Ashkan Yaldaie

FROM RESEARCH TO LIVING ROOMS: EVALUATING SMART HOME TECHNOLOGIES THROUGH SYSTEMATIC REVIEWS, USER STUDIES, AND PRACTICAL IMPLEMENTATIONS

ACTA UNIVERSITATIS LAPPEENRANTAENSIS 1251

LUT University

Ashkan Yaldaie

FROM RESEARCH TO LIVING ROOMS: EVALUATING SMART HOME TECHNOLOGIES THROUGH SYSTEMATIC REVIEWS, USER STUDIES, AND PRACTICAL IMPLEMENTATIONS

Dissertation for the degree of Doctor of Science (Technology) to be presented with due permission for public examination and criticism in the Auditorium 3 at Lappeenranta-Lahti University of Technology LUT, Lahti, Finland, on the 3rd of December 2025, at noon.

Acta Universitatis
Lappeenrantaensis 1251

Supervisors Professor Jari Porras
LUT School of Engineering Sciences
Lappeenranta-Lahti University of Technology LUT
Finland

Professor Olaf Drögehorn
Department of Automation and Computer Sciences
Harz University of Applied Sciences
Germany

Reviewers Associate Professor David Hästbacka
Faculty of Information Technology and Communication Sciences
Tampere University
Finland

Docent Jean-Nicolas Louis
Integrated Energy Networks and Technologies
VTT, Technical Research Centre of Finland
Finland

Opponent Professor Sadok Ben Yahia
Center of Industrial software
South Denmark University
Denmark

ISBN 978-952-412-356-3
ISBN 978-952-412-357-0 (PDF)
ISSN 1456-4491 (Print)
ISSN 2814-5518 (Online)

Lappeenranta-Lahti University of Technology LUT
LUT University Press 2025

Abstract

Ashkan Yaldaie
From Research to Living Rooms: Evaluating Smart Home Technologies Through Systematic Reviews, User Studies, and Practical Implementations
Lappeenranta 2025
74 pages
Acta Universitatis Lappeenrantaensis 1251
Diss. Lappeenranta-Lahti University of Technology LUT
ISBN 978-952-412-356-3, ISBN 978-952-412-357-0 (PDF), ISSN 1456-4491 (Print), ISSN 2814-5518 (Online)

Smart home technologies have changed the way people live, making homes more convenient, energy-efficient, and secure. Despite these benefits, many people are still hesitant to adopt them because of concerns about complexity, compatibility, and usability. This dissertation focuses on closing the gap between what these technologies can do and what users actually need, by designing smart home solutions that are practical and user-friendly.

To achieve this, the research employs a multiphase methodology including a systematic literature review, an international user survey, and the design and implementation of a Raspberry Pi–based smart home platform as a research artifact. The literature review identifies key trends and recurring barriers, emphasizing the need for a user-centric design. The survey captures different user opinions and concerns, revealing a strong demand for customizable, secure, and accessible systems designed for various levels of technical ability.

Based on these insights, a modular and affordable smart home system was created using open-source platforms. The prototype was evaluated using the technology acceptance model (TAM), showing that perceived usefulness (PU) and ease of use are critical drivers of adoption, while trust and privacy concerns continue to play a major role.

This dissertation introduces the user-aligned smart home development framework (UASH-DF), which provides actionable guidance for designing smart home technologies that are context-aware, secure, compatible with other systems, and inclusive. The framework and findings contribute to both academic discourse and practical innovation, supporting the creation of smart home environments that are not only technically robust but also responsive to the day-to-day life of modern households.

Keywords: smart home, home automation, IoT, remote monitoring, home security, energy efficiency

Acknowledgments

First and foremost, I owe my deepest gratitude to **Professor Jari Porras**, whose innovative teaching methods and strong ethical principles have profoundly shaped this research and my development as a scholar. His exceptional mentorship, characterized by thought-provoking guidance, unwavering integrity, and genuine encouragement, has been the cornerstone of my doctoral journey.

I would also like to thank my employers, **Markus Mettälä** and **Shannon Merritt**, whose leadership and support in my professional life greatly encouraged my academic pursuits and contributed to the successful completion of this research.

Finally, I wish to express my sincere appreciation to my wife, **Tatiana Yaldaie**, whose unwavering patience, love, and steadfast belief in me have been a constant source of strength and inspiration. Her support carried me through the most challenging moments of this journey and made the completion of this doctoral study possible. I am likewise truly thankful to my parents for their constant support and encouragement throughout my life. Their presence and encouragement have meant more than words can describe.

Ashkan Yaldaie
November 2025
Järvenpää, Finland

Contents

List of publications

This dissertation is based on the following papers. The rights have been granted by publishers to include the papers in this dissertation.

Publication I: Yaldaie, A., Porras, J., and Drögehorn, O. (2022). The Present State of Home Automation: A Systematic Literature Review. *International Journal of Hybrid Innovation Technologies*, vol. 2, no. 1, pp. 23–46, 2022, doi: 10.21742/ijhit.2653-309X.2022.2.1.03.

During this study, Ashkan Yaldaie was responsible for collecting the data, conducting the data analysis, and leading the writing of the publication. The coauthors contributed by helping to shape the research idea, providing critical feedback, and assisting with proofreading of the manuscript.

Publication II: Yaldaie, A., Porras, J., and Drögehorn, O. (2023). Who Are Smart Home Users and What Do They Want?—Insights from an International Survey. *Applied Computer Systems*, vol. 28, no. 1, pp. 114–124, 2023, doi: 10.2478/acss-2023-0011.

During this study, Ashkan Yaldaie was responsible for designing the survey, collecting the data, conducting the data analysis, and leading the writing of the publication. The coauthors contributed by helping to shape the research idea, providing critical feedback, and assisting with proofreading of the manuscript.

Publication III: Yaldaie, A., Porras, J., and Drögehorn, O. (2024). Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices. *Asian Journal of Computer Science and Technology*, vol. 13, no. 1, pp. 27–40, 2024, doi: 10.70112/ajcst-2024.13.1.4260.

During this study, Ashkan Yaldaie was responsible for designing the system architecture, developing the hardware and software components, conducting the testing procedures, and leading the writing of the publication. The coauthors contributed by helping to shape the research idea, providing critical feedback, and assisting with the proofreading of the manuscript.

Publication IV: Yaldaie, A., Porras, J., and Drögehorn, O. (2025). User Perceptions of a Home Automation System: A TAM-Based Evaluation. *Applied Computer Systems*, vol. 30, no. 1, pp. 98–104, 2025, doi: 10.2478/acss-2025-0012.

Ashkan Yaldaie designed and conducted the technology acceptance model (TAM) evaluation of the home automation system, carried out data collection and analysis, and led the writing of the manuscript. The coauthors contributed by helping to shape the research idea, providing critical feedback, and assisting with proofreading of the manuscript.

Nomenclature

AI	Artificial intelligence
BI	Behavioral intention
CPI	Consumer-perceived innovativeness
DSR	Design science research
GDPR	General data protection regulation
HEMS	Home energy management system
HVAC	Heating, ventilation, and air conditioning
IoT	Internet of things
PIR	Passive infrared
PU	Perceived usefulness
PEOU	Perceived ease of use
RF	Radio frequency
SLR	Systematic literature review
TAM	Technology acceptance model
VPN	Virtual private network
UASH-DF	User-aligned smart home development framework
Wi-Fi	Wireless fidelity
Zigbee	Zigbee protocol
Z-Wave	Z-wave (a trademarked name)

Declarations

Turnitin

The originality of this dissertation has been reviewed with the Turnitin similarity checking service.

AI use

During the preparation of this dissertation, the author, Ashkan Yaldaie, used Grammarly and Microsoft Copilot to support improvements in clarity, grammar, and presentation. All suggestions from these tools were critically reviewed and revised by the author, who retains full responsibility for the final content.

1 Introduction

In the last twenty years, residential living has experienced a deep transformation driven by the rapid advancement and spread of smart home technologies. These systems, including networks of interconnected devices capable of automating and remotely controlling household functions, have evolved from advanced concepts into tangible everyday tools. Today, smart home technologies offer more than just convenience and comfort. They can also improve security, save energy, and provide personalized living experiences. As part of the broader Internet of Things (IoT) ecosystem, smart homes represent a critical application domain in which digital intelligence meets domestic life (Rego et al., 2022; Schulz & Scilla, 2024).

The global market reflects this growing interest. According to Fortune Business Insights (2025), the smart home industry is projected to grow from USD 90.75 billion in 2023 to USD 237.07 billion by 2032. This expansion signals a significant social and technological shift toward more automated, responsive, and intelligent living environments. However, despite this promising trend and the wide array of products developed by leading technology companies, the path to widespread adoption remains full of challenges (Fortune Business Insights, 2025).

When this research began, smart home technologies were already well-established in the consumer market, yet their adoption was inconsistent and often limited to isolated functionalities such as smart lighting or voice assistants (Li et al., 2021). The increasing number of devices within households introduced new layers of complexity, requiring users to navigate scattered ecosystems, closed protocols, and inconsistent user interfaces (Schulz & Scilla, 2024). While the benefits of automation were clear, users frequently encountered barriers related to system setup, integration, and long-term usability (Li et al., 2021). Moreover, concerns about data privacy and cybersecurity were growing, as smart devices collected vast amounts of behavioral data, making them potential targets for surveillance and cyberattacks (Buil-Gil et al., 2023; Vardakis et al., 2024).

The literature consistently highlighted a gap between the technological capabilities offered by the smart home industry and the actual needs, expectations, and trust levels of users (Shuhaiber & Mashal, 2019; Yaldaie et al., 2022). High costs, a lack of perceived usefulness (PU), limited ease of use, and unclear data practices contributed to slower-than-expected adoption rates. Furthermore, many systems failed to support diverse user demographics, including older adults, renters, and individuals with limited technical proficiency. This limitation underscores the need for a more inclusive, user-aligned approach to smart home development.

This doctoral thesis tackles these challenges by presenting research aimed at better understanding and improving smart home technologies with the user in mind. The central assumption is that for smart homes to fulfill their potential, they must be designed, developed, and deployed with a deep understanding of user needs, preferences, and lived contexts. The research follows a trajectory *"from research to living rooms,"* aiming to bridge academic study with practical implementation by translating user insights into deployable, real-world solutions.

The study begins with a systematic literature review that identifies key themes and persistent issues in smart home research. Security and privacy emerge as main concerns, alongside usability, compatibility, and energy management. A critical finding is that many existing systems fail to strike a balance between robust security measures and easy-to-use design, often ignoring architectural consistency and user experience. These gaps informed the following phases of the research.

To build a more comprehensive understanding, this thesis pursued several linked objectives. First, it intended to explain the smart home user by asking the question: *Who are the users of smart home technologies? What features do they value most?* These questions were addressed through an international survey that captured diverse user perspectives across age groups, regions, and experience levels. The findings revealed a strong demand for customizable, secure, and user-friendly systems that could adapt to varying levels of technological proficiency.

Second, the research aimed to design and implement a practical, flexible, and cost-effective smart home system. Leveraging the Raspberry Pi platform and open-source tools, a prototype was developed that emphasized modularity, local control, and ease of setup. The system integrated a range of sensors and functionalities for security, energy management, and remote monitoring and was tested in diverse residential environments to ensure adaptability and real-world applicability.

Third, to evaluate the adoption dynamics of the system, the technology acceptance model (TAM) was employed. This theoretical framework allowed for the assessment of PU, ease of use, trust, and privacy concerns—factors known to influence user intentions. A mixed-methods evaluation combining structured surveys and qualitative interviews provided detailed insights into user perceptions and behavioral intentions (BIs).

The methodological approach adopted in this thesis is multifaceted, reflecting the complexity of the research domain. It integrates design science research (DSR) principles for iterative development, empirical data collection through surveys and interviews, and theoretical modeling using TAM. Each phase builds upon the previous, creating a logical narrative that moves from identifying gaps to delivering and evaluating solutions.

Collectively, the research presented in this dissertation makes several significant contributions to the field of smart home technologies. It offers in-depth empirical insights into user profiles, preferences, and pain points, providing valuable guidance for market segmentation and inclusive design. It introduces a novel, open, and adaptable system architecture that holistically addresses security, privacy, energy efficiency, and usability. It also provides an empirical evaluation of technology acceptance in the smart home context, producing actionable recommendations for developers, designers, and policymakers.

Building on these contributions, the dissertation introduces the user-aligned smart home development framework (UASH-DF). This framework guides practitioners and researchers through six interlocking phases: context exploration, open-platform design, security by design, affordability assessment, ecosystem compatibility, and continuous evaluation. UASH-DF offers a structured pathway for creating smart home systems that are not only technically robust but also aligned with the everyday experiences of users.

Ultimately, this thesis aims to create the way for smarter, safer, more efficient, and more straightforward home spaces. By centering the user in every phase of development, from design to deployment, it advocates for a future, where smart homes are not just intelligent but also empathetic, inclusive, and genuinely supportive of modern life.

2 Background

The arrival of the "smart home" marks a significant evolution in residential living, fueled by rapid advancements in the IoT[1], wireless communications, and sensor technologies. These innovations have enabled an ecosystem of interconnected devices designed to automate household tasks, enhance security, optimize energy usage, and provide greater comfort. However, the promise of seamless smart living is often held back by a scattered market with different closed systems, leading to compatibility issues. Furthermore, significant user concerns regarding data security, privacy, system reliability, and overall complexity have tempered widespread adoption. This technological landscape underscores a critical need for research focused on developing user-centric, secure, and integrated smart home solutions that address these persistent challenges.

2.1 Overview of smart home technologies

Smart home technologies have advanced rapidly in recent years, evolving from simple automation setups to complex, interconnected environments that improve comfort, security, and energy management (Schulz & Scilla, 2024; Shamili et al., 2024). In their study, Schulz and Scilla (2024) provide a detailed analysis of current smart home systems, differentiating between hub-based and hub-free configurations. Hub-based systems use a central controller or gateway to manage communication among devices, offering easier coordination but potentially higher costs and limited scalability. In contrast, hub-free systems allow devices to communicate directly with each other over standardized protocols, enhancing flexibility and reducing dependency on a single point of failure, although sometimes at the expense of seamless integration. Their study highlights how modern smart homes integrate diverse connected devices such as lighting, climate control, and surveillance, using either centralized or distributed control models to meet user needs effectively (Schulz & Scilla, 2024).

In addition to core automation functions, Schulz and Scilla (2024) also explored emerging trends such as the integration of healthcare monitoring systems, smart energy management through grid-aware appliances, and immersive technologies like augmented and virtual reality. Artificial intelligence plays a key role within smart environments by enabling context-aware and personalized interactions. Rego et al. (2022) and Schulz and Scilla (2024) argue that AI-driven systems can dynamically adapt to user behaviors and preferences, thereby enhancing the autonomy and responsiveness of the home. This comprehensive perspective provides a useful foundation for understanding the current and future path of smart home technologies and sets the stage for evaluating their social and technical implications (Rego et al., 2022; Schulz & Scilla, 2024).

A significant challenge in the evolution of smart home technologies has been the lack of compatibility between devices from different manufacturers (Belli et al., 2024; Gomez et

[1] Internet of Things: A network of interconnected physical devices that collect, exchange, and act on data via the internet.

al., 2017; Madadi-Barough et al., 2024). As the number of smart devices in homes increases, ensuring seamless communication and coordination among them becomes more complex. Many devices operate using company-owned protocols or closed ecosystems, making it difficult for users to integrate products from multiple vendors into a unified system. This fragmentation not only impacts the user experience but also creates technical barriers for developers and limits the widespread adoption (Belli et al., 2024) of smart home solutions (Madadi-Barough et al., 2024).

Madadi-Barough et al. (2024) stress that addressing integration has become a central focus in the advancement of smart home ecosystems. They explored standardized communication protocols, middleware solutions, and open platforms as key approaches to reducing fragmentation. According to their analysis, achieving effective integration is essential for enabling automation, data sharing, and intelligent coordination among devices. Overcoming these challenges would not only improve system functionality and user convenience but also support greater innovation by allowing developers to build on shared and extensible frameworks.

Conceptual clarity is also essential to the development of smart home technologies, especially as systems grow in complexity and adoption expands. The absence of a consistent framework and terminology has led to fragmented understanding across stakeholders in the field (FakhrHosseini et al., 2025). To address this, FakhrHosseini et al. (2025) conducted interviews with 21 experts from academia and industry to develop a comprehensive taxonomy that classifies smart home systems based on factors such as levels of automation, intelligence, user interaction, and compatibility. This structured approach provides a common language for researchers, developers, and consumers, promoting clearer communication and a more clear system design.

The proposed taxonomy also plays a crucial role in identifying and addressing barriers to adoption. FakhrHosseini et al. (2025) highlight the importance of aligning technical innovations with user-centric designs by incorporating factors such as usability, transparency, and security. By offering a unified lens through which smart home technologies can be understood and evaluated, the taxonomy supports comparative analysis, informed policy development, and coordinated innovation. This framework contributes significantly to the growth of the smart home domain, enabling more accessible, functional, and widely accepted automation solutions.

Home automation refers to systems that autonomously manage lighting, climate, security, and appliances through an integrated network of sensors, actuators, and control platforms. These setups can optimize energy usage by adjusting devices in response to real-time data and environmental conditions. They can also improve safety through automated monitoring and alerts and streamline household operations by coordinating multiple components at the same time. However, achieving these benefits requires overcoming technical challenges such as ensuring seamless communication among diverse devices and protecting data and control channels against cyberattacks. System complexity must be balanced with stability, as even small misconfigurations can disrupt multiple subsystems. Additionally, the initial investment and design decisions required for a unified automation network can have a major impact on both performance and scalability.

Home Assistant is a widely used open-source home automation platform that allows users to control and manage a broad range of smart devices through a centralized, customizable interface. Known for its flexibility and support for local control, it enables detailed automation across lighting, climate, security, and more. However, several studies and user reports indicate that the platform's steep learning curve presents challenges for many. Its configuration depends heavily on YAML[2] scripting and manual integration setup, which can be time consuming and error prone (Anik et al., 2024; Zargham et al., 2022). Users frequently encounter issues with designing effective automation, particularly when coordinating complex trigger–action sequences or managing dependencies between devices. Debugging is another common difficulty, as the platform offers limited real-time feedback, making it hard to trace misconfigurations (Zargham et al., 2022). These challenges underscore the need for enhanced user interfaces, validation tools, and clearer documentation to make Home Assistant more accessible and reliable for a broader user base.

Anik et al. (2024) examined the tangible benefits of smart home technologies. Their study highlights that automation can significantly enhance comfort by allowing residents to schedule routines, such as adjusting lighting and climate settings based on time of day or occupancy. Additionally, they note that properly configured automation contributes to energy efficiency by dynamically controlling resource-intensive devices such as HVAC systems only when needed. Beyond comfort and efficiency, Anik et al. (2024) emphasize that well-designed automation can improve safety and accessibility, enabling features such as automatic door locking, intrusion detection alerts, and voice-activated controls that benefit users with mobility limitations or visual difficulties (Anik et al., 2024).

Despite these advantages, Anik et al. (2024) identify several challenges that slow down widespread adoption and user satisfaction. A primary obstacle is the complexity of automation configuration: users often struggle with implementation details, such as selecting the correct triggers and actions or defining conditional logic for more advanced scenarios. Optimization is another pain point, as poorly configured automations can lead to unintended device behavior or excessive energy consumption, undermining the very efficiencies they aim to achieve. Debugging misbehaving automations further complicates the user experience, since the dependencies among devices and scripts can be difficult to trace. Anik et al. (2024) argue that to overcome these challenges, developers and platform providers must offer intuitive tooling, clear documentation, and real-time feedback mechanisms that guide users through the configuration process and help them troubleshoot issues effectively. The paper suggests that by addressing these usability gaps, the full potential of home automation, balancing practicality, safety, and sustainability, can be more readily realized.

[2] YAML is a human-readable format used to define structured data, commonly in configuration files.

Kormpakis et al. (2024) provide a detailed examination of home energy management systems (HEMSs) as a cornerstone of smart home automation, illustrating significant benefits in terms of energy optimization and integration into wider smart city ecosystems. They demonstrate that HEMSs can dynamically monitor and control energy-consuming devices such as HVAC systems, lighting, and appliances based on real-time consumption data and demand-response signals. By leveraging IoT-enabled sensors and actuators, these systems adjust device operation to match household needs while minimizing peak loads and utility costs. Furthermore, the authors show how HEMSs can aggregate data from multiple homes to contribute to grid stability and environmental sustainability, highlighting the potential for aggregated energy management to reduce carbon footprints and support renewable energy integration. Their analysis underscores that, beyond individual household benefits, HEMSs serve as building blocks for city-wide energy intelligence, fostering economic and environmental advantages on a broader urban scale (Kormpakis et al., 2024).

Despite these advantages, Kormpakis et al. (2024) also identify several technical challenges that limit the widespread deployment of HEMSs within home automation. A main challenge is the variety of devices and communication protocols: smart meters, sensors, and appliances often operate on different standards (e.g., Zigbee, Z-Wave, Wi-Fi), complicating seamless integration and data exchange. The paper argues that without a unified integration architecture, system reliability suffers, especially when scaling from pilot installations to full residential neighborhoods.

Additionally, edge computing restrictions, such as limited processing power and storage capacity on in-home gateways, pose difficulties for running advanced analytics locally, forcing reliance on cloud services and raising latency and privacy concerns. Finally, Kormpakis et al. (2024) emphasize the need for robust data analytics frameworks to handle large volumes of time-series energy data, enabling predictive maintenance and user-tailored optimization; designing such frameworks remains a challenging task given resource constraints and security considerations. The authors contend that by helping address these integration and processing challenges, HEMSs can more fully realize their promise within the broader smart home automation landscape.

Security and privacy are key concerns in the development and adoption of smart home technologies (Buil-Gil et al., 2023). In their paper, Vardakis et al. (2024) provide a comprehensive review of smart home security within the context of IoT, highlighting the vulnerabilities built-in connected home systems. The authors examined various attack vectors, such as unauthorized access, data breaches, and device manipulation, emphasizing the need for robust security protocols and user awareness. They advocate the implementation of standardized security frameworks and continuous monitoring to safeguard user data and ensure the integrity of smart home operations. By addressing these security challenges, the study underscores the importance of integrating security considerations into the design and deployment of smart home technologies, thereby enhancing user trust and facilitating broader adoption (Vardakis et al., 2024).

To conclude, smart home technologies have evolved from simple automation tools to complex, interconnected ecosystems that enhance everyday living. Recent studies highlight the architectural differences between hub-based and hub-free systems, the importance of integration, and the value of unified taxonomies for reducing fragmentation in design and communication. Researchers also emphasize the growing role of user-centric design and the critical importance of security and privacy in building trust and fostering adoption. At the practical level, home automation offers enhanced comfort through routine scheduling, improved energy efficiency via dynamic HVAC control, and increased safety through automated monitoring, even though challenges remain in configuration complexity, optimization, and troubleshooting. Similarly, HEMSs demonstrate the potential to optimize household consumption and contribute to smart-grid integration but face technical hurdles related to device diversity, limited edge-device resources, and the need for advanced data analytics frameworks. Together, these insights provide a comprehensive view of the current state of smart home development, outlining both opportunities and persistent challenges in creating more reliable, accessible, and intelligent home environments.

2.2 Barriers to adoption: When the user perspective is missing

Reisinger et al. (2023) explored how everyday life in the home, routines, emotional attachments, and social interactions often clash with technology-driven smart home solutions, creating barriers to user adoption. Through cultural studies, collaborative design, and focus groups, the authors reveal that many smart home designs fail to account for the complex "invisible boundaries" of individual households, such as the deeply habitual practices tied to specific rooms, the emotional significance of personal items, and the management of shared spaces. These mismatches between technology and lived experience lead users to perceive smart home systems as disruptive, effortful, or simply irrelevant to their actual needs. To overcome these barriers, Reisinger et al. (2023) propose a set of design dimensions: time (how routines evolve), space (how rooms are used), relations (interactions among household members), individual factors (abilities and comfort levels), and values (cultural or emotional priorities) that must support any user-centric smart home framework. By aligning system capabilities with these dimensions, designers can create features that match with real-world practices rather than imposing artificial workflows (Alsiyat et al., 2025; Bombik et al., 2022; Reisinger et al., 2023).

Building on these dimensions in their paper, Reisinger et al. (2023) identify seven concrete design goals to guide smart home development to reduce adoption barriers: (1) control (ensuring users feel in charge of technology rather than overwhelmed by it), (2) low effort (minimizing the cognitive and physical work required to set up and maintain automation), (3) integration (seamlessly blending new devices with existing household objects and routines), (4) evolvability (allowing systems to adapt as user needs and home configurations change), (5) identity (preserving the unique character and style of each home), (6) sociability (supporting shared experiences and communication among household members), and (7) benefits (making the tangible advantages clear and direct, such as energy savings or safety enhancements). By embedding these goals into the design process, smart home technologies can address the root causes of user resistance, namely, perceived complexity, loss of personal control, and misalignment with daily life, thereby promoting greater acceptance and sustained usage.

Magara and Zhou (2024) build on these insights by empirically examining how security and privacy concerns prevent potential users from embracing smart home technologies. Through an online survey of over 300 participants, they found that fears of data breaches, unauthorized surveillance, and insufficient encryption dramatically reduce trust in IoT devices, leading many respondents to hesitate or reject home automation solutions outright. Their analysis reveals that confidence in manufacturers' data-handling practices is a crucial factor: when users consider weak or unclear security measures, their perceived risk rises and adoption intentions decline. To address these challenges, Magara and Zhou (2024) recommend that designers implement transparent data governance policies, end-to-end encryption, and intuitive privacy dashboards that enable users, regardless of technical expertise, to easily configure and monitor their data-sharing settings. By prioritizing these user-driven security and privacy requirements, smart home systems can better align with consumer expectations, promoting greater trust and ultimately facilitating wider adoption (Magara & Zhou, 2024).

The TAM, originally proposed by Fred Davis in 1989, is a widely recognized theoretical framework used to explain and predict user acceptance of information technology. At its core, TAM suggests that two primary beliefs influence a user's intention to adopt a new system: perceived usefulness (PU), which is the degree to which an individual believes that using a particular system will enhance their job performance, and perceived ease of use (PEOU), defined as the degree to which an individual believes that using a particular system would be free of effort. These perceptions, in turn, shape a user's attitude toward using the technology and ultimately their BI to use it, providing a foundational understanding of adoption processes across various technological contexts.

Within the expanding field of smart home technologies, understanding user acceptance is essential for widespread adoption, with the TAM frequently serving as a foundational framework. A systematic literature review by Daruwala and Oberst (2023) highlights that TAM is the most commonly applied model in investigating smart home technologies' acceptance, consistently emphasizing PU and PEOU as critical factors. Despite the availability of smart home technologies for over two decades, their acceptance has been slower than anticipated, often hindered by factors such as technophobia, privacy concerns, and the need for greater clarity in value propositions. Research in this area frequently extends TAM by integrating additional variables, such as compatibility, trust, awareness, enjoyment, and perceived risks, to provide a more comprehensive understanding of the complex interplay of psychological, cultural, and technological factors that influence BI to adopt smart home solutions (Daruwala & Oberst, 2023).

Shuhaiber and Mashal (2019) extend the classic TAM to the smart home domain by incorporating additional user-centric factors such as trust, awareness, enjoyment, and perceived risk alongside PU and PEOU to explain residents' intention to adopt smart home systems (Shuhaiber & Mashal, 2019).

In their empirical study in Jordan, Shuhaiber and Mashal (2019) demonstrate that PU (a cognitive factor reflecting beliefs about how effectively a smart home system can improve daily routines) and PEOU (another cognitive factor indicating the anticipated effort required to use the system) remain primary drivers of users' attitudes. Trust and awareness further influence cognitive evaluations by shaping how users perceive the reliability and familiarity of the technology. At the same time, enjoyment serves as an emotional motivator (e.g., the pleasure derived from interacting with a responsive lighting system or voice-controlled thermostat), enhancing users' willingness toward adoption. In contrast, perceived risk, another emotional element tied to fears of privacy breaches, causes a strong negative influence. By showing that these extended TAM constructs collectively account for a substantial portion of the differences in adoption intentions, the authors underscore the necessity of addressing both emotional (e.g., enjoyment, fear) and cognitive (e.g., PU, PEOU) dimensions in designing and promoting smart home technologies.

Smart home adoption can vary depending on environmental and contextual factors, including cultural norms, economic conditions, and infrastructure (Basarir-Ozel et al., 2023; Bombik et al., 2022). Differences in energy awareness, sustainability priorities, and local living conditions may influence the ways households interact with smart technologies (Li et al., 2021). For instance, some households may prioritize energy efficiency, while others may focus more on convenience, security, or comfort. Similarly, access to information, available benefits, and the affordability of devices can shape adoption patterns. These variations indicate that the impact and uptake of smart home technologies are likely shaped by the surrounding environment rather than following a uniform pattern across regions (Basarir-Ozel et al., 2023; Bombik et al., 2022; Li et al., 2021).

2.3 Bridging research, design, and implementation

The translation from theoretical research to practical smart home implementation represents a critical challenge in the field, often characterized by a significant gap between academic findings and real-world applications. The "smart home" is a strongly technology-driven field, with a considerable ongoing gap for design, based on an everyday home context and the social and emotional nature of the home. This disconnect comes from the main focus on technological capabilities rather than user-centric requirements, resulting in solutions that may be technically sophisticated but fail to address genuine user needs and situational realities. Traditional research approaches often operate in isolation from practical implementation limitations, leading to prototypes and concepts that struggle to transition from laboratory environments to actual domestic settings (Reisinger et al., 2023).

The emergence of user-centric design methodologies offers a promising pathway to bridge this research–implementation gap. The optimal framework for smart home research lies in integrating technological innovation, service development, and user-centric experiences to bridge the gaps between advancements and diverse user needs. This integrated approach requires iterative design processes that incorporate user feedback throughout the development cycle, from initial conceptualization to final deployment. By embedding practical implementation considerations within the research phase and maintaining continuous dialogue among researchers, designers, and users, it becomes possible to develop smart home solutions that are technically viable and genuinely responsive to user requirements, thereby facilitating more successful adoption and sustained engagement (Park & Han, 2025).

The development of user-centric prototyping methodologies has emerged as a crucial component in bridging the gap between smart home research and practical implementation. An experimental smart home prototype was developed by Cerino et al. (2023) to demonstrate a secure, scalable service model that addresses future home service needs. The process was informed by user-centric design methods and iteratively refined based on feedback from target users (Cerino et al., 2023). This iterative approach emphasizes the importance of continuous user involvement throughout the development process, moving beyond traditional linear development models where user input is gathered only at the beginning or end of the project. Such methodologies enable researchers to identify and address implementation barriers early in the design process, resulting in more robust and adaptable solutions.

Collaborative design approaches have gained significant traction as a means to open up the smart home development process and ensure that diverse user perspectives guide both research and implementation strategies. Based on the analysis of the 55 papers by Yao et al. (2023), the research methods used across the 55 papers were primarily quantitative, qualitative, and developmental. The quantitative research methods mainly included A/B testing[3], questionnaires, statistical analysis, and other techniques. The qualitative research methods included semi-structured interviews, context awareness, co-design, collaborative design, and exploratory design (Yao et al., 2023). The integration of collaborative design within smart home research acknowledges that effective implementation requires active collaboration with users rather than passive consultation. This collaborative approach not only enhances the relevance and usability of the resulting implementations but also addresses issues of diversity and accessibility that are often overlooked in technology-driven development approaches.

Smart home research often faces challenges in moving from theory to real-world applications, largely due to a focus on technical innovation rather than user needs and everyday contexts. This gap leads to sophisticated but impractical solutions. User-centric

[3] A/B testing is a statistical method that compares two versions of a product or design by randomly showing different versions to different user groups and measuring which performs better based on specific metrics like user engagement or satisfaction rates.

and collaborative design approaches offer effective ways to bridge this gap by involving users throughout the development cycle. Through iterative feedback and collaboration, these methods help identify real-world constraints early and support the creation of more practical, adaptable, and inclusive smart home systems.

3 Research gaps, questions, and design

This section outlines the rationale, focus, and methodology of the study. It begins by identifying critical gaps in the existing research on smart home technologies, particularly those affecting user experience, adoption, and trust. Building on these gaps, the study formulates specific research questions that guide inquiry into user challenges, preferences, and perceptions. Finally, the section presents the multiphase research design and methods employed to systematically address these questions, integrating both empirical data collection and prototype development to produce actionable insights.

3.1 Research gaps

Despite the growing spread of smart home technologies, user adoption and sustained engagement remain limited. A significant portion of the existing research has largely focused on the technical aspects of smart homes, often overlooking the not easily simplified experiences and challenges faced by users. This tech-centric approach has led to a disconnect between the capabilities of smart home systems and the actual needs and preferences of users.

One of the primary barriers to widespread adoption is the complexity associated with setting up and configuring smart home devices. Users frequently encounter difficulties integrating devices from different manufacturers, leading to compatibility issues and fragmented user experiences. Moreover, the lack of standardized protocols worsens these challenges, making it difficult for users to achieve seamless automation within their homes.

Privacy and security concerns further get in the way of user trust in smart home technologies. Many users are worried about data collection practices and the potential for unauthorized access to their personal information. These concerns are often heightened by the unclear nature of data-handling policies and the limited control users have over their data within smart home ecosystems.

Additionally, there is a noticeable gap in understanding the diverse needs of different user demographics. For instance, elderly users may have different usability requirements than younger, tech-savvy individuals. Many current smart home solutions take a one-size-fits-all approach and often fail to account for differences in technical skills, accessibility needs, or users' countries and living environments.

Furthermore, the evaluation of smart home systems has largely been confined to laboratory settings and lacks real-world validation. This limitation restricts the understanding of how users interact with smart home technologies in their daily lives and the practical factors influencing their experiences.

In short, while technological advancements have driven the development of smart home systems, there remains a critical need for research that centers on the user experience.

Addressing the identified gaps, such as system complexity, integration challenges, privacy concerns, demographic-specific needs, and real-world usability, will be essential in enhancing user satisfaction and promoting the broader adoption of smart home technologies.

3.2 Scientific novelty and contribution

The scientific novelty of this dissertation lies in the introduction of the UASH-DF, a structured, research-driven framework that bridges user-centric design principles with technical system implementation in smart home environments. The framework systematically integrates user needs, behavioral insights, and usability feedback into each stage of technology design and evaluation.

The framework advances scientific understanding by showing how compatibility, usability, privacy, and trust can be jointly optimized through iterative, evidence-based development. This approach moves beyond product engineering, offering a generalizable methodology applicable to both academic research and practical system design in intelligent environments and human-technology interaction. Building on this foundation, the dissertation makes the following contributions:

- **Theoretical contribution**: Extends the Technology Acceptance Model (TAM) by incorporating trust and privacy constructs.
- **Empirical contribution**: Provides cross-cultural insights into user adoption barriers in smart home technologies.
- **Practical contribution**: Delivers a working prototype research artifact demonstrating the framework's real-world applicability.

3.3 Research questions

Informed by a comprehensive examination of existing research and grounded in the overarching goal of aligning smart home technologies with genuine user needs, this doctoral work frames its research questions as a stepwise progression through four interrelated phases. Each question builds upon insights derived from identifying user-reported gaps, collecting empirical data on preferences and pain points, iteratively designing a user-centric prototype, and evaluating acceptance through established theoretical constructs. By structuring the questions to address both conceptual issues (such as usability, compatibility, and privacy) and practical concerns (including design requirements and acceptance metrics), this approach ensures a unified, user-focused investigation of smart home technologies.

RQ1. What are the key usability, integration, and privacy challenges experienced by smart home users?

RQ2. How do users perceive and prioritize usability, interoperability, and security in smart home technologies?

RQ3. How can a home automation system be designed, implemented, and evaluated to enhance the user experience while ensuring usefulness and trustworthiness?

Together, these questions guide a logical flow from understanding "what is" (user challenges), to determining "what should be prioritized" (user perceptions), to constructing "what could be" (designing and building a prototype), and finally to evaluating "what is acceptable and valuable" (user acceptance). This structured trajectory not only uncovers theoretical insights about user needs and technological gaps but also produces a validated, practical artifact that represents best practices in user-centric smart home design.

3.4 Research design and methods

This doctoral research uses a multiphase, mixed-methods design to investigate smart home technologies from users' perspectives. The process is illustrated in Figure 1, which outlines four sequential phases: a systematic literature review to identify user-reported gaps, an international survey to capture user preferences, prototype development of a smart home system, and a final evaluation phase to assess user acceptance and satisfaction.

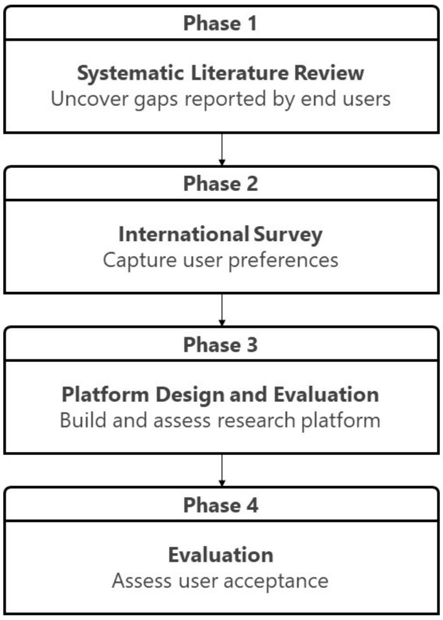

Figure 1: Multiphase research process integrating systematic review, empirical user study, platform development, and behavioral evaluation

In the first phase, a systematic literature review was conducted to uncover gaps reported by end users, such as usability obstacles, missing functionality, and integration shortcomings. By combining findings from a broad collection of studies, this phase established a clear understanding of what users want and what current solutions fail to deliver, laying the foundation for future empirical work.

In the second phase, an international, cross-sectional survey gathered quantitative data from smart home users across diverse demographics. The survey instrument was designed to capture user preferences, pinpoint common pain points (e.g., device interoperability, setup complexity, security concerns), and identify desired features that remain neglected in commercial offerings. Statistical analysis of these responses provided an empirical baseline for understanding how user needs vary by age, technical background, and geographic region, directly informing design priorities for the prototype.

The third phase applied a DSR methodology to construct a Raspberry Pi–based smart home platform, serving as a research artifact to investigate how user-reported needs can be translated into a tangible, testable system. This implementation laid the foundation for the final evaluation phase, enabling a structured assessment of usability, security, and adaptability. Iterative cycles of brainstorming, development, and refinement ensured that the platform addressed gaps identified in earlier phases and was suitable for behavioral evaluation.

In the fourth phase, the resulting prototype was evaluated through the lens of the TAM. A mixed-methods evaluation combining a structured questionnaire with follow-up interviews measured PU, PEOU, trust, and overall satisfaction. By statistically modeling these factors and triangulating them with qualitative feedback, this phase identified key drivers and barriers to user acceptance, providing actionable insights for both academic theory and practical system design.

Across all phases, the data collection and analysis procedures followed to rigorous ethical standards. Quantitative data were analyzed using summary statistics. Qualitative data were analyzed using thematic coding, a method for identifying and organizing recurring patterns or “themes” within textual feedback, allowing the researcher to capture users’ shared experiences and concerns systematically.

3.5 Research ethics

Throughout all phases of this dissertation, ethical considerations were carefully integrated into the research design, data collection, implementation, and reporting processes. Each of the four publications involved different methodological approaches—a systematic literature review, international survey, prototype development, and user evaluation—that required specific ethical practices tailored to the context of each study.

For the **systematic literature review** (Publication I), only publicly available, peer-reviewed sources were used. No personal or sensitive data were involved, and all findings were reported with academic integrity, ensuring proper citation and unbiased summary.

In the **international survey study** (Publication II), ethical measures included voluntary participation, informed consent, and full anonymity. Respondents were informed of the study's purpose and their right to withdraw at any point. No identifying information was collected, and the data were stored securely. The survey design was approved by institutional review procedures and complied with GDPR[4] principles for handling international participant data.

The **prototype development and testing phase** (Publication III) did not involve live end users during the initial deployment. However, ethical responsibility was applied in selecting secure, privacy-aware design decisions such as avoiding direct internet exposure via port forwarding, using key-based SSH authentication, and implementing GSM-based alerts to protect user safety in low-connectivity conditions. System logs and performance metrics used for evaluation were generated solely from controlled environments and did not include personal user information.

For the **TAM study** (Publication IV), ethical approval was obtained for user testing. Participants provided informed consent and were assured that their responses, both structured and open ended, would remain anonymous and confidential. They were informed of the voluntary nature of their participation, their right to skip any questions, and their freedom to withdraw at any time. The collected data were analyzed, summarized, and stored in a secure environment to protect the participants' privacy.

Across all studies, transparency, respect for participants, and responsible handling of data were fundamental guiding principles. No misleading practices were employed, and all analyses and findings were reported truthfully. The research complies with the ethical standards set by the academic institution and the broader research community, ensuring that the work meets the highest standards of integrity and respect for human participants.

[4] The general data protection regulation (GDPR) is a European Union law that governs the collection, processing, and storage of personal data to ensure privacy and data protection for individuals within the EU.

4 Overview of the publications

This chapter brings together four integrated studies that collectively trace the evolution of this research. It begins with a comprehensive review of the existing smart home literature to identify user-centric gaps, followed by a survey that captures diverse user needs and priorities. The chapter then details the design and iterative development of a fully integrated home automation prototype and finally presents an empirical evaluation of that prototype's usability, usefulness, and trustworthiness. Together, these studies form a unified story from identifying user challenges to gathering real-world input, to constructing a practical solution, and ultimately assessing its acceptance, demonstrating how each step builds upon the previous to advance both theoretical understanding and practical implementation in user-centric home automation.

4.1 Publication I: The Present State of Home Automation: A Systematic Literature Review

The first publication in this dissertation, titled *"The Present State of Home Automation: A Systematic Literature Review" (Yaldaie et al., 2022)*, lays the foundational groundwork for the later studies by critically examining the current landscape of smart home technologies. This comprehensive review identifies current trends, challenges, and gaps in the field, thereby informing the direction of the research presented in the following chapters. Table 1 summarizes the paper's structure, including its objectives, methodology, and contributions.

Table 1: Publication I Summary

Element	**Details**
Objective	A comprehensive review of existing smart home literature
Methodology	A systematic literature review with predefined inclusion/exclusion criteria
Key features	Identification of trends, challenges, and research gaps
Evaluation	A thematic analysis of selected studies
Outcome	A series of research gaps guiding following empirical work
Dependency	N/A (first study in sequence)

4.1.1 Motivation and scope

The drive for this literature review stems from the rapid growth of IoT devices and their integration into residential settings. Despite technological advancements, the widespread adoption of smart home systems remains limited due to factors such as usability issues, security concerns, and interoperability challenges. This study aims to summarize existing research to understand these barriers and identify areas requiring further investigation.

4.1.2 Methodology

A systematic literature review (SLR) was chosen as the methodological approach for this study due to its structured and rigorous nature, which minimizes bias and ensures comprehensive coverage of existing research. Unlike traditional literature reviews, which may be narrative and subjective, SLRs follow predefined criteria for inclusion and exclusion, allowing for a more objective summary of findings. The process began with a comprehensive search across four major digital libraries for English-language case studies exceeding three pages in length, focusing on various domains of smart home technologies. Thematic analysis was then conducted to extract data relevant to the research questions, ensuring a thorough understanding of the field.

The decision to employ an SLR was driven by several factors:

- **Comprehensive evidence synthesis:** An SLR provides a complete and balanced overview of existing research on a specific topic, ensuring that conclusions are based on the best available evidence.
- **Identification of research gaps:** By systematically evaluating existing studies, SLRs help identify areas where further research is needed, guiding future studies and funding priorities.
- **Reduced bias:** Following a structured protocol minimizes the risk of bias, ensuring that the findings are as objective and reliable as possible.
- **Informed decision-making:** SLRs provide evidence for policymakers, educators, and other stakeholders to make informed decisions based on comprehensive and up-to-date research.

By employing an SLR, this study aims to provide a robust foundation for understanding the current state of smart home technologies, thereby informing the subsequent research presented in this dissertation.

4.1.3 Key findings

The following key findings summarize the main insights from the literature review on smart home technologies. They highlight trends, challenges, and gaps in current research, providing a foundation for understanding how usability, security, interoperability, and user experience are being addressed in both practice and academia.

1. **Technological advancements and usability:** The review highlights significant progress in smart home technologies, including the development of motion sensors, remote-controlled devices, and voice-activated systems. However, it also reveals that many products prioritize either usability or security, often one at the expense of the other. This trade-off underscores the need for balanced design approaches that do not compromise one aspect for another.
2. **Security and privacy concerns:** Security and privacy emerge as critical issues, with many smart home products lacking robust protective measures. The review notes that some devices overlook basic security enhancements, making them vulnerable to unauthorized access and data breaches. This finding aligns with prior studies, which consistently show that privacy intrusions are among the most common threats to smart homes.
3. **Interoperability and standardization:** A significant challenge identified is the lack of standardization across smart home devices, leading to interoperability issues. The absence of common communication protocols prevents seamless integration, calling for the development of middleware and frameworks to facilitate better energy management and system efficiency.
4. **User interface and experience:** The diversity of users, spanning various age groups and technological proficiencies, requires intuitive and accessible user interfaces. The review emphasizes the importance of designing smart home systems that serve to this wide user base, ensuring that interfaces are both simple and effective.
5. **Research gaps:** The analysis reveals that most case studies are conducted in laboratory settings and lack real-world applicability. Additionally, there is a lack of research focusing on the comprehensive development of smart home systems that integrate usability, security, and performance.

4.1.4 Contribution to the dissertation

The systematic literature review conducted in this first publication serves as the cornerstone of the dissertation, providing a comprehensive and methodologically rigorous summary of existing research on smart home technologies. By employing a structured approach to identify, evaluate, and analyze relevant studies, the review offers an objective overview of the current state of the field, minimizing bias and enhancing the reliability of the findings.

This foundational work not only combines existing knowledge but also critically examines the methodologies and outcomes of prior studies, highlighting inconsistencies and areas where evidence is lacking or inconclusive. Such insights are invaluable for guiding future research efforts, as they pinpoint specific aspects of smart home technologies that require further exploration and development.

Furthermore, the review's emphasis on user-centric design, security, and interoperability issues underscores the diverse challenges that must be addressed to enhance the adoption and effectiveness of smart home systems. By systematically categorizing and analyzing these challenges, the review provides a clear framework for next investigations, ensuring that future studies are grounded in a thorough understanding of the existing literature.

In essence, this systematic literature review not only maps the current landscape of smart home technologies but also identifies critical gaps and opportunities for innovation. These insights set the stage for the ensuing research endeavors in this dissertation, which aim to address the identified challenges through empirical studies and practical implementations, thereby contributing to the advancement of user-friendly, secure, and interoperable smart home solutions.

4.2 Publication II: Who Are Smart Home Users and What Do They Want?—Insights from an International Survey

The second publication, titled *"Who Are Smart Home Users and What Do They Want?—Insights from an International Survey" (Yaldaie et al., 2023)*, presents the findings of a comprehensive user study aimed at understanding the current landscape of smart home adoption. Building on the gaps identified in the previous literature review, this study explores user demographics, behaviors, concerns, and expectations, providing valuable empirical insights to guide the user-centric design and development of smart home technologies. Table 2 summarizes the study's methodology and contribution to the dissertation, explaining how these insights informed the design of the prototype system developed in the next phase.

Table 2: Publication II Summary

Element	**Details**
Objective	Capture user experiences, preferences, and concerns via a survey
Methodology	Targeted literature review (to inform survey questions) + international online survey
Key features	Demographics, preferred features, cost considerations, and security concerns
Evaluation	Mixed-methods analysis

Outcome	Defined user requirements and preferences for prototype design
Dependency	Builds on identified research gaps and user concerns from Publication I

4.2.1 Motivation and scope

Building upon insights from the SLR, which highlights the complex challenges and opportunities in smart home technologies, this second study shifts from a theoretical exploration to an empirical investigation. In response to the identified gaps, particularly the lack of user-centric design approaches and the limited understanding of user expectations, this research seeks to explore the lived experiences, preferences, and concerns of both current and potential smart home users across diverse demographics. The goal is to generate practical insights that can guide the development of more accessible, secure, and user-friendly smart home solutions.

4.2.2 Methodology

To gain an in-depth understanding of user perspectives on smart home technologies, we designed and conducted an international survey that integrated both quantitative and qualitative elements. Recognizing that user needs and expectations can vary significantly across countries and cultural contexts, the survey instrument was carefully crafted based on insights from our prior SLR, ensuring alignment with identified research gaps and user-centric considerations. The questionnaire covered a diverse range of topics, including demographic information, current usage patterns of smart home devices, recognized benefits and challenges, privacy and security concerns, and desired functionalities. To ensure the clarity and relevance of the questions, a pilot study was conducted with a small, diverse group of participants, leading to refinements in question wording and structure. The finalized survey was shared online through various channels, including social media platforms, technology forums, and academic mailing lists, to reach a broad and diverse audience across different geographic regions, age groups, and levels of technological proficiency.

In analyzing the collected data, we employed a mixed-methods approach to capture both the variety and depth of user experiences and expectations. Quantitative data were analyzed using statistical techniques to identify patterns and correlations. This included using summary statistics to user characteristics and preferences. Qualitative responses were subjected to detailed analysis, allowing us to identify recurring themes and insights that provided the context for the quantitative findings. This dual approach enabled a comprehensive understanding of user needs and concerns, informing the following development of a prototype smart home system tailored to address the identified requirements.

4.2.3 Key findings

The survey aimed to explore users' experiences, preferences, and limitations regarding smart home technologies. The following key findings highlight patterns in demographics, awareness, feature preferences, and financial considerations, providing insight into factors that influence adoption and user satisfaction.

1. **Awareness vs. adoption:** While many respondents were aware of smart home technologies, full adoption remained limited. This gap suggests potential barriers, such as unfavorable cost–benefit balance, complexity, or privacy concerns that deter users from embracing these technologies fully. These patterns were particularly evident among younger adults living in rental accommodations, indicating the importance of designing solutions suited to this demographic.
2. **Preferred features:** Smart lighting systems emerged as a popular choice among users, indicating a preference for manageable and immediately beneficial smart home features. Security features also garnered significant interest, reflecting users' desire for safety and peace of mind.
3. **Cost considerations:** A notable finding was the budgetary limit among users, with most willing to invest a hundred euros or less in smart home technologies. This financial threshold highlights the necessity of cost-effective solutions in the smart home market.

These findings collectively emphasize the need for smart home technologies that are not only innovative but also affordable, user-friendly, and aligned with the specific needs and preferences of diverse user groups.

4.2.4 Contribution to the dissertation

This survey-based study plays a key role in advancing the dissertation's overarching goal of aligning smart home technologies with real user needs. Building on the theoretical foundation laid by the initial SLR, this paper introduces a critical empirical dimension by capturing the lived experiences and expectations of actual and potential smart home users. As part of this second publication, a targeted literature review was conducted to inform the design of the survey and ensure that the questions addressed the most relevant and pressing issues identified in prior research. The findings offer concrete evidence of user concerns, such as security, usability, and cost, that must be addressed to improve technology adoption.

4.3 Publication III: Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices

The third publication, *"Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices" (Yaldaie et al., 2024)*, marks a transition from theoretical exploration to hands-on implementation. Building on insights from the earlier literature review and international user survey, this study aimed to develop and evaluate a smart home prototype that responds to the most commonly reported user concerns: the need for intuitive usability, reliable security, and affordability. These priorities were identified as critical through both academic analysis and direct user feedback. The resulting system was designed to be easy to set up and operate, protective of user privacy, and financially accessible, ensuring that smart home technology could be more inclusive and practical for everyday households. This publication demonstrates how user-informed design choices can lead to more acceptable and adoptable smart home solutions. Table 3 summarizes the study's methodology and contribution to the dissertation, explaining how these insights informed the design of the prototype system evaluated in later sections.

Table 3: Publication III Summary

Element	**Details**
Objective	Design, develop, and validate a cost-effective smart home prototype
Methodology	Design science research (artifact creation and iterative evaluation)
Key features	Self-deployable system, extensible architecture; SSH key-based auth, Fail2Ban, firewall, GSM alerts
Evaluation	Testing across scenarios: responsive control, arm/disarm timing; GSM fallback
Outcome	Validated prototype meeting security, usability, and adaptability requirements
Dependency	Implements user requirements from Publication II and addresses gaps from Publication I

4.3.1 **Motivation and scope**

The motivation for this study stemmed from the need to bridge the gap between user expectations and smart home solutions. The prior survey revealed key user requirements, including intuitive interfaces, robust security features, and seamless integration of devices. In response, this study developed a prototype to meet these requirements and to serve as a flexible platform for future enhancements. The scope covered the integration of various sensors, the implementation of a user-friendly control interface, and the incorporation of security protocols to safeguard user data and system integrity. The developed prototype's source code are hosted in a public GitHub repository[5] to promote transparency, collaboration, and reproducibility. While the repository is publicly accessible, sensitive configuration data and credentials related to connected devices are excluded to maintain system security and integrity.

4.3.2 **Methodology**

This study adopts the DSR methodology, guided by the process model proposed by Peffers et al. (2007), which is well-suited for developing and evaluating IT artifacts that address real-world problems. DSR was chosen because it aligns with the goals of this research: to iteratively design, develop, and assess a functional smart home system prototype that directly responds to user expectations around usability, affordability, and security. Rather than only analyzing existing systems, this approach enabled active engagement in the creation of a novel solution and its evaluation in realistic residential contexts.

The research followed six key steps outlined by Peffers et al. (2007):

- Problem identification and motivation: Recognizing core user concerns—usability, affordability, and security—through a systematic literature review and international survey.
- Defining objectives for a solution: Establishing design goals based on user expectations and practical boundaries.
- Design and development: Creating a smart home prototype that reflects these objectives, using modular and cost-effective architecture.
- Demonstration: Deploying the system in realistic residential scenarios to showcase its functionality and adaptability.
- Evaluation: Assessing the system using user feedback and the TAM to measure PU, ease of use, trust, and privacy.
- Communication: Sharing results through academic publications and practical recommendations to inform future smart home development.

[5] https://github.com/Ashkan-Yaldaie/Smart_Home

While Hevner et al. (2004) provided foundational guidelines for DSR, this study adopts the process model proposed by Peffers et al. (2007), which offers a structured and sequential approach better suited for the iterative development and evaluation of a user-centric smart home system (Hevner et al., 2004; Peffers et al., 2007). This methodological choice ensured that the research not only contributed to academic knowledge but also delivered a tangible, user-aligned innovation in smart home technology.

4.3.3 Security features

Security emerged as a major concern in both the systematic literature review and the international survey presented in the first two publications. Users consistently emphasized the need for robust measures to protect against unauthorized access and data breaches and to ensure the trustworthiness of remotely accessible smart home systems. In direct response to these insights, the prototype smart home system developed in the third study incorporated a multilayered security approach, integrating several practical and well-established tools to safeguard the system and address these user concerns.

To ensure secure remote access, the system was designed with multiple layers of protection. Measures were put in place to control authentication, limit network exposure, and prevent direct internet access while still allowing necessary remote interactions. This approach provides a strong security posture without relying on overly complex or exposed configurations. Further details on the specific implementations are available in the papers referenced in this dissertation.

For secure remote control and monitoring, a chat-based interface was implemented. Users can send commands and receive real-time status updates through this application. This setup avoids exposing a web interface and ensures encrypted communication using the chat application's secure messaging protocol. When graphical access to the system was necessary, virtual network computing (VNC) was employed. VNC sessions were password protected and configured to require explicit permission before remote desktop sharing could begin, ensuring user control over remote visibility.

By incorporating these measures, SSH with key-based authentication, Fail2Ban, a strict firewall, secure remote access methods without port forwarding, and secure VNC, the system addresses key security concerns from earlier findings and demonstrates a strong commitment to user privacy and system integrity.

4.3.4 Testing and evaluation

Building on the security and usability concerns identified in the first two publications, the prototype smart home system underwent a comprehensive testing phase designed to ensure that it met real-world demands across a variety of operational constraints. Rather than focusing on specific dwelling types, the evaluation examined the system's adaptability, reliability, and performance under three general scenario categories: environments with limited space, setups requiring scalability and customization across multiple rooms, and contexts with unreliable internet connectivity. Each scenario was chosen to reflect the challenges and user requirements uncovered by earlier research: maintaining responsive control in confined areas, providing dependable, hands-off security features in more extensive layouts, and maintaining functionality when network access is unreliable.

To assess responsiveness and resource management in limited-space conditions, sensors for lighting and climate control were managed through frequent on/off cycles while commands were issued via the web interface. The system consistently provided smooth, nearly real-time feedback, and the core hardware remained well under capacity, even when multiple devices were running.

In scenarios demanding scalability and user customization, where multiple sensors and actuators operate simultaneously, the prototype's automatic arm and disarm features were rigorously tested. The system seamlessly transitioned into security mode when the occupants left and reliably reverted to a disarmed state upon their return, without requiring manual intervention. Occasional false triggers led to adjustments in the arm and disarm timing, ensuring a more reliable operation. These refinements guided future tuning to minimize false alarms while maintaining comfort, confirming earlier survey findings that users need both flexibility and dependable security in larger homes.

To evaluate resilience when internet connectivity was unreliable, the system employed a GSM-based security alert feature. Whenever a security breach was detected, such as motion detection while the network was offline, the system automatically sent a text message notification to a designated phone number. Concurrently, local control functions remained available, allowing occupants to manage devices on the home network without interruption. This capability directly addresses participants' concerns regarding data privacy and system trust.

Across all testing scenarios, the implemented security measures, including SSH with key-based authentication, Fail2Ban for unauthorized login prevention, a strictly configured firewall, secure VNC for graphical access, and GSM fallback for emergency alerts, demonstrated robust protection. Simulated intrusion attempts were consistently blocked, and remote connection responsiveness remained acceptable, even when relying on GSM. The control interface provided swift device toggling, dependable automatic arming and disarming, and timely SMS alerts during network outages. Performance observations confirmed that the prototype maintained reliable operation under varying network conditions and hardware demands.

In summary, this testing and evaluation phase confirmed that a Raspberry Pi–based smart home system can satisfy the key concerns identified in earlier studies. By successfully adapting to constraints on space, accommodating multiple devices and user behaviors, and providing robust fallback mechanisms for connectivity issues, the prototype demonstrated robustness, security, and user-centric design. These findings create a path for further enhancements, such as refining system calibration to reduce false alarms while underscoring the dissertation's central aim of creating accessible and reliable smart home solutions.

4.3.5 Contribution to the dissertation

This practical implementation study serves as a critical bridge between theoretical insights and empirical validation. By translating the requirements identified through the systematic literature review and international survey into a functioning prototype, the third paper demonstrates that a proof-of-concept system can effectively address core user concerns, particularly security, responsiveness, and adaptability, within real-world environments. The rigorous testing and evaluation confirmed that design choices (for example, SSH key-based authentication, dynamic sensor timing, and GSM fallback alerts) not only reduced previously identified barriers but also provided actionable lessons for refining sensor calibration and network-independent functionality.

Moreover, this study's successful implementation and validation will establish a solid foundation for the next phase of the dissertation and evaluate user acceptance via the TAM. By showing that a Raspberry Pi–based smart home can perform reliably, maintain robust security, and remain user-centric under diverse conditions, the third publication lays the groundwork for examining how PU and ease of use influence adoption decisions. Therefore, this contribution validates the feasibility of accessible home automation solutions and sets the stage for assessing their acceptance and long-term viability.

4.4 Publication IV: User Perceptions of a Home Automation System: A TAM-Based Evaluation

The fourth publication, titled "*User Perceptions of a Home Automation System: A TAM-Based Evaluation" (Yaldaie et al., 2025),* investigates how users view and accept the smart home prototype developed earlier in this research. Building on the functional implementation and user-driven design of previous studies, this paper applies the TAM to assess key factors influencing adoption, specifically PU, PEOU, trust, and privacy concerns. The study provides a behavioral perspective on system evaluation, offering critical insights into how users respond to its features, security mechanisms, and interface design. This publication represents the final step in linking user expectations, technical implementation, and actual acceptance, reinforcing the dissertation's focus on creating effective and adaptable smart home solutions. Table 4 summarizes the TAM-based evaluation, outlining the methodology, key constructs assessed, and the study's broader contribution to understanding user adoption.

Table 4: Publication IV Summary

Element	Details

Objective	To evaluate user acceptance of the developed smart home prototype using the TAM
Methodology	Mixed-methods: Structured TAM-based survey combined with open-ended questions to gather both quantitative and qualitative insights
Key features	Assessment of PU, PEOU, trust, and privacy concerns using Likert-scale questions and qualitative responses
Evaluation	Analysis of survey responses
Outcome	Validated that usefulness and ease of use drive acceptance; trust and privacy remain key concerns; user feedback guided future improvements
Dependency	Builds on technical implementation (Publication III) and user needs identified in earlier studies (Publications I and II)

4.4.1 **Motivation and scope**

The fourth publication addresses a critical question remaining after prototype development: Even if a system performs well technically, will users accept and adopt it? Earlier studies identified key user concerns, security, usability, cost, and adaptability, and produced a working Raspberry Pi–based prototype. However, without understanding the psychological factors driving user acceptance, broad deployment is unlikely. Accordingly, this study uses the TAM to investigate how PU, PEOU, trust, and privacy concerns influence the intention to adopt the newly developed home automation system. The scope includes both quantitative measurement of TAM constructs and qualitative exploration of lingering user reservations, ensuring that recommendations for future iterations are grounded in real user perceptions.

4.4.2 **Methodology**

A mixed-methods approach was employed in a controlled laboratory environment to ensure consistency across participants. Twenty individuals, each with prior experience using some form of home automation or security system, were invited to interact with the prototype. The protocol proceeded in three stages:

1. **System demonstration:** Facilitators walked participants through the system's core features (energy management, scheduled automation, secure remote access, and security alert mechanisms). This ensured that every participant had equivalent baseline exposure to functionality before the evaluation.
2. **Structured TAM survey:** Immediately following the demonstration, participants engaged in a hands-on session to experience the system directly. Once the hands-on activity concluded, participants completed a questionnaire designed to measure the primary TAM constructs (PU and PEOU) as well as supplemental constructs of trust and privacy concern. Each question used a five-point Likert scale (strongly disagree to strongly agree). Sample items included the following:
    - "Using this system would improve my management of household tasks" (perceived usefulness).
    - "The system's interface was intuitive and easy to navigate" (perceived ease of use).
    - "I trust this system to maintain the confidentiality of my data" (trust).
    - "I am concerned about unauthorized access to my home automation data" (privacy concern).
3. **Open-ended responses:** After completing the structured survey, participants were invited to answer a series of open-ended questions aimed at gathering deeper insights. These prompts encouraged them to share concerns, suggest potential improvements (such as implementing two-factor authentication or increasing transparency around data encryption), and propose additional features they would find valuable (such as appliance-specific control options). This qualitative input complemented the numerical survey data by revealing subtle perspectives and edge-case considerations that structured questions alone may not have uncovered.

4.4.3 Key findings

The user evaluation aimed to assess the participants' perceptions of the system in terms of usefulness, usability, trust, and privacy. The following key findings summarize both quantitative and qualitative insights, highlighting factors that influence acceptance, user satisfaction, and intentions to adopt the system.

- **Perceived usefulness (PU):** A large majority of participants agreed that the system would enhance task efficiency and improve control over household devices. Features cited most often as beneficial included the energy consumption leaderboard (which encouraged more sustainable habits) and automated scheduling of lights and climate control.
- **Perceived ease of use (PEOU):** Most participants found the interface straightforward. They praised its clear layout and logical menu structure and

reported that learning to navigate the system took minimal time. Suggestions for improvement focused on adding visual indicators (e.g., color-coded status indicators) and a search function for quicker navigation.

- **Trust:** While many participants endorsed the system's reliability—citing consistent performance during the demo—a few felt fully confident about data privacy. Concerns clustered around how user credentials are stored and whether communication channels (e.g., remote commands) are fully encrypted. Several interviewees requested two-factor authentication and clearer explanations of security protocols.
- **Privacy concerns:** Responses were mixed; some users expressed little worry, noting that they assumed any connected device carries some risk, while others remained skeptical. Common recommendations included visible indicators of encryption status and an audit log feature so that users could review access attempts.
- **Behavioral intention to use:** Despite security reservations, most participants indicated that they would like to use the system and would recommend it to others. The combination of energy management benefits and intuitive controls outweighed privacy concerns for these respondents.
- **Qualitative insights:** Through the open-ended responses, participants emphasized that transparent communication about data protection would increase their trust in the system. Several respondents suggested additional features, such as integration with appliances like washing machines or dishwashers. These insights provided a valuable context for the quantitative findings, highlighting specific user expectations for future system development.

4.4.4 Contribution to the dissertation

This fourth publication completes the dissertation's trajectory by connecting technical implementation with a user-centric evaluation. The results confirm that PU and PEOU remain prime drivers of adoption, as TAM predicts, but also reveal that trust and privacy concerns cannot be overlooked in a home automation context.

The study involved a sample of 20 participants, each with prior experience using home automation or security systems. While this sample size is appropriate for exploratory, mixed-methods research and gave valuable qualitative insights, its limited scope restricts the generalizability of the findings. The sample, composed entirely of users with prior home automation experience, may not represent the broader population, especially those with low technical literacy or first-time users. As such, conclusions drawn regarding PU, ease of use, and trust may be overly optimistic or not fully representative. Future studies should incorporate a larger, demographically diverse participant pool, including individuals from varied age groups, different income and education levels, and technology comfort levels. Doing so would enhance the external validity of the TAM constructs and provide a deeper understanding of adoption barriers across the full spectrum of potential users.

By measuring key acceptance factors and collecting in-depth qualitative feedback, the study provides concrete guidance for enhancing security architecture (e.g., two-factor authentication, clearer encryption indicators) and refining user interfaces (e.g., visual status cues, extended device compatibility). These findings validate the prototype's core design decisions, demonstrating that its energy-saving and security features are indeed valued, and highlight areas requiring further iteration. Ultimately, this publication bridges the gap between "Can we build it?" and "Will users adopt it?", ensuring that the study's recommendations are rooted in both technical feasibility and real human acceptance.

5 Discussion

The findings of this research demonstrate that a user-centric approach to smart home development—beginning with a systematic identification of usability, security, and interoperability gaps (Publication I), followed by an in-depth survey of users' priorities and challenges (Publication II), resulting in a flexible prototype implementation (Publication III) and a rigorous TAM evaluation (Publication IV)—can effectively bridge the gap between technical innovation and end-user needs. By iteratively aligning each phase with the specific concerns highlighted in the literature and by actual users (e.g., the need for intuitive interfaces, robust security protocols, and cost-effective solutions), the dissertation not only confirms that PU and ease of use are key drivers of adoption but also uncovers that trust and transparent privacy mechanisms are equally critical in building long-term engagement.

By emphasizing the importance of balancing usability with security, the work shows that adaptable architectures (e.g., Raspberry Pi–based systems with layered authentication and GSM fallback alerts) can satisfy diverse residential contexts, from compact living spaces to larger, multiroom installations without sacrificing user confidence or functionality. Moreover, the combined quantitative and qualitative insights reveal specific areas for enhancement, such as enhanced visual indicators, two-factor authentication, and appliance-level integration that directly inform the design of future smart home platforms. Taken together, these integrated contributions demonstrate that embedding continuous user feedback at every stage is essential for realizing smart home environments that are technically robust and genuinely responsive to the evolving expectations of modern households.

Overall, the main findings and design decisions from the research, show how the work addresses gaps in usability, interoperability, and privacy. The introduction of the UASH-DF provides a structured, practical approach for building smart home systems that are secure, adaptable, and easy to use.

The framework's elements, including context-aware design, open-source architecture, security by design, and ecosystem compatibility, were shaped by real user feedback and validated through testing and evaluation. The section also reflects on the original research questions, showing how they were answered through literature review, user studies, prototype development, and behavioral analysis. When combined, the findings confirm that smart home technologies can be designed to meet everyday needs and that a user-centered approach is essential for creating systems that people trust, enjoy, and are willing to adopt.

5.1 User-aligned smart home development framework

Drawing on the four interrelated studies presented in this dissertation, (1) a systematic literature review of smart home technologies, (2) an international survey of user preferences and concerns, (3) the design and implementation of a Raspberry Pi–based prototype, and (4) a TAM evaluation, we introduce the user-aligned smart home development framework. As illustrated in Figure 2, UASH-DF outlines six fundamental steps for designing, building, and sustaining smart home technologies that are secure, compatible, cost-effective, and, above all, closely aligned with the real-world experiences and expectations of real users.

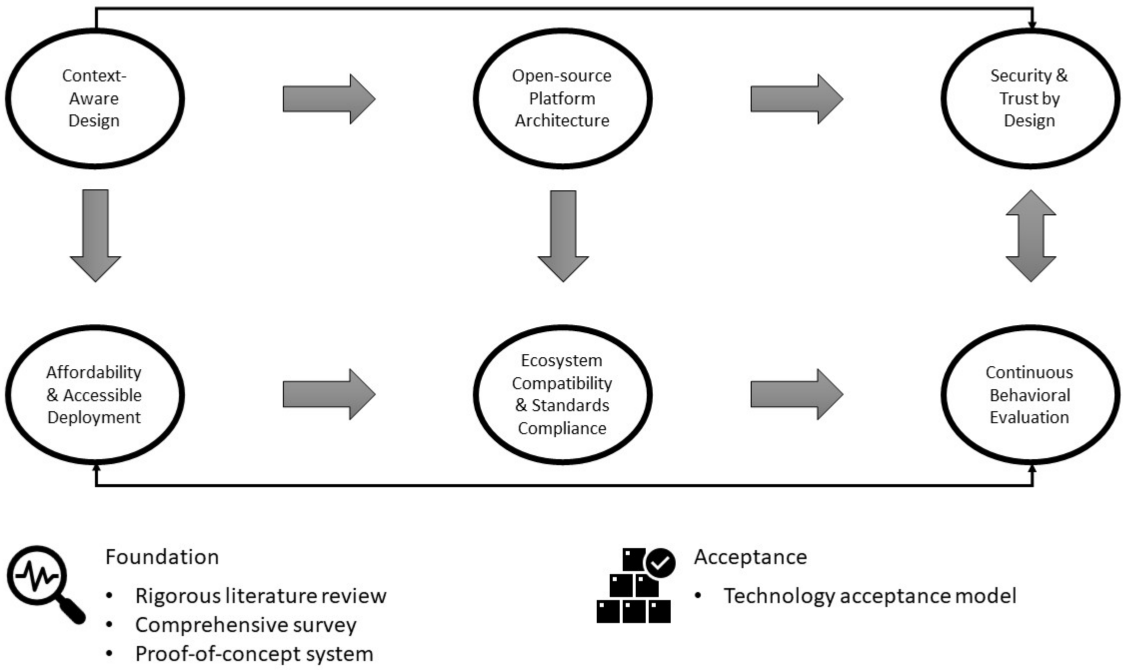

Figure 2: User-Aligned Smart Home Development Framework (UASH-DF)

5.1.1 **Context-aware design based on household living environments**

To ensure that system features and workflows are truly effective and appropriate for the context, they must be grounded in a deep understanding of everyday household practices. This includes not only practical routines, physical layouts, and usage patterns, but also the cultural norms, social dynamics, and environmental conditions that shape how homes are inhabited and used.

- **Living context exploration:** Begin by systematically analyzing common housing types, such as apartments, studios, shared homes, and detached houses, to identify recurring environmental configurations, typical room usage, and infrastructure limitations. This analysis supports design decisions related to device placement, automation triggers, and connectivity strategies.
- **Practical use scenario development:** Design system behavior around concrete, everyday use cases such as entering or exiting the home, adjusting lighting in

commonly used rooms, managing heating based on occupancy, or securing the premises at night. These straightforward, purpose-driven scenarios help define automation templates that are directly applicable to how people live, ensuring that the system remains simple, functional, and adaptable to a variety of home types.
- **Cultural and contextual considerations:** Drawing from the international survey and literature review, this step underscores the importance of accounting for differences across countries in housing types, lifestyles, cultural norms, and user expectations. Rather than relying on data from a single country or context, design decisions should be informed by a broad understanding of how smart home technologies are viewed and used around the world. Qualitative methods such as diary studies, home walkthroughs, and location-based photo documentation can further enrich this perspective by capturing how everyday activities unfold in diverse home environments and cultural settings.

5.1.2 Open-source platform architecture

To ensure system reliability, transparency, and long-term viability, the system should be built on platforms that avoid subscription dependencies, exclusive restrictions, and sudden version changes that may cause service disruptions. Furthermore, the platform should enable active contributions from both developers and end users to enable the system evolve in ways that reflect real-world needs and user-centric design principles.

- **Foundation on transparent and modifiable platforms:** Develop the system using widely adopted, community-supported platforms and libraries that allow full visibility into the codebase, strong peer collaboration, and the flexibility to audit, customize, or extend core features independently of commercial vendors. Encourage contributions from developers and users alike so that enhancements, bug fixes, and feature ideas reflect practical, user-driven priorities.
- **Subscription-free operation:** By avoiding cloud-dependent services and paid APIs, the system guarantees continuous access to essential functions, such as automation, control, and data logging, even without internet connectivity or when vendor services evolve or discontinue. This ensures sustainability and usability over the long term, particularly where ongoing costs are a concern.

5.1.3 Security and trust by design

To safeguard the system, embed robust protection at every layer while maintaining user transparency and control.

- **Secure defaults:** Enforce private-key SSH for administrator access, and disable password authentication. Apply firewall rules that whitelist only essential ports, and reject unauthorized inbound connections. Avoid direct port forwarding in favor of reverse-SSH tunnels or VPN connections for remote access.

- **Automated intrusion defense:** Integrate tools such as Fail2Ban to monitor authentication logs and dynamically block IP addresses exhibiting suspicious behavior. Augment with local anomaly detection (e.g., unusual sensor activation patterns) to trigger user alerts.
- **Transparent privacy dashboard:** Provide a dedicated user interface that visualizes device status, active data streams, storage locations, and recent remote connections.

5.1.4 Affordability and accessible deployment

To increase accessibility, lower cost barriers, and empower end users to adopt, configure, and evolve their systems with minimal technical overhead, the following measures should be adopted:

- **Cost-optimized components:** Source commodity sensors and actuators that are low cost and easily available. Provide detailed component lists in published reference designs to ensure that a basic home automation setup remains affordable and scalable.
- **Pre-configured system images:** Distribute ready-to-flash operating system images with all necessary services preinstalled and pre-wired for common scenarios (e.g., basic lighting control, security monitoring, energy tracking). The initial setup should require no command-line interaction.
- **Comprehensive documentation and tutorials:** Offer multi-format guidance, step-by-step written manuals, screencast videos, and an online FAQ knowledge base, all tailored to varying skill levels. Provide community support channels to help users troubleshoot issues and share practical examples.

5.1.5 Ecosystem compatibility and standards compliance

Address device variation by adopting widely supported compatibility standards and implementing middleware bridges.

- **Integration with major ecosystems:** Build native support for popular platforms such as Alexa, enabling seamless interaction with a broad range of devices across different vendors. This ensures that users can control and automate devices from multiple brands without complex setups or additional programming.
- **Middleware adapters:** Develop or incorporate middleware connectors that translate vendor-specific cloud APIs into a consistent internal data model. This

abstraction simplifies device onboarding and management, allowing the easy addition of new devices, regardless of vendor-specific protocols.

This approach is recommended based on insights and practical experience gained from our research, highlighting the importance of seamless integration with major ecosystems to build a robust and user-friendly smart home system.

5.1.6 Continuous behavioral evaluation

- **Embedded telemetry (with consent):** Collect anonymous usage metrics, feature invocation counts, automation success/failure rates, and session durations, to quantify real-world PU and detect issues.
- **Periodic TAM surveys:** At defined milestones (e.g., 3, 6, and 12 months post-deployment), prompt users with brief questionnaires to reassess PU, PEOU, trust, and privacy concern. Use aggregate scores to guide ranking of feature enhancements and security updates.
- **Qualitative feedback channels:** Maintain open feedback mechanisms and survey comment fields, community discussion boards, and periodic user focus groups, to capture edge-case suggestions (e.g., appliance-specific routines, advanced scheduling scenarios) and update the product roadmap.

5.1.7 Concluding remarks

The UASH-DF, developed through four integrated studies—a systematic literature review, an international user survey, a prototype implementation, and a TAM evaluation—offers a novel, domain-specific approach to smart home system design. While the overall research process was guided by the DSR methodology, outlined by Peffers et al. (2007), UASH-DF extends these principles into a practical framework tailored to the unique challenges of smart home adoption. It outlines six actionable phases: designing systems grounded in real household contexts and cultural diversity; building on transparent, subscription-free platforms; embedding security by design with user control; enabling affordable and easy-to-maintain solutions; ensuring compatibility with major ecosystems (e.g., Amazon Alexa) through middleware bridges; and continuously evaluating user behavior and trust to guide iterative improvements. This framework translates general DSR principles into a user-centric roadmap for creating secure, compatible, and inclusive smart home environments.

5.2 Revisiting the research questions and contributions

This section will provide a brief overview of how each of the original research questions has been addressed throughout the dissertation and will highlight the key contributions that have emerged from Publications I–IV, both individually and in combination. By systematically mapping empirical findings and design outcomes back to RQ1–RQ3, we will demonstrate how the theoretical insights, user-centric requirements, prototype implementations, and TAM evaluations collectively resolve the gaps identified at the beginning. The discussion will also emphasize the unique contributions of this work, such as the integration of systematic review findings with user feedback and the development of a proof-of-concept system for an scalable smart home architecture. These contributions clarify how the work advances both academic understanding and practical applications in the field of smart home technologies.

5.2.1 **RQ1: Key usability, integration, and privacy challenges**

To answer Research Question 1, *"What are the key usability, integration, and privacy challenges experienced by smart home users?"* the first stage of this research involved a systematic analysis of 56 empirical studies published between 2013 and 2022. This phase provided a comprehensive understanding of the recurring obstacles that users face when adopting and living with smart home technologies. However, beyond identifying these challenges, it is essential to reflect on their impact for future design and development.

While the systematic review captured studies up to 2022, more recent research confirms that these challenges remain highly relevant. A 2025 survey of 401 U.S. smart home users found that security-focused devices such as smart locks and cameras were trusted far more than voice assistants, reinforcing that privacy and protection remain the entry points to adoption rather than optional add-ons (Haney & Haney, 2025). Similarly, a 2024 review of older adults' experiences with smart home surveillance highlighted the same tension: safety was valued, but it was consistently balanced against deep concerns about autonomy and data handling (Campbell et al., 2024). Broader analyses echo this pattern. A 2023 systematic review of "digital harms" in smart homes identified persistent risks around surveillance, data misuse, and lack of transparency in vendor practices (Buil-Gil et al., 2023). Even as new compatibility standards gain traction, industry commentary notes that reliability and ease-of-integration remain works in progress rather than solved issues (Pattison Tuohy, 2025). Taken together, these newer sources demonstrate that usability, integration, and privacy challenges identified up to 2022 are not diminishing but are continuing to shape adoption trajectories today.

Usability emerged as one of the most widespread and persistent barriers. Despite the promise of seamless control, many systems demand a level of technical competence that excludes a large portion of potential users. The reliance on scripting, visual rule builders, and fragmented interfaces not only frustrates users but also undermines the comfort smart homes are meant to deliver. This highlights a clear gap between what the technology aims to do and what users are actually able to use. If smart homes are to become mainstream, they must be designed for the average household, not just for the tech-savvy minority. The fact that users spend more time troubleshooting than benefiting from automation is not a minor inconvenience; it is a design failure that must be addressed with urgency.

Integration challenges further worsen this issue. The fragmentation of communication protocols and ecosystems forces users into complex setups involving multiple hubs and apps. This is not just a technical inconvenience; it is a barrier to trust and long-term engagement. When users cannot rely on their systems to work together, the apparent intelligence of the home collapses. Overreliance on cloud-based processing introduces latency and vulnerability, making even basic functions dependent on external infrastructure. This raises a critical question: Can a home truly be "smart" if it cannot operate independently and reliably within its own environment?

Privacy concerns add another layer of complexity. The literature reveals a troubling disconnect between data collection practices and user awareness. Users are often left in the dark about what data is being gathered, how it is stored, and who has access to it. This lack of transparency undermines trust and leads to the disabling of features that could otherwise enhance safety and convenience. The fact that users must choose between functionality and privacy is unacceptable. Privacy should not be a hidden setting; it should be a visible, controllable, and integral part of the user experience.

What becomes evident is that usability, integration, and privacy are not isolated issues; they are deeply interconnected. Attempts to simplify setup often hide privacy controls. Enhancing interoperability through cloud services introduces new risks. These trade-offs reveal a fragile balance in current smart home design, where improving one dimension often compromises another. This interdependence demands a comprehensive approach that does not treat these challenges as separate checkboxes but as co-dependent pillars of user trust and satisfaction.

Reflecting on these findings, it is clear that the smart home industry must shift from a technology-first mindset to a user-first approach. Future systems must offer adaptive interfaces that scale with user skill levels, enabling both simplicity and customization. Integration must be seamless and vendor-neutral, supported by middleware that abstracts complexity without sacrificing transparency. Most importantly, privacy must be rethought, not as a compliance checkbox but as a core design principle. Users should be able to understand and control their data easily, without needing technical expertise.

In summary, the literature not only highlights challenges but also exposes a fundamental misalignment between smart home technologies and the lived realities of users. This reflection underscores the urgency of rethinking how we design, communicate, and deploy these systems. Only by addressing usability, integration, and privacy together, along with boldly prioritizing user empowerment, can smart homes evolve from fragmented gadgets into truly intelligent, trustworthy environments.

5.2.2 RQ2: User perceptions and prioritization of usability, interoperability, and security

To address RQ2, *"How do users perceive and prioritize usability, interoperability, and security in smart home technologies?"* the second phase of this research investigated real-world user attitudes through an online survey distributed to 73 participants. The sample included current smart home users and individuals who were not yet using such technologies but were familiar with the concept. Participants were asked to identify the most important features of a smart home system, the key benefits they had experienced or expected, and the most notable challenges. This analysis provides a detailed view of how these three dimensions—usability, interoperability, and security—are perceived in practical contexts and how they shape adoption, engagement, and trust.

The survey revealed a clear prioritization pattern: **Security** was consistently ranked as the most important and expected feature. Among non-users, 73.7% identified security functionality as critical, while 74.3% of current users reported actively using features such as remote surveillance, intrusion detection, or smart locks. This near-identical response rate across groups suggests that **security is not just a desirable feature but also a prerequisite for trust and engagement**. Users are unlikely to adopt or retain smart home systems that do not offer robust protection. This finding reinforces the idea that smart homes are perceived not only as convenience tools but also as guardians of personal space and safety. It also implies that any breach of security, whether technical or perceptual, can quickly weaken user confidence and lead to disengagement.

Yet, **security alone is insufficient**. The survey responses revealed that **usability is both a promise and a pitfall**. Non-users expected smart home systems to be “easy to use,” anticipating benefits such as remote accessibility and energy savings. Among users, some confirmed these expectations, especially when systems offered user-friendly interfaces or voice control. However, significant usability frustrations, such as “hard configuration,” and “installation complexity,” point to a deeper issue: **Smart home systems often fail to deliver on their promise of simplicity**. This disconnect between expectation and experience is not minor; it undermines the perceived value of the technology and introduces difficulty into everyday use.

What this means is that **usability must be redefined**. It cannot be limited to visual design or feature lists. True usability involves **guiding users through setup, minimizing cognitive load, and offering consistent, predictable interactions**. The fact that users resort to trial-and-error experimentation to configure their systems is a clear signal that current design practices are falling short. Moreover, usability is not just about convenience; it is about **empowerment**. When users feel in control, they are more likely to explore, personalize, and trust the system. When they feel confused or overwhelmed, they disengage.

Interoperability, while less frequently cited as a top feature, emerged strongly as a source of dissatisfaction. Users described challenges integrating devices from different brands, dealing with protocol mismatches, and managing fragmented ecosystems. These issues are not just technical; they are experience-based. When users must juggle multiple apps or abandon automation goals due to incompatibility, the system stops to feel “smart.” For non-users, the perception of complexity and incompatibility was a major deterrent, suggesting that **interoperability is a silent gatekeeper to adoption**. It may not be the first thing users think about, but it becomes critical as systems grow and diversify.

The open-ended responses revealed an implicit hierarchy: **security is the foundation, usability is the enabler, and interoperability is the integrator**. Without security, users will not engage. Without usability, they will not stay. Without interoperability, they will not scale. This hierarchy offers a practical lens for smart home development, one that prioritizes trust, simplicity, and consistency.

From a design perspective, these insights demand bold action. First, **security must be embedded by default** and not installed as an advanced option. This includes encrypted communication, local data storage, transparent privacy policies, and user-friendly access controls. Second, **usability must be treated as a continuous experience**, not as a one-time feature. It should span onboarding, configuration, and daily interaction, supported by guided setup, clear feedback, and accessible help. Third, **interoperability must be a core technical requirement**, not an afterthought. Systems should support open standards or provide middleware that enables seamless integration with minimal user effort.

In reflecting on these findings, it becomes clear that **user perception is not just a reaction; it is a design outcome**. The way users prioritize and experience security, usability, and interoperability reflects the choices made by developers and designers. If smart homes are to become truly mainstream, these choices must shift toward a **user-aligned, inclusive, and transparent design**. The results of this phase confirm that addressing user perception is not merely a matter of interface design; it is an essential necessity for sustainable smart home development.

5.2.3 RQ3: Design, implementation, and evaluation of a usable and trustworthy home automation system

To answer RQ3, *"How can a home automation system be designed, implemented, and evaluated to enhance the user experience while ensuring usefulness and trustworthiness?"* this research combined system development with empirical user evaluation.

5.2.3.1 System design and implementation

The third phase of this research involved the development and evaluation of a fully functional smart home prototype. This system was implemented using a Raspberry Pi as its central unit and was explicitly designed to minimize the technical complexity commonly associated with installation, configuration, and daily use. The solution aims to address some of the issues identified in earlier phases, such as steep learning curves, fragmented control interfaces, and a lack of easy-to-understand feedback in certain commercial platforms.

The system's hardware architecture is centered on a Raspberry Pi 3 Model B, chosen for its low cost, availability, and suitability for embedded control. This device functions as the master node and is integrated with a variety of sensors and actuators. These include passive infrared (PIR) motion sensors, smoke sensors, magnetic door contacts, temperature and humidity sensors, and smart plugs for switching loads such as lighting and appliances. The system supports both wired and wireless communication through protocols such as Wi-Fi and RF, ensuring flexibility in sensor placement and scalability across various home layouts.

To reduce configuration complexity for users, the system is delivered as a fully preinstalled and preconfigured software package. This approach removes the need for manual setup or command-line interaction, allowing users to begin using the system immediately after powering it on. By eliminating typical installation and configuration barriers associated with open-source platforms, this plug-and-play model directly addresses one of the most common usability challenges identified earlier: the need for technical expertise during system setup.

A key element of the system is its multi-interface interaction model, which is designed to support different user preferences and technical backgrounds. The primary interface is a browser-based control panel hosted on the Raspberry Pi, which provides a clear dashboard view of system status and sensor readings. Users can view real-time data from temperature, humidity, and smoke sensors, and receive alerts when motion is detected or when a door or window is opened. This dashboard avoids complex navigation structures and instead presents device information using clean, card-based visualizations and color-coded alerts.

To further support accessibility and remote monitoring, the system also includes integration with an **instant messaging application**. Users receive real-time updates about events such as motion detection, smoke detection, or door openings. They can also issue simple text commands to control devices (e.g., switching loads or requesting current sensor values) via a private chat interface. This messaging-based control channel allows for remote interaction without requiring the user to expose network ports or manage VPN[6] access, addressing security and ease of use at the same time.

In addition to passive monitoring, the system supports basic automation scenarios. For example, it can be configured to switch off connected loads automatically at a certain time for a predefined period or to trigger alerts when the smoke concentration exceeds the safe thresholds. These automations are implemented through rule definitions embedded within the system's Python-based backend and do not require user scripting. This is a critical usability improvement over many existing platforms that rely on users to define automation rules through code or complex logic editors.

[6] Virtual private network (VPN) is a secure connection method often used for remote access but can be complex for non-technical users to configure and maintain.

In addition to usability, the system incorporates key security and privacy safeguards to ensure safe deployment in real-world home environments. All data transmission occurs over the local network. This local-first architecture minimizes data exposure and reduces the risk of unauthorized access through external endpoints. Alerts and commands sent via the integrated messaging interface are limited to pre-authorized user accounts, and the system generates no open ports by default, avoiding common vulnerabilities associated with remote access. Furthermore, access to the control panel is password protected, and sensitive data such as event logs and sensor readings are stored securely in a local database on the device. By reducing reliance on cloud infrastructure and implementing lightweight local protections, the system addresses many of the privacy and security concerns identified in earlier phases while maintaining ease of use.

By focusing on usability as a core design goal, complemented by careful attention to security and privacy, the implemented system provides a viable solution to the most common barriers to smart home adoption. Through preinstalled software, guided setup, intuitive interfaces, automation without scripting, and secure local operations, the system enables users to confidently install and manage smart home functions. Its modular architecture also ensures affordability, flexibility, and future extensibility.

5.2.3.2 **User evaluation**

The final phase of this research applied the TAM to empirically assess the prototype system. The evaluation focused on key constructs from TAM, including PU, PEOU, trust, privacy concerns, and BI to adopt the system. A mixed-methods approach was employed, incorporating structured Likert-scale surveys and qualitative feedback sessions with 20 participants. All participants had prior experience with home automation or security systems, ensuring informed perspectives on the prototype.

The evaluation was conducted in a controlled lab environment, where participants observed a live demonstration of the system’s features, including energy monitoring, smart load control, security alerting, and remote access. Following the demonstration and interaction with the system, the participants completed a survey and participated in a Q&A discussion, providing both quantitative and qualitative feedback.

Perceived usefulness (PU) received strong ratings. Seventy percent of participants strongly agreed that the system would help them complete household tasks efficiently and that it improved device control and convenience. Another 25% selected “agree,” indicating a clear consensus on the prototype’s functional benefits. Participants especially valued features such as automated scheduling, energy-saving scenarios, and centralized control, affirming that the system could add tangible value to their daily routines. These findings support the conclusion that the usefulness of one of the central TAM constructs was effectively achieved through the system’s feature set and design.

Perceived ease of use (PEOU) also received positive feedback. Most participants (65%) strongly agreed that the system was straightforward to understand and navigate. The interfaces, visual indicators, and structured layouts were cited as supporting ease of use. The majority also reported that instructions and controls were intuitive, minimizing the learning curve. However, some respondents suggested improvements, such as a more modern interface and additional functions such as a search bar or customizable widgets. Despite these suggestions, the system was largely viewed as accessible users, reinforcing its usability across a broad audience.

In terms of **trust and reliability**, participant feedback was more mixed. While 60% agreed or strongly agreed that they trusted the system's security and performance, about 30% remained neutral, and 10% expressed concerns. Feedback highlighted the desire for additional protections such as two-factor authentication, better transparency about data handling, and visible indicators of security status. One participant noted that "the system is promising, but I'd feel more confident with clearer explanations about how data is stored and protected." Despite these reservations, many participants still believed the system would work reliably in practice and appreciated the focus on offline-capable security alerts and encrypted login mechanisms.

Privacy concerns emerged as an important factor influencing overall trustworthiness. Over half (55%) of the participants indicated confidence that their personal information would not be misused. However, 40% reported feeling neutral or somewhat concerned about unauthorized access to their data. Interestingly, the open-ended responses revealed that many of these concerns extended beyond the specific system and reflected a broader skepticism about smart technologies in general. Comments such as "every computerized system is hackable" and "even big corporations get breached" illustrate that user trust is not based solely on technical features but also on perceived transparency and familiarity with best practices. This highlights the need for not just secure system design but also clear, user-friendly communication about security and privacy mechanisms.

Despite these concerns, the participants expressed a strong **BI to use** the system. Seventy percent stated that they would recommend it to others, and 75% indicated that they would likely use it as their primary home automation platform. These responses were reinforced by positive perceptions of the system's ability to simplify tasks, increase comfort, and promote energy efficiency. Some participants, however, noted the need for broader device support (e.g., washing machines or dishwashers) and cautioned that the system cannot operate during power outages, which may affect its usefulness in certain contexts.

The qualitative feedback collected during the discussion sessions provided additional depth. Users appreciated the unified interface, customizable automation features, and responsiveness of the system during the demonstration. Several participants noted that the system could be particularly useful for elderly users or individuals with limited mobility, provided that accessibility features are enhanced. Others recommended minor UI enhancements, integration with voice assistants, or expanded control logic to further increase usability and value.

In summary, the evaluation results indicate that the home automation prototype demonstrates strong performance in PU and ease of use, aligning closely with the expectations outlined in the earlier phases of the research. The system was viewed as effective, approachable, and feature-rich. Trust and privacy, while reasonably established, revealed areas for improvement, particularly regarding transparency and user control over data. Nonetheless, the overall BI to adopt and recommend the system was high, suggesting that the system has strong potential for real-world adoption, especially if minor improvements are implemented based on the feedback received.

This evaluation validates the core usability principles embedded in the design and provides a concrete direction for future refinement. Addressing user concerns through transparent security communication, broader compatibility, and ongoing interface enhancements can significantly improve trust and promote wider acceptance. The findings ultimately affirm that the system meets core TAM criteria and is well positioned for successful deployment in diverse smart home environments.

5.3 Assessment of the research

This dissertation presents a comprehensive, multiphase investigation into smart home technologies, integrating theoretical analysis, empirical user research, practical system development, and behavioral evaluation. The research is assessed here in terms of its **methodological robustness, coherence across phases, and contributions to both academic knowledge and practical innovation**.

5.3.1 Methodological robustness

The research design is methodologically rigorous, employing a mixed-methods approach that combines qualitative and quantitative techniques across four distinct but interlinked phases:

- **Systematic literature review (Publication I)**: This phase established a strong theoretical foundation by identifying key usability, interoperability, and privacy challenges in existing smart home research. The use of a structured review protocol ensured objectivity and repeatability.
- **International user survey (Publication II)**: The survey captured diverse user perspectives across demographics, providing empirical evidence of user priorities, concerns, and expectations. The mixed-methods analysis enriched the findings with both statistical trends and qualitative insights.
- **Prototype development (Publication III)**: Using a DSR methodology, the study translated user needs into a functional, cost-effective smart home system. The iterative development process and scenario-based testing ensured real-world applicability.

- **Technology acceptance evaluation (Publication IV)**: The final phase applied the TAM framework to assess user acceptance of the prototype. The combination of structured surveys and open-ended feedback provided a nuanced understanding of PU, ease of use, trust, and privacy concerns.

Each phase was executed with attention to ethical standards, transparency, and user involvement, enhancing the credibility and relevance of the findings.

5.3.2 Coherence and integration

A key strength of the research lies in its seamless integration across phases. Each stage builds logically on the previous one:

- The literature review identified gaps that informed the survey design.
- The survey results shaped the design requirements for the prototype.
- The prototype was evaluated using constructs derived from both the literature and user feedback.

This iterative, user-centric approach ensured that the research remained grounded in real-world needs while advancing theoretical understanding. The dissertation demonstrates a rare balance between academic depth and practical relevance.

5.3.3 Contributions and impact

The research makes several notable contributions:

- **Theoretical**: It extends the application of TAM in the smart home context by incorporating trust and privacy as critical factors. It also combines fragmented literature into a clear framework of user-centric challenges.
- **Empirical**: It provides fresh, cross-cultural insights into user expectations, adoption barriers, and feature preferences, which are often underrepresented in existing studies.
- **Practical**: It delivers a validated, open-source smart home prototype that addresses key concerns such as usability, affordability, and security. The system's modular design and local-first architecture offer a replicable model for future development.

All in all, this research presents a smart home solution that is grounded in empirical evidence, shaped by real user needs, and validated through iterative design and behavioral evaluation. Rather than offering a generic automation platform, it delivers a context-aware, privacy-conscious, and user-empowering system that responds to the lived realities of diverse households. Its architecture, local-first control, and inclusive design principles make it a replicable model for ethical and sustainable smart home development.

5.4 Threats to validity

This section outlines potential threats to the validity of the research findings and conclusions presented in this dissertation. Following the framework proposed by (*Guide to Advanced Empirical Software Engineering*, 2019), threats are categorized into four types: construct validity, internal validity, external validity, and reliability (conclusion validity). Each is discussed in relation to the multiphase methodology employed in this study.

5.4.1 Construct validity

Construct validity concerns whether the concepts under investigation, such as usability, interoperability, security, and user acceptance, were accurately represented by the instruments and methods used. In this research, constructs were implemented through a combination of survey items, prototype features, and evaluation metrics based on the TAM. Although TAM is widely accepted in technology adoption studies, its application to smart home contexts may not capture all the nuances of domestic interaction. To mitigate this, the survey design was informed by a targeted literature review and pilot tested for clarity and relevance. Nonetheless, some constructs, particularly trust and privacy, may have been interpreted differently by the participants, depending on cultural or personal factors.

5.4.2 Internal validity

Internal validity refers to the extent to which observed outcomes can be attributed to research interventions rather than external or confounding factors. In this study, the iterative design and evaluation of the smart home prototype were guided by user-reported needs and tested in controlled scenarios. However, the interpretation of survey responses and qualitative feedback may be influenced by researcher bias or selective emphasis. To reduce this risk, a mixed-methods analysis was employed, and thematic coding was conducted systematically. Still, the possibility of confirmation bias, especially in aligning the findings with the proposed framework, cannot be entirely ruled out.

5.4.3 External validity

External validity concerns how well the findings can be generalized beyond the specific contexts studied. The international survey included participants from different backgrounds, and the prototype was designed to be modular and adaptable. However, the TAM evaluation involved only 20 participants, all with prior experience in smart home technologies. This relatively small and specialized sample limits how broadly the results can be applied, especially to first-time users or those with less technical experience.

These choices were mainly methodological. A smaller and more experienced group made it easier to manage the testing process and to collect richer feedback during the early validation stage. Likewise, running the prototype in simulated residential settings instead of long-term field studies helped maintain consistency while focusing on the main interaction patterns. Although these decisions limit external validity, they provided a solid foundation for refining both the system and evaluation method before moving to larger, real-world studies.

5.4.4 Reliability (conclusion validity)

Reliability concerns the consistency and repeatability of the research findings. The survey data were analyzed using established statistical techniques, and qualitative responses were coded using a structured thematic approach. The prototype testing followed predefined scenarios to ensure comparability across conditions. While these measures support reliability, the subjective nature of qualitative interpretation and the absence of inter-coder validation may affect reproducibility. Furthermore, the evaluation was conducted in a single lab setting, which may not reflect variability in real-world environments.

6 Conclusion

The evolution of smart home technologies reflects a broader societal shift toward intelligent, responsive, and personalized living environments. While the promise of automation, enhanced convenience, energy efficiency, and security is well recognized, the path to widespread adoption remains uneven. This dissertation has shown that the barriers to adoption are not merely technical but are deeply rooted in human factors: trust, usability, affordability, and contextual relevance. The main point of this work is that smart home technologies should be designed not only to work but also to fit the everyday lives of a wide range of users.

Through a multiphase investigation including a systematic literature review, an international user survey, a prototype implementation, and a behavioral evaluation, this research has provided a comprehensive understanding of the challenges and opportunities in smart home development. The literature review revealed persistent gaps in usability, compatibility, and privacy, while the survey highlighted users' detailed expectations across demographics. These insights informed the design of a Raspberry Pi–based smart home prototype. The final evaluation, grounded in the TAM, confirmed that PU and ease of use are critical drivers of adoption, but it also emphasized the importance of trust and transparency.

However, the importance of this research extends beyond its technical contributions. At a higher level, it encourages reflection on the purpose and potential of smart home automation. Why do we want to automate our homes? The answer lies in the evolving demands of modern life. Automation can support aging in place, reduce energy consumption, enhance safety, and enable inclusive living for people with disabilities or limited technical skills. It can also support sustainability by integrating homes into smart grids and enabling demand-response energy management. In short, smart homes are not just about controlling devices. They are about empowering people.

To realize this vision, several enabling conditions must be met. First, systems must be designed with human-centered design principles. This means understanding the emotional, social, and cultural dimensions of home life and embedding those insights into design decisions. Second, transparency must be a core principle. Users need to understand how their data is handled, what their systems are doing, and how to control them. Third, adaptability is essential. Homes are dynamic spaces, and technologies must evolve with changing routines, preferences, and household compositions.

The user-aligned smart home development framework (UASH-DF), introduced in this dissertation, offers a structured approach to achieving these goals. It emphasizes context-aware design, open-source architecture, security by design, affordability, ecosystem compatibility, and continuous behavioral evaluation. By following this framework, developers and researchers can create systems that are not only technically robust but also socially meaningful and ethically sound.

Looking forward, the future of smart home technologies will depend on our ability to balance innovation with inclusion. This includes integrating AI-driven personalization, supporting mainstream ecosystems such as Alexa and Google Home, and ensuring that systems remain open, compatible, and user-controlled. Long-term field studies are also required to understand how smart homes evolve with their users and how trust and engagement are sustained over time.

In conclusion, this dissertation affirms that the success of smart home technologies lies not in their complexity but in their capacity to serve human needs. By embedding context awareness, transparency, and adaptability into the design process, we can move toward smart homes that are not only intelligent and efficient but also trusted, inclusive, and genuinely supportive of modern life. The research presented here offers both a roadmap and a call to action for building the next generation of smart living environments that are aligned not just with technological possibilities but with the values and aspirations of the people who inhabit them.

6.1 Future research

This dissertation has demonstrated the value of a user-centric, technically grounded approach to smart home development. However, it also opens several promising avenues for future research. To guide future work effectively, these directions are categorized by their time horizon (short-term vs. long-term) and focus area (technical vs. social).

Table 5: Prioritized future research directions

Category	Focus Area	Priority	Description
6.1.1	Technical	Short-term	Ecosystem integration and open standards
6.1.2	Social	Short-term	Usable security and safety literacy
6.1.3	Technical	Long-term	Longitudinal deployment and energy integration
6.1.4	Social	Long-term	Adaptive, inclusive, and ethical smart homes

6.1.1 Seamless integration with ecosystems and standards

To improve accessibility and interoperability, future smart home systems should support **integration with mainstream platforms** such as **Amazon Alexa**, **Google Home**, and **Apple HomeKit**. These ecosystems offer voice control, centralized management, and compatibility with a wide range of devices. Research should focus on developing secure, privacy-conscious APIs and middleware that allow user-friendly smart home systems to interact with these platforms without compromising user autonomy.

The current system, developed as a research artifact for this study, already supports various brands and technologies including Tuya, Orvibo, TP-Link, Sonoff, VStarcam, Blink, and multiple radio frequency sensors *(Yaldaie et al., 2025)*. Building on this foundation and in parallel, the adoption of open standards like **Matter**[7] should be explored to reduce fragmentation and simplify device integration. Middleware solutions that handle protocol differences and enable plug-and-play functionality can significantly lower the barrier to entry for nonexpert users.

6.1.2 Usable security, privacy, and physical safety literacy

Security and privacy must evolve **beyond technical safeguards** to include **user education and empowerment**. Future work should explore how to design intuitive privacy dashboards, real-time alerts, and interactive tutorials that help users understand and manage their data. This is especially important as systems become more complex and interconnected.

Additionally, the **physical aspects of security**, such as the architectural placement of critical components like fuse boxes or network routers, must not be overlooked. Designing homes and buildings with these considerations in mind can help prevent unauthorized physical access and support a comprehensive approach to security literacy.

6.1.3 Real-world deployment and long-term evaluation

While this dissertation includes scenario-based testing, future research should conduct **longitudinal field studies** in real households. Observing how users interact with smart systems over time will produce deeper insights into trust development, system fatigue, and evolving needs. These studies can also uncover edge cases and contextual factors that are difficult to replicate in lab environments.

Such deployments should also explore **integration with smart grids and renewable energy systems**, enabling homes to participate in demand-response programs and contribute to broader sustainability goals. This would position smart homes as active nodes in future energy ecosystems.

6.1.4 Adaptive, inclusive, and ethical smart homes

Future systems should evolve beyond static rule-based automation toward adaptive, **context-aware** environments. By incorporating **machine learning**, smart homes can

[7] Matter is an open-source, royalty-free smart home standard developed by the Connectivity Standards Alliance (CSA) to ensure secure, reliable, and interoperable communication between devices across ecosystems like Apple HomeKit, Google Home, and Amazon Alexa.

learn from user behavior and environmental signals to personalize routines, reduce manual configuration, and anticipate needs, especially for users with limited technical skills or changing routines.

Inclusive design must also be prioritized. Future research should explore how smart homes can better serve older adults, people with disabilities, and culturally diverse households. Collaborative design methods involving these groups directly can ensure that systems are not only functional but also fair and empowering.

As autonomy increases, so do ethical concerns. Researchers must investigate how to embed **transparency**, **explainability**, and **user control** into AI-driven systems. This includes designing interfaces that make system operations and underlying rationales transparent, while granting users the ability to audit or override automated decisions.

References

Alsiyat, Y., Chang, Y., Zhang, N., & Flechais, I. (2025). *Smart Spaces, Private Lives: A Culturally Grounded Examination of Privacy Tensions in Smart Homes*. https://www.usenix.org/conference/soups2025/presentation/alsiyat

Anik, S., Gao, R., Zhong, H., Wang, X., & Meng, N. (2024). *Automation Configuration in Smart Home Systems: Challenges and Opportunities*. https://doi.org/10.48550/arXiv.2408.04755

Basarir-Ozel, B., Nasir, V. A., & Turker, H. B. (2023). Determinants of smart home adoption and differences across technology readiness segments. *Technological Forecasting and Social Change*, *197*, 122924. https://doi.org/10.1016/j.techfore.2023.122924

Belli, D., Barsocchi, P., & Palumbo, F. (2024). Connectivity Standards Alliance Matter: State of the art and opportunities. *Internet of Things*, *25*, 101005. https://doi.org/10.1016/j.iot.2023.101005

Bombik, P., Wenzel, T., Grossklags, J., & Patil, S. (2022). A Multi-Region Investigation of the Perceptions and Use of Smart Home Devices. *Proceedings on Privacy Enhancing Technologies*, *2022*(3), 6–32. https://doi.org/10.56553/popets-2022-0060

Buil-Gil, D., Kemp, S., Kuenzel, S., Coventry, L., Zakhary, S., Tilley, D., & Nicholson, J. (2023). The digital harms of smart home devices: A systematic literature review. *Computers in Human Behavior*, *145*, 107770. https://doi.org/10.1016/j.chb.2023.107770

Campbell, J., Buchan, J., Chu, C. H., Bianchi, A., Hoey, J., & Khan, S. S. (2024). User Perception of Smart Home Surveillance Among Adults Aged 50 Years and Older: Scoping Review. *JMIR MHealth and UHealth*, *12*, e48526. https://doi.org/10.2196/48526

Cerino, L. C., Lee, C., Lee, S.-H., Fakhr-Hosseini, S., Son, H., Shen, S., & Coughlin, J. F. (2023). *An Iterative Approach to User-Centered Design of Smart Home Systems* (pp. 3–16). https://doi.org/10.1007/978-3-031-34917-1_1

Daruwala, N., & Oberst, U. (2023). A systematic literature review of Smart Home Technology acceptance. *Journal of Ambient Intelligence and Smart Environments*, *15*(2), 115–142. https://doi.org/10.3233/AIS-220033

FakhrHosseini, S., Lee, C., Lee, S.-H., & Coughlin, J. (2025). A Taxonomy of Home Automation: Expert Perspectives on the Future of Smarter Homes. *Information Systems Frontiers*, *27*(2), 449–466. https://doi.org/10.1007/s10796-024-10496-9

Fortune Business Insights. (2025, May 12). *Home Automation Market Size, Share and Industry Analysis*. https://www.fortunebusinessinsights.com/industry-reports/home-automation-market-100074

Gomez, C., Paradells, J., Bormann, C., & Crowcroft, J. (2017). From 6LoWPAN to 6Lo: Expanding the Universe of IPv6-Supported Technologies for the Internet of Things. *IEEE Communications Magazine*, *55*(12), 148–155. https://doi.org/10.1109/MCOM.2017.1600534

Guide to Advanced Empirical Software Engineering. (2019). Scholars Portal.

Haney, J. M., & Haney, F. (2025). *Smart Home Users' Security and Privacy Perceptions and Actions Differ By Device Category: Results from a U.S. Survey*. https://www.nist.gov/publications/smart-home-users-security-and-privacy-perceptions-and-actions-differ-device-category

Hevner, March, Park, & Ram. (2004). Design Science in Information Systems Research. *MIS Quarterly*, *28*(1), 75. https://doi.org/10.2307/25148625

Kormpakis, G., Lekidis, A., Sarmas, E., Papias, G., Serepas, F., Stravodimos, G., & Marinakis, V. (2024). *Home Energy Management Systems: Challenges, Heterogeneity & Integration Architecture Towards A Smart City Ecosystem*. https://doi.org/10.48550/arXiv.2408.03707

Li, W., Yigitcanlar, T., Erol, I., & Liu, A. (2021). Motivations, barriers and risks of smart home adoption: From systematic literature review to conceptual framework. *Energy Research & Social Science*, *80*, 102211. https://doi.org/10.1016/j.erss.2021.102211

Madadi-Barough, S., Ruiz-Blanco, P., Lin, J., Vidal, R., & Gomez, C. (2024). Matter: IoT Interoperability for Smart Homes. *IEEE Communications Magazine*, *63*(4), 106–112. https://doi.org/10.1109/MCOM.001.2400274

Magara, T., & Zhou, Y. (2024). Security and Privacy Concerns in the Adoption of IoT Smart Homes: A User-Centric Analysis. *American Journal of Information Science and Technology*, *8*(1), 1–14. https://doi.org/10.11648/j.ajist.20240801.11

Park, Y., & Han, J. (2025). Smart Home Advancements for Health Care and Beyond: Systematic Review of Two Decades of User-Centric Innovation. *Journal of Medical Internet Research*, *27*, e62793. https://doi.org/10.2196/62793

Pattison Tuohy, J. (2025, January). *Matter will be better in 2025 — say the people who make it*. https://www.theverge.com/24349390/matter-csa-thread-group-wifi-alliance-interview-2025

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of*

Management Information Systems, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Rego, A., Ramírez, P. L. G., Jimenez, J. M., & Lloret, J. (2022). Artificial intelligent system for multimedia services in smart home environments. *Cluster Computing*, *25*(3), 2085–2105. https://doi.org/10.1007/s10586-021-03350-z

Reisinger, M. R., Prost, S., Schrammel, J., & Fröhlich, P. (2023). User requirements for the design of smart homes: dimensions and goals. *Journal of Ambient Intelligence and Humanized Computing*, *14*(12), 15761–15780. https://doi.org/10.1007/s12652-021-03651-6

Schulz, J. M., & Scilla, J. S. (2024). Broad Perspective of Smart Home Technology in 2024. *International Journal of Smart Technologies*, *1*(1), 1–27. https://doi.org/10.4018/IJST.350186

Shamili, Sinha, M., & Gowda, N. N. (2024). Enhancing residential life: The impact of home automation systems on convenience, security, and efficiency. *Https://Researchtrendsjournal.Com Online at: Https://Researchtrendsjournal.Com ISSN No: 2584-282X INTERNATIONAL JOURNAL OF TRENDS IN EMERGING RESEARCH AND DEVELOPMENT*, *2*(6), 286–289. https://doi.org/10.5281/zenodo.14671149

Shuhaiber, A., & Mashal, I. (2019). Understanding users’ acceptance of smart homes. *Technology in Society*, *58*, 101110. https://doi.org/10.1016/j.techsoc.2019.01.003

Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics*, *13*(16), 3343. https://doi.org/10.3390/electronics13163343

Yaldaie, A., Porras, J., & Drogehorn, O. (2022). The Present State of Home Automation: A Systematic Literature Review. *International Journal of Hybrid Innovation Technologies*, *3*(1), 23–46. https://doi.org/10.21742/ijhit.2653-309X.2022.2.1.03

Yaldaie, A., Porras, J., & Drögehorn, O. (2023). Who Are Smart Home Users and What Do They Want?—Insights from an International Survey. *Applied Computer Systems*, *28*(1), 114–124. https://doi.org/10.2478/acss-2023-0011

Yaldaie, A., Porras, J., & Drögehorn, O. (2024). Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices. *Asian Journal of Computer Science and Technology*, *13*(1), 27–40. https://doi.org/10.70112/ajcst-2024.13.1.4260

Yaldaie, A., Porras, J., & Drögehorn, O. (2025). User Perceptions of a Home Automation System: A TAM-Based Evaluation. *Applied Computer Systems*, *30*(1), 98–104. https://doi.org/10.2478/acss-2025-0012

Yao, Y., Huang, L., He, Y., Ma, Z., Xu, X., & Mi, H. (2023). Reviewing and Reflecting on Smart Home Research from the Human-Centered Perspective. *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–21. https://doi.org/10.1145/3544548.3580842

Zargham, N., Alexandrovsky, D., Erich, J., Wenig, N., & Malaka, R. (2022). "I Want It That Way": Exploring Users' Customization and Personalization Preferences for Home Assistants. *CHI Conference on Human Factors in Computing Systems Extended Abstracts*, 1–8. https://doi.org/10.1145/3491101.3519843

Publication I

Yaldaie, A., Porras, J., and Drögehorn, O.
The Present State of Home Automation: A Systematic Literature Review

International Journal of Hybrid Innovation Technologies
Volume 2, No. 1, 2022

International Journal of Hybrid Information Technology
Vol.2, No.1 (2022), pp.23-46
http://dx.doi.org/10.21742/ijhit.2653-309X.2022.2.1.03

The Present State of Home Automation: A Systematic Literature Review

Ashkan Yaldaie[1], Jari Porras[2] and Olaf Drögehorn[3*]

[1,2]LUT University, Lappeenranta, Finland
[3]Harz University of Applied Sciences, Wernigerode, Germany
[1]ashkan.yaldaie@student.lut.fi, [2]jari.porras@lut.fi, [3]odroegehorn@hs-harz.de

Abstract

Since ancient times, people have been trying to make life easier, for example, by bringing water to homes and taking care of wastewater through channelization. With the advancements in technology over the past few decades, people have gained access to smart devices and computerized systems, enabling us to automate tasks. For example, motion sensors help to automatically turn on the lights when entering a building. Also, remote-controlled, voice-controlled, and gesture-controlled devices are becoming smarter and enabling various types of activities. The objective of this literature review is to be a valuable source for software engineers to gain a better understanding of the current achievements in smart home development. This paper explores technological advancements, including the usability and security aspects of home automation. The authors choose four digital libraries to research published case studies related to the selected number of smart home domains. Papers with distinct titles that are written in English and are more than three pages are selected as research material. Furthermore, thematic analysis was performed to extract data linked to the research questions. Most of the chosen case studies are performed in labs. This literature review found that a portion of the current products overlooked the basic security and privacy enhancements in favor of usability or vice versa. The present research concluded that adequate knowledge management has the potential to improve smart home technology. Additionally, developers should not skip any of the three layers of the development architecture (UI layer, communication layer, and software system layer) because each stage is dedicated to addressing existing weaknesses in smart home products. The paper's findings provide potential solutions for developing better smart home devices in the future.

Keywords: *Smart home, Home automation, IoT, Remote monitoring, Home security, Healthcare, Energy efficiency*

1. Introduction

Internet of Things (IoT) devices such as sensors, smartphones, and controlling and monitoring devices surrounding us. Weiser and Brown predicted the arrival of ubiquitous computing, and with IoT, one can see this vision come to life [9]. Modern home automation is dependent on IoT devices [47]. Smart home systems need to deal with saving energy and other resources. It is estimated that by the year 2025, there will be 75 billion IoT devices installed, and these devices should provide solutions rather than becoming part of the energy

Article history:
Received (April 26, 2022), Review Result (June 30, 2022), Accepted (August 21, 2022)

mismanagement problem [34]. There are smart plugs and smart meters that enable users to manage and monitor energy consumption [28], yet most smart devices have specific standards and cannot be easily integrated [2]. One solution is to develop a standardized approach by using middleware and frameworks to generate communication between IoT devices and software to provide better energy management and energy-saving systems [8]. However, Home automation systems have some drawbacks. The development of home automation systems with a proper balance between usability, user experience, performance, and security can be challenging [12][27]. Smart homes have a wide variety of users in different age groups [14], and because of the age group diversity, developers have to level down the differences in people's interaction with IoT.

Usability and User Interface (UI) design are playing an important role in smart home development because the user interacts with the system through the UI. Smart home products should have a simple yet effective interface for the remote administration of the house [47]. In addition to controlling smart devices through the UI, providing valuable information, such as house temperature and humidity, may have a use case and be valuable for many users. Furthermore, in connection to elderly and patient monitoring, smart home systems are capable of analyzing and sending a patient's health status to interested parties [11]. Workflow management is a rather new subject linked to home automation, and the system needs to execute tasks based on a trigger, for example, turning on a coffee machine when someone enters the home [41]. Many smart devices are shared and used by different residents at home or in a building, and a home automation system can manage these shared devices through a usage timetable to provide comfort and ease for all users. [26]

Security issues are another concern that smart home users have. Software systems are capable of collecting critical metadata about the users through smart devices, and the gathered data are subjected to security risks [10]. These security concerns can compromise the total system's functionality, and users are worried about their home privacy and safety [2]. Still, proper security is not the only factor users are after, Zhen Ling et al., [50] and the current paper goes through the other concerns smart home users have.

Smart home and home automation devices come in all types and shapes. Such systems are becoming more advanced every year and are getting more attention from consumers. Inspecting the current state of the art of home automation systems in the literature and the provided guidelines to improve them can help developers and designers make better choices and improve products. The objective of the current paper is to study the current state of the art and the identified benefits and drawbacks of smart home systems, as described in the literature. This will be achieved by conducting a systematic literature review to answer the following research questions (RQ):

RQ1: What topics concerning smart home systems can be found in the literature?

RQ2: What are the identifiable concerns, that is, the benefits and drawbacks of smart home systems?

RQ3: How can the systems be optimized based on the identified benefits and drawbacks?

Answering the first question (RQ1) determines the topics addressed in the literature concerning home automation systems (including devices). Smart home devices can collect information about residents' behavior and even have a view of the inside of the house. This can present a notable security risk to homeowners. The second question (RQ2) covers concerns like the one mentioned. Recognizing such potential drawbacks can help all stakeholders expect and produce more sufficient systems. The question also addresses the benefits of utilizing a smart home system. The answer to the last question (RQ3) provides a set of guidelines for the developers for optimizing smart home systems based on the findings of the systematic literature review. The current paper stays away from basic and purely historical information; the objective is to examine the current state-of-the-art situation, so material published before 2013 would be excluded from the research scope. The cutoff period was selected based on the evolution of home automation systems and increased activity in the field. Google's trend data for the term smart home can be found in [Figure 1], which shows the term gained noticeable popularity in 2013.

Figure 1. Google's trend data for the term smart home. A value of 100 is the peak popularity

This document covers several topics linked to the development of smart home systems. The identified interrelated topics including usability, design, performance, and security are set to uncover the benefits and drawbacks of existing systems. In addition to the mentioned objectives, this paper aims to uncover real-world issues to help improve future smart home products e.g., compromising security in favor of usability and vice versa is not recommended.

2. Related work

The related work about the main contributions of this paper is discussed below. This study considered advancements and concerns linked to smart home systems; this can help gain an understanding of the completed work and how best to continue the research on the related study topic. Smart home research adds considerable value to people's lives because it has environmental, social, and ethical benefits. Having a clear view of smart technologies would assist stakeholders who are interested in the topic.

Smart home systems are becoming more advanced with the growth of technology. Mehedi Hasan et al [20] explain new ways to control a digital home through voice recognition, gesture control, and Wi-Fi. According to Hasan et al., [20] a variety of weaknesses have yet to be fixed when considering the mentioned technologies. For example, a voice-controlled system may give false and unpredictable results because of the surrounding noise; a smart light switch may turn on/off based on the similarity between the command word and some other words. Wi-Fi and Bluetooth systems also have some pros and cons. As stated by [20], a Bluetooth-based system is easy to use. However, the operating range of such systems is around 10–20 meters, and Wi-Fi-based systems are more flexible because of their wide range. Such systems have a high initial cost that can be less applicable to people with a lower budget.

In the literature, one can see important challenges linked to smart home development [39]. Availability and remote accessibility are some of the challenges developers are facing. This can be solved by utilizing cloud servers as a communication gateway between the potential controlling devices, for example, smartphones and smart home systems. However, Stojkoska and Trivodaliev [39] conclude that connecting to cloud servers has some drawbacks, including more bandwidth usage. Risteska, Stojkoska, and Trivodaliev [39] present several communication techniques, such as fog computing, to address the mentioned issue. Based on the study by Hisham Albataineh et al., [1] a combination of edge and cloud computing is more energy-efficient and has positive performance effects because most of the data analysis occurs locally, so the smart home system does not have to wait for the cloud server's response.

Smart elderly care with the help of smart homes is reviewed [30][31]. Monitoring the health status of users is possible with the use of sensors and monitoring devices. The authors start the discussion by going through the health-related needs of older adults. The elderly population is struggling with common diseases such as diabetes and blood pressure, and according to Petra Maresova et al., [30] the challenge is to encourage older adults to accept health-related smart solutions. Developing easy-to-use products in combination with artificial intelligence (AI) for automation and decision-making is a way to explore and potentially enhance smart healthcare. Wearable devices and sensors can collect valuable data linked to the movement and other activities of patients, and based on the findings of, [31] the collected information can be analyzed to measure users' health decline or improvements on a day-to-day basis.

Smart home energy efficiency is reviewed [42][44][45]. Smart electricity meters provide the possibility to monitor energy consumption and collect related data for further analysis. According to researchers, [42] smart thermostats can save up to 20% of heating and cooling costs each year, and based on the review completed by Vishwakarma et al., [45] the user can control the flow of electricity by utilizing a home automation dashboard. Member states of the EU are required to provide smart metering systems to consumers; a digital meter enables many possibilities. Combining a prepayment system with a smart meter's alert functionality can inform the customer about energy consumption, which may have positive environmental effects. For instance, smart electricity with a "traffic light" function can warn customers about high electricity loads [44].

Security and privacy have been a big burden when developing a smart home product because such devices are connected to the internet, and most of the time, the data travel between the home network and cloud servers. Some of the security threats addressed in the smart home concept are presented by Almusaylim and Zaman [4], in which the researchers recommend proper user authentication techniques and secure frameworks for communication between smart devices and smart home gateways. Privacy concerns in the smart home domain have been studied before [19]. Authors Guhr, Werth, and Blacha present privacy issues as potential barriers to smart home usage, they propose a common definition for information privacy: one's ability to control information about oneself [19].

The current literature review intends to continue on these related works. This paper explores eight topics linked to the study of smart homes that were found during the analysis phase. In addition to covering the current state of the mentioned subjects, this document examines topics such as design, performance, development process, and usability. The next section explains the research process and related activities.

3. Methodology

To complete the current paper, the process proposed by Kitchenham is applied, a systematic literature review method is used, and four digital libraries (databases) are selected to perform an automatic database search [25]. The process was managed by the first author of the paper, and other authors joined in to confirm and review the results. The literature review is drawn on the planned research questions for the current paper; that is, aiming to create an overview of smart home systems and their concerns by analyzing published articles and based on the findings; create some guidelines for smart home system developers. Built on the research questions, the authors have created a general search query (“home automation” OR “smart home” OR “internet of things”) AND “case study.” Derived from the process proposed by Kitchenham, four databases have been selected to apply the query parameters, as shown in [Table 1].

Table 1: The list of digital libraries and the applied search parameters

Library name	Search parameters
ACM Digital Library	[[Publication Title: “home automation”] OR [Publication Title: “smart home”] OR [Publication Title: “internet of things”]] AND [Publication Title: “case study”] AND [Publication Date: (2013 TO 2022)]
Springer Link	“home automation” OR “smart home” OR “internet of things” title=case study facet-start-year=2013 facet-end-year=2022
IEEE Digital Library	(("Document Title": "home automation" OR "Document Title": "smart home" OR "Document Title": "internet of things") AND ("Document Title": "case study")) ranges=2013_2022_Year
Science@Direct	(“home automation” OR “smart home” OR “internet of things”) AND “case study” date=2013-2022

The initial search resulted in 468 matches. The first step was to exclude everything except published journal articles and conferences. On further inspection, it was discovered that some of the papers' titles are not in line with the expectations, so a title-based exclusion is applied in the second step. The third filter excluded the papers not written in English, and the fourth step allowed papers of more than three pages to be included. Duplicate papers were excluded in step five, and finally, analyzed the content to see if they are in line with the research questions. After applying the inclusion and exclusion filters, the number decreased to the final set of 56 papers, as shown in [Figure 2]. Thus, the following set of inclusion and exclusion criteria was applied to the search results:

- Inclusion Criteria:
  - Published journal article or conference paper
  - Primary study
  - Clear case study reports related to the research questions
- Exclusion Criteria:
  - Book chapters and magazine articles
  - Languages other than English
  - Papers that focus on the basics and history of smart homes and home automation

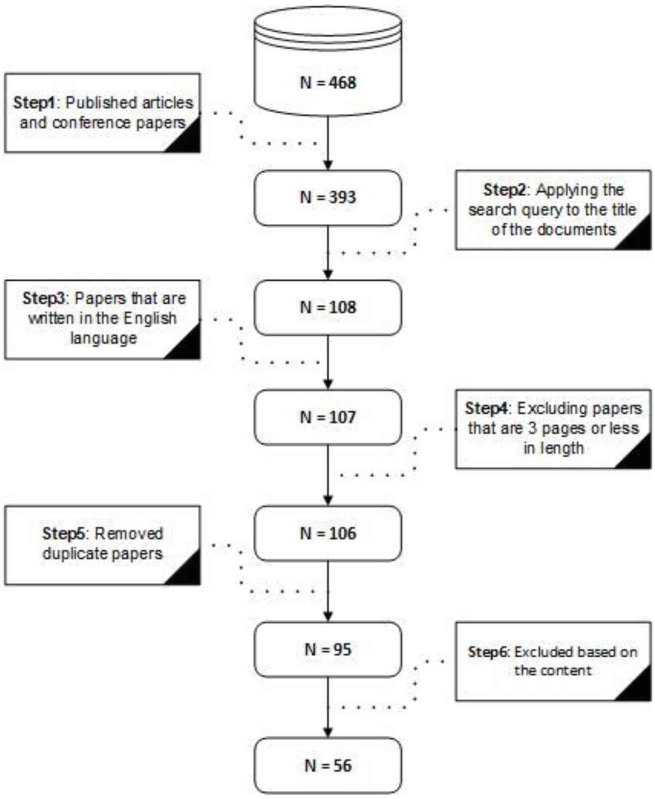

Figure 2. Number of papers after applying the inclusion and exclusion filters

Table 2. Number of papers per database after applying the inclusion and exclusion filters

Database	Initial number	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
ACM Digital Library	25	24	14	14	14	9	6
Springer Link	363	297	22	21	21	21	12
IEEE Digital Library	61	54	54	54	53	53	33
Science@Direct	19	18	18	18	18	12	5
Total:	468	393	108	107	106	95	56

[Table 2] presents the exact number of papers per database in every step after the filters were applied. As stated earlier, the objective is to answer the research questions, and as a result, an extra query is added to the data extraction form. (For which research question can the paper be utilized?). The data extraction description can be found in [Table 3].

Table 3. Data extraction

Item	Description	Research Question
Title	The title of the paper	RQ1
Year	Publication year	Metadata
Venue	The publication type: journal or conference	Metadata
Direct link to the document	A direct link to the document	Metadata
Special note	Free text about the paper (important remarks and reminder notes about the paper)	Metadata
Assumptions for benefits	What are the assumed benefits for the product analyzed in the paper?	RQ1
Assumptions for drawbacks	What are the assumed drawbacks of the product analyzed in the paper?	RQ1
Realized benefits	What are the realized benefits?	RQ2, RQ3
Realized drawbacks	What are the realized drawbacks?	RQ2, RQ3
What equipment and features are in used	What are the types of equipment and features used in the paper?	RQ1, RQ2
Study context	What does the paper aim to cover in connection to benefits and drawbacks? Is it security, price, or usability related? There can be more categories that are not defined here.	RQ1, RQ2, RQ3

Thematic analysis was performed by the first author on the research material; the process started by reading the material to highlight and extract the data relevant to the research questions. The extracted data were validated against the research questions by the other authors. The process continued by tagging the papers with their corresponding topics, and then, the topics were reviewed and combined appropriately. Finally, the papers were added in groups based on the realized categories; the results are shown in [Figure 4]. Additionally, Appendix 1 presents the realized study topic(s) for each analyzed paper.

4. Results

The current section is dedicated to answering the research question. The section starts with a presentation of the study topics found in the literature, which is followed by an explanation for each topic. Finally, the current section looks at the concerns linked to smart home systems and the ways to optimize them. The number of selected studies per year is shown in Figure 3. Additionally, the selected studies are divided into four categories based on the study settings; the results are shown in [Table 4].

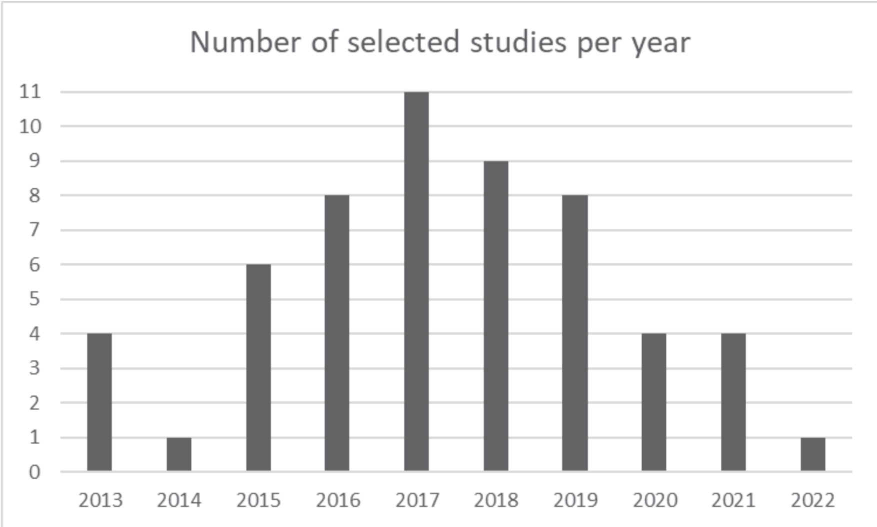

Figure 3. Number of selected studies per year

Most of the selected case studies were completed in laboratories, the devices were set up in a lab, and the developers conducted experiments to obtain the results. Furthermore, some of the case studies were done in simulated settings, meaning there was a controlled environment with the same features as the real environment. Field studies were done in real settings, and the developers set up a system to monitor the interactions between the user and smart home products. Finally, theory-based case studies were conducted to test a theory, which could include interviews with people in the smart home industry or analyzing the data from an existing product to report weaknesses and strengths.

Table 4. Number of papers per study setting

Study settings	Number of papers
Lab study	21
Field study	10
Simulating real settings	18
Theory-based study	7

4.1. Realized smart home topics (RQ1)

To find the answer to the first research question (RQ1), the first author analyzed the selected studies by reading the content and keywords of the documents to find the study topic(s) for each paper. Eight different topics were identified based on discussions among the authors; these topics were covered in the majority of the papers. Some papers address more than one topic, which was counted in the list of results. Improving future home automation products is the motivation behind covering the eight identified topics, and based on the performed analysis, refining security and the privacy of the home automation systems is the most popular study topic. Home automation systems are collecting a considerable amount of data; the question is then on securing and controlling the data, which may travel across networks throughout the world [23].

IoT systems have a wide range of applications. In addition to task automation, they monitor, analyze, and report. Improving the design and smart healthcare are the second most popular topics of the selected case studies. Having a design that can follow the requirements is a crucial factor in the success or failure of a product [5][22]. As mentioned in the introduction, the focus of the present paper is to help smart home developers and designers develop better products. The selected topics shown in [Figure 4] cover technical aspects and consumer concerns and development practices. Reviewing these topics covers the three high-level phases of the development process: planning, implementation, and improvement.

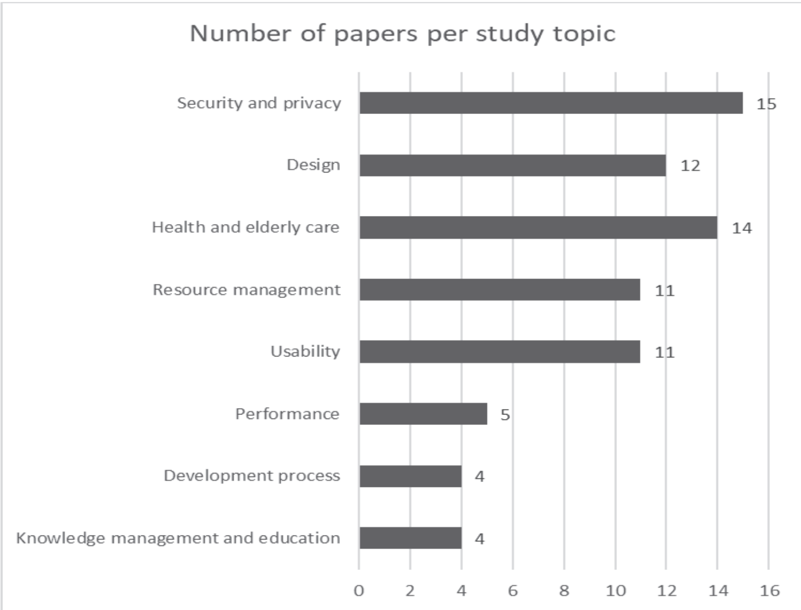

Figure 4. Number of papers per study topic

[Table 5] presents the distribution of the study topics per year. The data is collected to present the coverage of the topic within the given time range from 2013 until 2022. This can clearly show how important a topic is if it is covered repeatedly for several years. E.g., security and privacy are the most popular research subjects, and the topic is covered since 2013.

Table 5. Distribution of the study topics and the number of papers per year

Topic	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022
Security and privacy	2			1	4	3	4	1		
Design	1		2			3	4	2		
Health and elderly care	1		2		4	2	2	1	2	
Resource management			4	2	2	1	1			1
Usability	2	1		2	1	1	2	1	1	
Performance				1	2	1				
Development process			1	1		1	1			
Knowledge management and education				2				1	1	

4.2. Topics

To answer the second and third research questions (RQ2, RQ3), the current section explains the presented topics in Figure 4 and explores the benefits and drawbacks of smart home systems.

4.2.1. Security and privacy

IoT devices play an important role in various domains, such as home, agriculture, healthcare, tourism, transportation, and education [7]. Home automation products generally consist of several IoT devices that are connected to complete an objective. Furthermore, home automation products are inseparable parts of smart cities, so having proper security measures is a must. Security vulnerabilities may be in the IoT devices or in the way data travels between them and are stored in smart home storage for further analysis. One can attempt to hack a smart home system or even use a smart home system as a tool to hack the entire network of connected smart products or smart cities [50].

A way to handle the security concerns is by giving the power to the product users to control the flow of data, which means permitting the storage of data, monitoring the data flow, and restricting access to the data. According to Aung and Tantidham [7], this is possible by utilizing Ethereum (ethereum.org). Ethereum is a private blockchain, it is used to handle data flow based on the smart contract or authorized policies that are created by the user. Security and privacy can be taken care of in peer-to-peer networks with the utilization of blockchain. Applications running on Ethereum are available from anywhere, and the data flow is controlled by smart contracts between private and public networks. A smart home system is private data storage, while communication and sharing the data with the cloud for statistical purposes can be handled through public contracts specified in the Ethereum platform.

Improving privacy is a challenging topic, and according to Yulistiyan Wardhana et al [46], it should not compromise the well-being of the user. For example, limited access to a private room to just one person can have a negative outcome if the user gets a heart attack there and no one else can enter the room to help. In this case, smart devices should be able to inform and provide access to health officials. To address this issue, Wardhana, Hardian, and Guarddin are recommending a system for monitoring the user's status and habits when using a private room [46]. However, the developed system in question is not always accurate and cannot adapt to the habit changes of the user.

Security vulnerabilities can be in the hardware or software of smart home devices. It is almost impossible to implement flawless software. However, it is recommended that more resources be allocated to improve the security level of smart devices [13]. One of the ways to do this is by leveraging cryptographic techniques instead of using plain and human-readable text for storing sensitive data or communication between devices. Regarding the hardware, it is better to avoid using hardware with known security weaknesses like Bluetooth, which is vulnerable to Bluetooth signal-interfering attacks [49]. Most IoT devices focus on new features and cost reduction. Smart devices are often not designed with security in mind. One solution to the mentioned problem is for developers to implement new features by adapting existing frameworks and services to improve the security of the products [38].

4.2.2. Design

Among other benefits, a well-designed smart home system can reduce processing power, for example by dividing the load between the cloud server and local servers. The difference is more noticeable with the rising interest in IoT devices. According to research, it is possible to divide the load between the main server and local devices using a technology called edge computing. Most commercial IoT and smart home devices depend on cloud servers for processing data. Edge computing suggests using processing locally to save bandwidth and processing power. However, the cloud server can still be responsible for data storage. In this case, the local device does not have to wait for the cloud server to analyze the data and respond [32][35].

Smart home systems have a variety of different users, and the design should consider different people's needs. It is not possible to make a device that satisfies everyone, and the aim should be to fulfill the target group's requirements. It is correct to say that a smart home system is an integration of space, users, and smart devices. For example, scenario-based design can help users complete tasks based on user's actions, and this can be as simple as switching off the lights automatically when residents leave the house or turning up the heating during the winter when users arrive home [24].

4.2.3. Health and elderly care

The world's population is aging, and healthcare costs are growing because of this. The demand for automated healthcare and patient assistance services is growing. Smart home product developers are taking this growing demand into an account. This section will cover some of the benefits and drawbacks of the existing systems linked to the mentioned subject. One of the solutions proposed in the literature is elderly monitoring technology, which is a series of sensors such as infrared motion detectors and magnetic door sensors that are placed in different areas of a house e.g., kitchen, bathroom, and front door to check the irregularities in residents' activities. Usually, people have a routine of living; for example, people wake up and go to sleep around the same time. The sensors look for changes in such activities, and if enough abnormalities are detected, the system triggers a fitting response. [29]

Independent living is one of the issues concerning the elderly population. The user, in this case, may forget an important activity like taking medicine on time, which may result in the individual entering a dangerous state. In addition to the remote monitoring of a smart home's resent which may not be enough, a case study shows that it is possible to develop a system to assist the user in completing daily tasks [6]. An easy-to-use UI is the most important aspect when developing smart home systems for the elderly and a study shows that portable touchscreen devices with audio and video communication ability can fulfill most requirements. Furthermore, an event-based solution results in the automation of many tasks, and the user does not have to specifically interact with the system because an event-based design automatically reacts to certain conditions [43].

In addition to elderly assistance, IoT solutions can remove the pressure on hospitals by remotely monitoring patients at home. Some heart patients need continuous heart rate monitoring and case studies show that this can be done at home thanks to the collected data obtained through sensors and machine learning algorithms. There are some concerns related to the accuracy of the proposed solutions, and ongoing work aims to improve these remaining concerns, such as security concerns, energy efficiency, and data visibility. Health-related data are highly confidential and must be encrypted. However, the data should be visible to the user in real time, and because most health devices are wearable sensors, energy efficiency plays a crucial role. A device without sufficient power does not have any use [3][15].

4.2.4. Resource management

Enhancing home energy and water usage efficiency is a focus area of smart home systems. Creating a detailed profile of household equipment's energy consumption helps create a better model for saving energy. Smart systems can optimize energy usage by optimally scheduling and controlling household appliances. One of the realized drawbacks linked to the development of resource-efficient systems is finding and purchasing monitoring devices because some cannot be found off the shelf [16][37][48]. Sustainable IoT can have positive environmental impacts. People communicate through a massive network of sensors and IoT devices, and to save energy, product developers must consider the energy consumption of IoT devices in the early development phases, including the planning and design phases [23][40].

4.2.5. Usability

Integration between IoT devices is a challenge for smart home developers. Different manufacturers are following different standards for creating their products, and this can harm usability because most of the time, controlling the smart devices through a centralized system might not be possible. The need for middleware to integrate devices in the same network is an approach that can help address the mentioned problem, and a successful attempt has been made to connect a Rovio service robot to a smart system and automate the tasks. However, because of the large number of existing products, there is still a need for a standard communication channel between smart devices [8].

The designers of smart home devices do not explicitly or systematically consider usability in designing security features. Instead of relying on the technical support team, the users themselves should be able to configure the security features of the smart home systems. Consulting with security experts in the design phase to enhance the usability of the security features is costly, but the extra cost can be justified because cyberattacks are targeting smart homes and even using smart home systems as a hacking tools [10]. Another way to enhance usability is to automate tasks as much as possible by equipping home furniture with sensors and single-board computers. In this case, the user does not have to interact with the system through a dedicated UI. For example, a smart chair can identify the user and trigger a customized predefined event [21][43].

4.2.6. Performance

Using middleware and standard communication protocols has a positive effect on a digital home's performance. A standardized communication protocol allows for the circulation of data between the smart devices, in return resulting in a boost in performance because the devices do not have to independently collect the data and a network of connected devices is devoted to gathering the data, which can then be analyzed by software systems [17]. The importance of communication becomes more visible when talking about smart cities because the collected data from a network of smart homes can contribute to smarter environmental and social decisions [16].

Using standard communication protocols has positive performance effects; they have the potential to enhance developers' productivity. However, analyzing middleware components shows some inhibitors in the code, which indicates the need for further development to enhance the components [5]. In summary, utilizing middleware in combination with edge computing architectural techniques may potentially boost performance. The current literature review presents the definition of edge computing in the design section; additionally, it is important to mention that bandwidth can be saved and communication delay between the IoT devices and the cloud can be improved by edge computing techniques [35].

4.2.7. Development process

It is essential to take a look at the development process of smart homes and IoT devices; the lack of a systematic approach can result in security and design compromises. According to Gartner, IoT systems would be in 95% of new electronics products, meaning that smart devices have an enormous impact on society, businesses, and the environment. Dividing the product architecture into three layers a UI layer, a communication layer, and a software system layer is a way to make structural improvements and focus on the weaknesses of each layer [33]. The need for flexible and user-friendly solutions is undeniable, and the case study shows that etiquette requirements gathered from the stakeholders, prototyping, and a user-driven design can further improve the product. In this case, the user gets to test the product in the early stages of development, which means the final solution has a greater chance of meeting the requirements [36][43][47].

4.2.8. Knowledge management and education

Knowledge is an important asset for people in general and, in particular, for organizations to grow. Most often, different projects rely on a similar set of data, and keeping a record of the use cases in one project may be beneficial for other smart home projects. Furthermore, knowledge management can have positive environmental impacts; smart home residents can share their experience, for example, in a platform of connected digital homes to help the other residents make better choices linked to resource management [18]. Including the possibility for students to learn how to develop IoT solutions as part of their studies will help produce better smart home systems in the future. Students who participate in such courses have considered it enjoyable and gave positive feedback to the organizers. It is essential to improve the learning process linked to IoT development for students to gain hands-on knowledge and experience in the subject [22].

4.3. Smart home concerns (RQ2)

The current section is dedicated to answering RQ2. Table 6 offers a brief explanation of the benefits and drawbacks linked to the home automation-related topics covered in this paper. The table is summarizing the results provided in section 4.2, in addition, the reader can find sources associated with the benefits and drawbacks in the description column for further and more in-depth analysis. The collected items are based on the authors' analysis of the selected sources for this research.

Table 6. Benefits and drawbacks linked to home automation–related topics

Topic	Category	Description
Security and privacy	Benefits	Accessing the data through security protocols (contracts). [7] Smart home systems can make smart adjustments to privacy protocols [46]. Existing frameworks and services can improve the security of smart products [38].
	Drawbacks	Smart home systems can be used as a hacking tools [50]. Utilizing compromised hardware and insecure data handling [49]. Smart homes are not very accurate enough to decide on their own [46]. Cost reduction can lead to weak security features [38].
Design	Benefits	A well-designed system uses less power to operate [32][35]. Bandwidth usage can be reduced through the design [32][35] A scenario-based design can complete tasks based on users' actions. [24]
	Drawbacks	Some smart devices have to wait for the cloud server to respond [32][35]. The age gap of the users is not taken into account when designing smart homes [24][43].
Health and elderly care	Benefits	Elderly and patient monitoring is possible with the help of smart home systems [3][29]. Activity monitoring looks for changes in a patient's routine and notifies the interested parties [29]. An elderly-friendly smart home makes independent living possible for its users [6].
	Drawbacks	The accuracy of patient monitoring systems is still questionable [29]. Security, energy efficiency, and data visibility are other concerns related to patient monitoring features [15].
Resource management	Benefits	Reducing energy and water consumption is possible when utilizing smart home products [16][37][48]. Creating an energy consumption profile of household equipment [16].
	Drawbacks	Purchasing monitoring devices is difficult because some cannot be found off the shelf [48].
Usability	Benefits	Developers can use middleware to integrate the smart devices, and the user can control them through a centralized system [8]. Automating tasks with smart home products [21].
	Drawbacks	Integration between IoT devices is a challenge [8]. Usability in designing security features for smart home devices is not explicitly or systematically considered [10].
Performance	Benefits	A standardized communication protocol boosts performance because the devices do not have to independently collect the data and they can share the tasks [17]. Edge computing architectural techniques may potentially boost performance [35].
	Drawbacks	Middleware components show some inhibitors in the code [5].
Development process	Benefits	Requirements gathering from the stakeholders, prototyping, and a user-driven design can further improve the product [33].
	Drawbacks	The lack of a systematic development approach can result in security and design compromises [43][47].
Knowledge management and education	Benefits	Keeping a record of the use cases in one project may be beneficial for other projects [18]. Knowledge management can have positive environmental impacts, and smart home residents can share their experiences to help others make better choices [18].
	Drawbacks	It is essential to improve the learning process linked to IoT development [22].

4.4. Ways to optimize smart home systems (RQ3)

The answer to the last research question (RQ3) is discussed in this section. The aim is to provide brief guidelines based on the information found in the literature for improving smart home products, both in terms of their functional and non-functional features. The table below is divided into eight parts containing the related recommendations. The recommendations are collected after analyzing the selected sources (Appendix 1) and more information can be found in section 4.2 which covers the eight mentioned topics. The recommendation is for the reader to look for the provided sources in the table below to gain a better and more detailed understanding of the topic.

Table 7. Recommended guidelines for the selected topics

Topic	Guidelines
Security and privacy	Users need to have more control over the data flow. [7] Avoid using compromised hardware and use data encryption. [49] Allocate funds for developing the security features. [38, 49]
Design	Divide the load between the main server and the local devices. [32, 35] Design based on the target group's requirements. [24, 43] User-friendly design for the security features. [10]
Health and elderly care	Develop an easy-to-use and easy-to-control system, such as a voice-controlled system. [43] Automate tasks based on user activity. [6, 29] Provide wearable sensors to monitor users' health. [15]
Resource management	Creating an energy usage profile for the home equipment to optimize the energy usage of such devices. [16]
Usability	Middleware can provide the possibility of controlling the smart device through a centralized system. [8] Consult with the design expert to improve the product. [10]
Performance	Edge computing architectural techniques help to save bandwidth and processing power. [35]
Development process	Detailed requirements gathering from the stakeholders, prototyping, and a user-driven design can improve the product. [33]
Knowledge management and education	Documenting the system's use cases and developing solutions can help to improve future products. [18]

5. Discussion and lessons learned

Smart home systems have been constantly gaining popularity over the past few years, as shown in [Figure 1]. Furthermore, IoT and smart homes are inseparable parts of software development and software engineering research. The presented research may contribute to improving smart home products and the related development process.

The current paper presents some of the use cases for smart home systems, for example, smart healthcare. Smart home developers must find and research the problems they are trying to solve. The next step is to find a solution to the discovered problem by examining different ideas and scenarios. Prototyping and observing the end-user when interacting with the prototype can help improve the design and better equip the product with features that stakeholders require. Nevertheless, features like data security and user privacy should not be compromised, even though the user may not understand their importance immediately [49].

There is an important lesson to learn from the case studies. Smart home designers and developers must explain the real effect of weak security protocols to stakeholders to obtain adequate resources for fixing and enhancing security issues. The education system also plays an important role in training the computer since students have a critical viewpoint on security designs. It would be easier to discuss the required features for a product when both the developers and stakeholders are on the same page about the importance of the features in question.

Security and privacy improvements are constantly raised in the literature, and most of the recommended improvements are basic security enhancements such as encryption [49]. However, based on the content of Table 5, these security issues are not solved. It is almost impossible to implement flawless software. However, allocating more resources to improve the security level of smart devices can reduce security issues [13]. A case study shows that having a clear architecture and development process is beneficial in implementing the different features (UI, performance, security, etc.) of a product [33]. For example, it may be the case that enough attention is not given to usability in favor of performance improvements or vice versa [12][27]. A clear development process that does not skip any of the steps will lead to better results [33]. Documentation is an important step in the development process. Documentation helps share some ideas between the development teams and not to repeat the mistakes made before.

Following a clear development process is a must when talking about enterprise products that can potentially compromise people's privacy. The important lesson here is to find a process that is acceptable to the entire team and that can result in the development of a product based on the gathered requirements. Each stage of the process must be considered and not skipped. Dividing the development into separate layers, such as UI and communication layers, can help direct the focus on the entirety of each layer and its related features, which results in a more complete product.

In summary, the study results recommend producing smart home systems that can solve real problems through proper planning and interactions with actual users. The development team should consider both functional and nonfunctional features, document the development process, and further improve the product as technology advances and user requirements change. The current paper covered eight topics related to the three high-level phases of the development process (planning, implementation, and improvement). Topics such as resource management and elderly care are linked to the planning phase because the development team is discovering the user requirements and use cases. Other topics such as security, privacy, and performance are related to the implementation phase, and finally, topics such as knowledge management and education are linked to improving the product's functionality and stability.

6. Conclusion

The current paper has examined the status of home automation, including the benefits and drawbacks of such systems. Four digital libraries are selected to research published case studies related to the selected number of smart home domains. Papers with distinct titles that are written in English and are more than three pages are selected as research material. Furthermore, thematic analysis was performed to extract data linked to the research questions to study the current state of the art and to identify the benefits and drawbacks of smart home systems, as described in the literature. The positive impact of smart home products in automating some daily tasks has been shown. The research material is divided into eight topics, and Table 5 presents the distribution of the study topics per year.

As mentioned earlier and presented in Figure 4, security and privacy are the most popular research subjects. Table 5 shows that this topic has been covered since 2013. One can assume that this is because of the ongoing interest in current smart home products. Furthermore, studies show that even commercial products have security vulnerabilities [10][49]. The authors recommend going back to the whiteboard and focusing on solving the issues early on, in the planning and the design stage; this can result in a chain reaction and solve the other issues mentioned in this paper.

[Figure 4] also shows that not enough attention is given to knowledge management and home automation-related education. A knowledge management platform can help developers learn from each other's experiences, further improve their products, and solve real problems through proper planning and interactions with actual users [18]. More courses in the educational system, with a focus on home automation and IoT, may result in the development of better products. Studies show that such courses are welcomed by students [22]. In conclusion, more attention should be given to education and knowledge management to improve design and security, privacy, and performance. Additionally, developers should not skip any of the three layers of the development architecture (UI layer, communication layer, and software system layer) because each stage is dedicated to addressing existing weaknesses in smart home products [33]. Following the mentioned recommendations in [Table 7] and this section may improve future smart home products and set a baseline for future research.

This document is based on academic case studies. However, for future work, industrial contributions that are usually considered grey literature may be included. Grey literature was out of the scope of this paper.

References

[1] Hisham Albataineh, Mais Nijim, and Divya Bollampall. "the design of a novel smart home control system using smart grid based on edge and cloud computing," 2020 IEEE 8th International Conference on Smart Energy Grid Engineering (SEGE), pp. 88-91, (2020) TS-CrossRef. DOI:https://doi.org/10.1109/SEGE49949.2020.9181961

[2] Abdulrahman Alharthi, Michael Lipscomb, and Murat M Tanik, "Internet of things (IoT) in enterprise systems for process improvement: A case study in home security," In 2019 SoutheastCon, IEEE, pp.1–6, (2019) DOI:https://doi.org/10.1109/SoutheastCon42311.2019.9020487

[3] Areej Almazroa and Hongjian Sun, "An internet of things (IoT) management system for improving homecare - A case study," 2019 International Symposium on Networks, Computers, and Communications (ISNCC), pp.1-5, (2019) TS-CrossRef. DOI:https://doi.org/10.1109/ISNCC.2019.8909186

[4] Zahrah A Almusaylim and Noor Zaman, "A review on smart home present state and challenges: Linked to context-awareness internet of things (IoT)," Wirel. Networks vol.25, no.6, pp.3193–3204, (2019) DOI:https://doi.org/10.1007/s11276-018-1712-5 M4 - Citavi

[5] Md Sayedul Aman, Kumar Yelamarthi, Ahmed Mohamed Abdelgawad, and Saleh M Alnaeli, "Parallelization in software systems used in wireless sensor networks and internet of things: Case study," Middleware systems. 2016 IEEE 3rd World Forum on Internet of Things (WF-IoT), pp.342-347, (2019) TS-CrossRef. DOI:https://doi.org/10.1109/WF-IoT.2016.7845496

[6] Farzad Amirjavid, Abdenour Bouzouane, and Bruno Bouchard, "Intelligent temporal data-driven world actuation in ambient environments: Case study," Anomaly recognition and assistance provision in the smart home. 2013 IEEE/ACIS 12th International Conference on Computer and Information Science (ICIS), pp.287-29, (2013) TS-CrossRef. DOI:https://doi.org/10.1109/ICIS.2013.6607856

[7] Yu Nandar Aung and Thitinan Tantidham, "Review of Ethereum: Smart home case study," In 2017 2nd International Conference on Information Technology (INCIT), IEEE, pp.1–4, (2017) DOI:https://doi.org/10.1109/INCIT.2017.8257877

[8] R Borja, J R La Pinta, A Álvarez, and J M Maestre, "Integration of service robots in the smart home through UPnP: A surveillance robot case study," Rob. Auton. Syst. vol.61, no.2, pp.153–160, (2013) DOI:https://doi.org/10.1016/j.robot.2012.10.005 M4 - Citavi

[9] John N A Brown, Bonifaz Kaufmann, Franz J Huber, Karl-Heinz Pirolt, and Martin Hitz, "Language in Their Very Gesture" First Steps towards Calm Smart Home Input. In Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data, David Hutchison, Takeo Kanade, Josef Kittler, Jon M Kleinberg, Friedemann Mattern, John C Mitchell, Moni Naor, Oscar Nierstrasz, C Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y Vardi, Gerhard Weikum, Andreas Holzinger and Gabriella Pasi (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, pp.256–264, (2013) DOI:https://doi.org/10.1007/978-3-642-39146-0_22 M4 - Citavi

[10] George Chalhoub, Ivan Flechais, Norbert Nthala, Ruba Abu-Salma, and Elie Tom, "Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study," Extended Abstracts of the 2020 CHI Conference on Human Factors in Computing Systems, pp.1-9, (2020) TS-CrossRef. DOI:https://doi.org/10.1145/3334480.3382850

[11] Maheswaree Kissoon Curumsing, Niroshinie Fernando, Mohamed Abdelrazek, Rajesh Vasa, Kon Mouzakis, and John Grundy, "Emotion-oriented requirements engineering: A case study in developing a smart home system for the elderly," J. Syst. Softw. Vol.147, pp.215–229, ((2019)) DOI:https://doi.org/10.1016/j.jss.2018.06.077 M4 - Citavi

[12] Laura Daniele, Frank Hartog, and Jasper Roes, "How to keep a reference ontology relevant to the industry: A case study from the smart home," In Ontology Engineering, Valentina Tamma, Mauro Dragoni, Rafael Gonçalves and Agnieszka Ławrynowicz (eds.). Springer International Publishing, Cham, pp.117–123, (2016) DOI:https://doi.org/10.1007/978-3-319-33245-1_12 M4 - Citavi

[13] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," In 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), IEEE, pp.618–623, (2017) DOI:https://doi.org/10.1109/PERCOMW.2017.7917634

[14] Jan Dvorak, Ondrej Berger, and Ondrej Krejcar, "Universal central control of home appliances as an expanding element of the smart home concepts — A case study on a low-cost smart solution," In Computer Information Systems and Industrial Management, Khalid Saeed and Václav Snášel (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, pp.479–488, (2014) DOI:https://doi.org/10.1007/978-3-662-45237-0_44 M4 - Citavi

[15] Atis Elsts, George Oikonomou, Xenofon Fafoutis, and Robert Piechocki, "Internet of things for smart homes: Lessons learned from the SPHERE case study," In 2017 Global Internet of Things Summit (GIoTS), IEEE, pp.1–6, (2017) DOI:https://doi.org/10.1109/GIOTS.2017.8016226

[16] El Hassan Et-Tolba, Mohammed Ouassaid, and Mohamed Maaroufi, "Smart home appliances modeling and simulation for energy consumption profile development: Application to Moroccan real environment case study," In 2016 International Renewable and Sustainable Energy Conference (IRSEC), IEEE, pp.1050–1055, (2016) DOI:https://doi.org/10.1109/IRSEC.2016.7983908

[17] Gareth A. Gericke and Nicolaas Luwes, "Proposing the need for a protocol standard for Internet of Things: Internet of Things water heater case study," In 2017 Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech), IEEE, pp.128–132, (2017) DOI:https://doi.org/10.1109/RoboMech.2017.8261135

[18] Raghav Grover and Thomas M Froese, "Knowledge management in construction using a SocioBIM Platform: A case study of AYO smart home project," Procedia Eng. Vol.145, pp.1283–1290, (2016) DOI:https://doi.org/10.1016/j.proeng.2016.04.165 M4 - Citavi

[19] Nadine Guhr, Oliver Werth, Philip Peter Hermann Blacha, and Michael H Breitner. 2020. Privacy concerns in the smart home context. SN Appl. Sci. vol.2, no.2, (2020) DOI:https://doi.org/10.1007/s42452-020-2025-8 M4 - Citavi

[20] Mehedi Hasan, Parag Biswas, M Toufiqul IslamD Bilash, and Md. Ashik Zafar Dipto, "Smart home systems: overview and comparative analysis," Fourth International Conference on Research in Computational

Intelligence and Communication Networks (ICRCICN), pp.264-268, (2018) TS-CrossRef. DOI:https://doi.org/10.1109/ICRCICN.2018.8718722

[21] Jing He, Amir Atabekov, and Hisham M Haddad, “Internet-of-things based smart resource management system: A case study intelligent chair system,” In 2016 25th International Conference on Computer Communication and Networks (ICCCN), IEEE, pp.1–6, (2016) DOI:https://doi.org/10.1109/ICCCN.2016.7568533

[22] Jing He, Dan Lo Chia-Tien, Ying Xie, and Jonathan Lartigue, “Integrating the Internet of Things (IoT) into STEM undergraduate education: A case study of a modern technology infused courseware for embedded system course,” 2016 IEEE Frontiers in Education Conference (FIE), pp.1-9, (2016) TS-CrossRef. DOI:https://doi.org/10.1109/FIE.2016.7757458

[23] Dimitar Ivanovski, “The "Green" in the Internet of Things: A case study of faculty environment,” In Knowledge Management in Organizations, Lorna Uden, Marjan Heričko and I-Hsien Ting (eds.). Springer International Publishing, Cham, pp.561–571, (2015) DOI:https://doi.org/10.1007/978-3-319-21009-4_42 M4 - Citavi

[24] Anna Karagianni and Vasiliki Geropanta, “Smart homes: Methodology of IoT integration in the architectural and interior design process – A case study in the historical center of Athens,” In Intelligent Computing and Optimization, Pandian Vasant, Ivan Zelinka and Gerhard-Wilhelm Weber (eds.). Springer International Publishing, Cham, pp.222–230, (2020) DOI:https://doi.org/10.1007/978-3-030-33585-4_22 M4 - Citavi

[25] Barbara Kitchenham, O Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. 2009. Systematic literature reviews in software engineering – A systematic literature review. Inf. Softw. Technol. 51, 1 (2009), 7–15. DOI:https://doi.org/10.1016/j.infsof.2008.09.009 M4 - Citavi

[26] Minjoo Lee, Dasom Jeong, Hayoung Jeong, Enoch Lee, and Moonkyu Song, “A framework for designing UX of sharing ‘internet of things (IoT)’ system and service: A case study of UX development of community laundry machines,” In Design, User Experience, and Usability: Technological Contexts, Aaron Marcus (ed.). Springer International Publishing, Cham, pp365–372. (2016) DOI:https://doi.org/10.1007/978-3-319-40406-6_35 M4 - Citavi

[27] Gerhard Leitner, Anton J Fercher, and Christian Lassen, “End users programming smart homes – A case study on scenario programming,” In Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data, David Hutchison, Takeo Kanade, Josef Kittler, Jon M Kleinberg, Friedemann Mattern, John C Mitchell, Moni Naor, Oscar Nierstrasz, C Pandu Rangan, Bernhard Steffen, Madhu Sudan, Demetri Terzopoulos, Doug Tygar, Moshe Y Vardi, Gerhard Weikum, Andreas Holzinger and Gabriella Pasi (eds.). Springer Berlin Heidelberg, Berlin, Heidelberg, pp.217–236, (2013) DOI:https://doi.org/10.1007/978-3-642-39146-0_20 M4 - Citavi

[28] Xing Liu, Cheng Qian, William Grant Hatcher, Hansong Xu, Weixian Liao, and Wei Yu, “Secure internet of things (IoT)-based smart-world critical infrastructures: Survey, case study, and research opportunities,” IEEE Access, vol.7, pp.79523–79544, (2019) DOI:https://doi.org/10.1109/ACCESS.2019.2920763

[29] Sawsan M Mahmoud, Hesham A Alabbasi, and Tawfiq E Abdulabbas, “Monitoring and detecting outliers for elder’s life activities in a smart home: A case study,” In 2017 E-Health and Bioengineering Conference (EHB), IEEE, pp.458–461, (2017) DOI:https://doi.org/10.1109/EHB.2017.7995460

[30] Petra Maresova, Ondrej Krejcar, Sabina Barakovic, Jasmina Barakovic Husic, Petre Lameski, Eftim Zdravevski, Ivan Chorbev, and Vladimir Trajkovik, "Health-related ICT solutions of smart environments for elderly–systematic review,” IEEE Access vol.8, pp.54574–54600, (2020) DOI:https://doi.org/10.1109/access.2020.2981315 M4 - Citavi

[31] Melyani, Meyliana, Harjanto Prabowo, Achmad N Hidayanto, and Ford. L Gaol, “Smart home component using orange technology for elderly people: A systematic literature,” 2018 Indonesian Association for Pattern Recognition International Conference (INAPR), pp.166-171, (2018) TS-CrossRef. DOI:https://doi.org/10.1109/INAPR.2018.8626998

[32] Burhan A Mudassar, Jong Hwan Ko, and Saibal Mukhopadhyay, “Edge-cloud collaborative processing for intelligent internet of things: A case study on smart surveillance,” 55th ACM/ESDA/IEEE Design Automation Conference (DAC), pp.1-6, (2018) TS-CrossRef. DOI:https://doi.org/10.1109/DAC.2018.8465862
[33] Anh Nguyen Duc, Khan Khalid, Tor Lonnestad, Sohaib Bajwa Shahid, Xiaofeng Wang, and Pekka Abrahamsson, “How do startups develop internet-of-things systems - A multiple exploratory case study,” IEEE/ACM International Conference on Software and System Processes (ICSSP), pp.74-83, (2019) TS-CrossRef. DOI:https://doi.org/10.1109/ICSSP.2019.00019
[34] Andrzej Ozadowicz, Jakub Grela, Lukasz Wisniewski, and Krzysztof Smok, “Application of the internet of things (IoT) technology in consumer electronics - Case study,” In 2018 IEEE 23rd International Conference on Emerging Technologies and Factory Automation (ETFA), IEEE, pp.1037–1042, (2018) DOI:https://doi.org/10.1109/ETFA.2018.8502468
[35] Gopika Premsankar, Mario Di Francesco, and Tarik Taleb. 2018. Edge Computing for the Internet of Things: A Case Study. IEEE Internet Things J. 5, 2 (2018), 1275–1284. DOI:https://doi.org/10.1109/JIOT.2018.2805263 M4 - Citavi
[36] Raz Kamaran Radha. 2022. Flexible smart home design: Case study to design future smart home prototypes. Ain Shams Eng. J. 13, 1 (2022). DOI:https://doi.org/10.1016/j.asej.2021.05.027
[37] Batchu Rajasekhar and Naran M Pindoriya. 2015. Multi-stage scheduling for a smart home with solar PV and battery energy storage — A case study. 2015 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA), pp.1-6 TS-CrossRef. DOI:https://doi.org/10.1109/ISGT-Asia.2015.7386984
[38] T Reichherzer, A Mishra, E Kalaimannan, and N Wilde. 2016. A Case Study on the Trade-Offs between Security, Scalability, and Efficiency in Smart Home Sensor Networks. 2016 International Conference on Computational Science and Computational Intelligence (CSCI), pp.222-225 TS-CrossRef. DOI:https://doi.org/10.1109/CSCI.2016.0049
[39] Biljana L Risteska Stojkoska and Kire V Trivodaliev. 2017. A review of Internet of Things for smart home: Challenges and solutions. J. Clean. Prod. vol.140, pp.1454–1464, (2017) DOI:https://doi.org/10.1016/j.jclepro.2016.10.006 M4 - Citavi
[40] Diego G. Rossit and Sergio Nesmachnow. 2022. Energy-Aware Smart Home Planning: A Real Case Study in Montevideo, Uruguay. . 146–161. DOI:https://doi.org/10.1007/978-3-030-96753-6_11
[41] Ronny Seiger, Uwe Assmann, and Steffen Huber. 2018. A Case Study for Workflow-Based Automation in the Internet of Things. In 2018 IEEE International Conference on Software Architecture Companion (ICSA-C), IEEE, 11–18. DOI:https://doi.org/10.1109/ICSA-C.2018.00011
[42] Deniz Sönmez and Kivanç Dinçer. 2016. A review of modern residential thermostats for home automation to provide energy efficiency. 2016 4th International Istanbul Smart Grid Congress and Fair (ICSG), pp.1-4 TS-CrossRef. DOI:https://doi.org/10.1109/sgcf.2016.7492430
[43] Susanna Spinsante, Enea Cippitelli, Adelmo Santis, Ennio Gambi, Samuele Gasparrini, Laura Montanini, and Laura Raffaeli. 2015. Multimodal Interaction in an Elderly-Friendly Smart Home: A Case Study. In Mobile Networks and Management, Ramón Agüero, Thomas Zinner, Rossitza Goleva, Andreas Timm-Giel and Phuoc Tran-Gia (eds.). Springer International Publishing, Cham, pp.373–386. DOI:https://doi.org/10.1007/978-3-319-16292-8_27 M4 - Citavi
[44] Qie Sun, Hailong Li, Zhanyu Ma, Chao Wang, Javier Campillo, Qi Zhang, Fredrik Wallin, and Jun Guo. 2016. A Comprehensive Review of Smart Energy Meters in Intelligent Energy Networks. IEEE Internet Things J. 3, 4, pp.464–479, (2016) DOI:https://doi.org/10.1109/jiot.2015.2512325 M4 - Citavi
[45] Satyendra K Vishwakarma, Prashant Upadhyaya, Babita Kumari, and Arun Kumar Mishra. 2019. Smart Energy Efficient Home Automation System Using IoT. 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), pp.1-4 TS-CrossRef. DOI:https://doi.org/10.1109/IoT-SIU.2019.8777607

[46] Yulistiyan Wardhana, Bob Hardian, Gladhi Guarddin, and Hanif Rasyidi. 2013. Context-aware door access control on private room using fuzzy logic: A case study of a smart home. 2013 International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp.155-159 TS-CrossRef. DOI:https://doi.org/10.1109/ICACSIS.2013.6761568

[47] Muhammad Mudassar Yamin, Basel Katt, Espen Torseth, Vasileios Gkioulos, and Stewart James Kowalski. 2018. Make it and Break it. Proceedings of the 2nd International Symposium on Computer Science and Intelligent Control - ISCSIC '18, pp.1-6 TS-CrossRef. DOI:https://doi.org/10.1145/3284557.3284743

[48] Shuang-Hua Yang, Xi Chen, Xiaomin Chen, Lili Yang, Baichong Chao, and Jiangtao Cao. 2015. A case study of the internet of things: A wireless household water consumption monitoring system. 2015 IEEE 2nd World Forum on Internet of Things (WF-IoT), pp.681-686 TS-CrossRef. DOI:https://doi.org/10.1109/WF-IoT.2015.7389136

[49] Mengmei Ye, Nan Jiang, Hao Yang, and Qiben Yan. 2017. Security analysis of Internet-of-Things: A case study of the august smart lock. In 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), IEEE, pp.499–504. DOI:https://doi.org/10.1109/INFCOMW.2017.8116427

[50] Jeong-joong Yoon. 2019. The Case Study of Smart Home in LH. 2019 IEEE Transportation Electrification Conference and Expo, Asia-Pacific (ITEC Asia-Pacific), pp.1-4 TS-CrossRef. DOI:https://doi.org/10.1109/ITEC-AP.2019.8903732

Appendices

Realized study topic(s) per each analyzed paper

Topic	List of related paper ids
Security and privacy	S1, S2, S4, S5, S6, S10, S12, S14, S15, S31, S32, S34, S37, S38, S48
Design	S1, S5, S6, S11, S15, S18, S19, S26, S39, S40, S44, S45
Health and elderly care	S1, S7, S13, S20, S21, S23, S26, S28, S36, S41, S46, S49, S52, S55
Resource management	S3, S8, S15, S16, S23, S24, S27, S35, S39, S47, S56
Usability	S4, S11, S15, S20, S25, S29, S43, S44, S45, S50, S54
Performance	S8, S9, S17, S19, S33
Development process	S6, S22, S41, S42
Knowledge management and education	S3, S30, S51, S53

Id	Document's title
S1	Emotion-oriented requirements engineering: A case study in developing a smart home system for the elderly
S2	Cyber-physical systems information gathering: A smart home case study
S3	Knowledge Management in Construction Using a SocioBIM Platform: A Case Study of AYO Smart Home Project
S4	Integration of service robots in the smart home using UPnP: A surveillance robot case study
S5	Factoring User Experience into the Security and Privacy Design of Smart Home Devices: A Case Study
S6	Make it and Break it: An IoT Smart Home Testbed Case Study
S7	Maintaining multiple sclerosis patients' quality of life: a case study on environment control assistance in a smart home
S8	Proposing the need for a protocol standard for Internet of Things: Internet of Things water heater case study
S9	Door and light control prototype using Intel Galileo-based Internet of Things: (Case study: Embedded and robotics laboratory, department of computer engineering, Diponegoro University)
S10	Internet of Things (IoT) in Enterprise Systems for Process Improvement: A Case Study in Home Security
S11	An Analysis of the Impact of Uncertainty on the Internet of Things: A Smart Home Case Study
S12	Review of Ethereum: Smart home case study
S13	Monitoring and detecting outliers for elder's life activities in a smart home: A case study
S14	Context-aware door access control on private room using fuzzy logic: A case study of smart home
S15	The Case Study of Smart Home in LH
S16	Smart home appliances modeling and simulation for energy consumption profile development: Application to Moroccan real environment case study
S17	Describing the Internet of Things with an ontology: The SusCity project case study
S18	Edge-Cloud Collaborative Processing for Intelligent Internet of Things: A Case Study on Smart Surveillance
S19	Edge Computing for the Internet of Things: A Case Study
S20	Rapid prototyping Internet of Things solutions through a model-driven approach: A case study in AAL
S21	An Internet of Things (IoT) Management System for Improving Homecare - A Case Study
S22	How do Startups Develop Internet-of-Things Systems - A Multiple Exploratory Case Study
S23	Internet of Things for smart homes: Lessons learned from the SPHERE case study
S24	A case study of the internet of things: A wireless household water consumption monitoring system
S25	A Case Study for Workflow-Based Automation in the Internet of Things
S26	Fog Computing in Healthcare Internet of Things: A Case Study on ECG Feature Extraction
S27	Application of the Internet of Things (IoT) Technology in Consumer Electronics - Case Study
S28	Logging mechanism for Internet of Things: A Case Study of Patient Monitoring System
S29	Internet-of-Things Based Smart Resource Management System: A Case Study Intelligent Chair System
S30	Integrating the Internet of Things (IoT) into STEM undergraduate education: A case study of a modern technology infused courseware for embedded system course

S31	Secure Internet of Things (IoT)-Based Smart-World Critical Infrastructures: Survey, Case Study, and Research Opportunities
S32	Security analysis of Internet-of-Things: A case study of august smart lock
S33	Parallelization in software systems used in wireless sensor networks and the Internet of Things: Case study: Middleware systems
S34	Security Vulnerabilities of the Internet of Things: A Case Study of the Smart Plug System
S35	Multi-stage scheduling for a smart home with solar PV and battery energy storage — A case study
S36	Intelligent temporal data-driven world actuation in ambient environments: Case study: Anomaly recognition and assistance provision in smart home
S37	Blockchain for IoT security and privacy: The case study of a smart home
S38	A Case Study on the Trade-Offs between Security, Scalability, and Efficiency in Smart Home Sensor Networks
S39	An IoT Service Framework for Smart Home: Case Study on HEM
S40	Examining the Reusability of Smart Home Applications: A Case Study on Eclipse Smart Home
S41	Multimodal Interaction in an Elderly-Friendly Smart Home: A Case Study
S42	How to Keep a Reference Ontology Relevant to the Industry: A Case Study from the Smart Home
S43	Universal Central Control of Home Appliances as an Expanding Element of the Smart Home Concepts — Case Study on Low-Cost Smart Solution
S44	End Users Programming Smart Homes – A Case Study on Scenario Programming
S45	Smart Homes: Methodology of IoT Integration in the Architectural and Interior Design Process – A Case Study in the Historical Center of Athens
S46	Internet of Things for Enhanced Smart Cities: A Review, Roadmap, and Case Study on Air Quality Sensing
S47	The "Green" in the Internet of Things: Case Study of Faculty Environment
S48	Internet of Things Forensics – Challenges and a Case Study
S49	Deploying Mobile Middleware for the Monitoring of Elderly People with the Internet of Things: A Case Study
S50	A Framework for Designing UX of Sharing 'Internet of Things (IoT)' System and Service: Case Study of UX Development of Community Laundry Machines
S51	A Case Study of Project-based Learning on Internet of Things Course
S52	Edge-Assisted Control for Healthcare Internet of Things: A Case Study on PPG-Based Early Warning Score
S53	Designing an Educational Internet of Things Toolbox: A case study of a learner-centric tool design
S54	Flexible smart home design: Case study to design future smart home prototypes
S55	Convergence of Artificial Intelligence and Internet of Things in Smart Healthcare: A Case Study of Voice Pathology Detection
S56	Energy-Aware Smart Home Planning: A Real Case Study in Montevideo, Uruguay

This page is empty by intention.

Publication II

Yaldaie, A., Porras, J., and Drögehorn, O.
Who Are Smart Home Users and What Do They Want?—Insights from an International Survey

Applied Computer Systems
Volume 28, No. 1, 2023, pp. 114–124

Applied Computer Systems
ISSN 2255-8691 (online)
ISSN 2255-8683 (print)
June 2023, vol. 28, no. 1, pp. 114–124
https://doi.org/10.2478/acss-2023-0011
https://content.sciendo.com

Who are Smart Home Users and What do they Want? – Insights from an International Survey

Ashkan Yaldaie[1*], Jari Porras[2], Olaf Drögehorn[3]
[1,2]*LUT University, Lappeenranta, Finland*
[3]*Harz University of Applied Sciences, Wernigerode, Germany*

***Abstract* – Any set of devices for controlling home appliances that link to a common network and may be controlled independently or remotely are typically referred to as smart home technology. Smart homes and home automation are not completely unknown to people anymore; smart devices and sensors are part of daily life in the 21st century. Among other benefits of home automation devices, it is possible to manage home appliances and monitor resource usage, and security. It is essential to find practical information about smart home users, and possible use cases. The current survey covers smart home usage benefits and challenges for the users. The study presents the result of the collected information from different countries, and the participants are people from a variety of age groups and occupations. The questionnaire that contains both qualitative and quantitative questions was distributed through internet channels such as blog posts and social network groups. Furthermore, to generate the survey questions we conducted a literature review to gain a better understating of the subject and the related work. The research provides a better foundation for future smart home development. As a result of this survey-based study and in addition to finding the desirable home automation features, we discovered the amount of money users are ready to spend to automate their homes. Connecting the favourite smart home features to its users and the amount of money they are ready to spend on them can provide a bigger picture for the smart home industry as a whole and particularly be beneficial for developers and start-ups.**

***Keywords* – Energy efficiency, home automation, home security, IoT, remote monitoring, smart home.**

I. Introduction

According to a market research report published by Fortune Business Insights [1], the global market size for home automation was USD 64.58 billion in 2020 and based on their prediction, it is due to reach USD 163.24 billion in 2028. Wireless devices are a big portion of the market size. Because of the wireless systems and their accessibility, one can transfer any home into a smart home and start automating tasks, monitoring the activities for security reasons, or creating specific reports for resource usage for sustainability. There is no official definition for a smart home since the definition comes from different users' needs and desires. One may use the term for monitoring health complications through smart devices connected to the home, while others may consider a smart home for automating daily tasks such as locking the doors automatically when no one is at home.

The paper uses terms such as home automation, smart devices, smart home, smart systems, and the internet of things, and these terms in the scope of this paper refer to any system or device that links to a common network and may be controlled independently and remotely. Such devices are under the umbrella of smart home technology.

Internet of Things (IoT) devices such as sensors, control devices, and monitoring systems surround us. Weiser and Brown predicted the arrival of ubiquitous computing, and with IoT, we can see this vision come to life [2]. IoT is a means for the interconnection of things based on current or advancing innovation. One of the common use cases of IoT is smart home technology-related automation. The objective of this paper is to conduct a survey-based study to gather meaningful information about home automation users and possible use cases. This study helps us to answer the following three research questions (RQ):

RQ1. Who are the smart home users?
RQ2. What are the desirable home automation features for the users?
RQ3. How much money the users are ready to spend on home automation devices?

The answers to the first question (RQ1) reveal the background of the smart home user. This would provide a foundation for answering the remaining research questions. Research question two (RQ2) is set to clarify participants' preferred home automation features, systems, and devices. Furthermore, the answer to the second research question determines the extent of the current home automation usage for the participants. As a result of the third research question (RQ3), the current survey-based study discovered how much home automation costs for the participants, how much more they are willing to invest in home automation, and what desirable features they require for a home automation system. Connecting the favourite smart home features to its users and the amount of money they are ready to spend on them can provide a bigger picture for the smart home industry as a whole and particularly be beneficial for developers and start-ups.

* Corresponding author's e-mail: ashkan.yaldaie@student.lut.fi

The current survey-based study includes both qualitative and quantitative questions and it is distributed through internet channels. While a detailed discussion of the results will be presented in related sections, it is worth noting some key findings here. Most of the collected responses come from university-educated participants in their 30s and 40s, living in rental accommodations. Furthermore, the results indicate that although many people have heard about smart home technology, they have not yet adopted it fully. It appears that most of the participants are prone to utilizing smart light management systems which they purchased off the shelf. Security features for smart home systems are popular. However, costly systems are not attractive for the users since most of them are ready to spend a hundred euros or less on home automation systems. The survey participants are people from a variety of age groups and occupations. More details about the survey and its participants are provided in the paper related sections.

The paper is organised as follows: Section II provides an overview of the related work in the field of home automation. Section III presents the methodology employed in conducting the survey-based study. Section IV presents the detailed results obtained from the data analysis. Section V offers a critical discussion and analysis of the findings. Finally, Section VI concludes the paper, by summarising the key findings, their implications, and potential future research directions.

II. Related Work

The current section is set to present the related academic work linked to this survey-based study. As mentioned earlier, the aim is to answer the research questions and find out about the desirable home automation features and the money the participants are ready to spend on home automation devices.

Shin et al. [3] published a paper about smart home user demographics. The results show that aged consumers are more likely to purchase smart home products, and systematic marketing strategies are required to gain the interest of younger consumers. According to Shin [3], the spread of smart homes has been slower than expected despite a wide variety of products developed by leading technology players like Google and Amazon.

According to Coskun et al. [4], smart home users prefer features such as remote accessibility, multi-functionality, and autonomy. Remote accessibility and autonomy are interrelated since one can have control over house appliances from anywhere and on the other hand the users would like the smart systems to work independently. Sometimes controlling the functionality is uninteresting. Users prefer to spend time browsing the Internet, spending time with the children, and watching TV instead of constantly interacting with smart systems.

There is a gap between what smart home offers and what users need. The slow adoption of home automation is covered in numerous studies. Privacy and security, trust issues, reliability, and price are some of the challenges against the mass utilization of home automation. Data Protection Regulation (GDPR) requires actions to protect citizens within the EU. This could be a strong driver for smart home developers to implement yet stronger privacy measures. The aim is to establish a trustworthy platform that is not costly for the end users. Unless it is embraced by society and employed by customers, technology has no value [5], [6].

Reisinger et al. [7] proposed that adequate design goals are an important factor in creating a user-centred product. Reisinger realised that smart home users appreciate functionalities such as comfort, sustainability, security, lower heating and energy costs, and fun. Consumers would like to see the benefits of their investment in smart home services. Abi Sen et al. [8] suggests a way to bring down the cost of smart home by recycling old PCs and accessories. This might be a good solution since it is possible to create remote access and even voice-controlled systems at an affordable cost.

Technology is useful for supporting the elderly and people with chronic illnesses. However, that is not all, everyone can benefit from a functional system. The usage of smart meters demonstrated around three percent energy reductions and a goal-oriented smart home emphasizes the potential to help achieve energy demand cutback goals [9]. Security, safety, and monitoring are some of the features that users demand to have when it comes to purchasing smart home products. Additionally, users' income and education levels have significant effects on their choice, which means a user-centred system design is more likely to be accepted by the consumers [10], [11].

A survey conducted for the home automation domain by Zhai et al. confirmed the results of the above-mentioned studies. The several participants were from Asia and Europe. Among the smart home adaptation concerns, one can see privacy and costs-related concerns [12]. Another survey revealed that 92 % of the participants thought that smart devices had the potential to save time and energy. Furthermore, 55 % of the same survey participants believed that home automation would make life easier [13].

Smart systems are not widely adopted by mainstream users [3], [4]. This can be related to the high costs, privacy concerns, or the absence of a user-centred design. Yet, users still have a positive view of the subject. The literature also offers possibilities to address user interests. Our study aims to further improve the understanding of smart home user concerns and their favourite features. Additionally, the result of this questionnaire provides details about the monetary value of home automation for the participants. The next section discusses the methodology used to complete this paper.

III. Methodology

The current study employs a survey-based research approach to gather insights into smart home users and their preferences. This inductive research methodology involves collecting data from participants and subsequently analysing the collected data to identify trends, patterns, and generalizations that can contribute to the development of future smart home technologies.

To ensure a comprehensive data collection process, the survey questionnaire was designed to include both qualitative and quantitative questions that align with the research questions. The complete set of survey questions is available in Appendix 1. The questionnaire is organised in five sections, and participants are directed to the appropriate section based on their responses in the previous section. Figure 1 illustrates this process and indicates the percentage of participants directed to different paths within the survey.

The initial section of the survey focuses on gathering metadata from participants, including information about their background, gender, age group, and other relevant demographics. This metadata provides valuable contextual information that aids in understanding the characteristics of the survey participants.

To ensure the reliability and credibility of the study results, it is important to address the question of sample size and its adequacy. In this research, data were collected through internet channels such as social media and forums from a total of seventy-three survey participants spanning nine countries and five distinct age groups.

By implementing a sampling strategy, the study aimed to ensure a diverse representation across different geographical locations and age groups. This intentional selection process aimed to capture a broad range of perspectives and experiences related to home automation. By including participants from various countries and age groups, the study was able to gather valuable insights that reflected the global nature of the smart home industry.

By conducting a survey-based study and gathering data from a diverse group of participants, the research aims at providing valuable insights that can inform future smart home development. The results obtained from the survey will be analysed and discussed in detail in Section IV, shedding light on the preferences, needs, and expectations of smart home users.

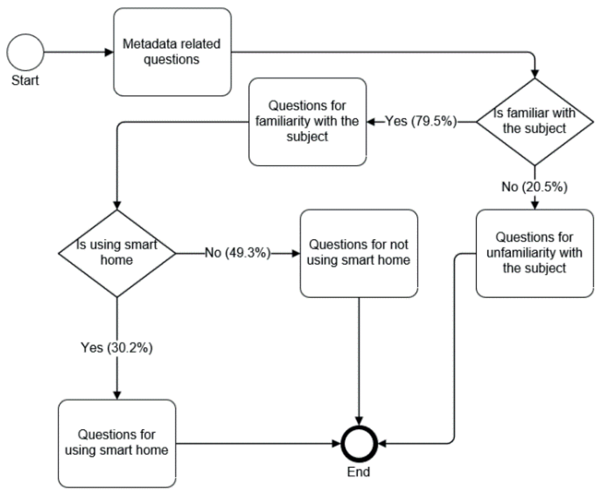

Fig. 1. Survey process and structure.

IV. Results

The current section of the research report is focused on addressing the research questions that were proposed at the beginning of the study. The section IV is divided into three sub-sections, each is dedicated to analysing and presenting the results of the survey that was conducted as part of the research.

Each of these sub-sections contains a variety of charts and tables that are designed to help visualize and interpret the data collected from the survey. These charts and tables are an important tool for presenting the findings of the research clearly and concisely, and they allow the reader to easily understand the key trends and patterns that emerged from the data.

In addition to presenting the survey results, the current section also includes detailed explanations and interpretations of the data, highlighting any notable trends or patterns that were identified. This is an important aspect of the research process, as it allows the researchers to draw conclusions and make recommendations based on the data collected. Overall, the current section is a crucial part of the research report, as it presents the findings of the study clearly and comprehensively which helps to provide insights and recommendations for future research or practice.

A. Who are the Smart Home Users? (RQ1)

Seventy-three people responded to the survey questions from nine different countries (Finland, Sweden, The Netherlands, Australia, India, Malaysia, the United States of America, Germany, and Russia) and most of them were in their 30s and 40s. In today's global market technology crossed boundaries and smart home systems are found in many places. The current study did not put any restrictions on the origin country of the participant. This section presents the survey results collected from the following countries. Additionally, Table I is set to present detailed information on the survey participants which is part of the answer to the first research question (RQ1).

TABLE I
Details about the Survey Participants

Gender	Age Group	Percentage of Participants
Female	Less than 20	0 %
	20–30	16.4 %
	31–40	26.0 %
	41–50	8.2 %
	Above 50	4.1 %
Male	Less than 20	0 %
	20–30	13.7 %
	31–40	23.3 %
	41–50	5.5 %
	Above 50	1.4 %
Prefer not to say	Less than 20	0 %
	20–30	1.4 %
	31–40	0 %
	41–50	0 %
	Above 50	0 %

Most of the participants are twenty to fourth years old. The presented results in Table I show that 54.8 % of the participants are female, 43.8 % are male, and 1.4 % preferred not to enclose their gender. The participants were also asked about their education level. 93.2 % of the participants have a university education:

- School – 1.4 %
- High school – 2.7 %
- Vocational school – 2.7 %
- University – 93.2 %

After processing the results, 34 unique professions were recognized. The professions /occupations then were divided into three categories: Information technology (IT), non-IT professions, and students. Table II presents results associated with professions.

TABLE II
PARTICIPANTS' PROFESSIONS (UNIQUE ENTRIES)

Profession Category	Number of Unique Entries	Example of Entries
IT professions	7	Software Developer, IT Professional, IT Consultant, etc.
Non-IT professions	25	Head of Sales, HR Professional, Banking, Kindergarten Teacher, etc.
Students	2	Doctoral student, etc.
Total of Unique Entries:	34	

In addition to the gender, age, education, and profession the survey inquired about participants' living arrangements. Figure 2 contains three charts that provide more details linked to this inquiry. Most of the entries belong to people who own their homes (41–100 m^2), which are placed in a town.

Smart Home Familiarity

The next section of the questionnaire was dedicated to finding out the level of familiarity of the participants linked to the research topic. 30.2 % of the people responded that they were extremely familiar or very familiar with the home automation topic. However, 20.5 % were completely unfamiliar with the topic. The participants were then instructed to explain their understanding of the topic (How do you define Home Automation?).

As seen in Fig. 3, some of the people (20.5 %) are unfamiliar with the research subject. The results do not show any particular age group participants from different age groups that have chosen the unfamiliarity option. It is important to know if they would like to know about home automation, which means they can be potential users in the future. Figure 4 shows the responses to the question (Would you like to learn more about Home Automation?) The question was specifically designed for the participants who are unfamiliar with the subject, which is 20.5 % of the total entries.

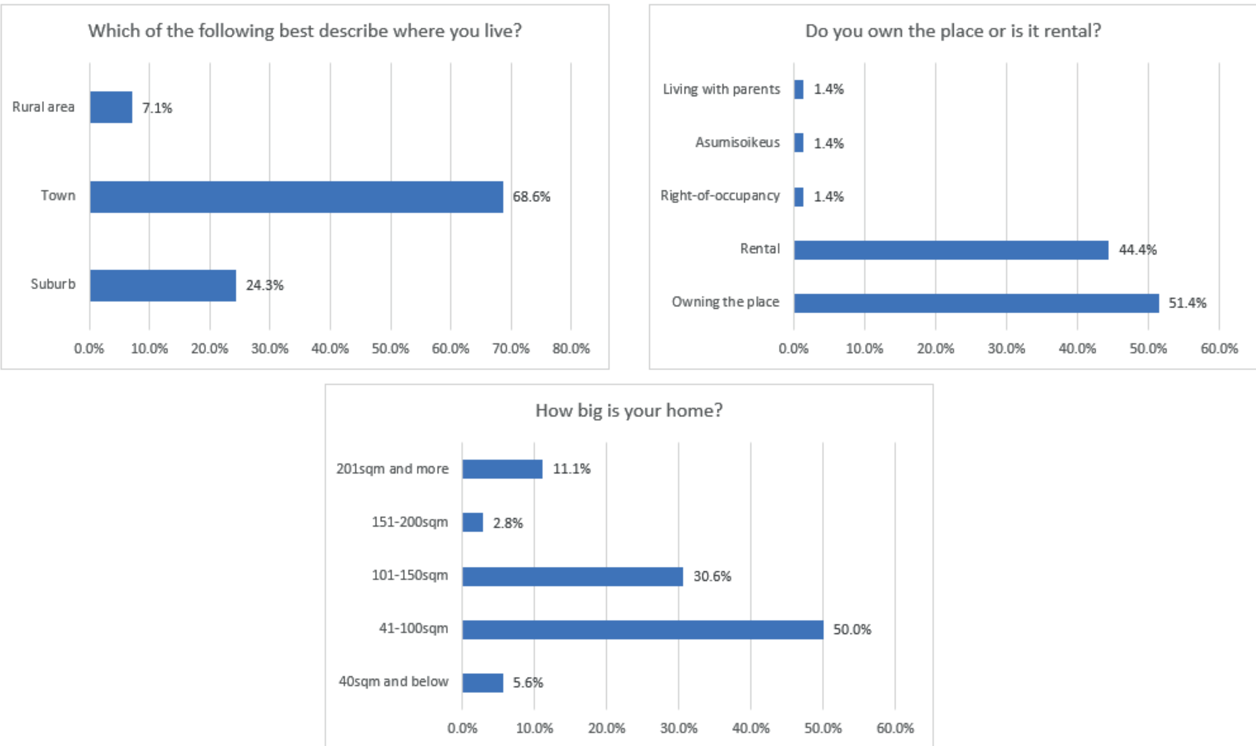

Fig. 2. Living arrangements of the participants.

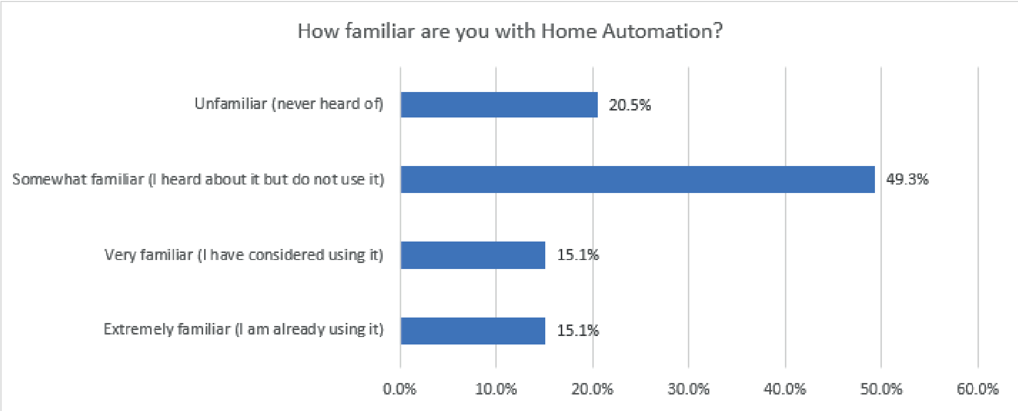

Fig. 3. How familiar are you with Home Automation?

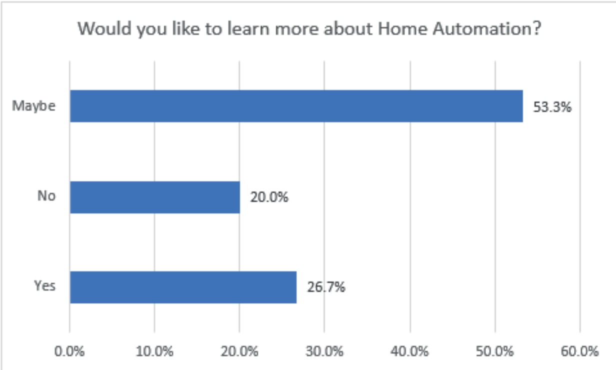

Fig. 4. Would you like to learn more about Home Automation?

B. What are the Desirable Home Automation Features? (RQ2)

The survey contains several open-ended questions related to participants' understanding of home automation and its desirable features. The current section is set to answer the second research question (RQ2) by summarising the results of the conducted survey. Concerning the definition of home automation for the survey participants the following categories were identified:

- Home automation is the ability to *remotely control and monitor* home appliances;
- *Resource management* is possible with smart home systems;
- Home automation is *task management* through technology;
- It means the ability to *automate daily tasks* without human intervention;
- Adding features to the home to ensure *security*.

The list above stresses five different categories and all the survey entries linked to the smart home definition can be linked to one of these categories: remote accessibility, resource management, task management, task automation, and security. It is interesting to point out that some people define a smart home as a means for task management without human intervention. Furthermore, according to the survey results, security and remote accessibility are inseparable parts of a smart home system. As explained earlier and shown in Fig. 1, the survey had different paths for people who were using smart home systems and the ones who were not using them. Figure 5 contains four questions; it shows the results of the questions related to smart home features and functionalities.

- Results that are marked with green and grey belong to people who are familiar with home automation but currently are not using it.
- Results that are marked with the orange and blue belong to people who are currently using home automation.

Participants could choose multiple items from the given list. Some interesting outcome is discovered when analysing Fig. 5. For example, 73.7 % of people who are familiar with smart home technology would like to have security as a functionality (marked with grey). Yet 74.3 % of people who are current users of home automation have security functions available. The importance of security for home automation is revealed here. According to Fig. 5, light management is a popular feature offered by the current home automation products. The green colour shows that 80 % of people who are familiar with home automation know the light management functionality and 85.7 % (marked with orange) of people have the light management functionality as part of their home automation system.

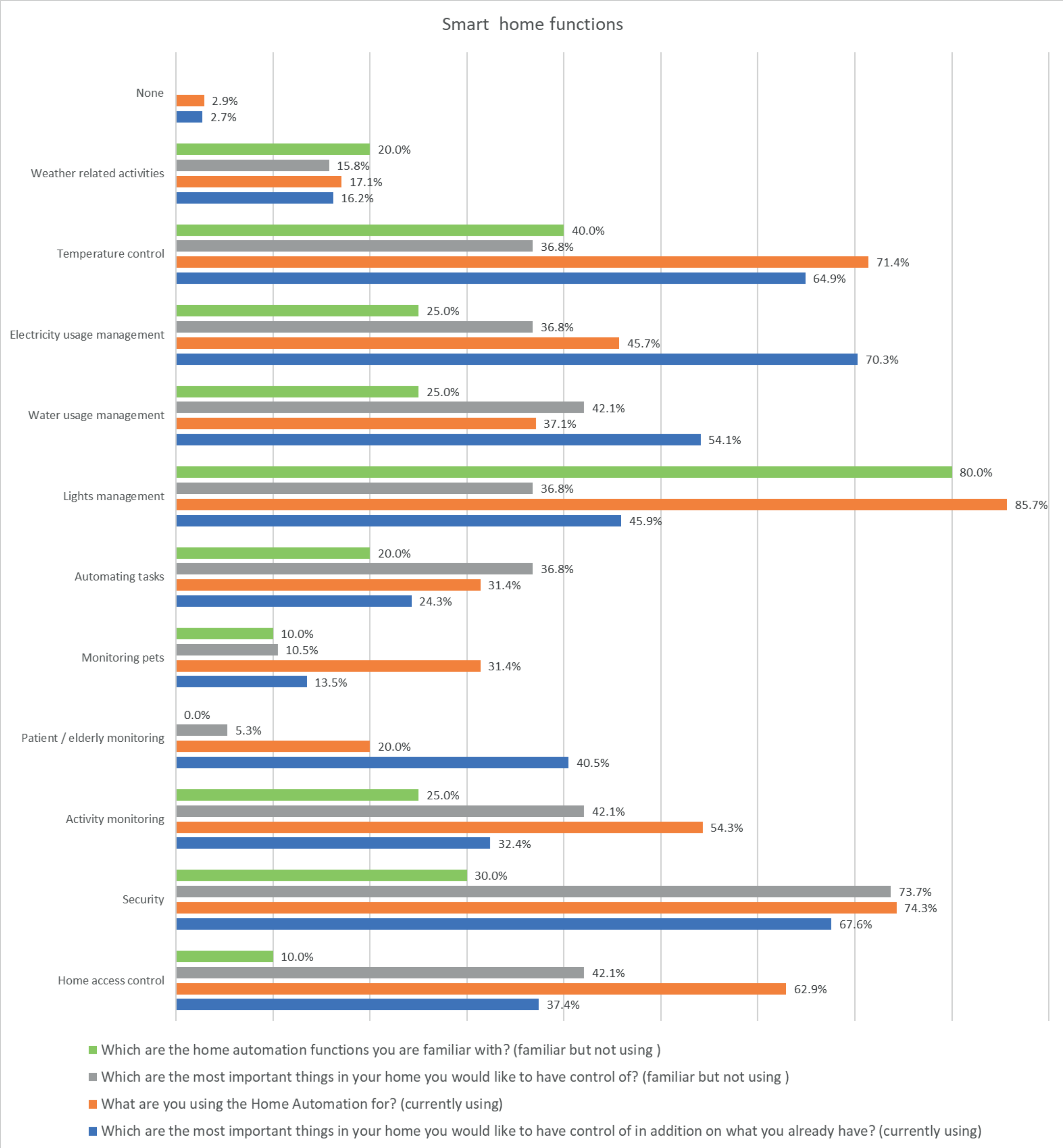

Fig. 5. Smart home functions.

Benefits and Drawbacks of Smart Home

The survey had dedicated sections for entries linked to the benefits and drawbacks of home automation systems. The answers are separated based on people who are using home automation currently and the ones who are familiar with the technology but not using it. The following two tables are summaries of the collected survey results.

TABLE III
ENTRIES OF PEOPLE WHO ARE FAMILIAR WITH HOME AUTOMATION BUT NOT USING IT

Question	Summary of responses
What are the benefits you expect from Home Automation?	Remote accessibility and monitoring; resource management; saving money; saving time; should be easy to use
What are the drawbacks you see in Home Automation?	Technology can be misused; security and privacy concerns; potential system failure; does not fulfil expectations; it is expensive; installation complexity

TABLE IV
ENTRIES OF PEOPLE WHO ARE CURRENTLY USING HOME AUTOMATION

Question	Summary of responses
What benefits have you experienced using Home Automation?	Saving energy; voice control; remote accessibility and monitoring; easy to use; security
What are the biggest drawbacks based on your experience while using Home Automation?	Hard to configure; expensive; it can make us lazy; kids can disable remote monitoring; security and privacy concerns; Integration and compatibility; system failure and reliability

C. The Monetary Value of Home Automation (RQ3)

Survey participants are divided into two groups to gain a better picture of the monetary value of home automation. The ones who are using home automation (63.8 %) and the ones who are not using the technology but are familiar with the subject (36.2 %). The current subsection has two subparts, the first part is dedicated to smart home users and the second part discusses the entries for the users who are not using smart homes but know the subject.

Users of Home Automation

The users of home automation have acquired the technology by purchasing it off the shelf or developing it on their own. The current survey study discovered a difference in money spent on these systems by the two groups. Figure 6 presents that 61.9 % have bought the systems off the shelf.

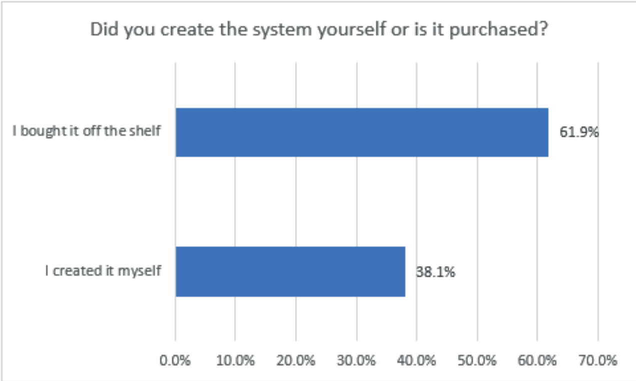

Fig. 6. Purchased it off the shelf or developed.

People who bought their products off the shelf have spent more; the results show that most of them paid approximately 100–500 euros to use the technology. Yet, most of the ones who created the system themselves have approximately spent 100–250 euros. Additionally, the survey asked both groups about the extra money they are ready to spend on home automation for enhancing it. Figures 7 and 8 are dedicated to presenting the results.

D. Non-users but Familiar with the Technology

Non-users were directed to answer questions linked to the monetary value of home automation. Figure 9 is set to present the results for the presented questions.

The current survey-based study, conducted among social media and internet users from nine different countries, has provided valuable insights into the preferences and needs of smart home users. In this section, we critically discuss the findings and implications of the study, focusing on key areas of interest for developers and start-ups in the smart home industry.

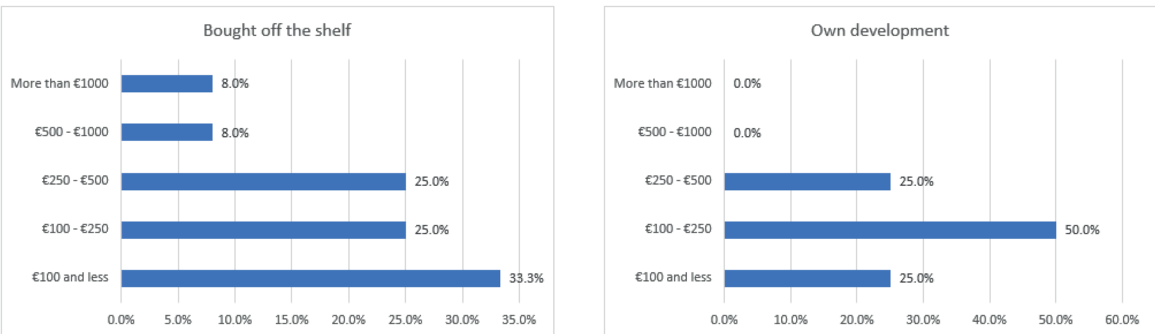

Fig. 7. Monitory value of home automation in use.

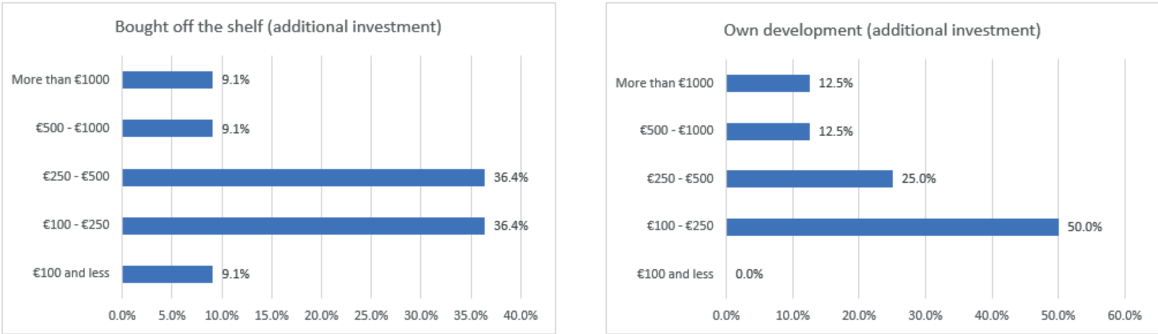

Fig. 8. Additional investment in home automation.

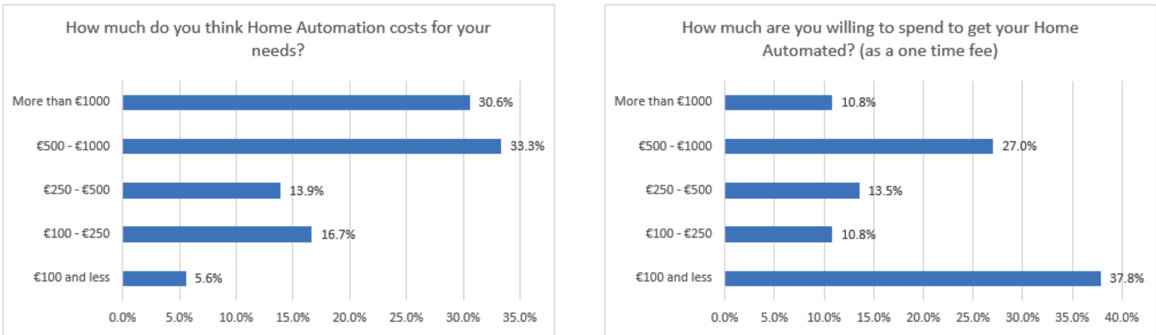

Fig. 9. Monitory value of home automation for non-users.

V. Critical Discussion

A. User Profile and Adoption

The study findings indicate that the majority of participants are university-educated individuals in their 30s and 40s living in rental accommodations. It is noteworthy that many respondents have heard about smart home technology but have not yet embraced it (Fig. 3). This represents a significant opportunity for developers to explore the barriers to adoption and design strategies to increase user acceptance. Future research efforts should delve deeper into understanding the specific reasons behind this hesitation and explore innovative ways to address them.

Recommendation
Developers should invest in targeted marketing campaigns and educational initiatives to raise awareness and alleviate concerns regarding smart home technology. Emphasising the practical benefits, such as increased security and convenience, can help overcome user scepticism.

B. User Needs and Desired Features

Regarding the desired features of smart home systems, the study findings reveal that simple automation features like light control are commonly used, while security features are highly desired (RQ2). However, participants expressed a desire for broader functionalities, including energy and water management as well as task automation (Figs. 5 and 6). These findings highlight the need for developers to prioritize and expand the range of features in their smart home products.

Recommendation
Developers should focus on enhancing the security aspects of smart home systems, as this remains a top priority for users. Additionally, integrating energy and water management functionalities, along with task automation capabilities, can enhance the overall user experience and appeal of smart home products.

C. Drawbacks and Concerns

While smart home products offer numerous benefits, this study also identified several drawbacks. Reliability and high costs were among the key concerns raised by participants. Additionally, users expressed worries about privacy and security issues associated with current smart home systems. These concerns should be addressed to foster user confidence and wider adoption, ensuring that smart home technology becomes more accessible and affordable for a broader range of consumers.

Recommendation
Developers should prioritize the development of reliable smart home systems by rigorously testing and improving product performance. Furthermore, addressing privacy and security concerns through robust data encryption, secure network protocols, and transparent data handling practices can instil trust among users.

D. Compatibility and Integration

The study findings suggest that the cost of smart home systems is often attributed to the lack of compatibility between products from different manufacturers and the complexity of installation (RQ3). Integrating smart home systems with existing household products and appliances can significantly reduce the need for costly upgrades.

Recommendation
Developers should strive for interoperability and standardization in the smart home industry. Collaborative efforts and partnerships among manufacturers can lead to more seamless integration of smart home systems with existing products, thereby reducing costs, and enhancing user experience.

E. Validity of the Results

This sub-section examines the validity of the results obtained in the survey-based research, focusing on four key aspects: construct validity, internal validity, external validity, and reliability.

Construct validity pertains to the accurate interpretation and measurement of theoretical constructs. The study ensured alignment with established definitions in the field when assessing constructs related to smart home development. Validated survey instruments and clearly defined variables were employed to enhance construct validity.

Internal validity concerns the study design and the extent to which the results can be attributed to the collected data. Rigorous data collection procedures, well-designed survey questions, and appropriate statistical analyses were employed to minimize the influence of confounding variables and enhance internal validity.

External validity addresses the generalizability of the research findings. The study sample consisted of 73 participants from 9 countries and 5 age groups, deliberately designed to ensure diversity. While caution is advised in generalizing the findings to the entire population, the study's approach enabled a comprehensive exploration of different perspectives and contributed to the understanding of smart home users.

Reliability focuses on the consistency and reproducibility of the study results. Standardized survey instruments with established reliability measures were employed, following best practices in survey design and implementation to enhance reliability. Transparency was maintained by making the survey instrument and data analysis code available for future replication.

In summary, although the sample size may appear modest, the deliberate sampling strategy aimed to capture diverse perspectives on smart home development. Limitations inherent in survey-based research, such as potential response bias and challenges in achieving a fully representative sample, were acknowledged. Nevertheless, careful data analysis and interpretation allowed for the identification of valuable patterns and trends. The study findings provide a foundation for further research and future efforts can consider expanding the sample size to strengthen the study conclusions.

VI. Conclusion

The fast advancement of technology can be overwhelming and keeping up with user requirements can be challenging for developers. The current survey-based study has been set to answer key questions linked to home automation development. What are the desirable features for the users and what is the monetary value they assigned to the requirements? The related work indicates clear demands from home automation users. Security, privacy, and price are among the most required concerns [5], [6]. Our research shows that DIY (do it yourself) systems have lower price tags than purchased ones. Furthermore, people who are not using smart home technology expect a higher price for the systems than their actual cost (the results are provided in Figs. 9–11).

In the end, the question is, what is the future of smart homes, does it even have a future, and is there enough interest? According to Fig. 1, most people are familiar with smart home technology, which means there is an interest in home automation. Yet, facts like privacy and security concerns and the potentially high price of such systems might reduce their usage. The authors' recommendation for start-ups is to conduct targeted and dedicated research about the potential customers and use cases. The current survey participants are from different age groups, genders, and nationalities. This can provide a better picture of the global market and its demands, which could be particularly beneficial for developers and start-ups.

References

[1] Fortune Business Insights, "Home automation market size, share and COVID-19 impact analysis," Report iD: FBI100074, 2022. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/home-automation-market-100074

[2] J. N. A. Brown, B. Kaufmann, F. J. Huber, K.-H. Pirolt, and M. Hitz, "'…Language in Their Very Gesture' First Steps towards Calm Smart Home Input," in *Human-Computer Interaction and Knowledge Discovery in Complex, Unstructured, Big Data*, vol. 7947, D. Hutchison *et al.*, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 256–264. https://doi.org/10.1007/978-3-642-39146-0_22

[3] J. Shin, Y. Park, and D. Lee, "Who will be smart home users? An analysis of adoption and diffusion of smart homes," *Technol. Forecast. Soc. Change*, vol. 134, pp. 246–253, Sep. 2018. https://doi.org/10.1016/j.techfore.2018.06.029

[4] A. Coskun, G. Kaner, and İ. Bostan, "Is smart home a necessity or a fantasy for the mainstream user? A study on users' expectations of smart household appliances," *Int. J. Des.*, vol. 12, Apr. 2018. http://www.ijdesign.org/index.php/IJDesign/article/view/2938

[5] A. Georgiev and S. Schlögl, "Smart home technology: An exploration of end user perceptions," 2018. [Online]. Available: https://www.researchgate.net/publication/327136969_Smart_Home_Technology_An_Exploration_of_End_User_Perceptions

[6] N. Guhr, O. Werth, P. P. H. Blacha, and M. H. Breitner, "Privacy concerns in the smart home context," *SN Appl. Sci.*, vol. 2, no. 2, Jan. 2020, Art. no. 247. https://doi.org/10.1007/s42452-020-2025-8

[7] M. R. Reisinger, S. Prost, J. Schrammel, and P. Fröhlich, "User requirements for the design of smart homes: dimensions and goals," *J. Ambient Intell. Humaniz. Comput.*, May 2022. https://doi.org/10.1007/s12652-021-03651-6

[8] A. Abi Sen and N. Bahbouh, "A novel cost-efficient framework for smart home creation," in *2021 8th International Conference on Computing for Sustainable Global Development (INDIACom)*, India, Jun. 2021. https://www.researchgate.net/publication/352261572_A_Novel_Cost-efficient_Framework_for_Smart_Home_Creation

[9] C. Wilson, T. Hargreaves, and R. Hauxwell-Baldwin, "Smart homes and their users: a systematic analysis and key challenges," *Pers. Ubiquitous Comput.*, vol. 19, no. 2, pp. 463–476, Feb. 2015. https://doi.org/10.1007/s00779-014-0813-0

[10] S. Chang and K. Nam, "Smart home adoption: The impact of user characteristics and differences in perception of benefits," *Buildings*, vol. 11, no. 9, Sep. 2021, Art. no. 393. https://doi.org/10.3390/buildings11090393

[11] B. Eggen, E. van den Hoven, and J. Terken, "Human-centered design and smart homes: How to study and design for the home experience?" in *Handbook of Smart Homes, Health Care and Well-Being*, J. van Hoof, G. Demiris, E. Wouters, Eds. Cham: Springer International Publishing, 2017, pp. 83–92. https://doi.org/10.1007/978-3-319-01583-5_6

[12] Y. Zhai, Y. Liu, M. Yang, F. Long, and J. Virkki, "A survey study of the usefulness and concerns about smart home applications from the human perspective," *Open J. Soc. Sci.*, vol. 2, no. 11, pp. 119–126, Nov. 2014. https://doi.org/10.4236/jss.2014.211017

[13] R. Rasheed, A. Ahmed, and F. Bukhari, "A survey base study about the effectiveness of smart home applications in Pakistan," in *2018 International Conference on Engineering and Emerging Technologies (ICEET)*, Lahore, Pakistan, Feb. 2018, pp. 1–5. https://doi.org/10.1109/ICEET1.2018.8338640

Ashkan Yaldaie is an accomplished principal engineer with a background in the Information Technology industry. He obtained a B.Sc. in Business Information Technology from Haaga-Helia University and an M.Sc in Computer Science from LUT University. Currently, Ashkan is pursuing a PhD in Computer Science, demonstrating his commitment to advanced research and academic excellence.
E-mail: ashkan.yaldaie@student.lut.fi
ORCID iD: https://orcid.org/0000-0002-8726-2825

Jari Porras is a D.Sc (Tech) Professor at Lappeenranta-Lahti University of Technology (LUT). He specializes in Software Engineering, particularly Distributed Systems. With extensive experience in research and supervision, his work focuses on parallel and distributed computing, wireless and mobile systems, and sustainable ICT.
E-mail: jari.porras@lut.fi
ORCID iD: https://orcid.org/0000-0003-3669-8503

Olaf Drögehorn is a Professor of Software Engineering and Internet Technologies and Rector for Information and Communication Technologies and E-Learning at Harz University of Applied Sciences. He serves as Vice Chairman of the Wireless World Research Forum working group for Services and Service Architectures and is a member of the ICT Advisory Board of the German state of Saxony-Anhalt.
E-mail: odroegehorn@hs-harz.de

A. APPENDICES
A.1. SURVEY QUESTIONS

Home Automation Usage
What is your gender?
How old are you?
What is your profession?
What is the level of your education?
What is the field of your education (if applicable)?
Country, where do you live?
Which of the following best describes where you live?
Do you own the place or is it a rental?
How big is your home?
How familiar are you with Home Automation?
What does Home Automation mean to you?

Unfamiliar with the subject
Would you like to learn more about Home Automation?

Familiar with the subject
Are you using any Smart technology or Home Automation technology now?

Not using Home Automation
Why are you not using the Home Automation technology?
Which are the subjects for home automation you are familiar with?
Which are the most important things in your home you would like to have control of?
What are the benefits you expect from home automation? (You may list several items)
What are the drawbacks you see in Home Automation? (You may list several items)
How much do you think Home Automation costs for your needs?
How much are you willing to spend to get your Home Automated? (As a one-time fee)
Thanks for participating in this survey. Please provide your e-mail address if you agree to have an interview about the subject.

Using Home Automation
What are you using the Home Automation for?
What benefits have you experienced using Home Automation?
What are the biggest drawbacks based on your experience while using Home Automation?
Did you create the system yourself or is it purchased?
How much have you paid for your existing Home Automation?
Which are the most important things in your home you would like to have control of in addition to what you already have?
How much more are you willing to invest in your Home Automation?
Thanks for participating in this survey. Please provide your e-mail address if you agree to have an interview about the subject.

Publication III

Yaldaie, A., Porras, J., and Drögehorn, O.
Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices

Asian Journal of Computer Science and Technology
Volume 13, No. 1, 2024, pp. 27–40

Asian Journal of Computer Science and Technology
ISSN: 2249-0701 (P); 2583-7907 (E)
Vol.13 No.1, 2024, pp.27-40

www.crijournals.org
DOI: https://doi.org/10.70112/ajcst-2024.13.1.4260

Innovative Home Automation with Raspberry Pi: A Comprehensive Approach to Managing Smart Devices

Ashkan Yaldaie[1], Jari Porras[2] and Olaf Drögehorn[3]
[1&2]LUT University, Lappeenranta, Finland
[3]Harz University of Applied Sciences, Wernigerode, Germany
E-mail: ashkan.yaldaie@student.lut.fi
(Received 3 March 2024; Revised 23 March 2024; Accepted 13 April 2024; Available online 18 April 2024)

***Abstract* - As our homes become increasingly interconnected with smart devices, managing this technological complexity has never been more challenging. In response, this paper outlines an innovative approach to home automation using the versatile Raspberry Pi platform to address the unique needs of modern households. The research adopts a design science approach, starting with a thorough analysis of the challenges associated with the growing number of smart devices. The need to manage and control these devices drives the development of effective solutions. Various designs are considered, leading to the selection of the Raspberry Pi due to its flexibility and capability to integrate different smart devices into the automation process. To provide a comprehensive solution that simplifies device management and benefits users, the development process includes both hardware and software components. Additionally, a rigorous testing program is implemented to ensure that the system meets key requirements such as security, privacy, energy efficiency, and user-friendliness. The system's effectiveness is evaluated through real-world applications, which helps identify potential areas for improvement and iterative enhancement.**
***Keywords:* Smart Home, Home Automation, IoT, Remote Monitoring, Home Security, Energy Efficiency**

I. INTRODUCTION

The reliance of modern homes on smart gadgets is growing [1], presenting several issues, including the difficulty of controlling and monitoring these devices, concerns about security and privacy [2], [3], and the potential for inefficient energy use [4], [5]. This research offers a unique solution to these problems by using the Raspberry Pi to build a home automation system. Created by the Raspberry Pi Foundation, the Raspberry Pi is a small, credit card-sized computer designed to be an accessible and affordable platform for various DIY projects and educational purposes. Despite its small size and low cost, the Raspberry Pi offers remarkable computational capability, making it a great option for applications like home automation [6].

In this research, we investigate how a Raspberry Pi can be seamlessly integrated with a range of sensors to create a comprehensive system that enhances home automation. Our methodology incorporates considerations for security, privacy, energy efficiency, and user experience, demonstrating how this integration can result in a smarter and safer home for homeowners.

A. Problem Statement

The number of smart devices in homes is growing rapidly. In 2020, the global market for smart home devices was valued at USD 78.3 billion [7]. This value is expected to reach USD 135.3 billion by 2025. This growth is driven by several factors, including the increasing availability of affordable smart devices, the rising popularity of smart home platforms, and the growing demand for convenience and security [7]. While the use of smart devices offers numerous benefits, it also introduces some challenges. One of the most significant challenges in smart home systems is the complexity of managing and monitoring the diverse array of devices. With numerous devices in use, keeping track of their connections, activities, and security can be daunting. Typically, these systems rely on a central hub for device control and monitoring. However, they often exhibit certain limitations, including:

1. They can be expensive
2. They can be difficult to set up and use
3. Devices from different manufacturers may not always be compatible

Security and privacy are two significant concerns associated with the use of smart devices. These devices are typically connected to the internet, making them vulnerable to cyberattacks. Additionally, the data collected by smart devices can be exploited to track user behaviour and habits, raising valid privacy concerns. Finally, the use of smart devices can lead to energy waste. Many smart devices are designed to remain always on, even when not in use, resulting in unnecessary energy consumption that can negatively impact the environment [3].

B. Research Questions

The following research questions will be addressed in this study:

- RQ1. How can a Raspberry Pi-based home automation system effectively prioritize security, privacy, and energy efficiency?
- RQ2. What Metrics and Methods can be used to Assess the Effectiveness of this System in Improving User Experience and Reducing Energy Consumption?

The first research question (RQ1) addresses the key challenges of designing and developing a home automation system that ensures both the physical security of the house and the cybersecurity of the system itself, while also maintaining energy efficiency and user engagement. Security is a major concern for many people regarding home automation systems, as cybersecurity threats pose risks such as unauthorized access, data theft, or potential physical harm through device manipulation. Additionally, privacy concerns arise from the extensive data that home automation systems can collect on users' habits and activities [2], [8].

The second research question (RQ2) aims to measure the impact of a home automation system on users' lives. Such a system can enhance the overall user experience by simplifying device control and automating tasks. It can also reduce energy consumption by turning off lights and appliances when they are not in use, thereby saving money on energy bills and reducing the environmental impact of home energy use. By addressing these questions, this paper provides valuable insights into the design, development, and effectiveness of home automation systems. This information can be utilized to improve the security, privacy, energy efficiency, and user experience of these systems.

C. Methodology

The methodology employed in this study adheres to the principles of Design Science Research (DSR). DSR is a structured approach used to develop and evaluate innovative artifacts, such as systems or solutions, to address specific real-world problems. In this research, DSR provides the foundation for creating and assessing an integrated smart home security and resource management system.

The research process unfolds through a series of structured phases.

1. *Problem Identification:* The research begins with the identification of a pertinent real-world problem, which is the multifaceted need for contemporary homeowners to enhance home security, optimize resource consumption, and improve the overall user experience.
2. *Artifact Design and Development:* In response to the identified problem, an innovative artifact is designed and developed. This artifact constitutes the integrated smart home security and resource management system. The design process entails a comprehensive exploration of hardware and software components, with a focus on security, resource management, and user experience.
3. *Evaluation:* The system undergoes rigorous evaluation to assess its effectiveness in addressing the identified problem. Evaluation criteria encompass enhanced home security, resource management, and user experience.
4. *Reflection and Communication:* The research findings, including insights derived from the design, development, and evaluation of the system, are thoughtfully reflected upon. The outcomes and contributions are then effectively communicated through this research paper.

D. Research Contributions

It is imperative to note that the methodology employed in this study combines the systematic rigor of design science with a practical focus on addressing real-world challenges. By following this methodology, the research endeavors to create a valuable and innovative contribution to the fields of home automation, security, and resource management.

Design Science provides a robust framework for crafting a novel system that not only fulfills user requirements but also confronts prevailing challenges [9]. This paper serves as an indispensable guide for developers seeking to devise pragmatic solutions for end-users. In this context, our primary focus is not only on the development of a comprehensive home automation system but also on guiding others, ensuring that our goal extends beyond creating a system, but also serves as a valuable guide for those who wish to undertake similar endeavors.

II. RELATED WORK

In this section, the existing literature and research related to Raspberry Pi-based home automation systems, with a particular emphasis on security, privacy, and energy efficiency, are explored. The research discusses innovative systems and their contributions, vulnerabilities within the Raspbian operating system, as well as insights into user profiles, needs, and recommendations. This exploration provides essential groundwork for the Design Science Research approach, guiding the development of an enhanced product.

A. Raspberry Pi-Based Home Automation Systems

In recent years, there has been a significant surge in interest regarding the use of Raspberry Pi for creating home automation systems. The Raspberry Pi, an affordable single-board computer, is exceptionally well-suited for this purpose. Its user-friendly setup and extensive compatibility with a wide range of smart devices make it an attractive choice. One of the primary advantages of using this single-board computer in do-it-yourself (DIY) projects is its ability to enable the creation of highly personalized solutions tailored to individual requirements. This includes integrating cameras, various sensors, and GSM (mobile communications) devices into the Raspberry Pi, allowing it to handle a variety of tasks. Kumar *et al.,* present compelling evidence of how these sensors and devices, as shown in Fig. 2, can be leveraged to develop a home surveillance system [10].

Home automation systems place security and privacy at the forefront, as emphasized by a systematic literature review in the field [3]. This comprehensive analysis underscores users' deep concerns about protecting their private data, particularly given the inherent security vulnerabilities in smart home systems [2], [11], [12]. Additionally, the same body of research consistently highlights users' strong desire for efficient resource management, especially in the realm of electricity usage, as a potential way to reduce household expenses [4], [5]. Considering these concerns and needs, developers must prioritize allocating ample resources to strengthen the security features of home automation devices. Importantly, the enhancement of security should be a central consideration from the very beginning of the development process, starting with the planning and design phases. This proactive approach ensures that vulnerabilities are systematically identified and addressed, minimizing potential risks throughout the device's lifecycle [3].

B. Innovative Raspberry Pi-Based Systems

Shruti and Pallavi's home automation system represents an impressive fusion of smart surveillance and energy management, effectively addressing the twin concerns of security and resource optimization in contemporary households [13]. A standout feature of their system is the smart energy meter, which meticulously monitors and stores electricity consumption data. This empowers users with insights to make informed decisions, ultimately leading to reduced energy usage and lower household expenses. Additionally, their system offers remote accessibility, allowing users to conveniently control lighting, thereby enhancing both convenience and energy efficiency.

On the security front, their smart surveillance system records images when motion is detected. This dual-purpose feature acts as a deterrent to potential intruders and provides homeowners with a visual record of unusual activities. For real-time monitoring, users can access a live feed of their homes via the Pi Camera, a high-quality camera module designed for use with Raspberry Pi single-board computers. Despite their impressive prototype, Shruti and Pallavi recognize areas for future improvement, including refining the user interface, expanding remote control capabilities, and integrating advanced algorithms. Their work showcases the potential of seamlessly combining resource management and security in home automation [13].

In the realm of Raspberry Pi devices, Nadafa *et al.,* have pushed boundaries by introducing a security system with human detection capabilities, thereby reducing false security alerts triggered by motion detection [14]. Their innovative work extends to a smart mirror capable of delivering personalized messages to users, effectively enhancing both user experiences and home security measures. Nadafa and their team acknowledge the need for advanced programming expertise to optimize the system's performance and suggest that future iterations could address this limitation by implementing training mechanisms to distinguish legitimate users from potential intruders.

Teja *et al.,* focus their paper on safeguarding loved ones and valuables in household settings, recognizing the dynamic landscape of research and development in IoT applications for home security [15]. To address concerns about potential system compromise, they propose an innovative solution centred around the integration of four essential sensors: the Piezo sensor, IR sensor, PIR sensor, and Sound sensor. These sensors collectively enhance the system's ability to detect and respond to intrusions effectively.

At the core of Teja's system is the Raspberry Pi controller, which orchestrates the functions of these sensors with its 40 GPIO pins. This seamless integration allows for comprehensive threat detection, continuously monitoring the entire floor for any signs of movement. Once an intruder is detected, the sensors promptly capture images and videos, which are transmitted to the Raspberry Pi controller. This controller, with an Internet connection, relays this crucial information to the homeowner for remote assessment.

Furthermore, Teja *et al.,* emphasize the role of IoT technology in user interaction by integrating IoT Cloud for a graphical user interface (GUI) [15]. This GUI delivers real-time alerts and presents captured data, enhancing user-friendliness and accessibility. The paper also outlines potential enhancements, including delay alarms and advanced photo recognition technology, to reduce false alarms and increase system sensitivity for a more robust and reliable home security solution.

C. Operating System Security

In the paper authored by Le *et al.,* the researchers delve into the realm of operating system security, with a particular focus on Raspbian-OS for Raspberry Pi devices [16]. They underscore the significance of addressing vulnerabilities in Raspbian-OS, given the widespread use of Raspberry Pi across diverse applications. Identified vulnerabilities include default username and password combinations, software and hardware bugs, issues in various Raspbian-OS releases, and the susceptibility of secure shell (SSH) keys to attacks, all of which raise concerns about unauthorized access and potential data breaches.

To mitigate these vulnerabilities and enhance the security of Raspberry Pi-based systems, the authors propose several practical recommendations. They emphasize the immediate change of default credentials upon Raspbian-OS installation, replacing them with strong, unique username and password combinations. Regular software updates and patches are also suggested to rectify known bugs and security flaws. Additionally, the paper advocates for the implementation of strong authentication methods and the use of public key infrastructure (PKI) to enhance SSH key management. These proactive measures significantly reduce the likelihood of unauthorized access and safeguard sensitive data, fortifying Raspberry Pi-based devices in IoT environments [16].

In the paper authored by Sainz-Raso *et al.,* the researchers explore the security challenges associated with Raspberry Pi in the context of IoT [17]. They highlight that, despite its advantages, Raspberry Pi's reliance on operating systems exposes it to potential software vulnerabilities, and they discuss hardware limitations resulting from cost-cutting design choices during production. The paper meticulously analyzes various hardware and software vulnerabilities linked to different operating systems running on Raspberry Pi devices, emphasizing the importance of securing these systems in unprotected IoT environments.

To mitigate the identified vulnerabilities and enhance the security of Raspberry Pi-based systems, the authors propose a set of best practices. They recommend changing passwords immediately after installation and securing public services, especially when Raspberry Pi is exposed to the Internet. The analysis reveals that some default installations have unsecured services like FTP and HTTP, which can grant unauthorized access to attackers. The authors suggest removing unnecessary public services and advocate for secure configurations to minimize risks. In conclusion, the paper provides valuable insights into securing Raspberry Pi devices, benefiting engineers, developers, and designers working with this popular platform in various IoT applications [17].

D. User Profile and Adoption Concerns in Smart Home Technology

A recent survey-based study provides valuable insights into user profiles, adoption trends, and needs in the context of smart home technology [2]. The study reveals that the majority of participants are individuals in their 30s and 40s with university-level education, typically residing in rental accommodations. Although many respondents have heard of smart home technology, a significant number have not fully embraced it, indicating an opportunity for developers to explore the barriers to adoption. Future research is recommended to investigate the reasons behind this hesitation and to develop innovative strategies to address these concerns.

To promote adoption, developers are encouraged to invest in targeted marketing campaigns and educational initiatives that emphasize practical benefits such as increased security and convenience. The study also examines user needs and desired features in smart home systems. It notes that simple automation features, such as light control, are commonly used, while security features are highly desired. Participants expressed a desire for broader functionalities, including energy and water management, as well as task automation. This underscores the need for developers to prioritize and expand the range of features in their smart home products. Enhancing security aspects, integrating energy and water management functionalities, and enabling task automation can improve the overall user experience and appeal of smart home products [2].

Surveys [2], [18] identify participants' concerns related to reliability, high costs, privacy, and security issues associated with current smart home systems. This highlights the importance of developers prioritizing product reliability, addressing cost concerns, and enhancing privacy and security measures to build user confidence and encourage wider adoption. Furthermore, studies emphasize the significance of compatibility and integration of smart home systems with existing household products and appliances to reduce costs and enhance the user experience. Developers are urged to work towards interoperability and standardization in the smart home industry through collaborative efforts and partnerships among manufacturers.

In conclusion, studies provide a foundation for further research in the field of smart home development, addressing construct validity, internal validity, external validity, and reliability while acknowledging its limitations. They shed light on user preferences and potential areas for improvement in smart home technology, offering valuable guidance to developers in this evolving industry [2], [18].

E. Research Gaps

The extant body of literature offers valuable insights into various aspects of Raspberry Pi-based home automation systems. However, there is a significant research gap, as no comprehensive study currently addresses the interrelated domains of security, privacy, energy management, and user experience. The existing body of work predominantly focuses on discrete elements or specific facets of home automation, leaving a gap where a comprehensive investigation of these crucial dimensions is lacking.

It is uncommon to find research in the current literature that integrates the themes of security, privacy, energy efficiency, and user-friendliness in the context of Raspberry Pi home automation. While individual studies address specific topics such as user profiles [2], innovative systems [13], and operating system security [16], [17], the overall picture remains unclear. In summary, the existing research landscape does not provide the holistic investigation needed. The current study aims to bridge these dimensions, offering a richer understanding and contributing to the development of smarter, more efficient homes.

III. SYSTEM IMPLEMENTATION

The related work in the field of home automation systems has highlighted several key aspects. Researchers and developers have predominantly focused on two major areas: the development of new features and the enhancement of cybersecurity and data privacy. These two facets have been pivotal in shaping the evolution of home automation systems [3]. This paper aims to bridge the gap between these domains by creating a comprehensive system that integrates security features and data privacy measures while considering effective resource management. This approach recognizes the multifaceted needs of modern homeowners, who seek not only convenience but also assurance of a secure and efficient home environment.

The existing literature provides insights into the current landscape of home automation, showcasing innovative solutions that emphasize security and resource management. For example, Shruti and Pallavi's system [13], which integrates smart surveillance and energy metering, demonstrates the potential for seamlessly merging these aspects. Furthermore, the importance of addressing vulnerabilities in operating systems, as highlighted by Le *et al.,* and Sainz-Raso *et al.,* underscores the critical role of cybersecurity in the context of IoT devices like Raspberry Pi [16], [17].

This research aims to synthesize security, data privacy, and resource management, making a significant contribution to the field of home automation. By combining these elements, our work has the potential to create a more holistic and user-centric approach to smart homes, addressing the concerns and needs identified in the literature.

A. System Design

In this section, the system design phase of the research, guided by the principles of Design Science Research (DSR), is presented. The primary objective of this phase is to engineer a comprehensive home automation system that meets the overarching goals of this paper. In line with DSR principles, the aim is to create a novel system that not only addresses user requirements but also tackles existing challenges.

TABLE I OBJECTIVES

Integrating Privacy and Energy Monitoring	The first objective is to seamlessly integrate smart surveillance features with energy metering within the home automation system. This integration is crucial for addressing security and resource management in modern homes, providing users with the ability to monitor their homes through surveillance features while also efficiently managing their energy usage.
Fortifying Cybersecurity	The second objective is to fortify the security features of the home automation system. There is an acute awareness of the security vulnerabilities in smart home systems, and the aim is to proactively address these concerns. Security is a top priority [3], to ensure that vulnerabilities are identified and addressed systematically, minimizing potential risks throughout the device's lifecycle.
Enhancing Usability and Adoption	The third objective revolves around enhancing the user experience and addressing user concerns regarding smart home technology adoption. Recognizing the importance of user-centric design, the aim is to create a system that is not only secure and efficient but also user-friendly, encouraging wider adoption.

TABLE II PRINCIPLES

Modularity and Scalability	The design emphasizes modularity and scalability to allow for flexibility in expanding and customizing the system as per users' needs. The system's architecture is designed to accommodate additional components and functionalities.
User-Centric Design	User needs and preferences are prioritized, ensuring that the system is intuitive and easy to use. User-friendliness is a central focus throughout the design process.
Security by Design	Security is integrated into the system's design from the outset, following security best practices to minimize vulnerabilities and protect users' data and privacy.
Energy Efficiency	Incorporating energy-efficient components and features is a fundamental aspect of the design, aiming to help users optimize their energy consumption and reduce household expenses.

B. Hardware Setup

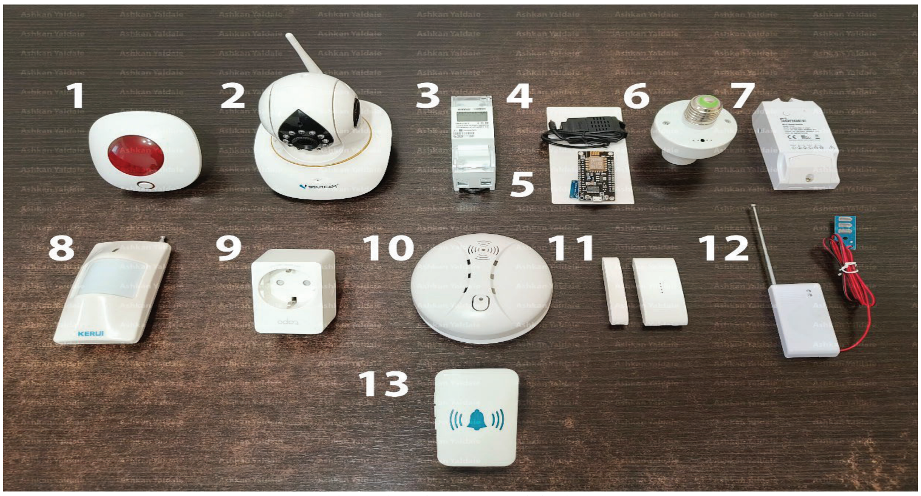

Fig.1 List of sensors and devices

1. Siren
2. IP Camera
3. Smart Electricity Counter
4. Temperature and Humidity Sensor
5. NodeMCU Board
6. Light bulb control device
7. Temperature and Humidity Sensor connector for transmitting the data
8. Motion Sensor
9. Remote Socket
10. Smoke Detector
11. Door Sensor
12. Water Leak Sensor
13. Doorbell Sensor

The hardware setup for this research project, as shown in Fig. 1, centers around the Raspberry Pi 3 Model B. This model was deliberately chosen due to its exceptional combination of processing power, memory, and versatile connectivity options. The selection of this model underscores our commitment to establishing a robust and efficient security system that seamlessly integrates user experience and resource management. This section provides a comprehensive exploration of the various hardware components meticulously integrated into our system, highlighting their crucial roles within the overarching framework.

1. *Motion Sensors:* Motion sensors are strategically placed throughout the premises to detect movements and trigger corresponding actions. Raspberry Pi 3 Model B interfaces with these sensors to receive real-time data.
2. *Remote Sockets:* Remote sockets, or smart plugs, enable remote control of electronic devices. They are integral to efficient resource management and can remotely activate lights and other home equipment.
3. *IP Cameras:* IP cameras serve dual roles, enhancing both home security and surveillance capabilities. Raspberry Pi connects to these cameras via the local network to capture and process video data.
4. *Smoke Detector:* A smoke detector is integrated into the system to enhance the smart home system. It promptly detects the presence of smoke, potentially signaling a fire hazard. Raspberry Pi is configured to receive and respond to signals from the smoke detector, triggering appropriate alerts and actions.
5. *Secure Housing for Raspberry Pi and Accessories:* To ensure the security and reliability of Raspberry Pi and its accompanying accessories, robust housing is utilized. This housing safeguards the components against physical harm and unauthorized access while maintaining a controlled environment for optimal performance.
6. *Incorporating GSM Modem for Security Alerts:* To ensure timely security alerts, a GSM modem is integrated into the system. This modem provides cellular connectivity, enabling the Raspberry Pi 3 Model B to send SMS notifications directly to the user in the event of a security intrusion, especially when Wi-Fi connectivity is unavailable. SMS is a text messaging service component of most mobile phones.
7. *NodeMCU Boards as Radio Frequency (RF) Signal Extenders:* To address limitations in RF signal coverage, strategically placed NodeMCU boards serve as signal extenders within the premises. These boards act as intermediaries, effectively expanding the RF communication range between the Raspberry Pi and other devices.
8. *Smart Electricity Counter for Resource Management:* Efficient resource management is facilitated through the integration of a smart electricity counter. This device tracks electricity consumption, providing valuable data for optimizing resource utilization.
9. *Temperature and Humidity Sensors:* These are integral components designed to monitor environmental conditions within the premises. These sensors provide real-time data on temperature and humidity levels, which are critical for user comfort. The system can adjust environmental settings, such as heating or cooling, based on this data, ensuring an optimal living environment and, in turn, enhancing user experience.
10. *Doorbell Sensor:* Further enhances home security and user convenience. This sensor is designed to detect and respond to doorbell rings. When triggered, it alerts the system, allowing for immediate user notification. This feature not only enhances security but also contributes to the overall user experience by providing a convenient way to monitor visitors and deliveries.
11. *Water Leak Sensors:* Water leak sensors are strategically placed to detect the presence of water in areas prone to leaks or flooding. These sensors promptly alert the system, helping to prevent water damage.
12. *Siren:* To provide an audible alert in case of security breaches or emergencies, a siren is integrated into the system. When triggered, the siren emits a loud alarm, alerting occupants and potentially deterring intruders. The siren adds a layer of security to the overall system.
13. *Door Sensors:* Door sensors are strategically placed at entry points throughout the premises. These sensors detect the opening of doors, providing crucial information about access points. Raspberry Pi interfaces with these sensors, promptly receiving status updates on door activities. The inclusion of door sensors enhances both security and user awareness, allowing the system to monitor and alert users to any unauthorized entry, thereby reinforcing the overall security posture.

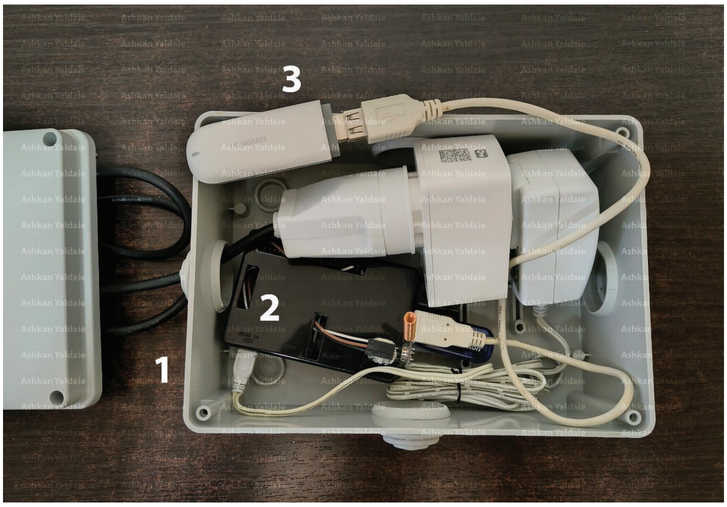

Fig. 2 Raspberry Pi and accessories

1. Secure Housing for Raspberry Pi and Accessories
2. The Raspberry Pi
3. Incorporating GSM Modem for Security Alerts

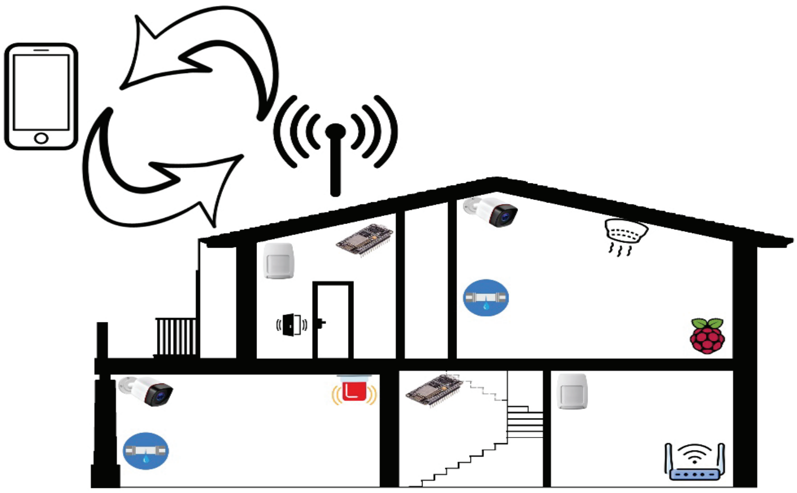

Fig. 3 Sensor placement in the house: a visual overview

In Fig. 3, a rough representation illustrates the placement of various house sensors, while Figs. 1 and 2 present lists of devices and accessories, accompanied by relevant illustrations. It is important to note that the communication infrastructure within the system plays a crucial role in ensuring seamless data transmission between the sensors and the central processing unit, the Raspberry Pi 3 Model B. In this context, radio frequency (RF) signals serve as the primary means of communication for most of the deployed sensors. To address the inherent limitations of RF signal range, NodeMCU boards have been strategically positioned within the premises. These NodeMCU boards function as signal extenders, effectively amplifying and expanding the RF communication range, thereby ensuring robust and uninterrupted data exchange between the sensors and the Raspberry Pi.

Additionally, it is essential to recognize that certain components within the system rely on Wi-Fi connectivity to communicate with the Raspberry Pi. Notably, IP cameras, the smart electricity counter, and temperature and humidity sensors utilize Wi-Fi technology for data transmission. This choice is driven by the specific requirements of these components, such as the need for higher bandwidth and the advantages of seamless integration into existing local area networks.

By harnessing Wi-Fi connectivity for these select devices, the system ensures efficient data conveyance to the central processing unit, contributing to the overall functionality and effectiveness of the integrated smart home security and resource management system.

C. The Software

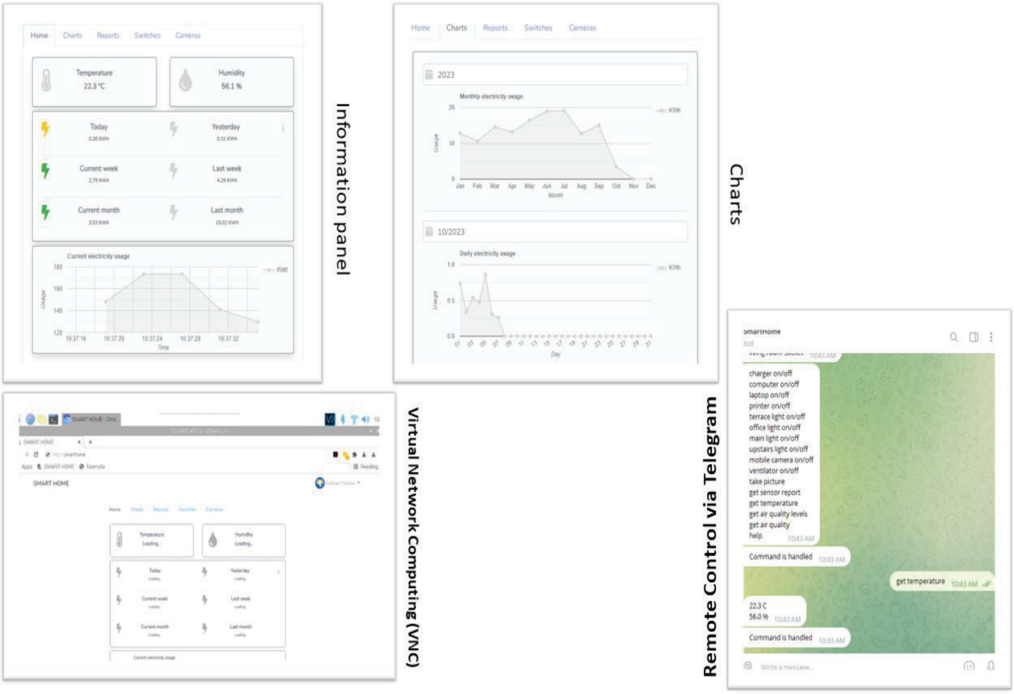

Fig. 4 Software in use

Fig. 4, titled "Software in Use," contains visual representations that showcase the practical application of the software within the system. As detailed in the preceding section, a diverse array of sensors and devices constitutes integral components within the system's architecture. This section shifts focus to the software development aspects that form the foundation for the effective integration and utilization of these sensors and devices. Specifically, it explores two key facets: system security and functionality. The first facet of this section is dedicated to system security. In an era where data breaches and cyber threats are persistent concerns, ensuring the utmost protection of user data and privacy is imperative. The intricacies of the cybersecurity measures implemented in the system - including encryption protocols, access controls, and intrusion detection mechanisms - will be thoroughly examined. The second goal of this section is to provide a comprehensive examination of the system's functionality.

This includes a detailed analysis of the operational aspects that facilitate the seamless integration and collaboration among the various sensors and devices. Additionally, it covers user interface and user experience considerations, highlighting how the system's design enhances user interaction and satisfaction. Furthermore, this section offers insights into the system's adaptability and scalability, elucidating how the architecture supports future expansions and modifications to maintain robustness and relevance in evolving technological landscapes. Finally, it addresses the system's performance metrics and optimization techniques, showcasing its commitment to achieving optimal resource utilization while maintaining high levels of efficiency and reliability.

1. System Security

Ensuring the cybersecurity of the Raspberry Pi-based security and automation system is of utmost importance for safeguarding both the device and the sensitive data it processes. In today's interconnected world, where cyber threats are pervasive, taking proactive measures to fortify the security of such systems is imperative. This section will delve into the comprehensive steps and best practices used to configure the Raspberry Pi with cybersecurity as a primary concern, providing a solid foundation for a resilient security infrastructure.

a. *Secure Operating System Installation:* The first critical step in securing your Raspberry Pi is the installation of a secure operating system. The authors have meticulously chosen Raspbian, the official Raspberry Pi OS, as the primary option. Selecting a minimal, hardened, and regularly updated distribution from official sources is essential. This approach minimizes the risk associated with compromised downloads and ensures the integrity of the system from the very outset.
b. *Modification of Default Credentials:* Following the installation phase, the authors have taken an additional step to fortify the system by modifying default credentials. Default usernames and passwords are known weak points in security. Robust and unique credentials have been adopted for accessing the Raspberry Pi, ensuring they are not easily guessable or common. This measure significantly raises the bar against potential unauthorized access attempts.

c. *Firewall Implementation:* The significance of implementing a firewall cannot be underestimated. In the ever-connected world of IoT devices, the Raspberry Pi requires a vigilant guardian in the form of a properly configured firewall. In this case, Uncomplicated Firewall (UFW) is the tool of choice. It is skillfully used to configure specific rules that restrict access exclusively to essential services, thereby minimizing exposure to potential threats.
d. *Regular Software Updates:* Security is a continuous journey, and regular software updates play a pivotal role in this ongoing process. The authors have made it a point to consistently apply security updates by keeping the operating system and software packages up to date. Automated update checks and installations have been configured to ensure timely patching and reduce vulnerabilities arising from outdated software.
e. *Enhancement of SSH Security:* SSH (Secure Shell) is employed for remote access, the default SSH port is modified to a non-standard value. Additionally, key-based authentication is configured in place of password-based authentication for heightened security.
f. *Intrusion Detection and Monitoring:* To truly fortify the security posture of the system, Intrusion Detection and Monitoring have been put into place. Robust intrusion detection systems (IDS) and monitoring tools continuously scrutinize system activity for signs of suspicion. Tools like Fail2ban automatically thwart repeated failed login attempts, further solidifying the system's resilience against potential threats.

By rigorously following these cybersecurity practices during the Raspberry Pi setup process, the system's security posture can be significantly strengthened. This enhancement serves as a robust defense against potential threats and vulnerabilities. It underscores the indispensable need for vigilant monitoring and continuous security updates in the ever-evolving landscape of cybersecurity, ensuring the safety of sensitive data and the integrity of the Raspberry Pi-based security system.

2. Remote Accessibility and Monitoring

The discussion in this section centers on the setup for controlling and monitoring the system. It explores the mechanisms employed to facilitate remote interaction with the home automation system, emphasizing the paramount importance of both security and usability. The implementation of various remote-control options, including Telegram integration, Virtual Network Computing (VNC), and a web-based user interface (UI), is meticulously examined.

These solutions are designed to provide users with seamless access to the system's functionalities while maintaining robust security measures. Additionally, the usability aspects of these choices are considered to ensure that user interactions with the system remain intuitive and efficient. By comprehensively addressing the setup for remote control and monitoring, this section underscores the commitment to delivering a holistic, user-centric, and secure home automation experience.

i. Remote Control via Telegram

Security Perspective	**Usability Perspective**
Remote control capabilities are an integral facet of our Raspberry Pi-based home automation system. To facilitate remote control while maintaining robust security, we have implemented Telegram integration. Telegram, a secure instant messaging platform, serves as the conduit for users to interact with the system from afar. Importantly, this choice aligns with our commitment to safeguarding the local network by avoiding the need to open any additional ports for external access. Telegram's inherent security features bolster the system's defense against unauthorized access. It employs end-to-end encryption for all communication, ensuring that messages exchanged between users and the system remain confidential.	Usability remains a pivotal concern in the design of our home automation system. Telegram's chat interface simplifies user interactions, reducing the learning curve for new users. Additionally, Telegram's cross-platform compatibility ensures that users can control the system from various devices, further enhancing usability. The system empowers users to monitor electricity usage, providing real-time insights into energy consumption. Users can seamlessly turn off devices remotely, promoting energy efficiency. Moreover, the system integrates temperature monitoring capabilities, allowing users to adjust heating or cooling systems based on real-time temperature data. This dual functionality not only enhances user convenience but also contributes to sustainable and energy-efficient living.

ii. Virtual Network Computing (VNC)

Security Perspective	**Usability Perspective**
Virtual Network Computing (VNC) serves as an additional component for remote system management. From a security standpoint, VNC incorporates password-based authentication to ensure that only authorized users can access the system remotely. Additionally, stringent access control measures are in place to limit the scope of remote interactions. Users must provide valid credentials to establish a VNC connection, further reinforcing security.	From a usability perspective, VNC offers a versatile solution for remote control. It enables users to access the system's graphical user interface (GUI) as if they were physically present, facilitating seamless interaction with the home automation system. This approach ensures a consistent and familiar user experience, which is especially valuable for tasks that require visual feedback or configuration adjustments.

iii. Web User Interface (UI)

Security Perspective	Usability Perspective
The web user interface (UI) is employed as an additional method for remote system management. From a security standpoint, it requires user credentials for access and operates within the local network without the need for port forwarding or exposure to external networks. This localized approach significantly reduces the system's attack surface, mitigating potential external threats.	The web UI provides a local control option for users within the network. It offers a simplified interface accessible through web browsers, allowing users to manage the system without needing VNC client software. This web-based approach enhances usability, particularly for users who prefer a browser-based interface.

3. Home Security Functionality

The home security functionality of the system comprises two key modes: Automatic Security and Continuous Security. When Automatic Security is activated, the system arms itself when the user(s) leave the house. This mode utilizes Bluetooth and Wi-Fi technology to monitor the physical presence of the user's phones, determining whether they are inside the house. By recognizing the absence of authorized devices, the system ensures that security measures are in place to safeguard the premises. In the interest of respecting user privacy, significant precautions have been taken regarding the security cameras.

When Automatic Security mode is active and the user(s) are at home, the security cameras are completely disconnected from the electrical supply. This deliberate action ensures that, during times when the system detects the presence of authorized users within the premises, the cameras are rendered inoperative. By cutting off their power, the system mitigates any potential privacy concerns that may arise from unintentional recording or monitoring while users are present.

This approach underscores the system's commitment to balancing security with the preservation of user privacy. Additionally, Continuous Security mode operates as an ongoing security measure, remaining armed until manually deactivated via the web interface. This persistent protection ensures that the property is consistently monitored, even when users are at home. To enhance security further, the system sends email notifications and SMS alerts to the user in the event of intrusion detection. These alerts provide timely awareness of potential security breaches. Alongside these notifications, a siren is activated to emit a Loud alarm, alerting occupants and potentially deterring intruders. The system also stores security camera clips of the intrusion, securely saving them in both local storage and Google Drive. This redundancy ensures that crucial evidence of security incidents is preserved and accessible, contributing to a comprehensive security posture.

4. Resource Management

The integrated smart home security and resource management system offers a range of functionalities designed to optimize resource consumption and enhance user awareness. These functionalities include dynamic control of devices based on temperature and specific timeframes, the generation of electricity usage reports, real-time monitoring of electricity consumption, and a traffic light system for comparative analysis.

A key feature of the resource management system is its ability to intelligently control devices based on temperature and specific timeframes. Users also have the flexibility to manually switch devices on or off using the provided on/off switches in the Web UI and through Telegram control. This dual functionality allows the system to automatically adjust devices for optimal energy use and user comfort while providing manual control for personalized adjustments. The system further supports detailed electricity usage reporting, offering users a comprehensive view of their consumption patterns. These reports include informative charts for selected timeframes, enabling users to gain insights into their energy utilization. Real-time monitoring is facilitated through a live chart, allowing users to track their electricity consumption as it occurs.

To enhance user awareness, the system features a traffic light system that compares current usage with historical data. This visual cue system uses colors that change from green to yellow and red based on usage compared to the previous day, week, and month. This intuitive feature helps users make informed decisions about their energy consumption and encourages energy-efficient practices. Additionally, the system includes a leaderboard that displays monthly electricity usage, fostering a sense of community and healthy competition. Users can choose avatars to represent themselves on the leaderboard, adding a personalized touch. This feature not only motivates users to conserve energy but also promotes data sharing and collaborative efforts toward sustainable living. The system leverages ThingSpeak, an open-source software for communication with internet-enabled devices. ThingSpeak is used to store and retrieve monthly usage data, providing a secure and accessible platform for sharing usage information.

IV. EVALUATION

The integrated smart home security and resource management system underwent rigorous evaluation to assess its performance, functionality, and usability in real-world scenarios. This evaluation process involved a series of tests conducted in a home environment, simulating various conditions to validate the system's effectiveness.

A. Security Evaluation

The Automatic Security mode, designed to activate when users leave their homes, underwent thorough testing. By leveraging Bluetooth signals from smartphones for user presence detection, the system consistently activated upon user departure, demonstrating robust detection capabilities. Notably, it exhibited a commendable ability to minimize false alarms when users were present, significantly enhancing the user experience.

Individual assessments of the intrusion detection mechanisms, including motion sensors and door sensors, were conducted to ensure prompt and accurate identification of unauthorized entry. The system reliably triggered alerts via email notifications and SMS messages, providing timely awareness of potential security breaches. Additionally, the integration of a siren in response to intrusions was validated, strengthening the overall security posture.

The innovative power management approach, which involves disconnecting security cameras from electricity when users are at home, was rigorously evaluated, particularly regarding its impact on user privacy. The deliberate disconnection during the Automatic Security mode ensured that security cameras remained inactive in the presence of users, effectively addressing potential privacy concerns.

B. Resource Management Evaluation

The resource management aspects of the integrated smart home security system underwent comprehensive testing to evaluate their effectiveness, usability, and impact on user experience. Real-time monitoring of electricity consumption proved effective, providing users with live data during periods of high electricity prices. This capability empowered users to make informed decisions about device usage, contributing to energy efficiency. The traffic light system, which indicates usage compared to historical data, offered an intuitive visual cue for regulating energy consumption.

The intelligent device control, based on temperature and predefined timeframes, demonstrated efficacy in optimizing resource utilization. Users could remotely turn off devices, even when away from home, contributing to energy efficiency during peak pricing periods.

The remote-control capabilities via Telegram, VNC, and the web-based UI were evaluated for usability and responsiveness, providing users with flexible and secure options for managing their smart home environment. Additionally, the leaderboard feature, which promotes a sense of achievement by comparing electricity usage to previous months, successfully added a gamified element through customizable avatars and monthly rankings.

C. Additional Tests

The range of radio frequency (RF) signals to reach the Raspberry Pi was tested in various locations within the home. This ensured that all sensors utilizing RF communication, including NodeMCU boards, operated within the required range, maintaining robust and uninterrupted data exchange. Each sensor - such as motion sensors, temperature and humidity sensors, door sensors, and water leak sensors - underwent individual testing. This approach ensured the reliability and accuracy of each sensor in detecting specific environmental conditions or events.

V. CRITICAL DISCUSSION

In this section, we conduct a critical examination of our integrated smart home security and resource management system, guided by the principles of Design Science Research (DSR). Our research aims to address the multifaceted needs of modern homeowners, prioritizing security, resource management, and user experience. We scrutinize the system's design, functionality, and contributions to the broader field of home automation, all while addressing the two core research questions posed in this study.

A. Research Question 1: How can a Raspberry Pi-Based Home Automation System Effectively Prioritize Security, Privacy, and Energy Efficiency?

Our integrated system significantly enhances home security through a combination of automatic and continuous security functions. The Automatic Security mode ensures that the system is armed when users leave their homes. This mode uses Bluetooth and Wi-Fi signals from user smartphones to determine their presence within the house. If users are not detected, the system activates, thereby fortifying the home's security. Notably, this approach reduces the likelihood of false alarms when users are present, improving the overall user experience.

Regarding security, the system employs intrusion detection mechanisms, email notifications, SMS alerts, and stores security camera clips both locally and on Google Drive. These robust security measures act as formidable deterrents to potential intruders and provide homeowners with timely awareness of security breaches. Additionally, the inclusion of a siren adds an audible layer of protection, boosting user confidence in the system's ability to secure their homes. The system's comprehensive approach to security also includes advanced cybersecurity features, as detailed earlier. By adhering to best practices-such as secure operating system installation, modification of default credentials, firewall implementation, regular software updates, SSH security enhancements, and intrusion detection and monitoring - the system ensures the utmost protection of user data and privacy. These cybersecurity measures form a solid foundation for a resilient security infrastructure, reinforcing the overall security posture of the integrated smart home security and resource management system.

An innovative aspect of the system's design is its power management approach, which prioritizes user privacy. When Automatic Security mode is active and users are at home, the security cameras are completely disconnected from the electricity. This feature addresses privacy concerns while maintaining vigilant security when users are away.

B. Research Question 2: What Metrics and Methods can be used to Assess the Effectiveness of this System in Improving User Experience and Reducing Energy Consumption?

Resource management is a critical aspect of our integrated system, providing a range of functionalities that empower users to optimize resource consumption. Users can intelligently control devices based on temperature and predefined timeframes, enhancing energy efficiency and contributing to cost savings. The system offers real-time monitoring of electricity consumption, complemented by a traffic light system that provides a comparative analysis of usage trends. This visual representation simplifies user awareness and decision-making, aligning with the principles of Design Science by offering intuitive feedback.

Additionally, the leaderboard feature fosters healthy competition among users to reduce electricity usage. This gamification element, which includes customizable avatars and user rankings, encourages active participation in resource management efforts. We have utilized ThingSpeak to store and retrieve monthly usage data, promoting user engagement and community sharing of usage information.

VI. CONCLUSION

In this study, we introduced an integrated smart home security and resource management system designed to meet the diverse needs of contemporary homeowners. Our exploration of the system's hardware and software components has provided insights into its architecture, demonstrating its potential to enhance home security and optimize resource utilization. It is noteworthy that our system is meticulously designed with an awareness of the constraints outlined in the related work section. The system's core strength lies in its ability to enhance home security through a combination of automatic and continuous functions. The Automatic Security mode uses Bluetooth signals to detect user presence, fortifying the home's security posture when users are away. This approach minimizes false alarms when residents are at home, contributing to an improved user experience. Additionally, intrusion detection mechanisms, email notifications, SMS alerts, and secure storage of security camera clips-both locally and in Google Drive-form a robust security ecosystem. The inclusion of a siren further augments security measures, instilling confidence in the system's ability to protect homes. Notably, the system also addresses user privacy by disconnecting security cameras from electricity when Automatic Security mode is active, and users are present at home. Cybersecurity remains a paramount consideration in the system's design, with stringent measures implemented to safeguard user data and privacy. The system adopts secure operating system installation, credential modification, firewall implementation, regular software updates, SSH security enhancement, and intrusion detection mechanisms to establish a resilient security infrastructure. In terms of resource management, the system offers dynamic device control based on temperature and specific timeframes, generates electricity usage reports, provides real-time monitoring, and employs a traffic light system for comparative analysis. These functionalities empower users to make informed decisions about resource consumption, potentially leading to cost savings and increased efficiency. To validate the practicality and effectiveness of our system, we deployed it in a real-world test environment. This validation phase allowed us to observe the system's performance in diverse scenarios, ensuring its effectiveness in the complexities of an actual home environment. However, we acknowledge certain limitations. Future iterations should consider that comprehensive home security ideally begins during the construction phase. Vulnerabilities, such as exposed electricity boxes that intruders can exploit to disable security systems, must be addressed. Innovative solutions, such as connecting critical components to power banks, may be necessary despite potential higher costs. A more holistic approach to securing vital infrastructure around electricity boxes is imperative for robust home security. In conclusion, our integrated smart home security and resource management system represents a significant advancement in meeting the evolving needs of homeowners. By combining advanced security measures with resource management capabilities, the system offers enhanced convenience, efficiency, and peace of mind for users. As technology continues to evolve, both homeowners and developers must prioritize security and resource management to create safer, more sustainable living environments.

REFERENCES

[1] R. El-Azab, "Smart homes: potentials and challenges," *Clean Energy*, vol. 5, no. 2, pp. 302–315, Jun. 2021, doi: 10.1093/ce/zkab010.

[2] A. Yaldaie, J. Porras, and O. Drögehorn, "Who are Smart Home Users and What do they Want? – Insights from an International Survey," *Appl. Comput. Syst.*, vol. 28, no. 1, pp. 114-124, Jun. 2023, doi: 10.2478/acss-2023-0011.

[3] A. Yaldaie, J. Porras, and O. Drögehorn, "The Present State of Home Automation: A Systematic Literature Review," *Int. J. Hybrid Innov. Technol.*, vol. 2, no. 1, pp. 23-46, Oct. 2022, doi: 10.21742/ijhit.2653-309X.2022.2.1.03.

[4] R. Rasheed, A. Ahmed, and F. Bukhari, "A survey base study about the effectiveness of smart home applications in Pakistan," in *2018 International Conference on Engineering and Emerging Technologies (ICEET)*, Feb. 2018, pp. 1-5, doi: 10.1109/ICEET1.2018.8338640.

[5] M. Z. Fakhar, E. Yalcin, and A. Bilge, "A survey of smart home energy conservation techniques," *Expert Syst. Appl.*, vol. 213, p. 118974, Mar. 2023, doi: 10.1016/j.eswa.2022.118974.

[6] X. Wen and Y. Wang, "Design of smart home environment monitoring system based on raspberry Pi," in *2018 Chinese Control*

And Decision Conference (CCDC), Jun. 2018, pp. 4259-4263, doi: 10.1109/CCDC.2018.8407864.

[7] R. and Markets, "Global Smart Home Healthcare Market (2020 to 2025) - Growth, Trends and Forecasts," 2021. [Online]. Available: https://www.globenewswire.com/en/news-release/2021/01/06/21544 42/28124/en/Global-Smart-Home-Healthcare-Market-2020-to-2025-Growth-Trends-and-Forecasts.html

[8] J. I. I. Araya and H. Rifà-Pous, "Anomaly-based cyberattacks detection for smart homes: A systematic literature review," *Internet of Things*, vol. 22, p. 100792, Jul. 2023, doi: 10.1016/j.iot.2023. 100792.

[9] A.-K. Carstensen and J. Bernhard, "Design science research – a powerful tool for improving methods in engineering education research," *Eur. J. Eng. Educ.*, vol. 44, no. 1-2, pp. 85-102, Mar. 2019, doi: 10.1080/03043797.2018.1498459.

[10] V. A. Kumar, V. Nandalal, M. Kousalya, P. Madhumitha, R. Kamaleshwari, and N. K. Selvi, "Implementation of Smart Home Assistance and Surveillance," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, Mar. 2021, pp. 1117–1121, doi: 10.1109/ICACCS51430.2021. 9442055.

[11] N. Pattnaik, S. Li, and J. R. C. Nurse, "A Survey of User Perspectives on Security and Privacy in a Home Networking Environment," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1-38, Sep. 2023, doi: 10.1145/3558095.

[12] D. Brand, F. D. DiGennaro Reed, M. D. Morley, T. G. Erath, and M. D. Novak, "A Survey Assessing Privacy Concerns of Smart-Home Services Provided to Individuals with Disabilities," *Behav. Anal. Pract.*, vol. 13, no. 1, pp. 11-21, Mar. 2020, doi: 10.1007/s40617-018-00329-y.

[13] S. Dash and P. Choudekar, "Home Automation using Smart Devices and IoT," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO)*, Sep. 2021, pp. 1-5, doi: 10.1109/ICRITO5 1393.2021.9596533.

[14] R. A. Nadafa, S. M. Hatturea, V. M. Bonala, and S. P. Naikb, "Home Security against Human Intrusion using Raspberry Pi," *Procedia Comput. Sci.*, vol. 167, pp. 1811-1820, 2020, doi: 10.1016/j.procs. 2020.03.200.

[15] P. A. Teja, A. A. F. Joe, and V. Kalist, "Home Security System using Raspberry PI with IOT," in *2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE)*, Mar. 2021, pp. 450-453, doi: 10.1109/ICACITE51222. 2021.9404551.

[16] C. Le, A. M. Grande, A. Carmine, J. Thompson, and T. Khan Mohd, "Analysis of Various Vulnerabilities in the Raspbian Operating System and Solutions," in *2022 IEEE World AI IoT Congress (AIIoT)*, Jun. 2022, pp. 01-06, doi: 10.1109/AIIoT54504.2022. 9817202.

[17] J. Sainz-Raso, S. Martin, G. Diaz, and M. Castro, "Security Vulnerabilities in Raspberry Pi–Analysis of the System Weaknesses," *IEEE Consum. Electron. Mag.*, vol. 8, no. 6, pp. 47-52, Nov. 2019, doi: 10.1109/MCE.2019.2941347.

[18] M. Ghafurian, C. Ellard, and K. Dautenhahn, "An investigation into the use of smart home devices, user preferences, and impact during COVID-19," *Comput. Hum. Behav. Reports*, vol. 11, p. 100300, Aug. 2023, doi: 10.1016/j.chbr.2023.100300.

Publication IV

Yaldaie, A., Porras, J., and Drögehorn, O.
User Perceptions of a Home Automation System: A TAM-Based Evaluation

Applied Computer Systems
Volume 30, No. 1, 2025, pp. 98–104

Applied Computer Systems
ISSN 2255-8691 (online)
ISSN 2255-8683 (print)
2025, vol. 30, no. 1, pp. 98–104
https://doi.org/10.2478/acss-2025-0012
https://content.sciendo.com

User Perceptions of a Home Automation System: A TAM-Based Evaluation

Ashkan Yaldaie[1*], Jari Porras[2], Olaf Drögehorn[3]
[1,2]*LUT University, Lappeenranta, Finland*
[3]*Harz University of Applied Sciences, Wernigerode, Germany*

Abstract **– The study explores user perceptions of a newly developed home automation system, using the Technology Acceptance Model (TAM) as a theoretical framework to guide the evaluation. The system includes advanced features for security, energy efficiency, and user convenience. It was tested in three different residential environments to evaluate its adaptability. Participants interacted with the system in a controlled laboratory setting and completed a structured survey. The study examines core TAM constructs – perceived ease of use, perceived usefulness, and behavioural intention – alongside additional factors such as trust and privacy concerns. The results highlight strong user satisfaction and intention to adopt the system, while also identifying areas for improvement, particularly in privacy assurance and device control. The findings offer practical recommendations for developers to enhance usability, transparency, and user trust. The research contributes to the smart home literature by demonstrating TAM's applicability to real-world systems and by providing insights into the practical and user-centred factors that influence technology acceptance.**

Keywords **– Energy efficiency, home automation, home security, IoT, remote monitoring, smart home, TAM.**

I. Introduction

The rapid advancement of smart technologies has transformed the landscape of home automation, offering users unprecedented control over various aspects of their living environments, such as lighting, security, heating, and entertainment systems. These innovations have not only increased convenience but also promised energy efficiency and enhanced security. Despite the potential benefits, the adoption of home automation systems remains inconsistent, with varying levels of acceptance among users. Understanding the factors that influence this acceptance is critical for the continued development and successful deployment of such technologies [1], [2].

The Technology Acceptance Model (TAM), developed by Davis in 1989, has been widely employed to examine user acceptance of new technologies. The model identifies two primary factors – perceived usefulness and perceived ease of use – that influence users' decisions to adopt technology. TAM has proven effective across various technological domains, from information systems to mobile applications, making it a suitable framework for evaluating home automation systems [3], [4].

This paper examines the application of the Technology Acceptance Model (TAM) in the context of a newly developed home automation system. The system, designed with features such as energy management, enhanced security, and user-centric automation, evolved through multiple iterations based on thorough research, which involved gathering requirements and conducting an international survey to identify the key preferences of modern smart home users. The system was tested in three distinct environments: one apartment, one studio, and one detached house. These varied test environments provided critical insights into its flexibility and functionality, demonstrating the system's adaptability across different living situations [5]–[7].

The home automation system offers a comprehensive set of features designed to enhance convenience, security, and energy efficiency. A leaderboard gamifies energy consumption, encouraging users to adopt more sustainable habits. The system supports time- and temperature-based scheduling for precise control of devices, ensuring comfort and energy savings. Security is a priority, with encrypted private and public key login to protect user data, and mechanisms to monitor and block suspicious login attempts, preventing unauthorized access. Users can control the system remotely through multiple methods, ensuring flexibility and reliability. Alerts are seamlessly delivered to users, even in offline scenarios, enhancing safety and awareness. The user-friendly interface simplifies navigation, making advanced features accessible to everyone. Additionally, the system enables energy consumption monitoring and supports integration with various brands and technologies, including Tuya, Orvibo, TP-Link, Sonoff, VStarcam, Blink, and multiple radio frequency sensors, ensuring compatibility with a wide range of devices [5]. For a detailed demonstration of the system's features and functionality, please refer to the footnote link[2].

By applying TAM in this context, the research aims to contribute to the growing body of literature on smart home technology adoption, offering insights into the psychological

[*] Corresponding author's e-mail: ashkan.yaldaie@student.lut.fi
Article received 2025-04-16; accepted 2025-07-01
[2] https://zenodo.org/records/14809262

and practical factors that drive user acceptance. These findings are particularly relevant for developers, designers, and stakeholders in the smart home industry who seek to create more user-friendly, widely adopted systems. The remainder of this paper is structured as follows: Section 2 reviews the literature on the Technology Acceptance Model and its applications in home automation. Section 3 outlines the research methodology. Section 4 presents the results and analysis. Section 5 provides a critical discussion of the findings and their implications, along with recommendations for future work. Section 6 concludes the paper.

This study contributes to the field by applying TAM to a fully developed home automation system, evaluated across three distinct residential environments. Although user interaction has been conducted in a controlled laboratory setting, the system's real-world deployment provides a strong foundation for assessing user perceptions. While much of the existing research has focused on conceptual models or survey-based evaluations, this study offers empirical insights through direct user engagement with a functioning system. It also extends TAM by incorporating trust and privacy concerns, and by examining underexplored features such as energy consumption gamification. These contributions provide practical guidance for developers and researchers aiming to bridge the gap between theoretical frameworks and real-world smart home adoption.

II. Literature Review

The Technology Acceptance Model (TAM) has been a fundamental framework for understanding the factors that drive technology adoption since Davis introduced it in 1989. Grounded in theories of reasoned action and planned behaviour, TAM simplifies the evaluation of user acceptance by focusing on two primary constructs: perceived usefulness (PU) and perceived ease of use (PEOU). Over time, TAM has been adapted and expanded across various technological domains, offering valuable insights into how users interact with different systems [3].

As home automation technologies have advanced, TAM has become increasingly relevant. Smart devices and the Internet of Things (IoT) now allow for the automation of household tasks, including lighting, security, and climate control. These technologies, while innovative, require broad user acceptance to fully integrate into everyday life. However, adoption rates have varied, depending on users' perceptions of the technology [8].

Many studies have investigated the factors influencing the adoption of home automation systems, with TAM frequently serving as a foundational framework. While perceived usefulness and perceived ease of use remain central, additional factors, such as trust in the system, privacy concerns, and the simplicity of use, have emerged as critical in determining user acceptance in home environments. This literature review consolidates existing research on TAM and its application to home automation, highlighting the primary factors that impact user decision-making [9], [10].

In the sections that follow, the core elements of TAM are discussed, along with key extensions and their relevance to home automation. This review also explores additional influences, such as privacy concerns and the perceived security of these systems, which play an increasingly important role in the context of smart home technology adoption.

In their paper, Yonghee Kim et al. integrate the Technology Acceptance Model with the Value-based Adoption Model (VAM) to explore the adoption of IoT-based smart home services. The study highlights that perceived value, influenced by perceived benefits and sacrifices, plays a crucial role in adoption decisions. TAM's core constructs, such as perceived usefulness and ease of use, are extended by incorporating factors like privacy risk and innovation resistance. This comprehensive approach provides a nuanced understanding of how users evaluate and decide to adopt smart home technologies, emphasizing the importance of balancing benefits with potential risks and sacrifices [10].

The paper written by Ahmed Shuhaiber and Ibrahim Mashal investigates the factors influencing the acceptance and usage of smart homes. By extending TAM to include trust, awareness, enjoyment, and perceived risks, the study provides a comprehensive analysis using the Structural Equation Modelling based on the Partial Least Squares approach. The findings reveal that trust, awareness, and enjoyment significantly impact users' attitudes towards smart homes, affecting their intention to use them. Additionally, perceived risks negatively influence trust. The study highlights the importance of educating users and ensuring the trustworthiness of smart home technologies to enhance adoption rates. This research offers valuable insights for smart home providers aiming to increase user acceptance and improve marketing strategies [8].

Alejandro Valencia-Arias et al. provide a comprehensive analysis of the factors influencing the adoption of smart home technologies. The authors systematically review existing literature to identify key theories, variables, and research trends. They emphasize the importance of perceived reliability, usefulness, and ease of use [2].

In their paper, Schuster and Habibipour [11] examine how privacy and security issues influence the adoption of IoT devices in smart homes. The study reveals that these concerns significantly affect two key constructs of TAM – Perceived Usefulness (PU) and Perceived Ease of Use (PEOU). The authors find that a lack of trust in the security measures of IoT devices negatively impacts users' perceptions of usefulness, as users may believe the risks outweigh the benefits of convenience. Similarly, concerns over data breaches and unauthorized access reduce the ease with which users feel they can safely operate these devices, negatively affecting their perception of ease of use. The study underscores the need for enhanced security protocols and better communication about privacy features to alleviate these concerns and improve both PU and PEOU, thus fostering greater IoT adoption in smart homes [11].

This aligns with the findings of Magara and Zhou, who also highlight the critical role privacy and security concerns play in shaping users' attitudes toward smart home technologies. Their research, based on a quantitative survey, reveals that security concerns are a major barrier to adoption, with around 76.2 % of the variance in adoption behaviour explained by these concerns. The paper concludes that perceived privacy risks and security vulnerabilities significantly reduce users' perceived ease of use and usefulness of IoT systems, emphasizing the need for secure design practices and privacy-by-design principles in smart home technologies [9].

In the paper "A Comprehensive Acceptance Model for Smart Home Services", the authors propose an integrated model that combines the Technology Acceptance Model with the Innovation Diffusion Theory (IDT) and the Theory of Planned Behaviour (TPB) to better understand user acceptance of smart home services (SHS). The study introduces several factors influencing the adoption of SHS, including perceived convenience, perceived connectedness, perceived cost, and perceived privacy risk. By conducting a survey of 750 participants and using structural equation modelling, the authors found that perceived ease of use and perceived usefulness, alongside these additional factors, significantly impact users' behavioural intentions to adopt SHS. The research highlights the importance of designing systems that not only focus on user convenience and cost-efficiency but also address privacy concerns and system integration. This comprehensive approach provides valuable insights into how users evaluate smart home technologies, emphasizing the critical role of perceived benefits and risks in shaping adoption decisions [12].

In the paper written by Yan Zhang, the author explores the influence of perceived privacy and security on users' behavioural intentions, particularly in the context of face recognition technology, through the lens of TAM. The study introduces trust as a mediating factor between perceived privacy, security, and the core TAM constructs – perceived ease of use (PEOU) and perceived usefulness (PU). The results highlight that while perceived security significantly enhances user trust and positively influences PU and PEOU, perceived privacy does not have a direct impact on trust. This suggests that users are more concerned with security guarantees than privacy, as long as they perceive the technology as secure. The study concludes that building trust through robust security features is essential for driving the adoption of face recognition technologies, and similar considerations may apply to other smart technologies, including IoT-based systems like smart homes [13].

Despite the extensive application of TAM in smart home research, most studies rely on hypothetical scenarios or conceptual models. Few have examined user perceptions of a fully operational system through hands-on interaction. This study fills that gap by providing empirical evidence from a lab-based evaluation of a complete home automation solution, incorporating underexplored features such as gamified energy management.

III. Research Methodology

This study adopts a mixed methods approach to evaluate user acceptance of the newly developed home automation system, using TAM as the guiding framework. The methodology consists of three key components: participant selection, data collection, and data analysis. These elements are designed to measure key factors such as perceived usefulness, perceived ease of use, trust, and privacy concerns, all of which contribute to the users' behavioural intentions toward adopting the system.

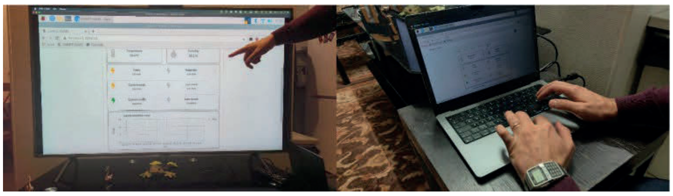

Fig. 1. System demonstration.

A. Participant Selection

A total of 20 participants were selected for the study, all of whom were familiar with smart home technologies and actively used some form of home automation or security system in their residences. This ensured that participants had prior experience with similar technologies, providing a knowledgeable perspective when engaging with and evaluating the home automation system during the study. Although the system was tested in real residential environments, participants interacted with it in a controlled lab setting, where its features and capabilities, such as energy management, security, and automated control of household tasks, were demonstrated to them. Following the demonstration, users were allowed to ask questions, fostering detailed discussions on the system's functionalities. This controlled setting ensured consistency in how participants were introduced to the system and enabled them to engage with it in a manner that facilitated meaningful feedback and insights.

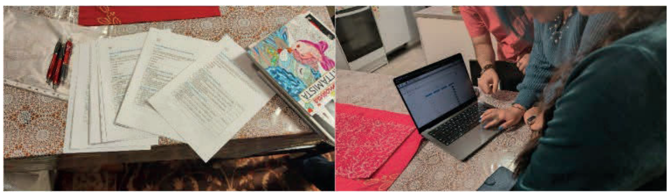

Fig 2. Q&A and survey completion process.

B. Data Collection

Data were collected using both quantitative and qualitative methods. A structured survey was employed to measure the core TAM constructs, including PU, PEOU, Behavioural Intention (BI), and additional factors such as trust and privacy concerns. The survey used a 5-point Likert scale ranging from strongly disagree to strongly agree to capture participant responses after their interaction with the system in the lab. The survey was structured into different sections to target specific TAM constructs and other relevant factors:

- Perceived Usefulness
  - The demonstrated home automation system would help me complete tasks efficiently.
  - The demonstrated system provided a convenient way to manage home devices.
  - I found the system helpful for improving the control of household devices.
  - Using the demonstrated system would make household management more effective in real life.
- Perceived Ease of Use
  - The home automation system was straightforward to understand during the session.
  - I found it easy to perform tasks and navigate through the system features.
  - The instructions provided made it easy to understand the system's capabilities.
  - The system's interface and controls were intuitive.
- Behavioural Intention to Use
  - I intend to continue using the home automation system regularly.
  - I would recommend this system to others interested in home automation.
  - I will likely use the system as my primary means of controlling home automation.
- Trust
  - I trust that the home automation system is secure and reliable.
  - I believe the system will work consistently as intended.
  - I trust the system to maintain the privacy of my data.
  - The system's performance gave me confidence in its overall dependability.
- Privacy Concerns
  - I am not concerned about the privacy of my data when using the home automation system.
  - I trust that my personal information will not be misused by the system.
  - I am not worried about unauthorized access to my home automation data.
  - I feel confident providing personal information to the system without concern for privacy risks.

IV. Results

The study evaluated user perceptions and acceptance of a home automation system, focusing on five key dimensions: user satisfaction, usability, reliability, security, and intention to use. Data were collected from a total of 20 participants through a structured survey. The survey responses were initially recorded on paper and later digitized to facilitate more efficient analysis.

Quantitative responses were analysed using frequency and percentage distributions to identify trends and patterns in user perceptions. Qualitative responses were carefully reviewed, categorised, and summarised to provide a richer understanding of participant feedback. This combination of quantitative and qualitative insights offers a comprehensive perspective on the strengths of the system and areas requiring improvement.

A. User Satisfaction and Usability

Most participants expressed high satisfaction with the system's ability to complete tasks efficiently and improve control over household devices. Statements such as *"The demonstrated home automation system would help me complete tasks efficiently"* and *"The demonstrated system provided a convenient way to manage home devices"* were overwhelmingly rated as "**Strongly Agree**" or "**Agree**" by the majority. For example, 16 out of 20 participants strongly agreed that the system made household management more effective, while others were neutral in their responses.

The system's usability was positively reviewed, with most participants finding it straightforward to understand and navigate. Key statements such as *"The home automation system was straightforward to understand during the session"* and *"The instructions provided made it easy to understand the system capabilities"* received **Strongly Agree** or **Agree** ratings from most respondents. However, some participants highlighted areas for improvement, such as incorporating a more colourful user interface and adding search functionality for enhanced usability.

TABLE I
PERCEIVED USEFULNESS

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The demonstrated home automation system would help me complete tasks efficiently.	70 %	10 %	15 %	5 %	0 %
The demonstrated system provided a convenient way to manage home devices.	70 %	25 %	5 %	0 %	0 %
I found the system helpful for improving the control of household devices.	70 %	25 %	5 %	0 %	0 %
Using the demonstrated system would make household management more effective in real life.	45 %	35 %	20 %	0 %	0 %

TABLE II

PERCEIVED EASE OF USE

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
The home automation system was straightforward to understand during the session.	65 %	30 %	5 %	0 %	0 %
I found it easy to perform tasks and navigate through the system features.	40 %	50 %	10 %	0 %	0 %
The instructions provided made it easy to understand the system's capabilities.	50 %	35 %	15 %	0 %	0 %
The system's interface and controls were intuitive.	55 %	35 %	10 %	0 %	0 %

B. Reliability and Security

Trust in the system's reliability and security was mixed. While many participants believed the system would work consistently as intended, concerns regarding privacy and unauthorized access were raised. A notable number of participants expressed neutral or negative opinions on statements such as *"I trust the system to maintain the privacy of my data"* and *"I feel confident providing personal information to the system without concern for privacy risks"*. Feedback comments emphasised the need for features like two-factor authentication, real-time hacking attempt notifications, and more transparent explanations of security mechanisms.

TABLE III

TRUST

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I trust that the home automation system is secure and reliable.	20 %	40 %	30 %	10 %	0 %
I believe the system will work consistently as intended.	20 %	45 %	30 %	5 %	0 %
I trust the system to maintain the privacy of my data.	40 %	30 %	30 %	0 %	0 %
The system's performance gave me confidence in its overall dependability.	10 %	65 %	10 %	15 %	0 %

TABLE IV

PRIVACY CONCERNS

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I am not concerned about the privacy of my data when using the home automation system.	10 %	20 %	40 %	25 %	5 %
I trust that my personal information will not be misused by the system.	35 %	20 %	35 %	5 %	5 %
I am not worried about unauthorized access to my home automation data.	10 %	35 %	25 %	25 %	5 %
I feel confident providing personal information to the system without concern for privacy risks.	10 %	35 %	25 %	30 %	0 %

C. Intention to Use

Participants indicated a strong intention to adopt the system for regular use. Statements such as *"I intend to continue using the home automation system regularly"* and *"I would recommend this system to others interested in home automation"* received mostly **Strongly Agree** or **Agree** responses. Despite the enthusiasm, several participants expressed concerns about the system's dependency on electricity and the lack of advanced features for controlling specific devices, such as washing machines and dishwashers.

TABLE V

BEHAVIOURAL INTENTION TO USE

Question	Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
I intend to continue using the home automation system regularly.	45 %	25 %	25 %	5 %	0 %
I would recommend this system to others interested in home automation.	70 %	20 %	5 %	0 %	5 %
I will likely use the system as my primary means of controlling home automation.	35 %	40 %	20 %	5 %	0 %

D. Qualitative Feedback

Open-ended responses revealed several recurring themes. Participants appreciated the system's ease of use, intuitive design, and engaging features such as the gamified leaderboard, describing it as a valuable addition to their home setup. However, they also provided constructive feedback on areas like user interface design, security enhancements, and accessibility features. For instance, one participant suggested integrating services tailored for individuals with disabilities, while another highlighted the importance of robust security measures to mitigate hacking risks.

During open discussions, participants expressed broader privacy concerns, noting that such apprehensions were not limited to the home automation system in question. Comments like *"every computerized system is hackable"* and *"even big corporations aren't immune to hacking attempts"* reflected general scepticism about the security of technology rather than specific criticisms of the demonstrated system.

V. Critical discussion

The findings from this study provide valuable insights into the user acceptance and perceptions of a newly developed home automation system. While the results indicate high levels of satisfaction, usability, and intention to use, the feedback also highlights important areas for improvement, particularly regarding system security, privacy, and advanced features.

A. User Satisfaction and Usability

The system's ease of use and intuitive design were universally appreciated by participants, with 80 % agreeing that it simplified household management and improved control over devices. Additionally, 95 % of participants stated that the system enhanced their control over household devices. These findings align with the established user-centric design principles, which prioritize simplicity and intuitiveness as critical factors for technology adoption. However, the study also uncovered a demand for a more visually appealing user interface and added functionalities such as search features to further enhance usability. These suggestions underscore the importance of iterative design processes that incorporate user feedback to refine system interfaces and maintain engagement.

B. Reliability and Security

The mixed responses to reliability and security questions reflect a critical area of concern for users. While most participants trusted the system's reliability, 30 % remained neutral about its ability to maintain privacy. Qualitative feedback revealed specific desires for two-factor authentication, hacking attempt notifications, and greater transparency regarding security measures. These concerns are consistent with broader industry trends, where user confidence in IoT systems often hinges on the robustness of their security features. Addressing these concerns is crucial to building trust and ensuring the system's long-term adoption.

C. Privacy Concerns

The study also highlighted privacy concerns, with only 55 % of participants indicating confidence that their personal information would not be misused. Interestingly, open-ended feedback suggested that these concerns were not unique to the home automation system but reflected broader apprehensions about technology in general. Comments like "every computerized system is hackable" and "even big corporations aren't immune to hacking attempts" indicate a pervasive scepticism about the security of digital systems. These insights suggest that while the system's privacy features need to be robust, clear communication about these features and their effectiveness is equally important to reassure users.

D. Intention to Use

Despite security and privacy concerns, the system demonstrated strong adoption potential, with 70 % of participants indicating they would recommend it to others and the same percentage expressing a willingness to use it regularly. This suggests that the perceived benefits of the system, such as ease of use and energy management features, outweigh user apprehensions for most participants. However, feedback about the system's dependency on electricity and the lack of advanced device control features (e.g., for washing machines and dishwashers) highlights areas where enhancements could further improve adoption rates.

The system included energy management features, such as a gamified leaderboard, and received positive feedback from participants, who indicated a willingness to use and recommend it. This shows that incorporating motivational design elements into smart home technologies can promote sustainable behaviour, a topic still underexplored in previous TAM-based evaluations.

E. Critical Reflection

This study highlights the strengths of the home automation system, particularly its usability and potential for widespread adoption. At the same time, it underscores the importance of addressing user concerns around security, privacy, and functionality. By leveraging user feedback and adopting an iterative design approach, the system can continue to evolve and meet the needs of a broader user base, solidifying its position as a reliable and user-friendly solution for smart home automation.

VI. Conclusion

This study provides valuable insights into user acceptance of home automation technology through the lens of TAM. The research, conducted with 20 participants in a controlled laboratory environment, revealed several key findings that contribute to our understanding of smart home adoption factors.

The results demonstrate strong support for the core TAM constructs, with perceived usefulness and perceived ease of use showing significant positive influence on users' behavioural intentions to adopt the system. Notably, 80 % of participants found the system effective for household management, and 95 % agreed it enhanced their control over household devices. These findings validate the system's fundamental design principles while highlighting the importance of user-centric development in home automation technologies.

However, the study also revealed critical areas requiring attention, particularly regarding security and privacy concerns. While participants expressed high satisfaction with the system's usability and functionality, their trust in data privacy and security features was more reserved, with only 55 % expressing confidence in the system's ability to protect personal information. This highlights a crucial gap between technological capability and user trust that needs to be addressed in future developments.

The research has several important implications for practitioners and developers in the smart home industry. First, it emphasises the need to balance advanced functionality with an intuitive user interface design. Second, it highlights the critical importance of implementing and communicating robust security measures to address user privacy concerns. Third, it suggests that future developments should focus on expanding device compatibility and implementing fail-safe mechanisms to address concerns about system reliability.

In conclusion, while the evaluated home automation system demonstrates strong potential for widespread adoption, its long-term success will depend on how effectively future iterations address user concerns related to privacy, security, and advanced device functionality. This study contributes to the smart home literature by applying TAM to a fully developed system evaluated through direct user interaction in a controlled lab setting, bridging the gap between theoretical models and practical implementation. Furthermore, the inclusion of user feedback on usability, security, and innovative features, such as energy gamification, underscores the importance of user-centred design in driving adoption. These insights provide a valuable foundation for future development and research in the field of smart home technologies.

References

[1] S. Nikou, "Factors driving the adoption of smart home technology: An empirical assessment," *Telematics and Informatics*, vol. 45, Dec. 2019, Art. no. 101283. https://doi.org/10.1016/j.tele.2019.101283

[2] A. Valencia-Arias, S. Cardona-Acevedo, S. Gómez-Molina, J. D. Gonzalez-Ruiz, and J. Valencia, "Smart home adoption factors: A systematic literature review and research agenda," *PLoS One*, vol. 18, no. 10, Oct. 2023, Art. no. e0292558. https://doi.org/10.1371/journal.pone.0292558

[3] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information Technology," *MIS Quarterly*, vol. 13, no. 3, pp. 319–340, Sep. 1989. https://doi.org/10.2307/249008

[4] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," *MIS Quarterly*, vol. 27, no. 3, pp. 425–478, Sep. 2003. https://doi.org/10.2307/30036540

[5] A. Yaldaie, J. Porras, and O. Drögehorn, "Innovative home automation with Raspberry Pi: A comprehensive approach to managing smart devices," *Asian Journal of Computer Science and Technology*, vol. 13, no. 1, pp. 27–40, Apr. 2024. https://doi.org/10.70112/ajcst-2024.13.1.4260

[6] A. Yaldaie, J. Porras, and O. Drögehorn, "Who are smart home users and what do they want? – Insights from an international survey," *Applied Computer Systems*, vol. 28, no. 1, pp. 114–124, Jun. 2023. https://doi.org/10.2478/acss-2023-0011

[7] A. Yaldaie, J. Porras, and O. Drögehorn, "The present state of home automation: A systematic literature review," *International Journal of Hybrid Innovation Technologies*, vol. 2, no. 1, pp. 23–46, Oct. 2022. https://doi.org/10.21742/ijhit.2653-309X.2022.2.1.03

[8] A. Shuhaiber and I. Mashal, "Understanding users' acceptance of smart homes," *Technol Soc*, vol. 58, Aug. 2019, Art. no. 101110. https://doi.org/10.1016/j.techsoc.2019.01.003

[9] T. Magara and Y. Zhou, "Security and privacy concerns in the adoption of IoT smart homes: A user-centric analysis," *American Journal of Information Science and Technology*, vol. 8, no. 1, pp. 1–14, Mar. 2024. https://doi.org/10.11648/j.ajist.20240801.11

[10] Y. Kim, Y. Park, and J. Choi, "A study on the adoption of IoT smart home service: using Value-based Adoption Model," *Total Quality Management & Business Excellence*, vol. 28, no. 9–10, pp. 1149–1165, Jul. 2017. https://doi.org/10.1080/14783363.2017.1310708

[11] F. Schuster and A. Habibipour, "Users' privacy and security concerns that affect IoT adoption in the home domain," *Int. J. Hum. Comput. Interact.*, vol. 40, no. 7, pp. 1632–1643, Apr. 2024. https://doi.org/10.1080/10447318.2022.2147302

[12] A. Al-Husamiyah and M. Al-Bashayreh, "A comprehensive acceptance model for smart home services," *International Journal of Data and Network Science*, vol. 6, no. 1, pp. 45–58, 2022. https://doi.org/10.5267/j.ijdns.2021.10.005

[13] Y. Zhang, "Impact of perceived privacy and security in the TAM model: The perceived trust as the mediated factors," *International Journal of Information Management Data Insights*, vol. 4, no. 2, Nov. 2024, Art. no. 100270. https://doi.org/10.1016/j.jjimei.2024.100270

Ashkan Yaldaie is an accomplished Lead Software Developer with a background in the information technology industry. He obtained a B.Sc. in Business Information Technology from Haaga-Helia University and an M.Sc. in Computer Science from LUT University. Currently, Ashkan is pursuing a PhD in Computer Science, demonstrating his commitment to advanced research and academic excellence.
E-mail: ashkan.yaldaie@student.lut.fi
ORCID iD: https://orcid.org/0000-0002-8726-2825

Jari Porras is a D.Sc. (Tech) Professor at Lappeenranta-Lahti University of Technology (LUT). He specialises in Software Engineering, particularly Distributed Systems. With extensive experience in research and supervision, his work focuses on parallel and distributed computing, wireless and mobile systems, and sustainable ICT.
E-mail: jari.porras@lut.fi
ORCID iD: https://orcid.org/0000-0003-3669-8503

Olaf Drögehorn is a Professor of Software Engineering and Internet Technologies and Rector for Information and Communication Technologies and E-Learning at Harz University of Applied Sciences. He serves as Vice Chairman of the Wireless World Research Forum working group for Services and Service Architectures and is a member of the ICT Advisory Board of the German state of Saxony-Anhalt.
E-mail: odroegehorn@hs-harz.de

1213. SEPPÄNEN, SAMI. Digital transformation in SMEs : drivers, challenges, and the impact of emerging technologies on decision-making and management control. 2025. Diss.

1214. CANSEVEN, HÜSEYIN. High-specific-power permanent magnet synchronous machine — design, analysis, and validation. 2025. Diss.

1215. BAHRAMIAN DEHKORDI, BAHAR. Digital technology adoption, impact and development in sustainable supply chain management : an exploratory study. 2025. Diss.

1216. ACHRÉN, LOTTA. Transformation of entrepreneurial ecosystems : dynamics and forces shaping the future of entrepreneurship in sparsely populated regions. 2025. Diss.

1217. JOHANSSON, LASSE. On the development of shipping emission models and their applications in global and local impact assessment. 2025. Diss.

1218. KOTHALAWALA, VEENAVEE NIPUNIKA. Extracting redox orbitals in nickel-rich lithium battery cathodes using X-ray Compton scattering. 2025. Diss.

1219. ALFASFOS, RAMI. Towards a resilient hydrogen economy : climate impact, safety, cybersecurity, and the foundations for public trust. 2025. Diss.

1220. DIAS SOUZA, DAYNARA. Cell-free massive multiple antenna systems : estimation techniques, scalability challenges, and aerial access point deployments. 2025. Diss.

1221. IGBOANUA, CHUKWUKA. Going further, looking ahead, and with others : how context shapes sustainability-oriented outcomes in start-ups and SMEs. 2025. Diss.

1222. ROUTAHARJU, LIISA. Leveraging Finnish engineering education for sustainable development : from marginal to mainstream. 2025. Diss.

1223. HAMZA, MUHAMMAD. The path to serverless migration : an empirical investigation of decision-making process. 2025. Diss.

1224. BACHÉR, JOHN. Managing metal losses from the mechanical treatment of waste electrical and electronic equipment. 2025. Diss.

1225. LAURÉN, MIKA. Computationally efficient modeling of internal combustion engine for system-level studies of vehicle power trains. 2025. Diss.

1226. PALU, RIINA. A framework for assessing national maritime supply chain resilience. 2025. Diss.

1227. LILJESTRÖM, TOM. Informal governance in small and medium-sized companies as a systematically managed activity : an owner, board and management perspective. 2025. Diss.

1228. KAREINEN, ELISA. Possibilities of personal carbon trading to tackle greenhouse gas emissions in the passenger mobility sector. 2025. Diss.

1229. TELKKÄ, JOONAS. Experimental characterization of open loop passive heat removal. 2025. Diss.

1230. ZAIKOVA, ANNA. Navigating the transition in municipal solid waste management systems. 2025. Diss.

1231. VIERU, KAARINA. SME internationalisation in smaller towns. 2025. Diss.

1232. KARKI, BISHAL RAJ. Towards sustainable digital maintenance services. 2025. Diss.

1233. SAARNI, KATI. Reducing software ecosystem failure : planning activities, conceptualizing digital services, and understanding failure factors. 2025. Diss.

1234. PHADNIS, NIKHIL. Enhancing innovation portfolio management : towards a pragmatic process centric approach. 2025. Diss.

1235. XUE, QIWEI. Human factors modeling using machine learning for fusion energy applications. 2025. Diss.

1236. HINA, MARYAM. Blockchain for sustainability : a multilevel perspective connecting consumers and organisations. 2025. Diss.

1237. RAUTIO, JUUSO. On the reliability of power semiconductor modules in corrosive environments. 2025. Diss.

1238. SCHERMAN, EERO. Dissimilar metal joining for rotors of high-speed axially laminated anisotropic synchronous reluctance machines. 2025. Diss.

1239. SUOMALAINEN, SARI. Urban open spaces for sustainability transformation — capturing citizens’ perceptions with arts-based methods. 2025. Diss.

1240. KORPINEN, KATRIINA. On the electrochemical migration of copper in electronics – effects of frequency. 2025. Diss.

1241. GALIMOVA, TANSU. Renewable electricity-based fuels and chemicals: demand, trading, and transportation. 2025. Diss.

1242. ADISA, MIKHAIL. Aligning ICT, civic engagement, and policy directives : a multi-level approach to sustainable practices and organizational compliance. 2025. Diss.

1243. MYERS, ALEXANDER. Strategizing through uncertainty in deep technology ventures : a design science approach. 2025. Diss.

1244. GYAWALI, ARUN. Utilisation of remote sensing, machine learning, and agent-based simulation for biophysical assessment of young boreal forest. 2025. Diss.

1245. NIELSEN, IBEN BOLUND. Business perspectives for enabling circular economy. 2025. Diss.

1246. SALCEDO PUERTO, ORLANDO ENRIQUE. Valorization of agricultural and industrial side streams : energy potential and environmental assessment. 2025. Diss.

1247. TERESHCHENKO, ELIZAVETA. Student-centered university-industry collaboration in software engineering : a modern multi-stakeholder model. 2025. Diss.

1248. TURKCU, DENIZ. Battling with the tensions in sustainable packaging. 2025. Diss.

1249. PARTANEN, LAURA. Environmental sustainability in software-intensive companies in Finland : towards actionable understanding. 2025. Diss.

1250. MARÍN CORTÉS, OSCAR ALBERTO. Advancing green mining : integrating sustainable water and tailings management in the copper mining industry. 2025. Diss.

ISBN 978-952-412-356-3
ISBN 978-952-412-357-0 (PDF)
ISSN 1456-4491 (Print)
ISSN 2814-5518 (Online)
Lappeenranta 2025