were not available in campus. The answers were mainly collected from known contacts of author and supervisor via email and Facebook messenger. Additionally, the survey represents a specific group of users who are residing in Finland and either student or employee of a university

which does not represent the massive part of global users from different countries and background.

3 Methodological relevance:

Surveys can be classified into two types according to their design, mentioned by Kitchenham (Kitchenham et al. 2002) and they are exploratory studies and confirmatory studies. Weak conclusions can be drawn from exploratory studies and strong conclusions can be drawn from the later one. The ultimate objective of the survey was to explore the importance of mobile authentication methods for usability and security from users' perspective and therefore this survey falls in the category of exploratory, observational and cross-sectional studies.

4 **Statistical Relevance:**

The validity of the study can be questioned because of the amount of collected answers from respondents (67 respondents). It is hard to establish a good statistical relevance from this relatively small number of responses. Still, if the data is investigated perfectly then this small number of answers is enough. (Iivari 1996)

6 SUMMARY AND FUTURE WORK

Throughout the thesis work, smartphone authentication methods are studied and discussed thoroughly to identify all of its categories, authentication methods that are in use practically, authentication methods that are not feasible for smartphones and the methods that can be potential for future development of authentication process. Thus, the research goal is partially achieved from the literature review. Moreover, a survey was conducted in the community of LUT, Finland to identify mostly preferred method, least preferred method, the factors of preferring or not preferring an authentication method, users' needs, experiences, satisfaction level in various existing methods. The results were analyzed, processed and presented as a part of this work and thus the main part of research goal was achieved.

It has been observed from the result of the survey that most of the users' main concern is related to usability while security is their expectation to meet their requirement. Otherwise they can ignore authentication process totally if they consider about only convenience (few respondents from the survey preferred 'no authentication'). In the recent trend of smartphone authentication, fingerprint, a biometric authentication method has gained users' preference mostly and mainly due to convenience. Though fingerprint does not ensure the strongest security, even though users prefer it after making the trade-off between security and usability according to their understanding (extensive part of respondents preferred, because it is a fast process). Again, Fingerprint is not available widely in all smartphones due to its additional hardware cost. The survey was conducted in a university of a first world country, Finland whereas the result might differ in a country like Bangladesh where majority of the users cannot afford fingerprint supported smartphones for their use. If we consider most smartphone users those who do not have a fingerprint supported phone then pattern based authentication can have the highest preference of the users and it is because of its convenience of use. PIN/password/pattern all these are traditional mechanisms for authentication and still any replaceable method is not available in smartphone industry which will be more secured and usable with the same affordable budget for smartphones.

The future goal of the research is to conduct a survey in larger sample group and possibly in different population groups to have more diverged opinions, identifying more patterns of authentication mechanisms which might lead to a solution for a standard, usable and secured method.

REFERENCES

Ali, Z., Payton, J. & Sritapan, V., 2016a. At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices. In *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*. pp. 272–275.

Ali, Z., Payton, J. & Sritapan, V., 2016b. At Your Fingertips: Considering Finger Distinctness in Continuous Touch-Based Authentication for Mobile Devices. *Proceedings - 2016 IEEE Symposium on Security and Privacy Workshops, SPW 2016*, pp.272–275.

Anon, 2003. Four grand challenges in trustworthy computing. *November 2003*. Available at: http://www.cra.org/resources/research-issues/four_grand_challenges_in_trustworthy_computing/ [Accessed April 5, 2015].

Anon, 2005. President's Information Technology Advisory Committee. Cyber security: A crisis of prioritization. *February*. Available at: https://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf [Accessed April 5, 2015].

Botha, R.A., Furnell, S.M. & Clarke, N.L., 2009. From desktop to mobile: Examining the security experience. *Computers and Security*, 28(3–4), pp.130–137. Available at: http://dx.doi.org/10.1016/j.cose.2008.11.001.

Braz,Christina;Seffah,Ahmed and MRaihi, D., 2007. Designing a Trade-off between Usablity and Security:A Metrics Based Model. Human Computer Interaction – Interact. , pp.114–126.

Burr et al., 2013. Archived NIST Technical Series Publication Superseding Publication(s) Electronic Authentication Guideline.

Chaffey, D., 2016. Mobile Marketing Statistics compilation. *Smart Insights*, pp.1–37. Available at: http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/.

Choong, Y.-Y., Franklin, J.M. & Greene, K.K., 2016. Usability and Security Considerations for Public Safety Mobile Authentication. *ational Institute of Standards and Technology Interagency Report 8080*. Available at: http://dx.doi.org/10.6028/NIST.IR.8080.

Feng, T. et al., 2013a. Continuous mobile authentication using virtual key typing biometrics. *Proceedings - 12th IEEE International Conference on Trust, Security and Privacy in*

Computing and Communications, TrustCom 2013, pp.1547–1552.

Feng, T. et al., 2013b. Continuous Mobile Authentication Using Virtual Key Typing Biometrics. , pp.1547–1552.

Fink, A., 2013. *How To Conduct Surveys* 6th ed., SAGE Publication.

Garfinkel, S.L., 2005. *Design Principles and Patterns for Computer Systems That Are Simultaneously Secure and Usable by*. Available at: http://dspace.mit.edu/handle/1721.1/33204.

Iivari, J., 1996. Why are CASE Tools Not Used? *Communications of the ACM*, 39, pp.94–103.

Kasurinen, J., Palacin-Silva, M. & Vanhala, E., 2017. What Concerns Game Developers ? A Study on Game Development Processes, Sustainability and Metrics Jussi. *2017 IEEE/ACM 8th Workshop on Emerging Trends in Software Metrics*, pp.15–21.

Kitchenham, B. a. et al., 2002. Preliminary guidelines for empirical research in software engineering. *IEEE Transactions on Software Engineering*, 28(8), pp.721–734. Available at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1027796%5Cnhttp://dl.acm.org/citation.cfm?id=636196.636197%5Cnfile:///C:/Users/matte/AppData/Local/Mendeley Ltd./Mendeley Desktop/Downloaded/Kitchenham et al. - 2002 - Preliminary guidelines for empi.

Luca, A. De & München, L., 2015. Is Secure and Authentication.

Nielsen, J., 1993. Iterative user-interface design. , pp.32–41.

Riva, O., Qin, C. & Strauss, K., 2011. Progressive authentication: deciding when to authenticate on mobile phones. *Proceedings of the 21 st ...*, pp.1–16. Available at: https://www.usenix.org/sites/default/files/conference/protected-files/riva_usenixsecurity12_slides.pdf%5Cnpapers3://publication/uuid/6A9A5626-79EB-4A19-901C-BD29F80E2194.

Roy, A., Halevi, T. & Memon, N., 2015. An HMM-based multi-sensor approach for continuous mobile authentication. *Proceedings - IEEE Military Communications Conference MILCOM*, 2015–Decem, pp.1311–1316.

Sametinger, J., Schlöglhofer, R. & Sametinger, J., 2012. Secure and usable authentication on mobile devices Secure and Usable Authentication on Mobile Devices. , (December 2012).

Schlöglhofer, R. & Sametinger, J., Secure and Usable Authentication on Mobile Devices. , pp.257–262.

Silva, M.V.P., 2015. *Green Aspects Study in Game Development*. Available at: http://urn.fi/URN:NBN:fi-fe201504022175.

Vongsingthong, S. & Boonkrong, S., 2015. A survey on smartphone authentication. *Walailak Journal of Science and Technology*, 12(1), pp.1–19.

Appendix 1: Survey questionnaires

Survey on User Experience in Smartphone Authentication

We request your time and support in enabling us to conduct a user research on user experiences while authenticating to your smartphones. This study is being conducted by Ahmed Imtiaz, a graduate student of Lappeenranta University of Technology, Finland as a part of his Master's thesis work. The work is supervised by Professor Ahmed Seffah and PhD candidate Bilal Naqvi. The research has three key objectives:

1. Identifying the most prevalent authentication methods and practices used in smartphones.
2. Understanding the user experiences while using different authentication methods. Are the methods usable and effective? To whom? When?
3. Eliciting the user preferences in terms of methods, which one is the most used, not used, usally used in combination with others. Why and when they are used?

The data collected from the survey will be used for research purposes only. Personal information of respondents will not be disseminated publicly and will be stored confidentially. It will not be possible to deduct information from the published result based on individual response. The respondents can be provided with copy of survey results upon request. For any query regarding this survey, please contact at: Imtiaz.Ahmed@student.lut.fi

The survey would not take more than 10 minutes of your time and we thank you for your kind participation.

Respondent's Consent *

□ I agree to perticipate in the survey

0% completed

Appendix 1 (Continues)

1. Respondent's Consent *

□ I agree to participate in the survey

2. Personal Information:

Role: *

○ Student

○ Employee

3. Gender *

○ Male

○ Female

4. Age *

○ 21 and below

○ 22-34

○ 35-44

○ 45-54

○ 55-64

○ 65 and above

5. Which mobile operating system (OS) do you use? *

○ Android

○ Apple iOS

○ Windows

Appendix 1 (Continues)

○ Other ________________________________

6. Which authentication method do you prefer to use in your smartphone? (If you prefer any method which is not in the list, please write the name in 'Other') *

○ PIN

○ Password

○ Pattern Based

○ Fingerprint

○ Voice recognition

○ No authentication scheme

○ Other (Please mention the name of the method that you prefer for smartphone authentication) ________________________________

7. Please select the reasons of preferring PIN as an authentication method: *

□ It is easy to remember

□ It is less complex to type

□ I find it secure

□ Other ________________________________

8. Which of the following reason/s describe the difficulties in entering PIN on touchscreen of a smartphone? *

□ Unclean hand

□ Poor touch screen quality

□ Small sized screen

□ I do not find it difficult

□ Other ________________________________

Appendix 1 (Continues)

9. Please rate the following statements about using PIN as an authentication method in the scale from strongly disagree, somewhat disagree, neutral, somewhat agree to strongly agree: *

	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
Using PIN is a convenient way to authenticate	○	○	○	○	○
I often experience failed authentication using PIN	○	○	○	○	○
PIN is easy to remember	○	○	○	○	○
Using PIN is a secured way to authenticate	○	○	○	○	○
I often find it hard to enter PIN on touchscreen	○	○	○	○	○

10. Any additional comments regarding usability of PIN in smartphone authentication:

____

____

____

11. Please select the reasons of preferring Password as an authentication method: *

□ I feel it is more secured than PIN/Pattern based authentication

□ It is easy to remember

□ I do not find it complex to type

□ Other

____

12. Which of the following reason/s describe the difficulties in entering password on touchscreen of a smartphone? *

□ Unclean hand

□ Poor touch screen quality

□ Small sized screen

□ Typing both alphabets and numbers is difficult

Appendix 1 (Continues)

□ Other

____

13. Please rate the following statements about using Password in smartphone authentication (in the scale from strongly disagree, somewhat disagree, neutral, somewhat agree to strongly agree) *

	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
Using Password is a convenient way to authenticate	○	○	○	○	○
I often experience failed authentication using Password	○	○	○	○	○
Password is easy to remember	○	○	○	○	○
Using Password is a secured way to authenticate	○	○	○	○	○
I often find it hard to enter Password on touchscreen	○	○	○	○	○

14. Any additional comments regarding usability of Password in smartphone authentication:

____

____

____

15. Please select the reasons of prefering pattern based authentication method: *

□ It is easy to remember

□ It is less complex to type

□ I feel it is more secured than PIN/Password based authentication

□ Other

____

16. Which of the following reason/s describe the difficulties in drawing pattern on touchscreen of a smartphone? *

Appendix 1 (Continues)

□ Small sized screen

□ Unclean hand

□ Poor touch screen quality

□ Other

____

17. Please rate the following statements about using Pattern as an authentication method in the scale from strongly disagree, somewhat disagree, neutral, somewhat agree to strongly agree: *

	Strongly disagree	Somewhat disagree	neutral	Somewhat agree	Strongly agree
Drawing pattern is a convenient way to authenticate	○	○	○	○	○
I often experience failed authentication using pattern based method	○	○	○	○	○
Pattern is easy to remember	○	○	○	○	○
Using Pattern is a secured way to authenticate	○	○	○	○	○
I often find it hard to draw Pattern on touchscreen	○	○	○	○	○

18. Any additional comments regarding usability of pattern based authentication method:

____

____

____

19. Please select the reasons of preferring fingerprint as an authentication method: *

□ It do not need to memorize authentication secrets

□ It is a fast process for authentication

□ I feel it is more secured than PIN/Password/Pattern based authentication

□ Other

____

Appendix 1 (Continues)

20. Which of the following reason/s describe the difficulties in using fingerprint for smartphone authentication? *

□ Unclean hand

□ Poor fingerprint reader quality

□ Dirty fingerprint reader

□ Other ______________________________

21. Please rate the following statements about using fingerprint as an authentication method in the scale from strongly disagree, somewhat disagree, neutral, somewhat agree to strongly agree: *

	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
Using fingerprint is a convenient way to authenticate	○	○	○	○	○
I often experience failed authentication for using fingerprint	○	○	○	○	○
Using fingerprint is a secured way to authenticate	○	○	○	○	○
I often find fingerprint scanner dirty	○	○	○	○	○

22. Any additional comments regarding usability of Fingerprint based authentication method:

____

____

____

23. Please select the reasons of preferring voice recognition as an authentication method: *

□ I do not like typing for authentication

□ It is a fast process for authentication

□ I feel it is more secured than PIN/Password/Pattern based authentication

Appendix 1 (Continues)

□ Other

____

24. Please rate the following statements about using voice recognition as an authentication method (in the scale from strongly disagree, somewhat disagree, neutral, somewhat agree to strongly agree) *

	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
Using voice recognition is a convenient way to authenticate	○	○	○	○	○
I often experience failed authentication for using voice recognition	○	○	○	○	○
Voice recognition is easy to use in all environment	○	○	○	○	○
Using voice recognition is a secured way to authenticate	○	○	○	○	○

25. Any additional comments regarding usability of voice recognition as an authentication method:

____

____

____

26. What are the reasons for not using any authentication method to protect your device? *

□ I find it difficult to use

□ I do not know how to use any authentication methods

□ I am not aware of any such feature in my phone

□ I do not consider it important

□ Other

Appendix 1 (Continues)

____

27. Any additional comments from the experience of not using any authentication method:

____

____

____

28. Please rate the following statements about using your preferred authentication method (in the scale from strongly disagree, somewhat disagree, neutral, somewhat agree to strongly agree) *

	Strongly disagree	Somewhat disagree	Neutral	Somewhat agree	Strongly agree
Preferred method is a convenient way to authenticate	○	○	○	○	○
I often experience failed authentication for using the preferred method	○	○	○	○	○
Using the preferred method is a secured way to authenticate	○	○	○	○	○

29. Would you please state any explicit reason for choosing your selected authentication method? *

____

____

____

30. Please rate your satisfaction for the preferred authentication method in the scale from strongly unsatisfied, somewhat unsatisfied, neutral, somewhat satisfied to strongly satisfied *

○ Strongly unsatisfied

○ Somewhat unsatisfied

○ Neutral,

○ Somewhat satisfied

○ Strongly satisfied

Appendix 1 (Continues)

31. Please select from the options below which will increase your satisfaction regarding the preferred authentication method *

□ If it takes less time

□ If I do not need to remember any secrets for authentication

□ If I can switch between different methods easily

□ No change needed, I am completely satisfied

□ Other ______________________________

32. Would you like to receive a report of the survey result? *

○ Yes (Please write your name and email address) ______________________________

○ No

33. Any comment about the survey:

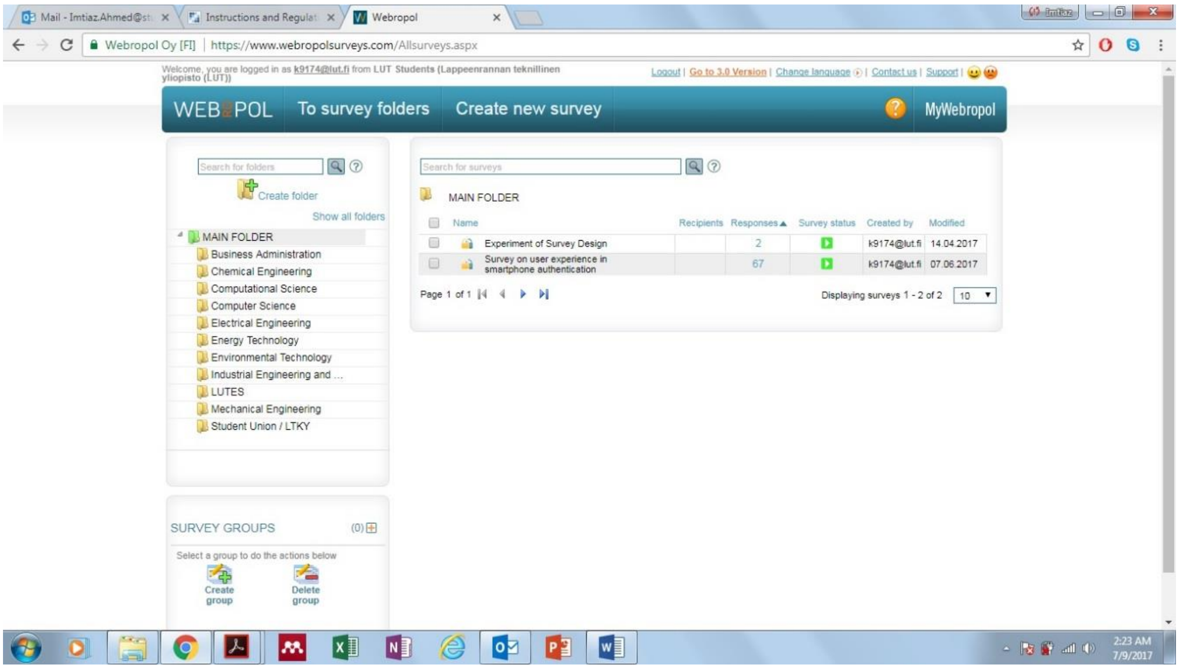
____

____

____

100% completed

Appendix 2: Few screenshots of survey tool (Webropol)



Welcome, you are logged in as k9174@lut.fi from LUT Students (Lappeenrannan teknillinen yliopisto (LUT))

MAIN FOLDER
- Business Administration
- Chemical Engineering
- Computational Science
- Computer Science
- Electrical Engineering
- Energy Technology
- Environmental Technology
- Industrial Engineering and ...
- LUTES
- Mechanical Engineering
- Student Union / LTKY

MAIN FOLDER

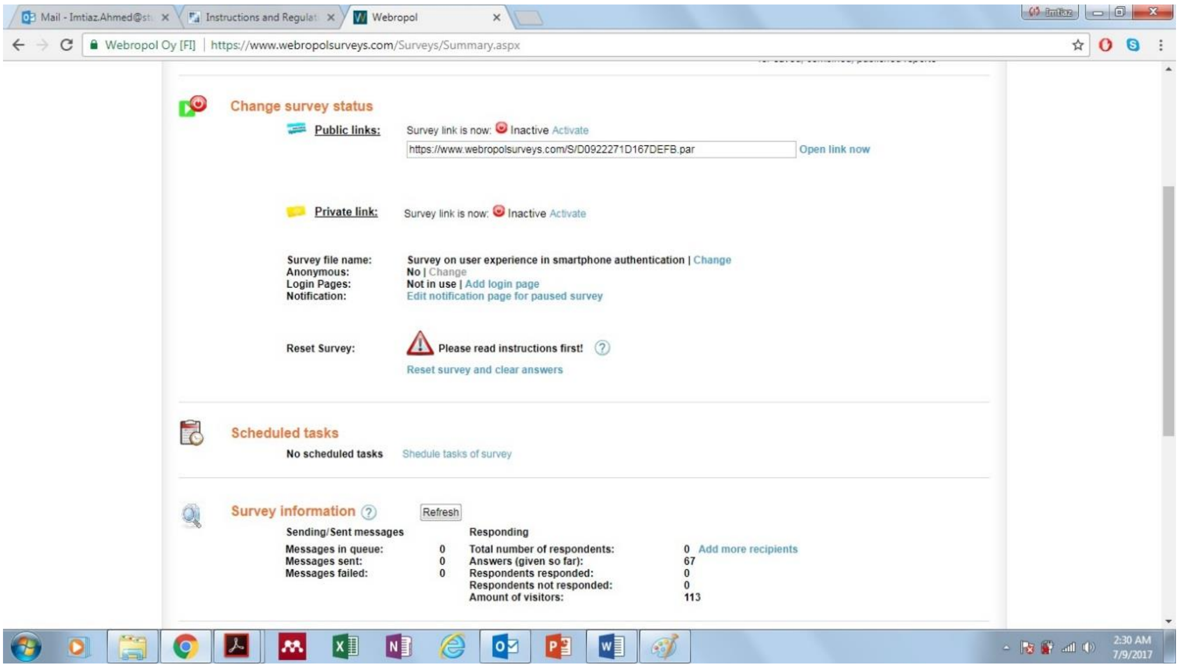
□	Name	Recipients	Responses ▲	Survey status	Created by	Modified
□	Experiment of Survey Design		2	▶	k9174@lut.fi	14.04.2017
□	Survey on user experience in smartphone authentication		67	▶	k9174@lut.fi	07.06.2017

Page 1 of 1

Displaying surveys 1 - 2 of 2 10

SURVEY GROUPS (0)

Select a group to do the actions below



Change survey status

Public links: Survey link is now: Inactive Activate
https://www.webropolsurveys.com/S/D0922271D167DEFB.par Open link now

Private link: Survey link is now: Inactive Activate

Survey file name: Survey on user experience in smartphone authentication | Change
Anonymous: No | Change
Login Pages: Not in use | Add login page
Notification: Edit notification page for paused survey

Reset Survey: Please read instructions first!
Reset survey and clear answers

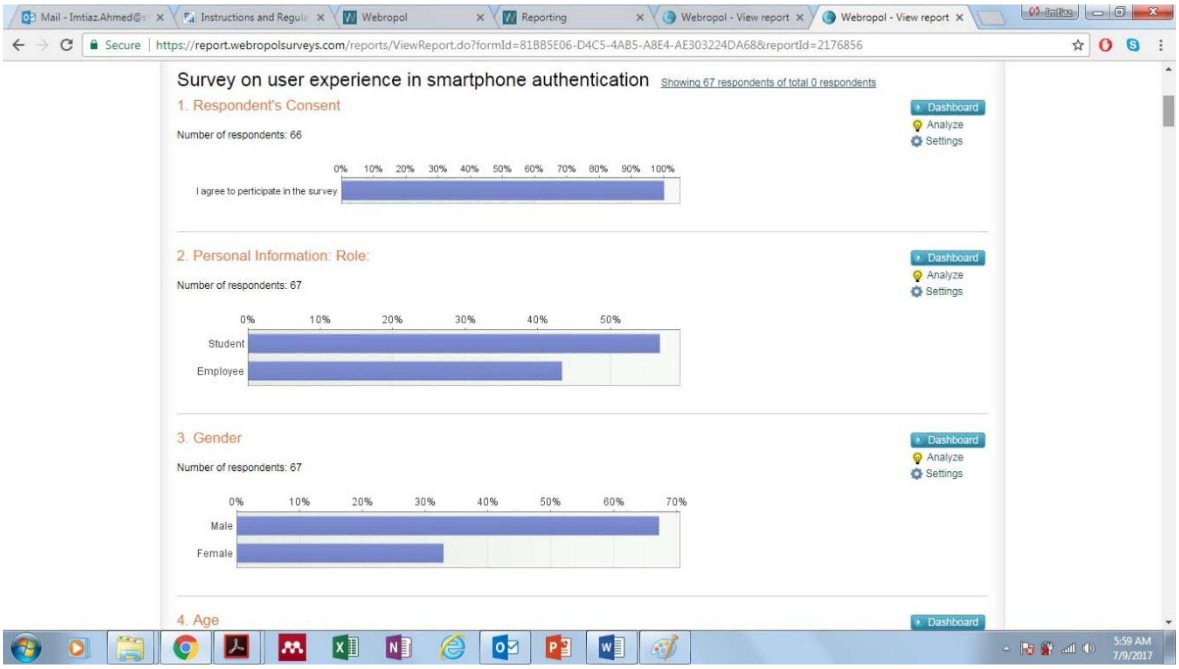
Scheduled tasks

No scheduled tasks Shedule tasks of survey

Survey information

Sending/Sent messages		Responding	
Messages in queue:	0	Total number of respondents:	0 Add more recipients
Messages sent:	0	Answers (given so far):	67
Messages failed:	0	Respondents responded:	0
		Respondents not responded:	0
		Amount of visitors:	113

Appendix 2 (Continues)



Survey on user experience in smartphone authentication

Showing 67 respondents of total 0 respondents

1. Respondent's Consent

Number of respondents: 66

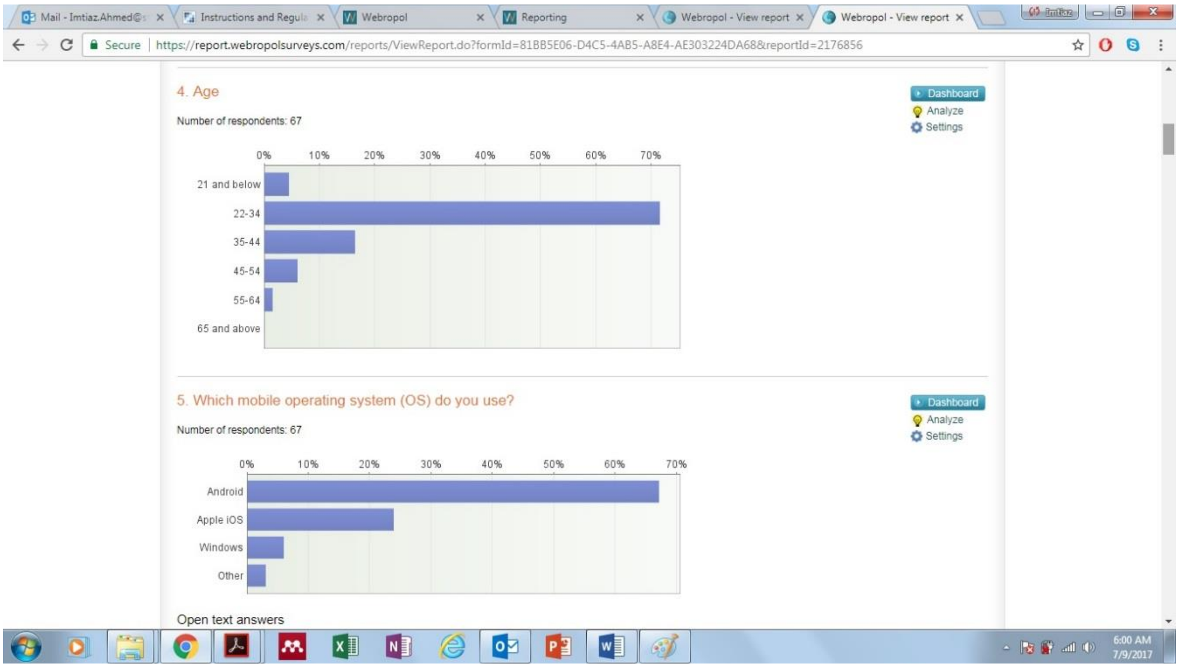
2. Personal Information: Role:

Number of respondents: 67

3. Gender

Number of respondents: 67

4. Age



4. Age

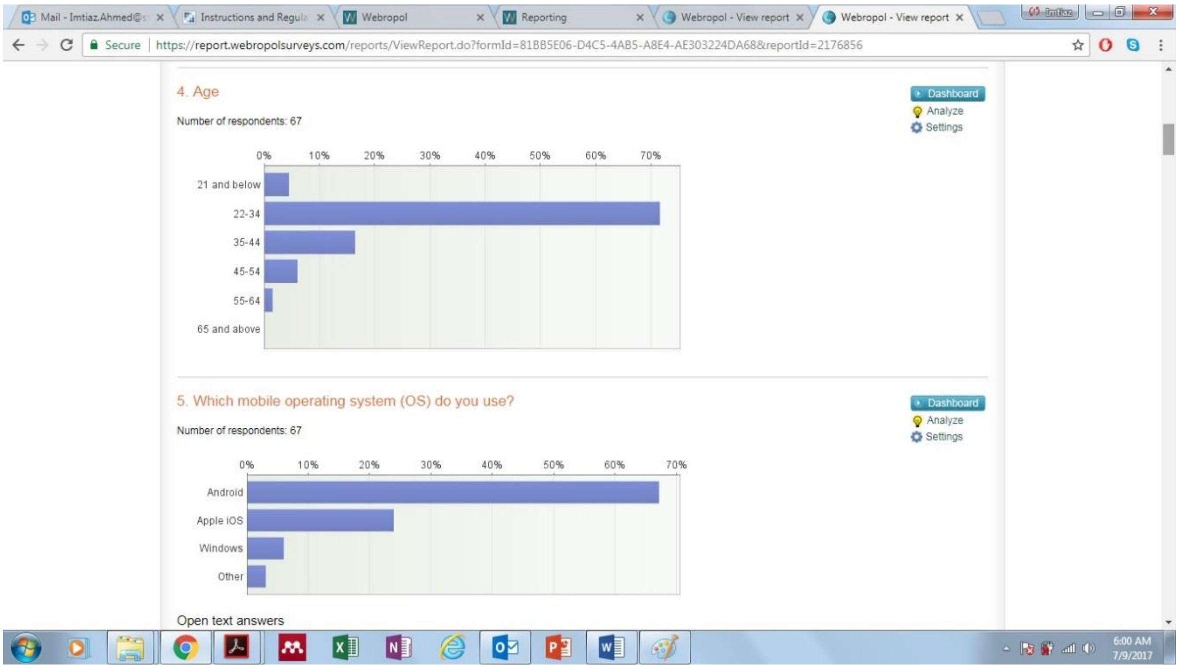
Number of respondents: 67

5. Which mobile operating system (OS) do you use?

Number of respondents: 67

Open text answers

Appendix 2 (Continues)



Mail - Imtiaz.Ahmed@
Instructions and Regula
Webropol
Reporting
Webropol - View report
Webropol - View report
Imtiaz
Secure
https://report.webropolsurveys.com/reports/ViewReport.do?formId=81BB5E06-D4C5-4AB5-A8E4-AE303224DA68&reportId=2176856

4. Age

Number of respondents: 67

5. Which mobile operating system (OS) do you use?

Number of respondents: 67

Open text answers