



Improving Security and Privacy Insights for Smart Home Users

Thesis submitted to the University of Nottingham for the degree of Doctor of
Philosophy

November 2025

Samiah Ahmad Alghamdi
20379893

Supervisors: Prof. Steven Furnell
Dr Steven Bagley

School Computer Science
Faculty of Science
University of Nottingham

TABLE OF CONTENTS

<i>Abstract.....</i>	<i>v</i>
<i>Acknowledgements.....</i>	<i>vii</i>
<i>List of Figures.....</i>	<i>x</i>
<i>List of Tables.....</i>	<i>xii</i>
<i>Declaration.....</i>	<i>xiii</i>
<i>Copyright.....</i>	<i>xiv</i>
<i>Chapter 1: Introduction.....</i>	<i>2</i>
1.1 Research Context.....	2
1.2 Motivation and Problems	4
1.3 Aim and Objectives	6
1.4 Thesis Outline.....	7
<i>Chapter 2: Security and Privacy Issues in Smart Homes</i>	<i>10</i>
2.1 The Smart Home Concept.....	10
2.2 Security and Privacy Vulnerabilities in Smart Home Devices.....	13
2.3 Privacy Challenges in Smart Homes	18
2.4 Existing Solutions and Research Gaps.....	21
2.4.1 Smart Home Dashboards Focused on Security and Privacy	21
2.4.2 Other Smart Home Dashboards.....	24
2.4.3 Commercial Smart Home Dashboards.....	25
2.4.4 Resulting Challenges and Research Direction	26
2.5 Research Methodology and Study Design	28
2.5.1 Research Approach	28
2.5.2 Research Design.....	29
2.5.3 Research Methods	31
2.5.4 Ethical Considerations.....	32
2.6 Summary	32
<i>Chapter 3: Evaluating User Experience with Security and Privacy Features</i>	<i>35</i>

3.1 Assessment of the Devices	36
3.2 Evaluating Feature Accessibility in Smart Speakers.....	42
3.2.1 Main Security and Privacy Issues in Smart Speakers	45
3.2.1.1 Weak Authentication	45
3.2.1.2 Weak Authorisation	46
3.2.1.3 Fundamental and Integrated Technologies.....	47
3.2.2 Practical Evaluation of Security and Privacy Feature Accessibility	49
3.2.2.1 Listening and Recording.....	49
3.2.2.2 Audio Purchases	50
3.2.2.3 Turning off Location Services	51
3.2.2.4 Updating Software	52
3.2.2.5 Setting Up Voice Recognition.....	52
3.2.2.6 Example: Steps required to Delete all Voice Recordings	53
3.3 Summary	57
Chapter 4: Evaluating the Consistency of Security Feature Provision	60
4.1 Security Challenges.....	60
4.2 A Comparative Analysis of the Security Features on Smart Home Devices	65
4.3 Privacy Challenges.....	68
4.4 A Comparative Analysis of The Privacy Features on Smart Home Devices.....	71
4.5 Data Management Challenges.....	74
4.6 A Comparative Analysis of The Data Management on Smart Home Devices	75
4.7 Summary	78
Chapter 5: A Harmonized Security and Privacy Dashboard for Smart Homes.....	80
5.1 Dashboard Requirements	80
5.2 Dashboard Design Process	82
5.3 Dashboard Structure	86
5.4 Dashboard Architecture	88
5.5 Usability Principles in Dashboard Design.....	90
5.6 HCISec Principles Relevant to Security Dashboards.....	93
5.7 Dashboard Interfaces.....	94
5.7.1 Home Interface.....	97
5.7.2 Rooms Interfaces.....	105

5.7.3 Devices Interfaces	107
5.7.4 User Data Interfaces	107
5.7.5 Data Type Interfaces	108
5.8 Summary	110
Chapter 6: User Evaluation of the Dashboard Prototype.....	112
6.1 Methodology	112
6.1.1 Study Design and Context.....	113
6.1.2 Participants	118
6.1.3 Pilot Study	119
6.1.4 Evaluation Procedure	119
6.1.5 Usability Measurements	121
6.1.6 Data Analysis	122
6.1.7 Ethical Considerations.....	123
6.2 Results and Analysis	124
6.2.1 Participant Demographics	125
6.2.2 Efficiency Metrics	129
6.2.2.1 Task Completion Time	129
6.2.2.2 Clicks Per Task	137
6.2.2.3 Qualitative Feedback on Efficiency.....	143
6.2.3 Effectiveness Metrics	146
6.2.3.1 Task Completion Rate	146
6.2.3.2 Qualitative Feedback on Effectiveness.....	151
6.2.4 Satisfaction Metrics.....	155
6.2.4.1 System Usability Scale (SUS) Results	155
6.2.4.2 SUS Questions Analysis	163
6.2.4.3 Qualitative Feedback on Satisfaction	175
6.2.5 Comparative Analysis	178
6.3 Summary	182
Chapter 7: Implications and Further Implementation.....	184
7.1 Key Findings	184
7.2 Implications for Design.....	185
7.3 Technical Feasibility	188
7.4 Summary	189
Chapter 8: Conclusions	191
8.1 Achievements	191

8.2 Thesis Contributions.....	193
8.3 Challenges and Limitations	196
8.4 Future Research Directions	198
8.5 The Future of Security and Privacy in Smart Homes.....	199
<i>References</i>	<i>202</i>
<i>Appendix A: Usability and User-Centred Design Principles</i>	<i>218</i>
<i>Appendix B: Evaluating Provision of Information</i>	<i>224</i>
<i>Appendix C: Evaluating the Accessibility of the Security and Privacy Features.....</i>	<i>247</i>
<i>Appendix D: Additional Dashboard Interfaces</i>	<i>262</i>
<i>Appendix E: Recruitment Advertisement Sample.....</i>	<i>272</i>
<i>Appendix F: Participant Question Sheets.....</i>	<i>273</i>
<i>Appendix G: Ethics Material.....</i>	<i>286</i>
G.1 Ethics Application Form.....	287
G.2 Consent to Participate.....	298
G.3 Data Management Plan.....	301
<i>Appendix H: Analysis of Prior Dashboard Prototype</i>	<i>305</i>

Word Count: 67900

Abstract

In recent years, the number and range of Internet-connected devices have increased rapidly, mainly due to their adoption within the Internet of Things (IoT) and smart home contexts. As a result, users are increasingly required to manage the security and privacy of a growing variety of devices.

This study explores the challenges users face in understanding the security and privacy features available on their devices, as well as the additional difficulties they encounter when using these features effectively. The first part of the work assesses user-facing materials (e.g., instruction manuals and online guidance) for a wide range of smart home devices to determine the extent to which security and privacy aspects are highlighted and explained. This analysis provides an overview of how information is communicated to end users and identifies gaps between the technical implementation of privacy features and the level of support offered through documentation.

Having established that the situation is inconsistent, the study then examines the user experience by evaluating how easily several security- and privacy-related tasks can be performed across three popular smart speaker platforms. The findings reveal further inconsistencies and suggest that users face considerable challenges in keeping track of the security settings and status of multiple devices within a smart home. These results emphasise that even technically advanced devices often fail to prioritise usability in the design of privacy and security functions, leaving users dependent on trial and error to achieve desired configurations.

In response to these challenges, a harmonised approach was developed through the design and evaluation of a unified dashboard that enables users to view and manage security and privacy settings across all their smart home devices. The design process focused on simplifying

complex technical concepts into intuitive visual elements that enhance user understanding and control. A user-centred design methodology was followed throughout the process, incorporating iterative feedback and evaluation to refine both layout and functionality.

The resulting prototype was compared with three leading commercial platforms, and the evaluation demonstrated that the proposed solution significantly improves usability, awareness, and overall user confidence in managing smart home privacy and security. Beyond its practical implications, the work also contributes conceptually by demonstrating that consistency and transparency are essential for fostering user trust in connected environments, thereby helping to reduce the security and privacy challenges commonly experienced in smart homes. The research, therefore, contributes to the development of user-centred Dashboard that make security and privacy management more consistent, transparent, and accessible across the smart home ecosystem.

Acknowledgements

First and foremost, all praise and gratitude are due to Allah for granting me the strength, patience, and determination to complete this journey. Without His guidance and mercy, this achievement would not have been possible.

I would like to acknowledge my sponsor, the Saudi government (represented by the Ministry of Education and the Saudi Cultural Bureau in London), for funding and supporting my PhD studies.

I would like to express my deepest appreciation and sincere gratitude to my supervisors, Professor Steven Furnell and Dr. Steven Bagley, for their guidance, support, and valuable feedback throughout my PhD studies.

I am especially grateful to my main supervisor Professor Steven Furnell, whose patience, kindness, and wisdom have had a profound impact on my academic growth. His unwavering support, constructive feedback, and genuine care gave me the confidence to move forward even during difficult times. It has been a great privilege to work under his supervision and to learn from his professionalism and integrity.

I would also like to thank my beloved parents, Ahmad and Norah, for their unconditional love, prayers, and constant support throughout my studies. Their encouragement and generosity have given me the strength and stability to pursue my studies with confidence.

I owe my sincere gratitude to my dear husband, Ayman Alghamdi, for his love, patience, and encouragement. I truly appreciate his support and help during his time with me in the UK, and his sacrifice and understanding while we were apart throughout my studies. I am deeply thankful for all that he has done for me during this journey.

My warm and heartfelt thanks go to my beloved sons, Basel and Faris, who have been my greatest source of strength and joy. I am thankful for all the beautiful moments I have been given with you, and I am forever indebted to you for your attempts to make me happy when I was feeling down. I am both delighted and honoured to be your mother.

I owe my deepest thanks to my brother Nabeel and my sisters Abeer, Sahar, Najla, Nada and Rawan for always being there for me. Thank you for filling me with happiness and supporting me in a multitude of ways. Special thanks to Sahar for always listening and encouraging me, and Najla for her invaluable advice and help with my research.

I am also grateful to my dear friends Dalal, Kholoud, Sana, Mashael, Arwa, and Haneen for their kindness, understanding, and companionship. Your support made the difficult times easier and the long days brighter, and I will always cherish the joyful moments we shared and your positive presence throughout this journey.

Finally, I would like to thank my colleagues, especially Nourah, for their support, collaboration, and valuable discussions throughout this study.

List of Abbreviations

Abbreviations	Meaning
BLE	Bluetooth Low Energy
CSI	Channel State Information
DDoS	Distributed Denial-of-Service
EoL	End-of-Life
FAQ	Frequently Asked Questions
HAN	Home Area Network
HCI	Human–Computer Interaction
HCISec	Human–Computer Interaction for Security
HTTP	Hypertext Transfer Protocol
IoT	Internet of Things
ISO	International Organization for Standardization
PUF	Physical Unclonable Functions
RTSP	Real-time Streaming Protocol
SUS	System Usability Scale
TRNG	True Random Number Generators
UCD	User-Centred Design
UI	User Interface
Zeroconf	Zero Configuration Networking

List of Figures

Figure 1.1: The Number of IoT-connected Devices Installed Worldwide in Ten Years	3
Figure 1.2: Basic Building Block of the IoT Ecosystem	4
Figure 2.1: A Standard Smart Home Contains Heterogeneous Networks and Many Smart Devices.....	11
Figure 3.1: Smart Speakers selected for evaluation (a) Amazon Echo (b) Google Nest and (c) Apple HomePod.....	44
Figure 3.2: Smart Speaker Market Size Globally in US Dollars (GVR, n.d.).....	44
Figure 3.3: Steps Required to Delete Siri History from HomePod via the Home application	53
Figure 3.4: Steps Required to Delete all the Recording from Amazon Smart Speakers	54
Figure 3.5: Steps Required to Delete all Recordings in Google Nest Speaker.....	55
Figure 5.1: Initial Version Dashboard Design.....	84
Figure 5.2: Final Version of Dashboard Design.....	85
Figure 5.3: Dashboard Navigational Structure	87
Figure 5.4: Conceptual Architecture of the Dashboard Prototype.....	88
Figure 5.5: Full Figma Workspace Showing Dashboard Flow	95
Figure 5.6: Home Interface	98
Figure 5.7: Information Page Interface	99
Figure 5.8: Health Status Interface	100
Figure 5.9: Software Update Interfaces	101
Figure 5.10: People Interface.....	102
Figure 5.11: Device Management Interfaces – Device Overview	103
Figure 5.12: Device Management Interfaces – Role-Based Permissions	103
Figure 5.13: Setting Interface	104
Figure 5.14: Rooms Interfaces.....	106
Figure 5.15: Devices Interfaces	107
Figure 5.16: User Data Interfaces	108
Figure 5.17: Data Type Interfaces.....	109
Figure 6.1: Age Group Distribution of Participants.....	126
Figure 6.2: Experience Level Distribution.....	127
Figure 6.3: Mean of Task Completion Time with Standard Deviation.....	130
Figure 6.4: Mean Task Completion Time with Standard Deviation by Experience Level	131
Figure 6.5: Mean Task Completion with Standard Deviation Time by Gender	133

Figure 6.6: Mean Task Completion Time with Standard Deviation by Initial Platforms	135
Figure 6.7: Mean Clicks per Task with Standard Deviation for all Platforms.....	137
Figure 6.8: Mean Clicks per Task with Standard Deviation by User Experience Level	139
Figure 6.9: Mean Clicks per Task with Standard Deviation by Gender	140
Figure 6.10: Mean Clicks per Task with Standard Deviation by Initial Platform	142
Figure 6.11: Mean Task Completion Rate with Standard Deviation	146
Figure 6.12: Mean Task Completion Rate with Standard Deviation by User Experience Level	148
Figure 6.13 Mean Task Completion Rate with Standard Deviation by Gender	149
Figure 6.14: Mean Task Completion Rate with Standard Deviation by Initial Platform.....	150
Figure 6.15: Mean SUS with Standard Deviation	156
Figure 6.16: Mean SUS Score with Standard Deviation by Experience Level	158
Figure 6.17: Mean SUS Score with Standard Deviation by User Gender	160
Figure 6.18: Mean SUS with Standard Deviation by Initial Platform.....	162
Figure 6.19: Q1. I think that I would like to use this platform frequently.....	164
Figure 6.20: Q2. I found the platform unnecessarily complex	165
Figure 6.21: Q3. I thought the platform was easy to use	166
Figure 6.22: Q4. I think that I would need the support of a technical person to be able to use this platform.....	167
Figure 6.23: Q5. I found the various functions in this platform were well integrated.....	168
Figure 6.24: Q6. I thought there was too much inconsistency in this platform.....	169
Figure 6.25: Q7. I would imagine that most people would learn to use this platform very quickly.....	170
Figure 6.26: Q8. I found the platform very cumbersome to use.....	172
Figure 6.27: Q9. I felt very confident using the platform.....	173
Figure 6.28: Q10. I needed to learn a lot of things before I could get going with this system	174

List of Tables

Table 3.1: Availability of Device-related Security/Privacy Information at Different Stages	41
Table 3.2: Comparison of Smart Speakers Features on the Selected Platforms	56
Table 4.1: Comparing Security Features Across Multiple Smart Devices and Devices Categories.....	65
Table 4.2: Comparing Privacy Features Across Multiple Smart Devices and Devices Categories.....	72
Table 4.3: Comparing Data Management Features Across Multiple Smart Devices and Devices Categories	75
Table 5.1: Mapping Nielsen's Usability Principles to the Dashboard Design	90
Table 6.1: Summary of Dashboard Evaluation Scenarios	115
Table 6.2: Participant Demographic Information	125
Table 6.3: SUS Scores for All Participants	155

Declaration

No portion of the work referred to in the thesis has been submitted in support of an application for another degree or qualification of this or any other university or other institute of learning. This study was financed with the aid of a scholarship from the Kingdom of Saudi Arabia - Royal Embassy of Saudi Arabia Cultural Bureau in London.

Publications:

1. Alghamdi, S., Furnell, S., & Bagley, S. (2024). Towards a harmonised approach for security and privacy management in smart home contexts. In A. Moallem (Ed.), *HCI for Cybersecurity, Privacy and Trust: HCII 2024. Lecture Notes in Computer Science* (Vol. 14728, pp. 170–187). Springer Cham. https://doi.org/10.1007/978-3-031-61379-1_12
2. Alghamdi, S., & Furnell, S. (2023). Assessing security and privacy insights for smart home users. In Proceedings of the 9th International Conference on Information Systems Security and Privacy. <https://doi.org/10.5220/0011741800003405>

Copyright

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

Chapter One

Introduction

Smart devices play a significant role in modern daily life, with a growing range of technologies now commonly found in households, leading many residents toward a smart home environment. However, while these technologies offer convenience and efficiency, their adoption also introduces security and privacy risks that are not always immediately apparent to non-expert users. As the responsibility for managing these interconnected systems increasingly shifts to end users, it becomes essential for them to understand the associated risks and use available features effectively to protect their personal information and digital safety. Therefore, this research focuses on addressing these challenges by developing and evaluating a user-centred interactive dashboard that helps smart home users better understand, monitor, and manage the security and privacy features of their connected devices.

1.1 Research Context

To better understand the context and evolution of smart home technology, it is important to consider how the Internet and related innovations have contributed to its development. In recent decades, there have been remarkable improvements in computer science, particularly in the use and accessibility of the Internet (Itair et al., 2023; Ndaguba et al., 2023). The Internet of Things (IoT) is defined as a network of interconnected physical devices embedded with sensors, software, and connectivity, enabling them to collect and exchange data, with or without direct human intervention (Karimi and Atkinson, 2013). Among the various applications of IoT, smart homes have emerged as one of the most widely adopted and user-facing domains. Today, a large part of daily activities is connected to online services (Kapucu and Bilim, 2023; Rani et al., 2023), and the integration of IoT technologies has become an essential part of our daily lives (Padmanaban et al., 2023; Umair et al., 2023). Globally, as shown in Figure 1.1, the number of IoT-connected devices has grown from around 15 billion in 2015 to an estimated 75 billion by 2025 (Salih et al., 2022), reflecting the rapid expansion and adoption of smart technologies within households.

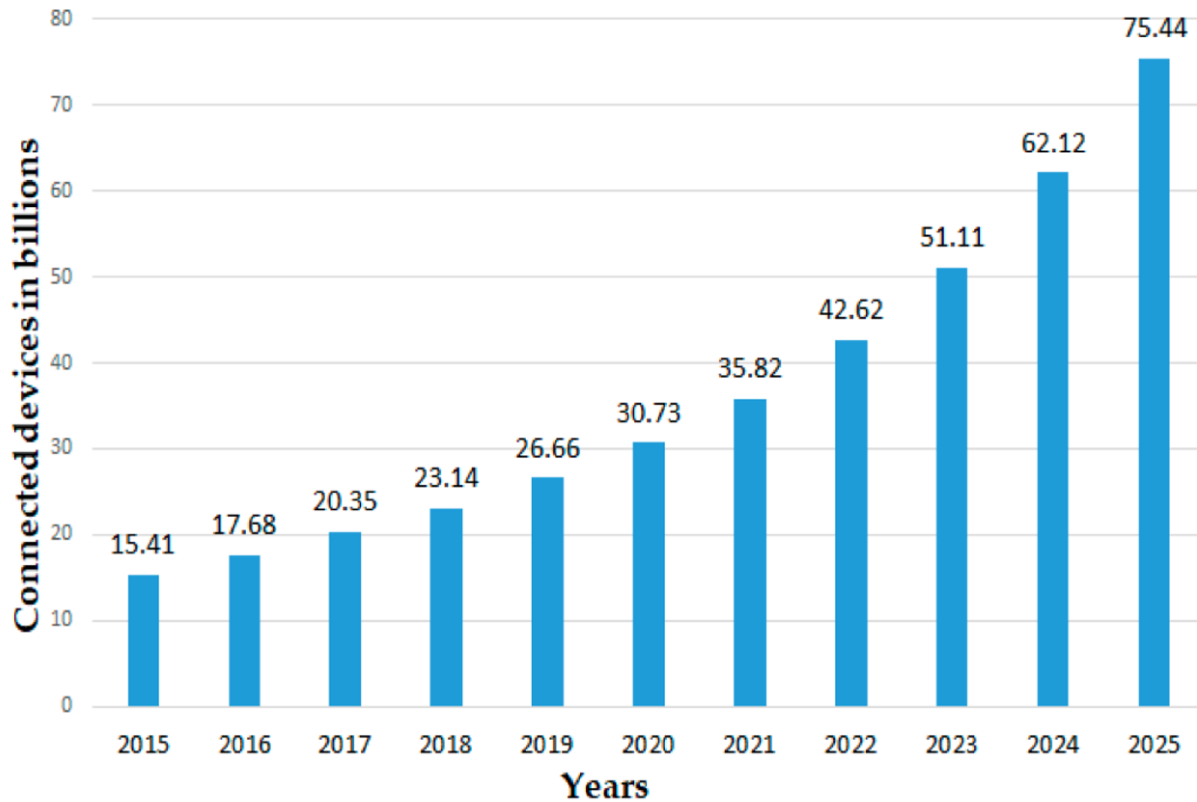


Figure 1.1: The number of IoT-connected devices installed worldwide in ten years (Salih et al., 2022)

The concept of the IoT is illustrated in Figure 1.2 (Vardakis et al., 2024), which depicts the key layers and components of a typical IoT ecosystem. These include applications, access technologies, gateways, and connected devices that interact to create an automated environment. These advancements aim to establish a fully automated ecosystem, increasingly evident in smart homes, where everyday devices are interconnected and controlled via the Internet. This ecosystem leverages Internet connectivity and various smart devices, such as smart TVs, home assistants, smart locks, and robotic vacuums, to enhance convenience and efficiency.

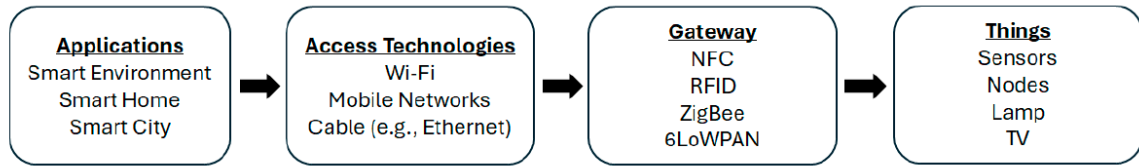


Figure 1.2: Basic Building Block of the IoT Ecosystem

These advancements form the foundation of modern smart home development. However, as smart homes continue to evolve, users increasingly face the challenge of managing complex networks of interconnected devices. This increasing complexity introduces significant security and privacy challenges, particularly for non-technical users.

With this rapid technological growth, the smart home environment has emerged as one of the most practical and widely adopted applications of IoT. A standard smart home features multiple IoT devices linked together via a router or modem. The router serves as the central hub connecting all smart devices within the edge system, allowing for communication with the Internet and cloud services. Smart devices in the home typically do not connect directly to the Internet connection, but users can interact with these smart devices via their smartphones, which have a direct broadband connection. Generally, this router acts as the primary line of defence between the external network and the private house. Consequently, ensuring the security and correct configuration of this interconnected system is essential to protect users' data and privacy.

1.2 Motivation and Problems

Recent studies indicate that managing security and privacy in smart homes poses a significant challenge due to the rapid growth and increasing diversity of smart devices and technologies. Modern households often include multiple smart devices from various manufacturers that rely on different protocols and platforms. This heterogeneity leads to inconsistencies in device

operation, interactions, and information presentation, complicating effective management in smart environments (Gavra et al., 2020; Geneiatakis et al., 2017; Islam et al., 2012).

Research has shown that the complex architecture of connected smart devices, along with continuous Internet access, creates numerous security and privacy vulnerabilities (Ahmed and Ko, 2016; Fahrurrozi et al., 2020; Gavra et al., 2020; Geneiatakis et al., 2017; Islam et al., 2012). Without unified standards or intuitive interfaces, users face fragmented ecosystems and limited guidance, leading to inconsistent configurations and significant security gaps (Gupta et al., 2018; Hatzivasilis et al., 2020; Smyrlis et al., 2021; Zhu et al., 2023).

Studies further highlight the seriousness of these issues, revealing that up to 70% of smart devices are vulnerable to known threats and that nearly 90% of personal data transmissions can be intercepted (Kobialka, 2014). These statistics further emphasise the widespread vulnerabilities in smart homes and the urgent need for enhanced, user-oriented security solutions. Moreover, the integration of smart home systems with cloud services, artificial intelligence, and mobile applications introduces additional security complexities. As digital ecosystems extend beyond local networks, it becomes increasingly difficult to define and maintain secure boundaries. Cyber attackers can exploit weak configurations and unencrypted communication channels to intercept sensitive information or gain unauthorised access (Ahmed and Ko, 2016; Kalbo et al., 2020; Pandya et al., 2018).

In addition, smart home devices frequently share data collected by smart applications, often without clear user consent, which represents a serious privacy breach (Keshavarz and Anwar, 2019). Studies have also identified privacy risks from insecure communication channels that expose sensitive information about residents (Cui and Stolfo, 2010). For instance, while cameras and baby monitors are designed to provide security for users, compromised devices have been involved in incidents of remote access and eavesdropping (Keshavarz and Anwar,

2019). Attackers often analyse Internet traffic to and from smart homes to assess resident behaviour and presence (Hassija et al., 2019). Therefore, preserving user privacy is a significant challenge in the smart home ecosystem (Gubbi et al., 2013).

These challenges underscore the complexity of ensuring consistent security and privacy management across heterogeneous smart home environments. Despite ongoing advances in encryption and authentication, existing research has primarily focused on technical approaches rather than user-oriented solutions. The fragmentation of smart home devices and the limited control users have over them continue to present significant research challenges in cybersecurity (Vardakis et al., 2024). Accordingly, this emphasises the importance of developing an interactive dashboard designed to simplify smart home security and privacy management, bridging the gap between technical complexity and user accessibility. A more accessible and transparent management interface would empower users to enhance awareness, control device configurations, and better protect their personal information (Edu et al., 2020; Liu et al., 2023; Shuhaiber and Mashal, 2019; Sudharsan et al., 2022).

1.3 Aim and Objectives

The rapid growth of smart home technologies has posed new challenges for end users, who often struggle to understand and manage the complex security and privacy settings on their smart devices. Despite advances in IoT security, most existing solutions focus primarily on technical mechanisms rather than user experience, leaving users uncertain about the overall protection of their connected homes.

Therefore, this research aims to improve the user experience in understanding and managing the security and privacy of smart home devices. The goal is to empower users with clearer insights and greater control over their smart home devices. The resulting objectives are:

1. To investigate the extent to which security and privacy issues are apparent to users of smart home devices.
2. To assess the nature of the user experience when attempting to perform security- and privacy-related operations across various smart devices and platforms.
3. To identify usability gaps and inconsistencies that hinder effective management of security and privacy settings.
4. To design and prototype an interactive dashboard that harmonises information from multiple smart home devices.
5. To evaluate the proposed dashboard with users compared to existing solutions in terms of efficiency, effectiveness, and overall satisfaction.

1.4 Thesis Outline

This thesis is organised into eight chapters that collectively explore, design, and evaluate an approach to improve the management of security and privacy for smart home devices within smart home environments. The structure ensures a logical flow from background and motivation to the implementation, evaluation, and conclusion.

Chapter 2 reviews the current state-of-the-art in smart home security and privacy. It introduces the smart home concept, outlining its main features and services, and examines key security challenges and privacy concerns arising from continuous data collection and device interconnectivity. The chapter analyses existing studies, identifies gaps in current research and solutions, and highlights the importance of usability and user-centred design principles in developing practical, secure systems that enable users to manage their smart home devices confidently.

Chapter 3 examines how users engage with security and privacy aspects of smart home devices through two complementary investigations. The first examines how clearly these

features are presented on product webpages, while the second analyses user interaction with smart speaker devices such as Amazon Echo, Google Nest, and Apple HomePod.

Chapter 4 assesses various security and privacy features implemented across different smart home devices and examines their consistency. The findings establish the requirements and design principles that guide the development of the proposed dashboard.

Chapter 5 presents the design and implementation of the proposed dashboard. It summarises the design process from initial concepts to the high-fidelity prototype, highlighting the main interface components and their roles in helping users manage security and privacy tasks effectively.

Chapter 6 illustrates the evaluation methodology and results, comparing the Dashboard with the leading three platforms: Google Home, Amazon Alexa, and Apple HomeKit. It outlines the experimental setup, participant demographics, and usability metrics used to assess efficiency, effectiveness, and satisfaction. The results combine quantitative data and qualitative feedback to provide a comprehensive evaluation of the dashboard's performance.

Chapter 7 presents the broader implications of dashboard design. It explains how the dashboard addresses usability gaps in existing solutions and considers technical feasibility factors.

Chapter 8 concludes the thesis and outlines future work. It summarises the study's contributions, explains how the research questions were answered, and suggests directions for future work.

Chapter Two

Security and Privacy Issues in Smart Homes

Over the past two decades, smart homes have rapidly evolved from a technological concept to a practical reality that integrates automation, connectivity, and intelligent control within everyday life. These systems promise greater comfort, convenience, and energy efficiency by enabling residents to interact seamlessly with their environments through interconnected devices. However, the increasing dependence on digital connectivity has also introduced new risks concerning data security, privacy, and user trust. Many users still find it difficult to understand or manage the complex security settings embedded in smart home technologies, which can leave them vulnerable to misuse or unauthorised access.

In the context of smart homes, information security refers to protecting data from unauthorised access, while privacy focuses on user control over how personal data is collected and used (Kotz et al., 2009). Understanding this distinction is essential before analysing the related challenges.

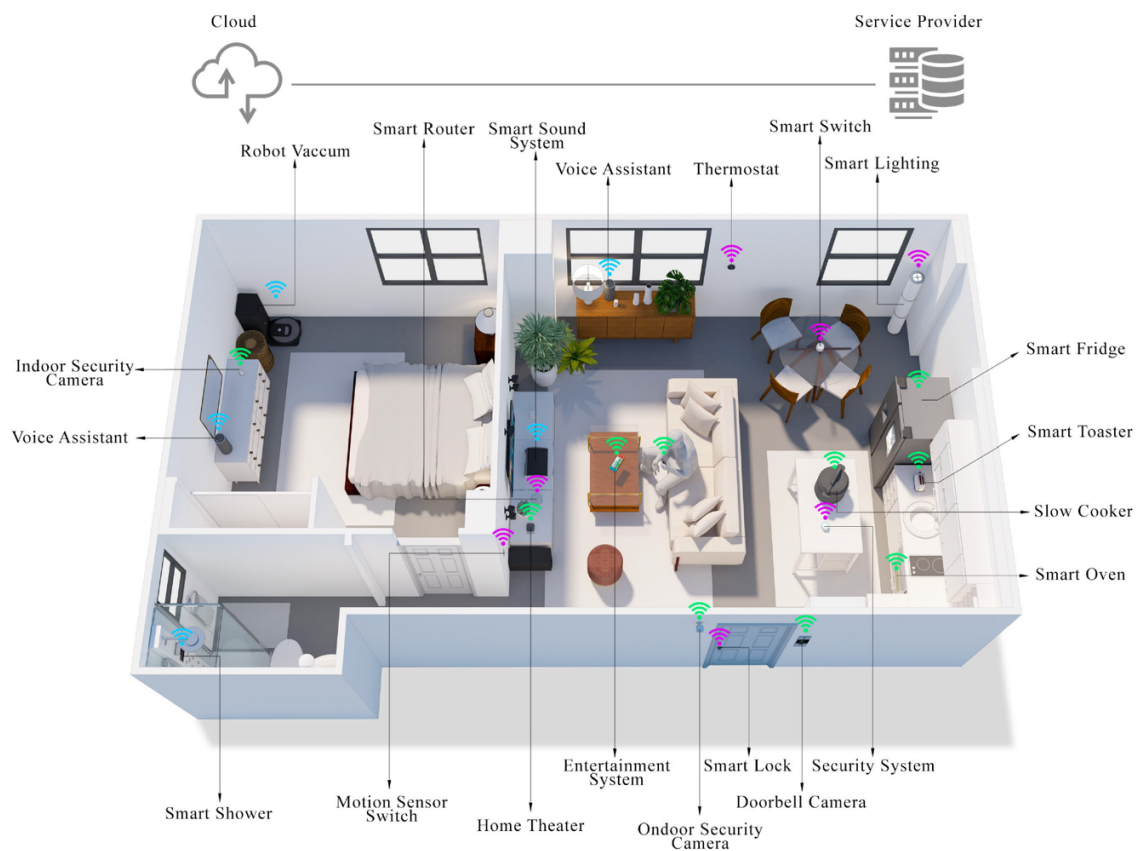
Given these challenges, it is essential to examine how smart home systems are designed, how their security and privacy mechanism's function, and how users engage with them in practice. This chapter provides an overview of the smart home concept and examines the key factors influencing its adoption. It then discusses the major security and privacy issues associated with connected smart devices and applications, highlighting the importance of interaction design.

2.1 The Smart Home Concept

A smart home is a residential environment in which interconnected digital and mechanical devices enable the automated and remote control of household functions, such as lighting, heating, and security, in order to enhance comfort, safety, and efficiency (Satpathy, 2006).

As Figure 2.1 illustrates, smart homes typically use heterogeneous networks. The three signals indicate different wireless technologies: blue signals represent Bluetooth networks, purple

signals represent ZigBee networks, and green signals represent Wi-Fi networks. Many smart home devices may even be linked to a management system using a Home Area Network (HAN). Furthermore, an effort is underway to characterise smart home device security risks and vulnerabilities on a large scale (Davis et al., 2020). In addition, a proposal for reference architectures for executing security at the system level is presented (Augusto-Gonzalez et al., 2019).



*Figure 2.1: A Standard Smart Home Contains Heterogeneous Networks and Many Smart Devices.
(Allifah and Zuolkernan, 2022)*

According to Madakam and Ramaswamy (2014), the five fundamental features of smart homes as follows:

- **Automation:** the capability to perform tasks automatically or adapt smart devices without manual intervention.
- **Adaptability:** the capability to understand, expect, and fulfil users' requirements.
- **Multifunctionality:** the capability to perform multiple tasks and achieve various outcomes.
- **Efficiency:** the capability to carry out tasks efficiently, saving both time and cost.
- **Interaction:** the capacity to enable communication between users and smart devices.

Smart homes can improve residents' quality of life by providing various services that support their daily activities. Generally, the services of a smart home can be categorised into four main types: healthcare, convenience, energy, and security (Balta-Ozkan et al., 2013; Baudier et al., 2020):

- Healthcare assistance can enable residents to monitor and manage their health daily. In addition, smart home healthcare systems provide effective control of personal health data through monitoring infrastructures such as fall detection systems, health information platforms, and smart thermometers. They can also collect and share environmental data that may affect human health, such as air quality and pollution (Chan et al., 2009). Smart homes are expected to provide families with greater stability and independence. Moreover, they support vulnerable residents by monitoring the health conditions of elderly, disabled, and chronically ill individuals, automatically flagging any abnormal activities (Balta-Ozkan et al., 2014; Demiris and Hensel, 2008; Thielke et al., 2011).
- Convenience services aim to improve residents' comfort and overall quality of life. For example, environmental management is one of the most representative and typical functions of a smart home. Moreover, environmental management can automatically schedule or remotely control smart home devices such as smart ventilators, kitchen

appliances, thermostats, lighting systems, and video doorbells (Hubert et al., 2019; Wilson et al., 2017). It allows effortless management of residential environments, ensuring convenience for residents and reducing household labour.

- Smart homes can efficiently and effectively reduce the economic and environmental costs of living by decreasing energy consumption and management expense. Energy control services provide users with information and automatically optimise energy consumption without the need for human intervention (Balta-Ozkan et al., 2013; Ford et al., 2017; Khan et al., 2018; Koupaei et al., 2020; Paetz et al., 2012).
- Security services in smart homes help residents manage home security and prevent potential accidents. For instance, smart security systems detect unusual activities within the home to identify potential intrusions and issue alerts when windows or doors are opened (Coskun et al., 2018).

As a result, a modern smart home environment consists of interconnected smart devices such as smart TVs, speakers, cameras, music streaming systems, and thermostats. These smart devices communicate through wireless networks and cloud-based platforms to exchange data and enable remote management. While these technologies provide convenience, automation, and enhanced control, their increasing interconnectivity also expands the potential attack surface for privacy breaches and security threats. Therefore, understanding the architecture and functionality of smart home devices is essential before examining the specific security and privacy challenges they pose, as discussed in the following section.

2.2 Security and Privacy Vulnerabilities in Smart Home Devices

Numerous vulnerabilities have been identified in smart home devices. Eavesdropping, for instance, occurs when an attacker intercepts data transmitted between devices (Ashari et al., 2019; Mohammad et al., 2019). These vulnerabilities highlight not only technical weaknesses,

but also the challenges users face in understanding and managing security risks in smart home environments. Moreover, smart home devices are susceptible to various attacks, such as sleep deprivation, node capture, and replay attacks (Lu and Xu, 2018; Prathibha and Fatima, 2018). Devices remain vulnerable to attacks for several reasons, with the primary enablers being telepresence and Internet connectivity (Ly et al., 2018). Additionally, default configuration protocols, such as Zero Configuration Networking (ZeroConf) automatically connect smart devices without user intervention, often retaining manufacturers' predefined security settings (Bai et al., 2016).

Examples of the security and privacy issues in different types of smart home devices are summarised as follows:

- **Smart Speakers**

Smart speakers have various security and privacy flaws. Different reports have highlighted vulnerabilities in smart speakers, including continuous listening and recording (Jackson and Orebaugh, 2018) and poor speech authentication (Lei et al., 2018). Moreover, the recent inclusion of Alexa's calling and texting capabilities has also sparked customer concerns about security and privacy. In May 2018, a family from Portland claimed that their privacy had been violated when Amazon's Alexa captured a private conversation in their house and forwarded the recording to someone on their contact list (Horcher, 2018). Likewise, it has been proven that voice instructions that are incomprehensible to human listeners can be used to control smart devices with speech interfaces (Carlini et al., 2016). Likewise, the dolphin attack has the ability to deceive speech recognition systems into understanding and obeying voice commands that are completely undetectable by humans (Zhang et al., 2017). According to Abdi et al. (2019) and Malkin et al. (2019), users' worries about security and privacy when using smart speakers include device hacking,

recording private conversations, continued listening to activities and the gathering, sharing, and storing of personal data.

- **Smart Thermostats**

A smart thermostat has many advantages, but it has also been demonstrated to have a variety of security flaws. For instance, the Nest thermostat has vulnerabilities that enable hackers to hijack the system and access users' data (Hernandez et al., 2015). Moreover, Hernandez et al. (2015) discovered a "back door" that enabled complete control of the thermostat by holding the device button for 10 seconds and connecting a USB device with custom firmware.

- **Robotic Vacuums**

There are many security and privacy issues with robotic vacuum devices. Several reports have emphasised its shortcomings. For example, three security flaws in Eufy's management device and two video storage vulnerabilities were discovered in June 2022 (Munshaw, 2022). Hackers could have exploited them to remotely control, take over the hub or steal video data. Solutions to these security flaws were created by Eufy, who promptly made them available to users. Furthermore, cameras on robot vacuums raise noticeable security and privacy concerns such as hacking and spying on the user's home (Velasco, 2020). Nevertheless, researchers discovered that LIDAR vacuums could be hacked and then voice conversations spied upon in the smart home even without a microphone (ScienceDaily, 2020).

- **Security Cameras**

Although the intention of smart cameras is often for home security purposes, these systems tend to leak personal data, such as private audio and video records (Bugeja et al., 2018). Moreover, smart cameras allow hackers to observe unaware homeowners in their living rooms or bedrooms. For example, (Bitdefender, 2017) discovered two camera models

vulnerable to buffer overflow flaws. The attack can be created by injecting commands that allow them to overwrite passwords, monitor camera activity and reposition the camera for illicit objectives, such as espionage. Security vulnerabilities in smart cameras include unsecured configuration management, credential security flaws and weak passwords (Bugeja et al., 2018). A homeowner might believe that authorized persons can only access its camera. However, it might become accessible to anyone with an Internet connection with the benefit of Shodan IoT search engine or any search engine in the IoT. This is feasible since most cameras have open ports for Real-time Streaming Protocol (RTSP) and Hypertext Transfer Protocol (HTTP) web services (Li et al., 2017). Regrettably, these ports can be left open either with or without the default password settings.

- **Smart Video Doorbells**

Liu (2021) stated that smart doorbell security issues can be similar to those of smart camera security issues. Moreover, Liu (2021) conducted a study involving ethical hacking on a smart video doorbell and discovered that penetration testing and threat modelling was used to analyse the security vulnerability of this device. The findings indicate that the target system is not sufficiently secure and has exploitable flaws, including data disclosure, a lack of logging and inadequate password encryption. Furthermore, Spring (2020) emphasises this “many brands of smart doorbells have potential cybersecurity vulnerabilities ranging from hardcoded credentials, authentication issues and devices shipping with unpatched and longstanding critical bugs” after testing several devices.

- **Smart TVs**

A smart TV can connect to the Internet, which means it is vulnerable to security risks (Niemi et al., 2016). Numerous attacks can occur on TVs, such as pivot attacks and distributed Denial of Service (DDoS) attacks (Michele and Karpow, 2014). Moreover, two-factor authentication, unencrypted services, username enumeration, weak passwords,

plain-text patches, firmware versions and storage media access are some vulnerabilities to which a smart TV device may be exposed.

Although these examples demonstrate a wide range of technical vulnerabilities, they also reveal a common limitation where users often lack clear and accessible ways to understand or manage these risks. In addition to the issues with individual devices, the varying interface design of connected applications and implicit trust is another common cause of device vulnerability (Fernandes et al., 2017). For instance, more than 55% of the applications in an IoT app store were overprivileged (Fernandes et al., 2017). Furthermore, over-the-air application and firmware updates cause smart home devices to be vulnerable (Yaqoob et al., 2017). For example, firmware verification can be bypassed for a generally used thermostat, providing a mechanism to change the unit's behaviour completely (Hernandez et al., 2015). Consequently, a hacked thermostat can operate as a malicious node or bridgehead to penetrate additional nodes in the network, so any data stored internally is accessible to a hacker. Voice commands have become a common interface for multiple smart home devices. Voice spoofing is a recent threat in which inaudible voice commands are injected to control devices that cannot be heard or understood by users though they can be understood by the system (Meng et al., 2018).

Smart devices are vulnerable to a variety of hardware-level attacks (Hu et al., 2020). These attacks include architectural threats, hardware trojans, side-channel and covert attacks, counterfeiting threats and intellectual property theft. To address these threats, several device security countermeasures have been suggested. While these countermeasures provide important technical solutions, they are often designed for developers or security experts rather than for everyday users. As a result, there remains a gap in how these protections are presented and managed from a user perspective, which motivates the approach taken in this research. For instance, Wang et al. (2018) created tools called ProvThings, which is designed to detect

malicious activations and configuration errors within IoT deployments, such as misconfiguration and weak authentication. For clarification, the ProvThings tool can detect approximately 26 known attacks on the Internet, such as spyware side-channel attacks.

Tian et al. (2017) presented the SmartAuth tool, which is executed by device manufacturers and allows users to specify which third-party applications have permission to access, thereby eliminating the need for privileged applications. As a potential explanation for authentication vulnerabilities, (Santoso and Nicholase, 2015) presented a mutual public key authentication protocol for smart devices. Moreover, Han et al. (2015) claimed that data integrity, confidentiality and access control needed trustworthy and secure services. Meng et al. (2018) demonstrated that it was feasible to utilise Channel State Information (CSI) to prevent voice spoofing without using any devices. Physical Unclonable Functions (PUF), True Random Number Generators (TRNG), architectural and system protection techniques, side channel protection techniques, trusted execution environments and intellectual property protection techniques such as hardware watermarking and steganography have all been proposed as countermeasures to hardware attacks (Santoso and Nicholase, 2015).

2.3 Privacy Challenges in Smart Homes

Information security is defined as protecting data from unauthorised access. Privacy concerns involve a user's control over the creation and usage of their data (Kotz et al., 2009). Consequently, privacy depends on security, as the data must be genuinely secure before privacy concerns arise. Nevertheless, privacy is essential for smart home applications, as multiple smart devices often access and share the same user data, which raises concerns about who owns and controls this data.

Related work on smart home privacy has involved technical challenges (Bugeja et al., 2017). However, many of these studies focus on technical privacy risks without fully addressing how

users understand, access, or manage privacy controls in everyday use. Moreover, several studies have presented possible attacks to identify users and behaviour from data gathered from intelligent environments (Apthorpe et al., 2017; Conti et al., 2016). In contrast, many articles recommend design and analytical frameworks (Jacobsson and Davidsson, 2015; Perera et al., 2016; Williams et al., 2016) and suggested methods for managing data and visualisation in smart home environments (Carminati et al., 2016; Ouaddah et al., 2017). The domain of suggested solutions for IoT privacy covers network, design and socio-technical efforts. Nevertheless, an article emphasised that it is essential to understand users to generate usable privacy tools (Jacobsson and Davidsson, 2015). This motivates us to assess the availability of security and privacy information to users if they opt to search for it. Previous Human-Computer Interaction (HCI) researchers have investigated the mental models of users using smart home devices. For example, Zheng (2017) conducted semi-structured interviews with the users of smart homes to comprehend their privacy concerns and mental models. The study showed that users often accepted privacy trade-offs for convenience, partly because they lacked a clear understanding of how their data was being collected and used. Similarly, Emami-Naeini et al. (2019) and Gorski et al. (2018) investigated smart home security perceptions, determined characteristics that impact security decisions, and studied users' concerns before and after buying the smart devices. Their findings highlighted that users' security and privacy decisions were influenced by trust, perceived risk, and the usability of available controls. Other researchers investigated access-control procedures for smart home devices (Colnago et al., 2020; He et al., 2018; Zeng et al., 2019). For example, Zeng et al. (2019) created a prototype and assessed the usability of an access control application. Colnago et al. (2020) analysed personalised privacy assistants in the IoT to permit users to discover and manage data collection by nearby smart devices. He et al. (2018) explored how access control policies in smart home devices vary based on contextual aspects such as device

capabilities and user relationships. These studies demonstrate that users often face challenges in understanding access control settings, especially when controls are distributed across a fragmented ecosystem of smart devices and interfaces. This highlights the need for simpler and more centralised ways of managing privacy in smart home environments.

Most user privacy experiments concerning IoT technologies have been performed in temporary or laboratory environments. While these studies provide useful insights into user attitudes and privacy concerns, many are limited by short-term or controlled settings, which may not fully reflect how users manage privacy in everyday smart home environments. One such experiment was conducted with five users in a single week with a custom IoT device (Worthy et al., 2016). Moreover, experiments conducted to understand user privacy concerns with smartwatches (Udoh and Alkharashi, 2017) and smart toys connected to the internet (McCreynolds et al., 2013) have also examined user attitudes and identified more functional designs for IoT privacy. Few studies have addressed concerns about the nature of data itself; with apparent worries about how businesses would manage the data (Rodden et al., 2013). Participants in this experiment were primarily concerned about their data being used for advertising and marketing purposes for profit.

Overall, previous studies have highlighted important privacy concerns in smart home environments, particularly in relation to user awareness, trust, and access control. However, there remains a lack of solutions that bring these issues together in a clear, user-friendly way that supports both understanding and action. This gap motivates the user-centred approach adopted in this research.

Having examined the principal vulnerabilities and privacy concerns, the following section reviews existing research and practical efforts that aim to address these challenges within the smart home ecosystem.

2.4 Existing Solutions and Research Gaps

A wide range of research has explored methods to enhance security and privacy, as well as user convenience, in IoT and smart home environments. These initiatives encompass a diverse range of work, including analytical frameworks, backend enforcement systems, experimental interfaces, and commercial platforms for smart homes. Moreover, each component plays a vital role in advancing our understanding and application of the underlying principles. This section organises the literature on the smart home ecosystem into four subsections to outline its evolution from foundational frameworks to practical applications and to identify the persistent gaps that motivate this study.

2.4.1 Smart Home Dashboards Focused on Security and Privacy

Several studies have explored ways to visualise and enhance security and privacy in IoT and smart home devices through the development of interactive prototypes. These prototypes aim to facilitate a better understanding of security features and improve user engagement with these technologies. However, despite these benefits, most of these approaches focus on separate aspects of security and privacy, rather than integrating them into a single system that is easy for users to understand and use. For example, SmartAuth has introduced a user-centred authorisation framework specifically designed for IoT platforms. Moreover, the prototype work by analysing app code semantics presents end-users with more straightforward permission prompts to prevent unauthorised actions (Tian et al., 2017). While SmartAuth improves permission management, it primarily focuses on authorisation mechanisms and does not provide integrated interface for managing security and privacy features.

SaferHome presented both digital and physical dashboards that communicate privacy risks to smart homeowners and bystanders through spatial visualisation of device activity and sensitivity (Windl et al., 2022). While SaferHome effectively visualised privacy risks, its

evaluation was restricted to short-term laboratory testing, preventing conclusions about long-term usability in real households. Similarly, Peekaboo introduced a hub-based model to enhance transparency in data processing in smart homes. This model visualises the specific data that each device shares externally with cloud servers, while also providing basic control mechanisms that allow users to manage their data more effectively (Jin et al., 2022). Nevertheless, Peekaboo concentrated on data transparency and lacked unified device control or integrated privacy management functions. These examples illustrate that while existing dashboards improve transparency, they often separate visualisation from actionable control, limiting their effectiveness for everyday users.

Additionally, the SAFER framework was designed to enhance security and privacy in the business sector (Oser et al., 2020). This interface enables users to track their smart devices and ensures they receive immediate notifications about updates to security and privacy reports for their registered smart devices. The findings indicate that users value a framework like SAFER in private contexts. However, it is important to note that the SAFER framework was tested using mock data and mock devices, limiting its applicability within residential smart home ecosystems.

Among the studies reviewed, two recent works stand out as particularly relevant to this research and merit closer examination. Both focus specifically on designing dashboards that prioritise security and privacy in smart home environments, making them directly comparable to the conceptual framework of the current study.

Abbott et al. (2023) conducted a five-week field study that utilised an IoT ecosystem featuring a simple Android-based dashboard to examine users' perceptions of security and privacy in connected homes. Their research offered valuable qualitative insights into how users understand privacy risks and interact with various smart devices. However, the system

primarily functioned as a monitoring and perception tool, lacking significant interactivity and quantitative usability metrics.

Bos et al. (2024) proposed a privacy-focused data flow visualisation dashboard that enables users to monitor the traffic and destinations of data leaving their smart home networks. While their design effectively increased awareness of data sharing behaviour, it relied heavily on technical visualisations, such as packet graphs and world maps. Consequently, the system promoted awareness rather than direct control, requiring users to interpret complex network information without providing mechanisms to manage or restrict data flow. This supports a key limitation in existing approaches, where increasing awareness does not necessarily translate into improved user control or decision-making.

The reviewed studies collectively show significant progress in developing security and privacy focused interfaces for smart homes. Each study provided valuable insights, including improved clarity, data-flow visualisation, and a better understanding of user perceptions and behaviours. These contributions have established an important foundation for future research, demonstrating that interactive dashboards can enhance user awareness and engagement with security and privacy issues. However, most current prototypes are conceptually fragmented. They tend to focus on specific aspects, such as data visibility or access control, without providing a unified experience that connects various devices, data types, and user roles. None has successfully tackled the challenge of harmonising these elements into a single framework. This framework should simplify how users monitor and manage both security and privacy across diverse smart home ecosystems.

This research builds on recent advancements by introducing an integrated, user-centred dashboard that brings together the various fragmented aspects of smart home data. By providing users with a single, cohesive interface to visualise, manage, and protect their smart

home information, this work aims to enhance previous efforts towards a more comprehensive and practical approach to everyday privacy and security management.

2.4.2 Other Smart Home Dashboards

In addition to security-oriented frameworks, numerous smart home dashboards have been developed with goals such as energy efficiency, environmental monitoring, and household convenience. However, these dashboards primarily focus on energy and environmental data, with limited attention to how users manage security and privacy within the same interface. For instance, Smart Electricity Dashboards (Jing et al., 2022) and Home Energy Management Systems (Zafar et al., 2020) offer real-time visualisations of energy consumption. These systems allow users to optimise appliance usage and automate scheduling. Similarly, Al-Ali et al. (2017) introduced an IoT-based Smart Home Energy Management System that leverages big data analytics to improve energy efficiency and enhance user comfort. These systems illustrate how interactive dashboards can foster sustainability and automation through user-friendly visual interfaces and continuous feedback.

Beyond academic prototypes, numerous open-source platforms exemplify the growing emphasis on dashboards that promote energy efficiency and environmental comfort. Notably, platforms such as Home Assistant (Home Assistant, 2023) and openHAB (OpenHAB, 2024) provide robust interfaces that facilitate the monitoring of household devices and tracking energy generation and consumption through their integrated Energy Dashboards. These systems enable users to visualise real-time data from a range of sensors, including smart plugs, thermostats, and photovoltaic inverters. This functionality not only encourages sustainable energy practices but also enables personalised comfort settings tailored to individual preferences. Despite their strong usability and visualisation capabilities, these platforms do not provide clear mechanisms for users to understand or control security and privacy risks.

In a similar vein, the Open Energy Monitor (Emoncms, n.d.) platform enables visualisation of data on electricity, heat, and solar energy. This allows residents to track their usage patterns and environmental conditions with impressive temporal resolution.

While these dashboards improve usability and centralised control of energy data, they do not address security and privacy management in a meaningful way. This oversight is an important consideration as the reliance on such technologies continues to grow.

Therefore, this research aims to enhance the existing understanding of dashboard interaction by prioritising user-centred approaches to security and privacy management. By doing so, it seeks to address a significant gap identified in both the academic literature and practical applications.

2.4.3 Commercial Smart Home Dashboards

A significant part of the smart home market is driven by commercial ecosystems such as Samsung SmartThings Energy, Sense Home Energy Monitor, Apple Home, Google Home, and Amazon Alexa. These platforms provide user-friendly interfaces, innovative designs, and seamless automation, primarily focusing on convenience and interoperability. However, they often overlook aspects of security and privacy. Their dashboards allow users to control multiple connected smart devices, such as cameras, lighting, and thermostats, but offer limited insight into data flows, permissions, and exposure to vulnerabilities.

Each ecosystem primarily functions within its own network or partner network. For instance, SmartThings Energy integrates seamlessly with Samsung appliances, while Sense Monitor operates with its proprietary sensors and cloud service. Amazon Alexa pairs naturally with Ring cameras and Echo devices, Google Home relies on Nest products, and Apple HomeKit is designed to work primarily with Apple-certified accessories.

This ecosystem-based design improves reliability and user experience but restricts interoperability between brands and centralises data within company-controlled cloud systems. As a result, privacy management becomes unclear: users often do not understand how their data is collected, processed, or shared among manufacturers and partners. There is a noticeable lack of real-time transparency in dashboards and security alerts, leaving users to rely on trust rather than control over their information. The fragmentation among corporate ecosystems points to a broader issue highlighted in existing literature: modern households consist of smart devices from various manufacturers that use different communication protocols (Gavra et al., 2020; Geneiatakis et al., 2017; Islam et al., 2012). This diversity results in inconsistent device behaviour, scattered control interfaces, and varying privacy standards. Consequently, these challenges emphasise the need for a unified framework that streamlines the information users receive from various smart devices. This research aims to improve users' understanding of security and privacy management in smart home ecosystems by creating a user-centred dashboard for interaction. In doing so, it addresses a significant gap identified in both academic literature and practical applications.

2.4.4 Resulting Challenges and Research Direction

Current smart home dashboards have achieved notable advancements in automation, efficiency, and user experience across various academic, open-source, and commercial platforms. However, several persistent limitations hinder their effectiveness in addressing critical security and privacy challenges.

1. The majority of these existing dashboards emphasise functionality and usability at the expense of transparency. While designed to enhance comfort, convenience, and energy management, they often fail to facilitate users' understanding of and engagement with

the flow of their personal data. Security configurations tend to be technical and buried within complex system menus, rendering them inaccessible to non-expert users.

2. The fragmentation of data across diverse smart home devices and manufacturers obstructs the development of a coherent security and privacy overview. Each platform presents information in its own format and is often limited to its specific ecosystem, leaving users without a unified perspective on potential risks throughout their home environment. This inconsistency complicates management and exacerbates security vulnerabilities due to varying authentication practices, differing encryption standards, and proprietary integration policies.
3. The absence of unified, user-facing frameworks means that security measures typically operate invisibly in the background, remaining unseen and unmanageable for end users. Although analytical tools such as ProvThings or SmartTracer can detect anomalies, they are primarily designed for researchers or system administrators rather than for everyday residents seeking awareness and control.
4. There is a consistent disconnection between security and privacy management. Existing dashboards tend to focus on one dimension while neglecting the other: security-oriented systems often concentrate on threat detection or network protection without addressing data transparency, whereas privacy-oriented designs highlight data consent or visibility but overlook underlying security vulnerabilities. This separation ignores the interdependence of the two concepts and prevents users from achieving holistic protection.

These challenges underscore a significant research and design gap: the need for a comprehensive, user-centred dashboard that effectively integrates security, privacy, and usability into a single interface. This research seeks to address this gap by developing a multi-view interactive dashboard that consolidates fragmented device information. It empowers

smart home users to monitor and manage their security and privacy risks directly. By embedding HCI principles, the proposed solution aims to integrate security and privacy mechanisms into unified, accessible, and actionable components suitable for everyday smart home use.

Given these challenges and limitations, it is important to explore how usability and user-centred design principles can enhance security and privacy awareness in smart home dashboards. The following section will discuss the theoretical foundations and practical significance of usability and user-centred design principles that inform the design of the proposed dashboard.

2.5 Research Methodology and Study Design

This section presents the research methodology adopted in this study. It outlines the research approach, design, and methods used to investigate how users interact with security and privacy features in smart home environments.

2.5.1 Research Approach

Building on the challenges identified in the literature review, this study adopts a user-centred approach. Moreover, this research investigates how smart home users understand and manage the security and privacy features of their connected smart devices. As discussed in the previous chapters, smart home technologies provide many benefits such as convenience, automation, and improved energy management. However, the increasing number of connected smart devices also introduces significant security and privacy risks for users.

Many existing studies in the field of smart home security focus primarily on technical solutions such as encryption mechanisms, authentication protocols, and network protection techniques. While these technical approaches are essential for protecting smart home devices and networks,

they do not always consider how users interact with these systems or how easily users can understand and manage the available security and privacy settings.

Therefore, this research adopts a user-centred approach that aims to bridge the gap between technical security solutions and the everyday users who must manage smart home technologies. The study focuses not only on the technical capabilities of smart home devices but also on how security and privacy information is presented to users and how effectively users can understand and control it.

This approach combines perspectives from cyber security and HCI. By integrating these perspectives, the research considers both the technical environment of smart home ecosystems and the usability challenges faced by non-technical users when interacting with multiple connected smart devices and platforms.

This research therefore follows a structured process that moves from understanding the problem to designing and evaluating a solution. The study first investigates existing smart home security and privacy features and how they are presented to users. The findings from this analysis then inform the design of a prototype dashboard aimed at improving the usability of security and privacy management. Finally, the proposed dashboard is evaluated with users to examine its effectiveness in supporting security and privacy management tasks.

2.5.2 Research Design

To address the research aim, the study follows a multi-stage research design, where each stage builds on the findings of the previous stage and contributes to the overall development and evaluation of the proposed solution.

The research begins with a review of the existing literature on smart home technologies, security and privacy challenges, and user-centred approaches to cyber security. This stage

establishes the theoretical background of the study and identifies key challenges related to usability, transparency, and the management of security and privacy features in smart home environments.

Following the literature review, the research examines the security and privacy features available in current smart home devices and platforms. This stage focuses on how these features are presented to users and how they can be accessed and managed in practice.

The next stage explores the consistency of security and privacy features across different smart home devices and platforms. Since many households use devices from different manufacturers, this analysis helps identify inconsistencies in how security and privacy information is presented to users.

Based on the insights obtained from these analyses, a prototype dashboard was designed to improve how security and privacy information is presented and managed in smart home environments. The dashboard aims to harmonise information from different devices and provide users with a clearer overview of their device settings and potential risks.

The design of the dashboard was guided by principles from HCI. In particular, the interface design was informed by Nielsen's usability heuristics (Nielsen, 1994) and Human-Computer Interaction for Security (HCISec) principles relevant to security dashboard design, ensuring that the system is understandable, consistent, and easy for users to interact with.

Finally, the proposed dashboard was evaluated through a user study in order to examine its usability and usefulness. This evaluation investigated whether the proposed interface improves users' ability to understand and manage the security and privacy features of their smart home devices.

2.5.3 Research Methods

This research uses a combination of analytical investigation and user-centred evaluation methods.

First, an analysis of smart home devices and platforms was conducted to examine the security and privacy features available to users. This analysis helped identify the types of security controls provided by different systems and revealed inconsistencies in how these features are implemented and presented across smart devices and platforms.

Second, based on the insights gained from the device evaluation, a prototype dashboard was developed to address the usability challenges identified in the earlier stages of the research. The dashboard was designed to provide a unified view of security and privacy information and to simplify how users interact with these settings.

Third, the proposed dashboard was evaluated through a user-based study involving 16 participants. During the evaluation, participants were asked to complete a set of predefined tasks related to managing security and privacy features in a smart home environment.

The study compared the proposed dashboard with several existing commercial smart home platforms, including Google Home, Amazon Alexa, and Apple Home. Participants performed similar tasks across these platforms in order to explore differences in usability and user experience.

The evaluation focused on three commonly used usability measures in Human–Computer Interaction research, which are effectiveness, efficiency, and user satisfaction (ISO, 2018). Effectiveness was assessed by examining whether participants were able to successfully complete the assigned tasks. Efficiency was evaluated by measuring the time required to

complete each task. User satisfaction was assessed through participant feedback collected after interacting with the systems.

2.5.4 Ethical Considerations

The study was approved by the School of Computer Science Research Ethics Committee (CS-2024-R21). Participants were informed about the purpose of the study and that their participation was voluntary. Data was collected anonymously, and participants were informed that they could withdraw from the study at any time.

2.6 Summary

This chapter reviewed the existing body of knowledge on smart home technologies, highlighting their evolving functionality, associated risks, and ongoing efforts to mitigate security and privacy challenges. The chapter starts by laying the conceptual groundwork for smart homes. It outlines their key features, which include automation, adaptability, multifunctionality, efficiency, and interaction. The chapter explains how these features improve residents' daily lives by offering benefits in healthcare, convenience, energy management, and home security services.

The discussion then turns to the security vulnerabilities inherent in smart home devices and ecosystems. Examples across different device categories, such as smart speakers, thermostats, robotic vacuums, cameras, doorbells, and smart TVs, revealed that connectivity and interoperability often create opportunities for unauthorised access, data breaches, and device manipulation. These vulnerabilities arise from factors such as weak authentication, insecure firmware updates, and the lack of user awareness of security settings.

Closely related to these risks are privacy concerns, where user data is continuously collected, processed, and transmitted, often with limited transparency or control. Previous studies have

shown that residents tend to prioritise convenience over privacy and often accept default configurations. Furthermore, laboratory-based privacy experiments have demonstrated that while users express strong concerns about data exposure, they struggle to understand how to manage permissions or interpret risk indicators.

Following the review of vulnerabilities and privacy issues, the chapter examined existing research and practical solutions developed to enhance smart home security and privacy. These include analytical and backend frameworks such as ProvThings, SmartTracer, and Aegis; enforcement systems such as IoTGuard, Soteria, and ContexIoT; prototype dashboards such as SaferHome, Peekaboo, and SmartAuth; and commercial ecosystems such as Google Home, Apple Home, and Amazon Alexa. While these contributions represent meaningful progress, they share a common limitation, which can be summarised as focusing either on technical protection or on specific interface features, without offering a unified, user-centred framework that allows residents to visualise and manage security and privacy comprehensively.

The analysis identified a clear research gap: current approaches lack integration between technical robustness and user empowerment. Security mechanisms often operate invisibly in the background, while privacy controls remain fragmented or hidden. Few systems provide contextual, easy-to-understand feedback that allows users to make informed security decisions.

In conclusion, Chapter 2 demonstrated that while significant progress has been made in smart home technologies, existing solutions remain limited by their technical focus and lack of user integration. Accordingly, the following chapter presents the analysis of how users interact with security and privacy features in smart home devices.

.

Chapter Three

Evaluating User Experience with Security and Privacy

Features

As smart home technologies become increasingly embedded in daily life, concerns about user security and privacy have grown alongside the convenience and functionality of these technologies. These systems collect, process, and share large volumes of personal data, raising important questions about the extent to which users can understand and control the associated risks. Consequently, evaluating user experience in the context of security and privacy is essential to identifying gaps between technical protection mechanisms and user awareness.

Therefore, this chapter is divided into two main sections. The first section examines the availability of security and privacy information provided to users about smart home devices, while the second section explores how these features are presented and managed in practice.

To achieve this aim, this chapter examines how effectively security and privacy information is communicated to users across various smart home devices. While these technologies enhance everyday convenience and functionality, they also introduce new concerns regarding the visibility and accessibility of security and privacy guidance. Building on the literature reviewed in Chapter 2, this evaluation investigates the extent to which manufacturers provide clear and accessible information to end users, both online and within product documentation.

Following this broad assessment, the chapter then narrows its focus to smart speakers as a representative case study. Smart speakers are among the most widely used smart home devices and often act as central hubs through which users interact with other connected technologies. By analysing how users can locate and manage key security and privacy features, such as voice recordings, location settings, and purchase authorisation, the study explores the usability and accessibility of these controls in practice.

Smart speakers were selected as a representative case study because they integrate continuous listening, personal data processing, and multi-account functionality. These characteristics make

them a useful example for examining the balance between usability and privacy within smart home ecosystems.

3.1 Assessment of the Devices

Although services provided by smart home devices improve our quality of life, they invariably increase concerns regarding the privacy of personal information. It is therefore relevant to consider the extent to which security and privacy issues are highlighted to users, and the extent to which they must search to find relevant information. With this in mind, we evaluate what users could find out about the smart home devices from online sources and the extent to which users are presented with this information as part of the standard guidance. The analysis used a qualitative content evaluation approach that focused on the visibility, clarity, and accessibility of security and privacy information in publicly available materials. Moreover, the evaluation considered seven types of smart home devices: TVs, speakers, thermostats, robotic vacuums, security cameras, smart video doorbells and displays. We then evaluated three companies per category on average. Furthermore, we selected companies with large, medium, and small market shares in smart homes. In each case we examined whether security/privacy aspects were mentioned in the manufacturer's product web page, the user manual, an online Frequently Asked Questions (FAQ) page or other online sources. The latter would include the privacy policies of smart home devices. Many companies present privacy policies that are long and complex, which usually include legal jargon and are difficult for users to read (Fabian et al., 2017), making it cumbersome, if not challenging, for them to use and control their data effectively.

The assessment of the available information was conducted as part of a wider evaluation of the smart devices, which also considered the nature of the information they could collect and share.

The full findings from this activity are presented in Appendix B. The sub-sections that follow present a summary of the findings for each category of smart device.

- ***Smart Speakers***

Smart speakers enable users to control and interact with the devices via voice commands, using a virtual/voice assistant (Alexa, Google, Siri) to perform tasks and access online services.

This assessment evaluates Google Nest, Amazon Echo Dot, and Apple HomePod. Most smart devices and their applications have the potential to invade the user's privacy by collecting personal data, addresses, voice recordings, and the geolocation of the user's smartphone. Moreover, most smart speakers share voice recordings with third parties for purposes such as marketing and improving functionality (the HomePod did not share data with third parties).

Regarding privacy-related information presented in the user manual page, we found that Google Nest speakers indicated how to turn off the microphone. The HomePod presented more information about user privacy than other smart speakers. It is difficult for the users to read and understand privacy policy pages because they were overly long and complex.

- ***Smart Thermostats***

Smart thermostats are a recent technology that connects the heating system in a home to the Internet, allowing the user to change the temperature or turn off the heating from anywhere using the application.

This review examined the Netatmo smart thermostat and the Amazon smart thermostat. Most smart thermostats and their applications have the potential to invade the user's privacy. All smart thermostats collect personal information. Furthermore, Netatmo can

collect the house location, whereas Amazon collects voice recordings because the user will require the speaker to control the device via voice activation.

We found that none of the smart devices presented privacy-related information in the user manual page. Again, the privacy policy pages are too long and complicated for users to read and understand.

- ***Robotic Vacuums***

A robotic vacuum is a self-propelled floor cleaner. It works using LiDAR lasers or room-mapping sensors on the vacuum to scan and map the house without human intervention. Moreover, some vacuums are provided with a built-in camera.

This assessment examined smart devices from four companies: Eufy, Ecovacs Deebot, Wyze, and iRobot. All collected personal data and tracked the location using the applications, and all share users' information with third parties. Furthermore, all the applications have the potential to invade the user's privacy by tracking the location because they work using LiDAR lasers or room-mapping sensors on the vacuum to scan and map the house.

The devices did not include privacy-related information in user manual pages. Their separate privacy policy pages were complex.

- ***Security Cameras***

Smart security cameras contain standard HD video, motion activation and night vision to place the user's home under observation all day.

This assessment involves Amazon Ring Security Cameras, Google Nest Cameras, and Eufy security cameras. Security cameras manufacturers typically collect personal data, house

location, voice, video recording and face images. Further, security camera devices and applications can invade the user's privacy via cameras, microphones, and track the location.

Devices did not present privacy-related information in user manual web page. Again, the privacy policy pages are too long and complicated for users to read and understand.

- ***Smart Video Doorbells***

Smart Video Doorbells are an internet-connected smart device that combines a doorbell, microphone, and camera into a single device. As a result, users can video record who is at the door. Smart doorbells are linked to Wi-Fi and to a smartphone application that allows live viewing for users.

This assessment examined Netatmo, Eufy and Ring. Providers usually collect personal data, house location, video recording, and face images. Further, most smart devices and applications can invade the user's privacy via cameras, microphones, and track location. Moreover, Eufy and Ring share data with third parties, while Netatmo applies the strictest regulations to data collection.

Regarding privacy-related information on the user manual page, we found that all smart devices do not present any information.

- ***Smart Displays***

A smart display usually functions as the hub in the smart home and permits the user to watch YouTube, view their photos, listen to podcasts, and maintain domestic lighting control with their voice.

This assessment investigated Google Nest Hub, Amazon Echo Show, and Facebook Portal. All collect personal data, voice recording for the users and the geolocation of the user's smartphone. Additionally, Facebook Portal collects contact because it requires signing in

with a WhatsApp or Facebook account. Moreover, most smart displays share data with third parties, including advertisers, analytics services, and measurement partners. Besides, all smart devices and their applications have the potential to invade user privacy.

Regarding how much privacy-related information is presented on the user manual page, we found that just the Facebook Portal mentioned how to turn off the camera and the microphone.

- ***Smart TVs***

A smart TV is a television connected to the internet with computational abilities. These upgrades to the standard TV group allow the smart TV to operate interactive applications and stream content from the Internet.

This review investigated the Sony and Samsung Smart TV. All collect personal data, and social contact, and may share data with third parties. Furthermore, it may share geolocation, personal information and browsing history.

Regarding privacy-related information presented on the user manual page, we found that Samsung mentioned how to agree to use the privacy policy without any further explanation.

In contrast, Sony does not present any related information.

Table 3.1 presents a summary of the extent to which users may find security and privacy related information, in terms of whether these aspects are headlined in relevant places such as users' manuals and privacy policy pages. The ticks (✓) and crosses (✗) denote whether security/privacy-related information was identified at each stage, while a dash (-) indicates that the related element was not found. For example, there was no FAQ page for Nest at the time of the assessment. The 'Other' column represents content identified in sources such as privacy policies and privacy notice.

Table 3.1: Availability of Device-related Security/Privacy Information at Different Stages

	Product web page	User manual	FAQ page	Other
Speaker				
Echo Dot	✗	✗	✓	✓
HomePod	✓	✓	✓	✓
Nest	✗	✓	-	✓
Thermostat				
Amazon	✗	✗	-	✓
Netatmo	✗	✗	✗	✓
Robotic Vacuum				
Eufy	✗	✗	✗	✓
Ecovacs	✗	✗	✗	✓
Wyze	✗	✗	✓	✓
iRobot	✗	✗	✗	✓
Security Cameras				
Ring	✗	✗	✗	✓
Nest	✗	✗	-	✓
Eufy	✗	✗	-	✓
Video Doorbell				
Netatmo	✗	✗	✓	✓
Eufy	✗	✗	-	✓
Ring	✗	✗	✗	✓
Display				
Nest Hub	✗	✗	-	✓
Echo Show	✗	✗	✓	✓
Portal	✗	✓	✓	✓
Smart TV				
Sony	✗	✗	✓	✓
Samsung	✗	✓	-	✓

A comparative analysis of seven categories of smart home devices reveals a consistent pattern: while most manufacturers acknowledge security and privacy concerns, the information provided to users is often fragmented, buried in lengthy documents, or difficult to understand. Specifically, user manuals and FAQs frequently fail to offer clear, actionable guidance on managing security and privacy settings.

These findings indicate that merely providing information does not necessarily empower users. Therefore, it is essential to go beyond evaluating the availability of information and to consider how easily users can access security and privacy features in practice.

To explore this issue in depth, the following section will focus on smart speakers as a representative case study. Smart speakers were chosen because they are among the most widely owned smart home devices and serve as central control hubs for other connected technologies. Their continuous listening capability, integration with multiple user accounts, and voice-based interaction make them particularly significant for exploring the usability and accessibility of security and privacy controls.

3.2 Evaluating Feature Accessibility in Smart Speakers

Building on the findings from the previous section, this part of the study investigates how easily users can locate and manage security and privacy features in smart speakers. As highlighted earlier, the availability of privacy information alone does not guarantee user comprehension or effective data control. Smart speakers were chosen because they are among the most integrated and widely used smart home devices, handling large volumes of personal data through continuous voice interaction. They represent an ideal case for exploring how security and privacy features are embedded in user interfaces and how easily such controls can be accessed.

This assessment provides a focused context for analysing the usability and accessibility of security and privacy controls in real-world scenarios. It examines how users interact with smart speakers from different manufacturers and how similar privacy and security outcomes can be achieved across these platforms, offering insights into the broader usability implications of security management in smart homes.

According to Laricchia (2022), "Smart speakers powered by a voice-enabled virtual intelligent assistant are the central controlling hubs for many smart home functions and are used for entertainment, answering questions, searching the web and many other things". Like a variety of smart home devices, smart speakers consist of sensors that measure the environment's physical properties, controls that process sensory data and possible triggers that execute actions

(Bugeja et al., 2017). The alert word triggers smart speakers. For example, "Hey Siri" for Apple, "Alexa" for Amazon, and "Hey Google" for Google, to work appropriately. Nevertheless, this requires the smart speaker to be on continuously and therefore always responsive, which may lead it to pick up something the user or home resident wants to keep private.

Smart speakers usually integrate with the service of the parent company. For instance, users of Amazon Echo speakers can create purchases from Amazon, while the users of Google Nest speakers access their calendar via Google Home. The abilities of smart assistants can be extended via third-party applications, which are also recognized as actions for Google and skills for Alexa (Lau et al., 2018). Moreover, many smart speakers even provide the capability to create calls and links to different accounts in houses with different users. Even though microphones are the most significant sensors on speakers, they are considered one of the most privacy penetrating sensors besides cameras (Bugeja et al., 2017; Oulasvirta et al., 2012). This, along with the complex array of capabilities of smart speakers and their placement in homes, leads to the emergence of smart speakers that pose certain privacy challenges.

Existing smart speakers are provided with several security and privacy features (Lau et al., 2018). Therefore, this study specifies three features of security and privacy aspects: listening and recording, purchasing and location. In the listening and recording feature, we analysed and investigated the user's ability to control and improve security and privacy at home in terms of listening and recording their conversations, for example, muting the microphone, deleting all voice recordings from history, deleting a specific voice recording and scheduling deletions for a specific time. Moreover, for purchasing features, smart speakers can purchase items via voice commands, indicating that smart speakers connect to the user's credit cards, which breaches the user's security and privacy. Therefore, we investigated how the users can control their smart

speakers by turning off audio purchases and demand codes for voice purchases. Finally, smart speakers provide users with local news and weather, which identifies users' locations. Therefore, we investigated how the user can turn off location services in smart speakers to improve security and privacy.

The Amazon Echo, Google Nest, and Apple HomePod devices (Figure 3.1) were chosen, reflecting three popular options that typical users may own and use as illustrated in Figure 3.2.

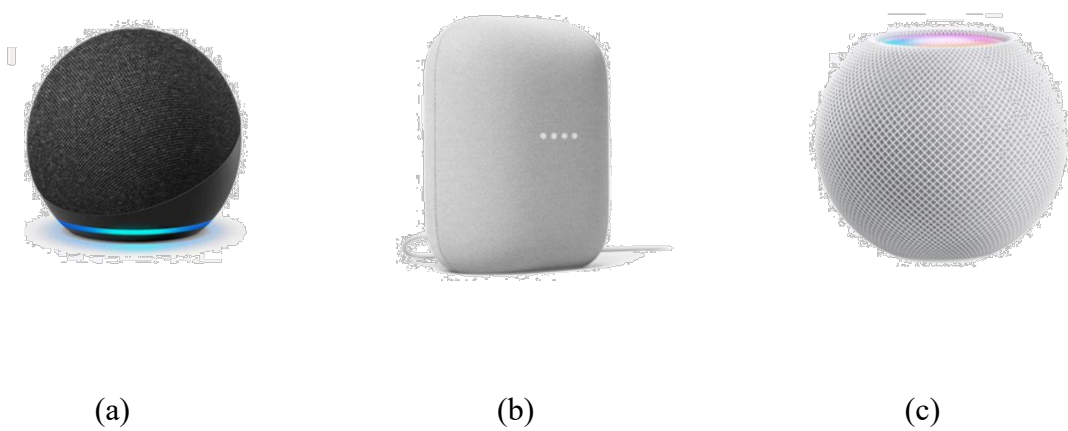


Figure 3.1: Smart Speakers selected for evaluation (a) Amazon Echo (b) Google Nest and (c) Apple HomePod

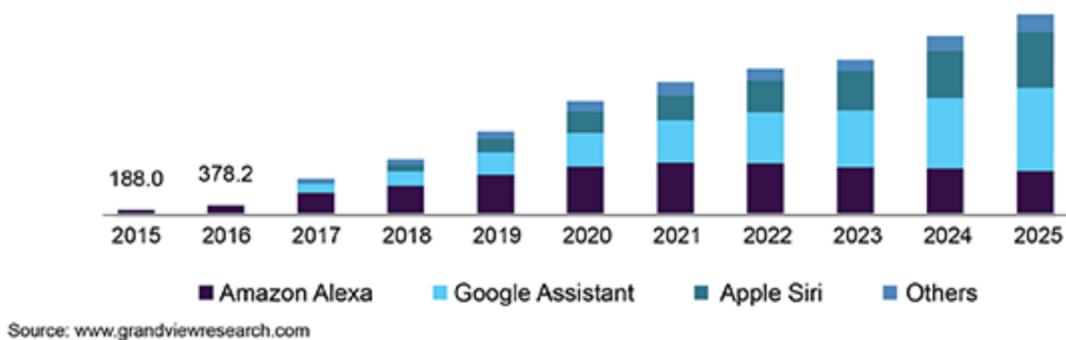


Figure 3.2: Smart Speaker Market Size Globally in US Dollars (GVR, n.d.)

3.2.1 Main Security and Privacy Issues in Smart Speakers

This section outlines the paramount security and privacy challenges associated with smart speakers, drawing upon prior research and real-world incidents. As voice-controlled devices that constantly listen and interact with multiple services, smart speakers present unique vulnerabilities that differ from those of other smart home devices. These vulnerabilities primarily arise from weaknesses in authentication and authorisation mechanisms, as well as from the integration of third-party services and connected smart home devices.

The following subsections analyse these key issues in detail, identifying how each contributes to potential risks for end users and how they inform the subsequent practical evaluation of security and privacy controls.

3.2.1.1 Weak Authentication

This subsection examines the authentication mechanisms employed by smart speakers and highlights how weaknesses in these mechanisms can compromise user security and privacy. Authentication in this context refers to how the device verifies a user's identity and determines when to activate voice interactions. Weak or superficial authentication processes can expose users to unauthorised commands, accidental activations, and potential data leakage, making authentication a central vulnerability in voice-controlled environments.

- ***Wake-up Words***

Smart speakers' authentication is achieved by default using wake-up words identified locally on the device. Moreover, the user can choose a wake-up word from a predefined list, with one set as the default. As a result, an attacker can easily deduce the user's wake-up word. Many studies have indicated that weak authentication can be utilised as a front for more security and privacy attacks (Lei et al., 2018; G. Zhang et al., 2017; N. Zhang et al., 2019).

- ***Always On, Always Listening***

As previously stated, smart speakers continuously listen for user phrases while waiting for the wake word. Owning a device that is always on and listening raises serious security and privacy considerations. Voicing the wake-up word or any other phonetically identical word will trigger the smart speaker's recording. As a result, any subsequent conversation will be recorded and uploaded to the Internet. This problem may threaten users' privacy if confidential or private chats are leaked.

Similarly, it may impact device security because an attacker may issue an unauthorised order to compromise these smart devices and use them to reach and attack other smart connected devices. Previously, this feature accidentally documented a couple's private conversation and randomly sent it to varying contacts via the Amazon Echo device (Horton, 2018). This illustrates that users do not completely control their voice data.

3.2.1.2 Weak Authorisation

This subsection discusses how insufficient authorisation mechanisms in smart speakers can expose users to security and privacy risks. Authorisation determines the level of access granted to users or services after authentication. Therefore, weak or poorly implemented controls may allow unauthorised individuals or even third-party applications to access sensitive data or perform actions without explicit consent. Such weaknesses are especially evident in shared household environments, where multiple users interact with the same device.

- ***Smart Speakers with Multiple User***

Many smart speakers are designed for environments that are shared by multiple family members or visitors, enabling them to interact with the same device. However, these smart devices often lack role-based access controls, which can make it challenging to distinguish authorised from unauthorised users. For example, anyone within range can issue commands

or access information from linked accounts. The absence of a clear permission structure raises privacy concerns, as sensitive data such as messages, calendars, or shopping lists could be accessed, either inadvertently or maliciously, by other users.

- ***Weak Payment Authorisation***

Voice-controlled purchases are becoming more common, but the authorisation required for these transactions is often minimal. For instance, Amazon Alexa users can set a 4-digit PIN to confirm purchases. However, this measure offers only limited protection, as family members or guests might overhear or reuse the code. Additionally, some platforms offer one-time authorisation settings that remain active until manually disabled, increasing the risk of unintended or fraudulent purchases.

- ***External Party***

Authorisation vulnerabilities can also affect external services and third-party integrations. Smart speakers rely heavily on third-party "skills" or "actions" to enhance their functionality. If these integrations are not adequately checked or if users are unaware of the permissions they have granted, personal data may be exposed to unauthorised access or sharing. Furthermore, users often lack insight into how third parties store, use, or monetise their data, thereby increasing privacy risks.

3.2.1.3 Fundamental and Integrated Technologies

This subsection explores the implications of the broader technological ecosystem associated with smart speakers, which includes third-party applications, connected smart home devices, and cloud services. Such integration can create additional vulnerabilities and exacerbate privacy concerns. As smart speakers seldom operate in isolation, weaknesses in these interconnected components can affect the speaker itself or be exploited through it.

Understanding these vulnerabilities is crucial to addressing the privacy risks posed by smart speakers in our daily lives.

- ***Third-party***

An attacker could exploit the interaction between the user and the smart speaker's devices by taking advantage of lax enforcement of skill implementation policies. For instance, by impersonating the handover procedure, a malicious action can deceive users into thinking they are interacting with a different skill such as Voice Masquerading attack, to eavesdrop on user conversations and gather sensitive data. Subsequently, the ambiguity of voice commands makes it difficult for the user to decide if they are performing the correct skill at a given time. On the other hand, a malicious skill can ignore or fake the skill cancellation instruction and continue operating invisibly.

- ***Smart Home Devices***

While smart speakers' integration with other smart home devices brings the smart home into one verbally controlled system, it establishes a single point of focus for attackers. It can be exploited in two different ways. Attacking the smart speakers can give attackers access to many connected smart home devices. Furthermore, privacy problems may arise due to data collection, data accumulation, and integration as the authors review privacy threats of information linkage from data integration in the IoT domain. Hence, vulnerabilities in connected smart home devices can be utilised as an intermediate phase to breach smart speakers.

In summary, the analysis of security and privacy issues in smart speakers reveals that many of the challenges stem from design-level weaknesses rather than isolated technical flaws. Weak authentication and authorisation mechanisms, combined with the extensive integration of third-party applications and smart home devices, create a complex environment in which users often

have limited visibility or control over their data. Therefore, these findings emphasise that improving security and privacy in smart speakers requires more than just addressing individual vulnerabilities. Moreover, it also mentions the importance of creating a user-centred approach that enhances transparency and manageability.

Building on this understanding, the following section examines how these underlying challenges are reflected in practice by evaluating how users can access and manage key security and privacy features within smart speakers. This practical assessment provides insight into the extent to which existing controls support or hinder effective user engagement with security and privacy settings.

3.2.2 Practical Evaluation of Security and Privacy Feature Accessibility

This section provides a practical evaluation of user interactions with the security and privacy controls available in smart speakers. The aim is to assess how easily these features can be found, understood, and managed across different platforms, offering insight into users' ability to engage with key aspects of device security and privacy. Building on the issues identified in the previous section, the analysis focuses on five key areas that represent typical security and privacy actions users may wish to perform: listening and recording, audio purchases, location services, software updates, and voice recognition. Collectively, these functions illustrate how the design of smart speaker interfaces can facilitate or constrain user control over personal data.

3.2.2.1 Listening and Recording

Listening and recording are essential functions of smart speakers, but they also raise significant privacy concerns. These devices constantly monitor ambient sounds for activation words, meaning that parts of user conversations may be captured unintentionally and transmitted to cloud servers for processing. As discussed in the previous section, this continuous listening reveals persistent weaknesses in transparency and user control over personal data.

Consequently, users often rely on existing controls, such as muting the microphone and deleting stored voice recordings, to reduce privacy risks and limit unnecessary data exposure.

- ***Microphone muting***

The microphone remains active by default to detect trigger words that enable device interaction. This "always-on" mode raises concerns, particularly in shared environments where users expect a degree of privacy. Devices such as Google Nest and Amazon Echo include a physical switch that lets users mute or unmute the microphone, providing a straightforward way to suspend data collection. However, the dependence on manual activation and the absence of default privacy modes demonstrate the limited automation and convenience available for protecting user privacy.

- ***Deleting recordings***

Voice data can be deleted manually through companion applications or scheduled for automatic removal. Amazon Echo and Google Nest speakers offer options for periodic deletion, which, in theory, enhances user control. In practice, however, the multi-step and inconsistent processes across platforms often discourage regular maintenance. As a result, while privacy management features exist, they remain difficult for ordinary users to exercise effectively.

3.2.2.2 Audio Purchases

Smart speakers enable users to add items to a shopping basket and complete purchases through voice commands, linking the device directly to the user's payment card. While this feature enhances convenience, it also introduces potential security and privacy risks, particularly when smart devices are accessible to multiple users or located in shared environments. As such, smart speakers require effective safeguards to prevent unauthorised purchases. The following

features illustrate the available mechanisms designed to protect users' financial information and reduce the likelihood of accidental transactions.

- ***Turning off Audio Purchase***

The most secure approach is to turn off the voice purchasing feature altogether, thereby eliminating the risk of unintended or unauthorised orders. However, this option reduces convenience and highlights the ongoing trade-off between usability and security in voice-enabled systems.

- ***Payment Authorisation***

Amazon Alexa allows users to set a 4-digit voice code to confirm purchases. While this feature offers a basic level of protection, it can be easily bypassed by anyone who hears or guesses the code. Additionally, some users turn off this feature to simplify their experience, which further diminishes its effectiveness. These limitations highlight that, even when security mechanisms are in place, their practical use often relies on user behaviour and the balance they perceive between convenience and safety.

3.2.2.3 Turning off Location Services

Location data allows smart speakers to provide regional news, including weather updates, traffic information, and details about nearby businesses. However, these conveniences come with the risk of exposing sensitive information about users' routines and home locations. For example, on the Apple HomePod, location services affect all connected smart devices in the household; thus, changing the settings for one speaker impacts all linked smart devices. While users can turn off this feature in the Home app, they should exercise caution. Continuous location sharing may reveal behavioural patterns or exact home coordinates, compromising security and privacy.

3.2.2.4 Updating Software

Regular software updates play a crucial role in maintaining the security, stability, and overall performance of smart speakers. These updates typically include fixes for known vulnerabilities, improvements in system functionality, and enhancements to user privacy controls. However, users do not always install updates promptly, often due to limited awareness or the inconvenience of manual installation. As a result, delayed updates can leave smart devices exposed to preventable security risks, such as the exploitation of outdated software components.

Although most smart speakers are designed to install updates automatically, users frequently lack visibility into the content of these updates. The lack of clear communication about whether privacy protections are included may create uncertainty and mistrust. Enhancing transparency about updated content and promoting consistent update practices is, therefore, essential to maintaining user confidence and ensuring the long-term security of smart speaker ecosystems.

3.2.2.5 Setting Up Voice Recognition

When a smart speaker is shared among multiple users, it may inadvertently expose information that is not specific to the primary user or disclose personal data to others. This situation introduces potential authorisation challenges, as the device cannot always distinguish between individual speakers. To mitigate this issue, the Voice Match feature has been developed to enable the device to accurately identify users and grant access only when the recognised voice matches the authorised profile. This enhances both security and personalisation by limiting access to user-specific data. However, the effectiveness of voice recognition technology remains inconsistent. Factors such as background noise, accent variation, or similar-sounding voices may still compromise accuracy and increase the risk of unauthorised access. Therefore,

careful consideration of these limitations is essential when evaluating the overall reliability of voice recognition systems in smart speakers.

3.2.2.6 Example: Steps required to Delete all Voice Recordings

The steps involved in deleting voice recordings data are presented as a specific example. A summary of the steps involved across the other tasks are presented in Table 3.2. Moreover, full detail of the steps in each feature can be found in Appendix C.

▪ Apple HomePod

The user can delete recordings from the Home application by following the steps shown in Figure 3.3. Although it requires fewer steps than the other application, the second and third steps may not be intuitive.

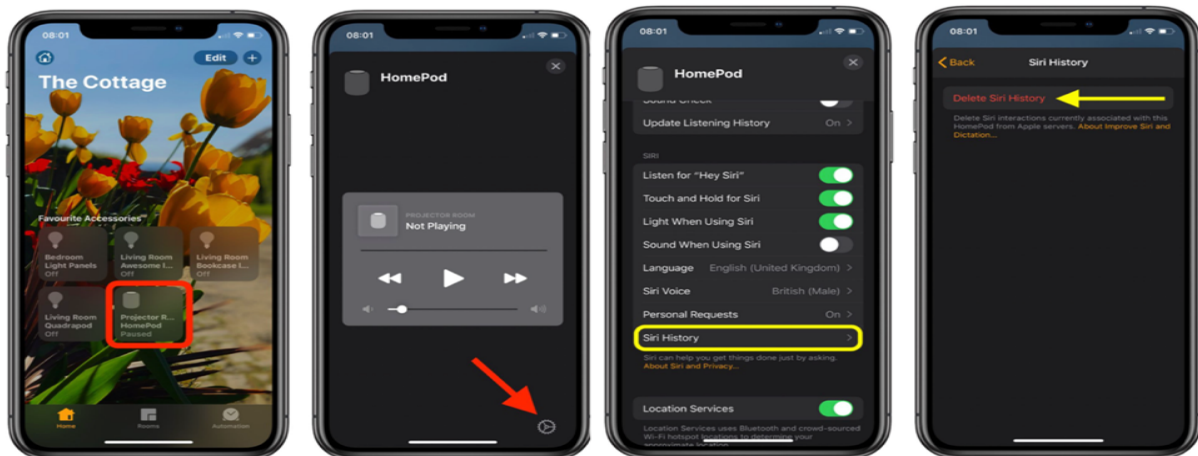


Figure 3.3: Steps Required to Delete Siri History from HomePod via the Home application

▪ Amazon Echo Dot

The user can delete recordings manually via the Alexa application settings, as shown in Figure 3.4. To delete all recordings, they must perform at least eight steps. Moreover, they may need help due to ambiguous options. For example, when opening Settings (Step 3),

how will they know to choose Alexa Privacy rather than Account Setting? Therefore, the users may waste time trying to find the correct route, which can be cumbersome.

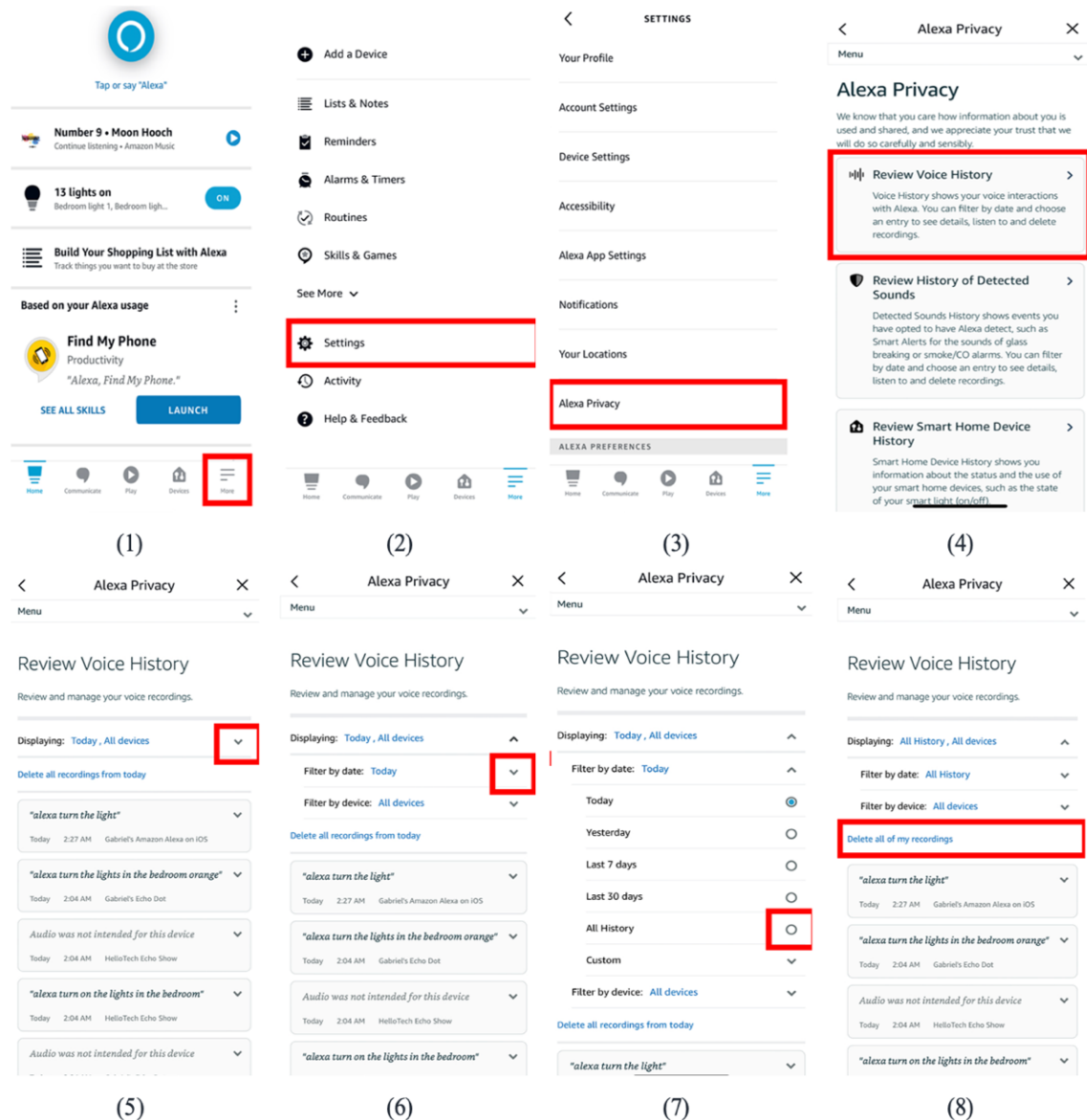


Figure 3.4: Steps Required to Delete all the Recording from Amazon Smart Speakers

- Google Nest

The user can delete all recordings from their Google account by following several steps, as shown in Figure 3.5. It indicates that they must select various options and scroll down via pages to find the Voice and Audio Activity page to delete all voice recordings. These steps

are not obvious due to the variety and unclear choices and scrolling down via pages, which can make the user try several options and undo them to reach the chosen option. For example, if the user opens the setting page, how will they know to select Google Assistant and not Voice?

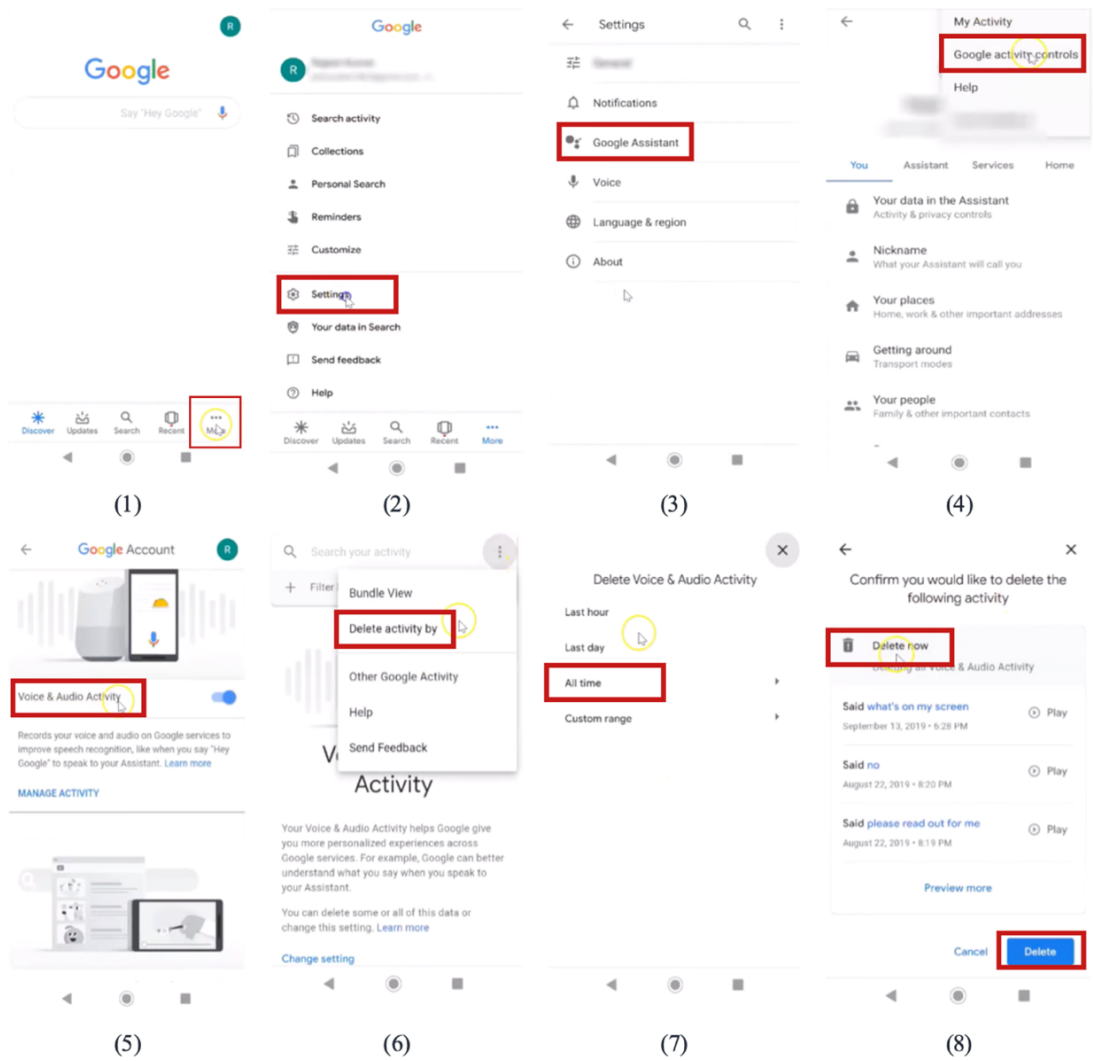


Figure 3.5: Steps Required to Delete all Recordings in Google Nest Speaker

Table 3.2 summarises the overall findings and the steps that a user needs to perform for each feature. This highlights the differences in how the same feature is executed across the three platforms. It also illustrates how variations in interface design can affect the usability and accessibility of key security and privacy functions.

Table 3.2: Comparison of Smart Speakers Features on the Selected Platforms

Platforms Features	Amazon Echo Dot	Google Nest Speaker	Apple HomePod
Microphone Muting	Done via Physical Button in the device	Done via Physical Button in the device	- Via voice command or Home app - No physical mute button
Deleting a Specific Recording	- Done via the Amazon website or Alexa app - User needs to select each specific recording and confirm the deletion request (user must do this N times to delete N records recording)	- Via the Google Account or Google Home app - The process needs at least nine steps to complete, and the user must select each recording and confirm the deletion request	N/A
Deleting all Recordings	- Via the Amazon website or Alexa app - Needs at least nine steps to complete.	- Via the Google Account or Google Home app - Needs at least ten steps to complete.	- Via Home app - Requires around four choices to complete.
Scheduling Deletions	- Done via the Amazon website or Alexa app - Needs at least eight steps to complete.	- Via the Google Account or Google Home app - Needs around eight steps to complete	N/A
Turning off audio Purchase	- Done via the Amazon website or Alexa app - Needs around four steps to complete	- Via the Google Account or Google Home app - Needs around five steps to complete	N/A
Payment authorisation	- Via the Amazon website or Alexa app - Needs around seven steps to complete	N/A	N/A
Turning off Location Services	N/A	N/A	- Via Home app - Requires around three choices to complete
Updating Smart Speaker Software	- Can be done automatically - Requires muting mic and waiting for some time	- Can be done automatically - It takes around 10 minutes	- Via Home app - Requires around three choices to complete
Setting Up Voice Recognition	- Via the Amazon website or Alexa app - Needs at least seven steps to complete	- Via the Google Account or Google Home app. - Needs at least eight steps to complete	- Via Home app - Requires around five choices to complete

The comparison of the three smart speaker platforms reveals significant differences in how they implement security and privacy controls for smart home users. Although all smart devices technically allow users to manage similar settings, the complexity and number of steps required vary greatly. Overall, our analysis of the procedural steps needed to access key security and

privacy features shows that Apple's HomePod offers a more straightforward, guided process. In contrast, Amazon and Google rely on multi-layered menus that require greater effort and user awareness. These differences suggest that many users struggle to locate and adjust security and privacy settings effectively, thereby restricting their capacity to manage and protect their personal information.

3.3 Summary

This chapter provided a comprehensive evaluation of how security and privacy information is communicated to users and how accessible the related controls are across smart home technologies, with particular emphasis on smart speakers. Section 3.1 examined how users locate security and privacy information on manufacturers' websites and accompanying documentation. Therefore, seven categories of smart home devices were reviewed to evaluate how effectively manufacturers reveal important information through product webpages, user manuals, and online materials. The analysis showed that while this information is usually accessible, it is often fragmented, overly complex, and presented in a way that reduces user comprehension and engagement.

Section 3.2 focused on the steps users must take to access and manage security and privacy features in practice, using smart speakers as a representative case study. This section examined both the security and privacy risks associated with smart speakers and the effectiveness of user-facing controls designed to address them. By analysing key functionalities such as listening and recording, audio purchases, location services, software updates, and voice recognition, the findings revealed notable inconsistencies in how these controls are implemented and presented across different platforms.

Overall, the results indicate that while smart home manufacturers increasingly recognise the importance of security and privacy, these aspects are not yet fully embedded within user-

centred design practices. Users continue to encounter difficulties in locating, understanding, and effectively managing security and privacy settings. These findings establish the foundation for the broader comparative evaluation presented in Chapter 4, which extends the analysis beyond smart speakers to assess how security, privacy, and data management features are implemented across a broader range of smart home devices.

Chapter Four

Evaluating the Consistency of Security Feature Provision

This chapter presents a comparative evaluation of the security, privacy, and data management features found in various categories of smart home devices. Additionally, it examines the consistency of these features across smart devices, and the challenges users face in understanding the overall security and privacy status of their smart home ecosystem.

Five distinct categories of smart home devices were considered, namely Smart TVs, Smart Speakers, Thermostats, Robotic Vacuums, and Security Cameras. Within each category, an average of three smart devices sourced from different manufacturers were selected for a comprehensive evaluation. This approach provides an extensive and well-rounded understanding of the security and privacy landscape across various smart home devices.

4.1 Security Challenges

In the context of smart home devices, ensuring security is essential to protect smart devices and the data they handle against unauthorised access, attacks, and breaches (Duezguen and Mayer, 2021; Muller, 2022). Thus, this necessitates measures to protect the integrity, functionality, and availability of the devices and their data. Consequently, various security approaches are implemented to achieve these measures, such as access controls, encryption, authentication, intrusion detection, timely software updates, and vulnerability patches.

The growing number of smart devices has undoubtedly improved the convenience and productivity of our daily lives. However, these smart devices also introduce security challenges that can occur during regular use. To ensure the safety of smart devices, users should be aware of these common security issues.

This section clarifies the security challenges that users may face while using their smart devices for daily activities. When using smart devices, there are various vulnerabilities that users need

to be aware of. These vulnerabilities include weak passwords, inadequate access controls, and authentication mechanisms. By focusing on these challenges, users can take steps to minimise risks and improve the security of their smart device ecosystem.

- **Registration**

Registration is essential in creating a unique identity for users to access their smart home devices. Registration involves two processes: (i) creating an account by providing a valid email address and generating a new password or (ii) linking through social media accounts such as Twitter or Facebook. Failure to register prevents users from accessing their smart home devices. Therefore, users must complete the registration process promptly to use smart home devices.

The variation in registration processes across different smart devices, which can range from the creation of dedicated accounts to the linking of social media credentials, highlights the lack of standardised onboarding methods among manufacturers. These inconsistencies can extend the setup process, confuse users, and increase the risk of incomplete or insecure configurations for smart devices within the same household.

- **Authentication**

Accessing smart home devices requires users to complete an authentication process that verifies their identity. This process typically requires using usernames, passwords, and email addresses to ensure secure access and authentication. Nevertheless, some users may find it difficult to manage multiple passwords, resulting in password fatigue becoming a common challenge in their daily lives. Unfortunately, many smart home hubs that connect all the smart devices on the network have weak passwords, making them vulnerable to hacking. These vulnerabilities could allow attackers to gain unauthorised access to the smart home hub and its connected devices. Therefore, to decrease these risks, it is essential

to use complex and unique passwords and implement two-factor authentication whenever possible.

The inconsistent use of two-factor authentication and the acceptance of weak password schemes demonstrate a significant vulnerability across smart home devices. Therefore, the absence of uniformity requires users to manage multiple credentials, which are often insecure. Consequently, the lack of standardisation leads to confusing IoT authentication practices, which significantly increases the risk of unauthorised access (Haney et al., 2020). This situation emphasises the need for stronger security standards to protect users, considering the rapid advancement of smart home technology.

- **Authorisation**

Authorisation refers to the process of verifying a user's access rights and permissions within a smart home system. It often includes implementing family-sharing features and defining role-based access among household members. Establishing a robust system for logging and monitoring user interface activities is essential for identifying and examining security incidents. Insufficient mechanisms can impede the ability to detect and mitigate potential threats or unauthorised actions. Therefore, clear and robust authorisation measures are important for maintaining system integrity and security.

Limited and inconsistent authorisation frameworks, especially in the context of family sharing, create uncertainties regarding who has control over specific smart devices or functions. This ambiguity can lead to two significant challenges: first, overly permissive access, which can compromise security; and second, overly restrictive access, which can impair usability. These challenges highlight the continued difficulty of achieving a balance between convenience and security in smart home environments with multiple users.

- **Security Update**

Smart home devices, such as cameras, thermostats, and smart speakers, typically operate on lightweight operating systems, which are inherently more vulnerable due to their limited processing power and specialized functionality (Mcgee, 2016). These smart devices require comprehensive security measures compared to traditional computers and mobile devices. Unfortunately, many IoT manufacturers often do not provide sufficient security solutions to protect these smart home devices.

All smart home devices are required to be updated with the latest firmware and security patches in order to avoid security vulnerabilities. For clarification, security patches are released by manufacturers to fix known vulnerabilities and security faults. On the other hand, firmware provides updates to the device's operating system and other embedded software. Therefore, it is necessary to ensure that all smart home devices are updated regularly with the latest firmware and security patches.

Consistently updating firmware and applying security patches allows smart devices to benefit from the latest security enhancements and resolve existing bugs. These required updates often contain necessary patches that address known vulnerabilities, which malicious actors may seek to exploit. Failing to update smart devices can leave them vulnerable to potential attacks, as cybercriminals may take advantage of these weaknesses to gain unauthorised access or seize control of the device. By staying current with updates, users not only protect their smart devices but also protect their sensitive information from potential threats.

Recent research highlights continuous challenges in maintaining software security across smart home devices. For example, a study analysed network traffic from the IoT dataset and found that many smart devices continue operating with outdated and vulnerable

software components, including legacy versions of cURL, Wget, OkHttp, and Python requests, despite newer patches being available (Prakash et al., 2022). Their research highlighted that update processes for smart devices are frequently unclear, delayed, or non-existent, which leaves these smart devices vulnerable to known exploits for extended periods. Moreover, Chen et al. (2024), conducted another study, AutoFirm, which examined over 6,900 IoT firmware and discovered that manufacturers failed to update outdated libraries in 67% of cases, with vulnerabilities staying for an average of 1.34 years before being addressed.

Besides, in a large-scale measurement study of End-of-Life (EoL) embedded devices, Wang et al. (2021) discovered that millions of these smart devices remain active and connected to the Internet for a long time after vendor support has ended. Many of them do not receive the necessary security patches during this time. Their analysis highlights that these unpatched EoL devices frequently carry high-risk vulnerabilities, thereby posing significant risks to broader smart home and IoT ecosystems.

The findings point to a systemic issue, which is that smart home ecosystems are at continual risk due to their dependence on outdated software and unsupported smart devices. Hence, this situation highlights the urgent need for centralised update monitoring, automated patch management, and long-term responsibility from manufacturers to minimise exposure to known threats.

Having outlined the key security challenges that users encounter in smart home environments, the next step is to examine how these challenges are addressed in practice across different smart devices. Therefore, the next section presents a comparative analysis of security features, highlighting the similarities and differences in their implementation among various smart home platforms.

4.2 A Comparative Analysis of the Security Features on Smart Home Devices

This section compares the security features of five types of smart home devices, which are smart TVs, smart speakers, thermostats, robotic vacuums, and security cameras. These features include registration, authentication, authorisation, and security updates. This section assesses the availability of features on each device and platform, and documenting the number of steps needed to execute each feature. Table 4.1 shows that the same feature may be controlled differently on various platforms of the same device, and some features may not be available on certain smart devices. Furthermore, the number of steps needed to access certain features may vary, which may cause inconvenience to the user.

Table 0.1: Comparing Security Features Across Multiple Smart Devices and Devices Categories

Features Platform	Registration	Authentication	Authorisation	Security Update
Amazon Echo Dot Speaker	Username, Email and Password ▪ Via the Alexa app ▪ Requires at least eight steps to register the device.	▪ Voice Recognition ▪ Two-factor authentication	Setting Up Voice Recognition ▪ Via the Amazon website or Alexa app ▪ Needs at least seven steps to complete. Payment authorisation ▪ Via the Amazon website or Alexa app ▪ Needs at least seven steps to complete	▪ Can be done automatically. ▪ Requires muting mic and waiting for some time
Google Nest Speaker	Username, and Password ▪ Done via the Google Home app. ▪ Requires at least twelve steps to complete.	▪ Voice Recognition ▪ Two-factor authentication	Setting Up Voice Recognition ▪ Via the Google Account or Google Home app. ▪ Needs at least eight steps to complete. Payment authorisation ▪ N/A (no information available)	▪ Can be done automatically. ▪ It takes around 10 minutes
Apple HomePod Speaker	Username, Email and Password ▪ Via Home app	▪ Voice Recognition (Voice ID) ▪ Two-factor authentication	Setting Up Voice Recognition ▪ Via Home app	▪ Via Home app ▪ Requires around three choices to complete

Features Platform	Registration	Authentication	Authorisation	Security Update
	Requires around seven steps to complete.		- Requires around five choices to complete. Payment authorisation - N/A (no information available)	
Sony TV	Name, Email, and password. - Via product registration site - Requires around nine choices to complete	N/A	Pin code - Via Remote Control - Requires seven steps to complete.	Can be done automatically.
Samsung TV	Name, Email, and password. - Via Remote Control - Requires six choices to complete.	N/A	Pin code - Via Remote Control - Requires seven steps to complete	- Via Remote control - Can be done automatically while the user is watching the TV. - The update will apply the next time the device is turned on.
Roku TV	Name, Email, and password. - Via Roku website. - Requires five choices to complete.	N/A	Setting Up Voice Recognition - N/A Pin code - Via Roku website - Requires six choices to complete.	- Via Remote control - Requires around seven choices to complete
Amazon Thermostat	Username, and Password - Via Amazon Product Registration or Alexa app. - Requires around seven steps to complete	N/A	N/A	Can be done automatically.
Netatmo Thermostat	Username, Email and Password - Via Netatmo Energy app. - Needs around five choices to complete.	Oauth2 code	N/A	Can be done automatically.
Ecovacs Deebot Vacuum	Username, Email and Password To register the user to ensure the Deebot is less than 5 feet from the router and phone. - Via Ecovacs app. - Requires around five choices to complete	N/A	N/A	- Must place on the base station. - The battery should be over 50%. - Done via Ecovacs app. - Requires around four choices to complete
Eufy Vacuum	Username, Email and Password Eufy home app.	Two-factor authentication	N/A	Must be placed on the charging base.

Features Platform	Registration	Authentication	Authorisation	Security Update
	Requires six choices to complete.			- Make sure the WiFi is stable. - Via Eufy Home app. - Requires four choices to complete.
iRobot Vacuum	Username, Email and Password - To register the user to ensure the iRobot is less than 5 feet from the router and phone. - Via iRobot HOME app - Requires four steps to complete.	N/A	N/A	Can be done automatically.
Ring Security Camera	Username, Email and Password - Via Ring app - Requires nine choices to complete	Two-factor authentication	N/A	- Via Ring security app - Requires seven steps to complete.
Nest Security Camera	Username, Email and Password - Via Nest app - Requires at least twelve choices to complete.	Two-factor authentication	N/A	Can be done automatically.
Eufy Security Camera	Username, Email and Password - Via Eufy home app - Requires around six choices to complete.	N/A	N/A	- Via Eufy home app - Requires seven choices to complete.

The analysis of security features across smart home devices in Table 4.1 shows significant inconsistencies in manufacturers' implementations of essential protections. While most smart home devices offer basic registration and authentication, there is considerable variation in the number of steps required, ranging from four to twelve. This disparity adds unnecessary complexity for users. Additionally, two-factor authentication is not consistently available, leaving some platforms vulnerable to unauthorised access. Furthermore, several products lack automated security updates, meaning users must manually initiate updates, which is often ignored. These findings highlight the fragmented nature of security design in smart home

ecosystems and emphasise the need for effective management tools of smart home devices, as proposed in the dashboard of this research.

4.3 Privacy Challenges

Privacy pertains to protecting data and personal information against unauthorised access or utilisation (Abrishamchi et al., 2022). It encompasses the degree of influence individuals have over their personal information, including the entities that gather it, how it is utilised, and the individuals who may access it. Within smart home devices, privacy involves empowering users to make informed decisions regarding the collected data, its utilisation, and its sharing with third-party entities. To clarify further, privacy concerns involve ensuring that any data obtained by a voice-controlled assistant, such as conversations or user queries, is not stored or shared without clear and explicit consent from the user.

The increasing integration of smart home devices into our daily routines has brought significant privacy challenges concerning the tracking and intrusiveness of such technologies. These concerns are deeply personal and present questions concerning data autonomy and management boundaries. For clarification, intrusiveness refers to the feeling of being excessively monitored or surveilled, whether by the devices themselves or the manufacturers who design them. In contrast, tracking occurs when companies collect and analyse data about an individual's behaviour and activities, which is often enabled by smart home devices.

- **Intrusiveness**

Intrusiveness in this context relates to the perception of excessive monitoring or surveillance, which can be attributed to either the smart devices themselves or the manufacturers accountable for their design. The utilization of cameras and microphones is known to elicit feelings of intrusiveness among users.

1. Cameras

Utilising smart home devices equipped with cameras, such as security cameras or smart display cameras, may elicit an uncomfortable feeling among certain users. Cameras within their living areas can instil a sense of continuous monitoring, potentially threaten their privacy rights and increase concerns about misuse or unauthorised access to the camera footage. A study by Nguyen et al. (2008) found that individuals who utilise smart home devices equipped with cameras often experience a sense of being surveilled, while those who use voice-activated devices tend to feel like they are being eavesdropped on.

The presence of cameras in smart home environments increases users' perception of being watched, especially in private areas such as living rooms and bedrooms. This feeling of constant surveillance can diminish user trust and discourage them from fully utilising the device's features. Additionally, the absence of clear indicators showing when cameras are active intensifies these concerns, underscoring the need for more transparent privacy-by-design elements.

2. Microphones

The existence of microphones in voice assistants found in some smart home devices, such as smart speakers and smart displays, can raise privacy concerns for users. Many individuals worry that their conversations and activities may be recorded or monitored without their consent, leading to anxieties about unauthorised access to or misuse of the recorded audio data. For instance, Nguyen et al. (2008) found that users of voice-activated smart devices often feel as though they are being eavesdropped on.

Microphones integrated into voice-activated devices pose considerable concerns, as users often feel that their conversations may be subject to continuous monitoring, even

while the smart devices are in standby mode. The difficulty in effectively muting microphones or verifying whether they are truly disabled exacerbates anxiety regarding unauthorised data collection. These observations underscore the importance of developing intuitive controls that enable users to take proactive measures in managing audio data collection.

- **Tracking**

Certain individuals may express concerns regarding the observation of their actions and movements through smart home devices by manufacturers or service providers. This type of tracking may include the collection of data on the utilization of smart devices, personal preferences, interactions, or confidential information. One of the main concerns related to tracking is the potential violation of individuals' privacy rights and the importance of protecting the collected data. Additionally, there is a risk of misusing the gathered information, leading to unintended consequences. Therefore, it is important to handle tracking data with great care and attention to ensure that individuals' rights are upheld.

The issues of intrusiveness and tracking emphasize the need for transparent privacy policies, strong security measures, and clear communication from manufacturers regarding the collection and use of data. The most crucial factor is the user's ability to control their personal information and make informed decisions about the privacy implications of their smart home devices. It is essential that users are aware and educated about these technologies to ensure their safe and responsible use.

Tracking features such as location monitoring and behavioural analytics offer significant convenience for users; however, they often fail to provide adequate consent mechanisms and transparency about data usage. This lack of clarity can lead to discomfort among users, fostering reluctance to adopt smart home technologies. Moreover, the lack of

straightforward tracking controls emphasises the need for a centralised interface that standardises privacy settings across various smart devices. Such an approach could enhance user trust and promote broader acceptance of technology in the home.

While this section discussed the major privacy concerns raised by the use of cameras, microphones, and tracking mechanisms, it remains important to evaluate how these issues translate into practical controls available to users. Thus, the following section provides a comparative analysis of privacy features across smart devices, assessing both their availability and the ease with which users can activate them.

4.4 A Comparative Analysis of The Privacy Features on Smart Home Devices

This section presents a comparative analysis of the privacy features available across five categories of smart home devices: smart TVs, smart speakers, thermostats, robotic vacuums, and security cameras. The analysis examines essential privacy functions, such as microphone muting, disabling location services, turning off cameras, and monitoring usage habits. Each device and platform underwent a detailed evaluation to determine the availability of various features, as well as the specific steps required to activate them effectively. Table 4.2 highlights that the same feature may be controlled differently across platforms of the same device, and some features may not be available on certain smart devices. Furthermore, the number of steps required to execute certain features may vary, which could cause inconvenience to the user.

Table 0.2: Comparing Privacy Features Across Multiple Smart Devices and Devices Categories

Features Platform	Microphone Muting	Turning off Location Services	Turning off Camera	Monitoring Usage Habits
Amazon Echo Dot Speaker	Done via Physical Button in the device.	N/A	N/A (no camera)	N/A
Google Nest Speaker	Done via Physical Button in the device.	N/A	N/A (no camera)	N/A
Apple HomePod Speaker	- Via voice command or home app - No physical mute button	- Via Home app - Requires three choices to complete	N/A (no camera)	N/A
Sony TV	- Via remote control - Requires five choices to complete	- Via remote control - Requires four choices to complete	N/A	Automatic Content Recognition (ACR) - Via Remote Control - Requires six choices to complete
Samsung TV	- Via Physical Button in the TV or remote control - Requires six choices to complete using remote control	- Via remote control - Requires five choices to complete	N/A	Automatic Content Recognition (ACR) - Via Remote Control - Requires seven choices to complete
Roku TV	- Via remote control - Requires five choices to complete.	- Via remote control - Requires seven choices to complete	N/A (no camera)	Automatic Content Recognition (ACR) - Via Remote Control - Requires around six choices to complete
Amazon Thermostat	- Via Alexa app. - Requires five steps to complete	N/A	N/A (no camera)	Temperature Settings - Via Thermostat or the Alexa app. - It requires around five choices to complete
Netatmo Thermostat	N/A (no microphone)	N/A	N/A (no camera)	Temperature Settings - Via mobile app or web app - Requires at least five choices to complete. - It may take up to a few minutes for the correction to be applied.
Ecovacs Deebot Vacuum	- Via Ecovacs app. - Requires five choices to complete	Called Obstacle Detection	N/A (no camera)	N/A

Features Platform	Microphone Muting	Turning off Location Services	Turning off Camera	Monitoring Usage Habits
		- Done via Ecovacs app. - Requires around five choices to complete		
Eufy Vacuum	N/A (no microphone)	- Via Eufy Clean app. - Requires four choices to complete.	N/A (no camera)	N/A
iRobot Vacuum	N/A (no microphone)	Not applicable	N/A	N/A
Ring Security Camera	- Via Ring app - Requires seven choices to complete	- Via Ring app - Requires five choices to complete	N/A (The user needs to unplug it)	Motion Detection - Via Ring app - Requires five steps to complete.
Nest Security Camera	- Via Nest app - Requires five choices to complete	- Via Nest app - Requires five choices to complete	- Via Nest app - Requires five choices to complete	Motion Detection - Via Nest app - Requires seven choices to complete
Eufy Security Camera	- Via Eufy app - Requires six choices to complete.	N/A	N/A	Motion Detection - Via Eufy app - Requires five choices to complete.

Table 4.2 highlights significant differences in privacy controls among various device categories. For clarification, muting the microphone and turning off the camera are included in some smart devices, like smart speakers and security cameras. However, these features are often missing in other smart devices, such as robotic vacuums and thermostats. Furthermore, even when these privacy features are available, the process for activating them can vary significantly, ranging from straightforward physical switches to complex navigations through multiple menus in companion apps. In addition, proactive privacy measures, such as automated content recognition controls and location disabling, remain largely underdeveloped across the board. This inconsistent approach to privacy management restricts user independence and underscores the pressing need for centralised tools that enable users to manage their privacy effectively.

4.5 Data Management Challenges

Managing personal data in smart devices within smart homes remains a significant challenge due to fragmented interfaces, unclear policies, and inconsistent data handling practices among different manufacturers. For instance, studies like Buil-Gil et al. (2023) indicate that users often have difficulty locating and deleting sensitive recordings because data is spread across various device-specific applications, and there is little standardisation in how these features are presented. Additionally, the study discovered that customers are rarely informed about what data is collected, where it is stored, or how long it is retained. This lack of clarity creates considerable barriers to user trust and informed consent.

Lau et al. (2018) identified a major data management challenge in smart speakers: audio logs, which serve as a key privacy control, are often buried deep within companion applications and not presented to users. This lack of visibility makes it difficult for users to recognise that these logs can be reviewed or deleted, a process conceptually similar to clearing a browser's history. The study found that users prefer proactive privacy controls, such as an "incognito mode" that completely prevents data collection, over retroactive deletion methods, which require them to remember to delete logs after the data has already been collected manually. This dependence on retroactive controls increases users' cognitive load and raises privacy risks, highlighting the need for more intuitive and centralised data management solutions.

Apthorpe et al. (2017) emphasise the ambiguity surrounding data flows in smart home devices. This lack of clarity presents significant challenges for users, who often find it difficult to understand what information is being transmitted and to whom. As a result, managing or deleting their data effectively becomes a complicated task. The collective findings from their research point to a broader issue: a systemic deficiency in clarity, centralised control, and user-friendly tools within smart home ecosystems. This situation highlights the need for

comprehensive solutions, such as the proposed dashboard outlined in this study, which aims to integrate security, privacy, and data management features into a single, accessible interface.

Addressing the challenges of fragmented data management discussed in this section, the following section evaluates the implementation of data management functions across various smart devices. Additionally, it includes a comparison of key features, such as the ability to delete recordings and schedule deletions. This comparison highlights the inconsistencies and complexities that users face.

4.6 A Comparative Analysis of The Data Management on Smart Home Devices

This section provides a comparative analysis of data management features across five categories of smart home devices. It evaluates the availability and usability of core functions such as deleting a specific recording or all recordings, scheduling deletions, and monitoring usage history.

The results in Table 4.3 demonstrate that the same feature may differ in how it is controlled on different platforms of the same device. Additionally, some features may not be available on certain smart devices, and executing certain features may require varying steps, which could cause inconvenience to the user.

Table 0.3: Comparing Data Management Features Across Multiple Smart Devices and Devices Categories

Features Platform	Deleting a Specific Recording	Deleting all Recordings	Scheduling Deletions	Monitoring Usage Habits
Amazon Echo Dot Speaker	Voice Recording - Done via the Amazon website or Alexa app. - User needs to select each specific recording and confirm the deletion request (user	Voice Recording - Via the Amazon website or Alexa app - Needs at least nine steps to complete.	Voice Recording - Done via the Amazon website or Alexa app. - Needs at least eight steps to complete.	Voice Recording - Done via the Amazon website or Alexa app. - Needs at least four steps to complete.

Features Platform	Deleting a Specific Recording	Deleting all Recordings	Scheduling Deletions	Monitoring Usage Habits
	must do this N times to delete N recordings			
Google Nest Speaker	Voice Recording - Via the Google Account or Google Home app - The process needs at least nine steps to complete, and the user must select each recording and confirm the deletion request.	Voice Recording - Via the Google Account or Google Home app - Needs at least ten steps to complete.	Voice Recording - Via the Google Account or Google Home app - Needs at least eight steps to complete.	Voice Recording - Via the Google Account or Google Home app - Needs at least three to four steps to complete.
Apple HomePod Speaker	N/A	Voice Recording - Via Home app - Requires four choices to complete.	N/A	Voice Recording - Via the Home app or Siri - Requires three steps to complete. - Alternatively, activate Siri by saying “Hi Siri” and then ask Siri “Show me my Siri history.”
Sony TV	Recorded Content such as photos or video. - Via remote control - Requires three choices to complete	Recorded Content such as photos or video. - Via remote control - Requires five choices to complete	N/A	N/A
Samsung TV	Recorded Programme - Via remote control - Requires six choices to complete	Recorded Programme - Via remote control - Requires five choices to complete	N/A	Recorded Programme - Via remote control - Requires three choices to complete
Roku TV	N/A (It lacks storage capabilities)	N/A (It lacks storage capabilities)	N/A (It lacks storage capabilities)	N/A (It lacks storage capabilities)
Amazon Thermostat	Temperature and voice recordings - Via Alexa app - Requires seven steps to complete	Temperature and voice recordings - Via Alexa app - Requires eight steps to complete	N/A	Temperature and voice recordings - Via Alexa app. - Needs at least four steps to complete.
Netatmo Thermostat	Temperature and boiler activity - Via Netatmo Energy app - Requires five steps to complete.	N/A	N/A	Temperature and boiler activity - Via Netatmo Energy app - To view the history for seven days.

Features Platform	Deleting a Specific Recording	Deleting all Recordings	Scheduling Deletions	Monitoring Usage Habits
				Requires five steps to complete.
Ecovacs Deebot Vacuum	Photos or Videos - Via Ecovacs app. - Requires five choices to complete. Navigation data - Via Ecovacs app - Requires five steps to complete.	- Via Ecovacs app. - Requires five choices to complete	N/A	Photos or Videos History - Via Ecovacs app. - Requires five choices to complete
Eufy Vacuum	N/A (no information available)	N/A (no information available)	N/A (no information available)	N/A (no information available)
iRobot Vacuum	Photos or video - N/A Location information - Via iRobot app - Requires six choices to complete.	N/A	N/A	Cleaning History - Via iRobot app - Requires two steps to complete.
Ring Security Camera	Recorded Video - Via Ring app - Requires six choices to complete	Recorded Video - Via Ring app - Requires six choices to complete	N/A	N/A
Nest Security Camera	Recorded Video - Via Nest app - Requires five choices to complete	Recorded Video - Via Nest app - Requires five choices to complete	Recorded Video - Via Nest app - Requires seven choices to complete	Recorded Video - Via Nest app - Requires three choices to complete
Eufy Security Camera	Recorded Video - Via Eufy app - Requires six choices to complete.	Recorded Video - Via Eufy app - Requires six choices to complete.	N/A	Recorded Video - Via Eufy app - Requires three steps to complete.

The comparative analysis of data management capabilities presented in Table 4.3 indicates significant inconsistencies and challenges in managing personal data across smart home devices. For instance, the process of deleting specific recordings often required multiple confirmations for each item, which can be complex for users. Furthermore, the lack of options for scheduled deletions, which is an important feature for maintaining long-term privacy, exists in most smart devices. Some platforms, such as certain televisions and vacuum cleaners, do not offer any means of data deletion, leaving users to retain sensitive information indefinitely. These differences point to a wider issue: the absence of standardised data management within

smart home devices. This highlights the urgent need for a proposed dashboard that aims to simplify and unify these data management processes, enhancing user control and privacy.

4.7 Summary

This chapter critically examines the security, privacy, and data management features of various smart home devices, showing significant inconsistencies in their implementation across different manufacturers and device categories. The analysis exposes systemic challenges, such as fragmented authentication mechanisms, irregular security update practices, limited privacy controls, and the lack of standardised data management options. These gaps not only complicate the user experience but also expose households to increased security and privacy risks. Additionally, the absence of clear, centralised interfaces forces users to navigate multiple applications and complex procedures, resulting in reduced transparency and control over their data. Collectively, these findings highlight the need for an integrated solution. Building on this analysis, the following chapter introduces the proposed harmonized security and privacy dashboard for smart home devices, designed to unify and simplify these functions, thereby providing users with a consistent and intuitive way to manage security, privacy, and data across various smart home ecosystems.

Chapter Five

A Harmonized Security and Privacy Dashboard for
Smart Homes

This chapter presents and discusses the design requirements and development of the proposed Smart Home Security and Privacy Dashboard. It details the evolution of design concepts, the design process, and the final implementation, emphasising the decisions and refinements that shaped its functionality and user experience. The chapter traces the progression from early design concepts to the high-fidelity prototype used in this research, explaining the design approach, tools, and iterative improvements made throughout the process. It also describes the overall structure of the Dashboard and the usability considerations that guided its development. Finally, it provides detailed descriptions of the individual interfaces and their roles in helping users manage security and privacy tasks effectively, concluding with a summary of the primary design outcomes.

5.1 Dashboard Requirements

The examination of security, privacy, and data management features across different smart home devices reveals significant inconsistencies, fragmented controls, and restricted user authorisation. Therefore, these observations highlight the importance of showing a clear set of requirements that the proposed Dashboard must meet to address the existing gaps in smart home devices effectively.

1. Provide a Unified Interface

Establishing a centralised platform that provides unified access and control over security, privacy, and data management settings across all smart home devices, regardless of manufacturer, is essential. Such an approach simplifies the user experience, reduces fragmentation, and supports a more integrated ecosystem. Consolidating device management into a single application enables coherence and usability, which in turn enhances both functionality and user trust in smart home technologies.

2. Consolidate Security and Privacy Controls

The Dashboard should harmonise related functionalities, such as device status, tracking permissions, and update management, into a single comprehensive view. This integration aims to minimise cognitive overload and enhance the user's decision-making process, thereby promoting a more intuitive management experience.

3. Real-Time Status and Alerts

It is essential to maintain consistent awareness of the health of smart home devices, potential security risks, and pending updates. Utilising clear visual indicators and receiving timely notifications ensures that users remain informed about their smart home environment. Such a proactive approach strengthens overall security while enabling users to act quickly and confidently when issues arise.

4. Unify Data Management Mechanisms

It is important to provide consistent methods for deleting specific recordings, all recordings, scheduling automatic deletions, and reviewing usage history for all smart home devices. Such standardisation not only simplifies the user experience but also ensures alignment with data privacy regulations, instilling greater trust in users and demonstrating responsible data handling.

5. Clear Categorisation of Data

It is necessary to differentiate between various types of data, including tracking information and stored content, in order to promote transparency and help users understand data flows more effectively. This clarity is crucial for users to grasp how their information is collected, processed, and retained.

6. Role-Based Access Control

In order to enhance both security and usability in environments with multiple users, it is essential to implement support for various user roles, such as admin, adult, child, and guest. Establishing tailored permissions for each role enables a balanced approach between protection and accessibility across diverse user interactions.

7. Cross-Device Compatibility

The proposed Dashboard aims to seamlessly manage a comprehensive range of device types, including Smart TVs, Smart Speakers, Smart Thermostats, Security Cameras, and Robotic Vacuums, among others. By ensuring compatibility across this diverse landscape of innovative technologies, the Dashboard will cultivate a more integrated and user-friendly experience. This approach not only enhances functionality but also caters to the unique preferences and requirements of various households, enabling users to control and monitor their smart home devices easily.

Consequently, meeting these requirements will ensure that the proposed Dashboard can effectively address the systemic challenges of the current smart home ecosystem. The design will harmonise information from various smart home devices, providing a consistent and user-friendly platform. This will enhance users' control over their personal data while improving the security and privacy of their smart home devices.

5.2 Dashboard Design Process

The design process for the proposed dashboard was driven by the necessity to address specific requirements and overcome the limitations identified in existing solutions, including the preliminary MSc prototype documented in Appendix H. After critically examining that prototype and identifying its fragmented approach to security and privacy management, this section introduces the evolution of the PhD dashboard. By building on the lessons learned

regarding the need for unified information presentation and simplified navigation, the PhD prototype underwent two major iterations. These included a low-fidelity sketch created in draw.io followed by a high-fidelity interactive prototype developed in Figma. These iterations represent a strategic shift from conceptual exploration to an evaluative platform designed to support user studies and measure the effectiveness of the proposed interface in enhancing user control and comprehension within the smart home environment.

The initial version, as presented in Figure 5.1, was created using draw.io, a web-based diagramming tool that enables the creation of diagrams, flowcharts, and other visual representations of data. At this stage, this tool facilitated rapid exploration of low-fidelity concepts, and the focus was primarily on establishing the information architecture rather than aesthetics or detailed interaction flows. The Dashboard was structured around four top-level entry points, which are Rooms, Devices, User Data, and Data Types, reflecting the different ways in which users conceptualise control in a smart home. This early conceptual mapping enabled evaluation of whether navigating these distinct routes would help users locate and manage security and privacy features effectively. During the initial design phase using the draw.io tool, several refinements were made, including clarifying icon labels and enhancing visual elements such as imagery and colour schemes, to improve usability and maintain visual coherence. This conceptual version was presented in the publication of the Dashboard work, where it functioned as a pivotal proof-of-concept for the proposed structural framework. This early iteration demonstrated the Dashboard's potential features, highlighting its innovative design and user interface.

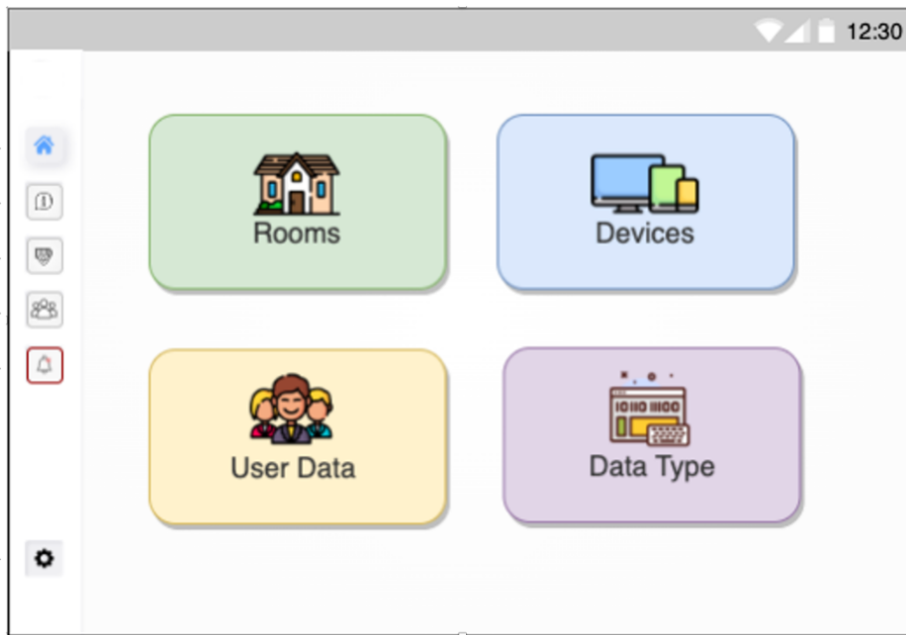


Figure 5.1: Initial Version Dashboard Design

After conducting a thorough validation of the structural logic, the design progressed to an advanced high-fidelity prototype developed in Figma, as shown in Figure 5.2. This version introduced a significant visual and functional evolution. Unlike the abstract icons in the draw.io version, the Figma design utilised photographic images, refined colour palettes, and an enhanced visual hierarchy, creating a more realistic and engaging user environment.

In the initial draw.io prototype as presented in Figure 5.1, the side navigation bar featured placeholders that served as a conceptual framework for the overall structure of the Dashboard. These placeholders, while indicative of the intended layout, lacked any functional interfaces, making them purely illustrative at that stage of development. In contrast, the high-fidelity Figma prototype fully developed each icon into dedicated interfaces, as illustrated in Figures 5.7–5.13. These included the Information Page, Health Status, Software Update, People, Device Management, and Settings.

This transition marked a significant shift from abstract structural planning to interactive and visually polished interfaces that facilitated realistic user interactions and evaluations.

Furthermore, the Figma version enhanced its functionality by enabling users to perform practical tasks, such as turning off a microphone, managing location settings, and deleting recordings, which were not possible in the initial prototype.

This transition from low-fidelity sketches to a polished high-fidelity interface demonstrates a careful and methodical design process. By advancing from conceptual exploration to a realistic and interactive environment, the Dashboard was developed into an evaluative platform. This platform is suitable for usability testing and for assessing how users interact with and utilise the integrated security and privacy features.

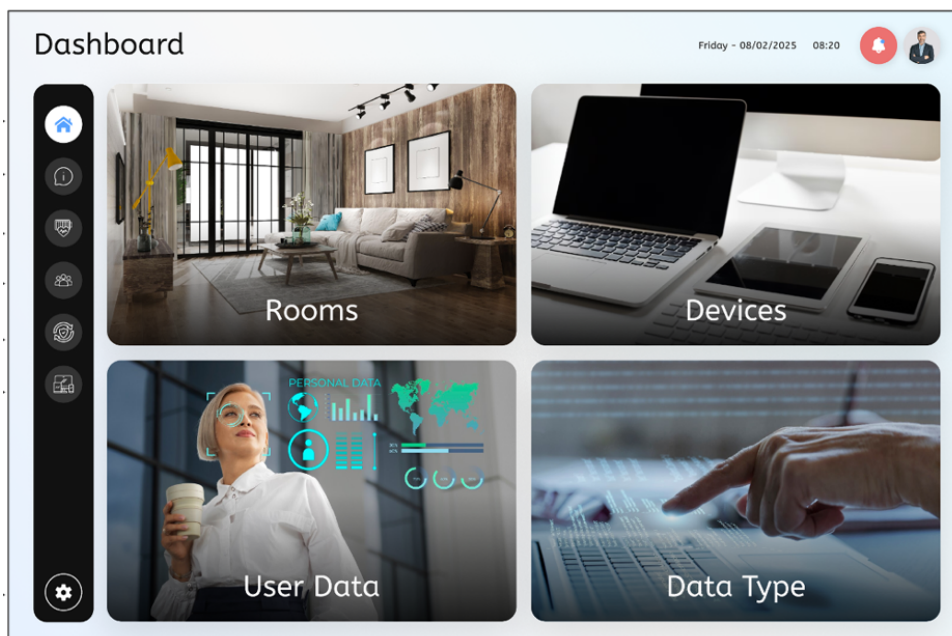


Figure 5.2: Final Version of Dashboard Design

5.3 Dashboard Structure

The Dashboard is designed to provide users with an efficient means to ascertain the status of their smart home devices from different perspectives, such as room locations, device types, device users, and data locations. These perspectives serve as the top-level entry points, allowing users to navigate to specific routes that provide views of individual devices and their associated status and settings. The structure of the dashboard and some of the routes to individual devices are illustrated in Figure 5.3. It is important to note that the dashboard's design is tailored to enhance user experience, providing them with the necessary information in a clear, concise, and intuitive manner.

In our comprehensive analysis of various smart devices, the features of interest were categorized into three significant categories, namely are Security, Privacy, and Data Management. These categories have been identified based on earlier research into the features, which has revealed that all smart devices include these aspects, though often presented in different menu formats. The Security category encompasses registration, authorisation, authentication, and security updates, which are essential for safeguarding user data. The Privacy category encompasses microphone access, location services, camera use, and usage habits, all of which are essential to protecting user privacy. The Data Management category comprises deleting specific or all recordings, scheduled deletions, and usage history, all of which are important for effectively managing user data. The Dashboard's tablet-centric prototype design is detailed in Section 5.7, which provides a comprehensive overview of its interfaces.

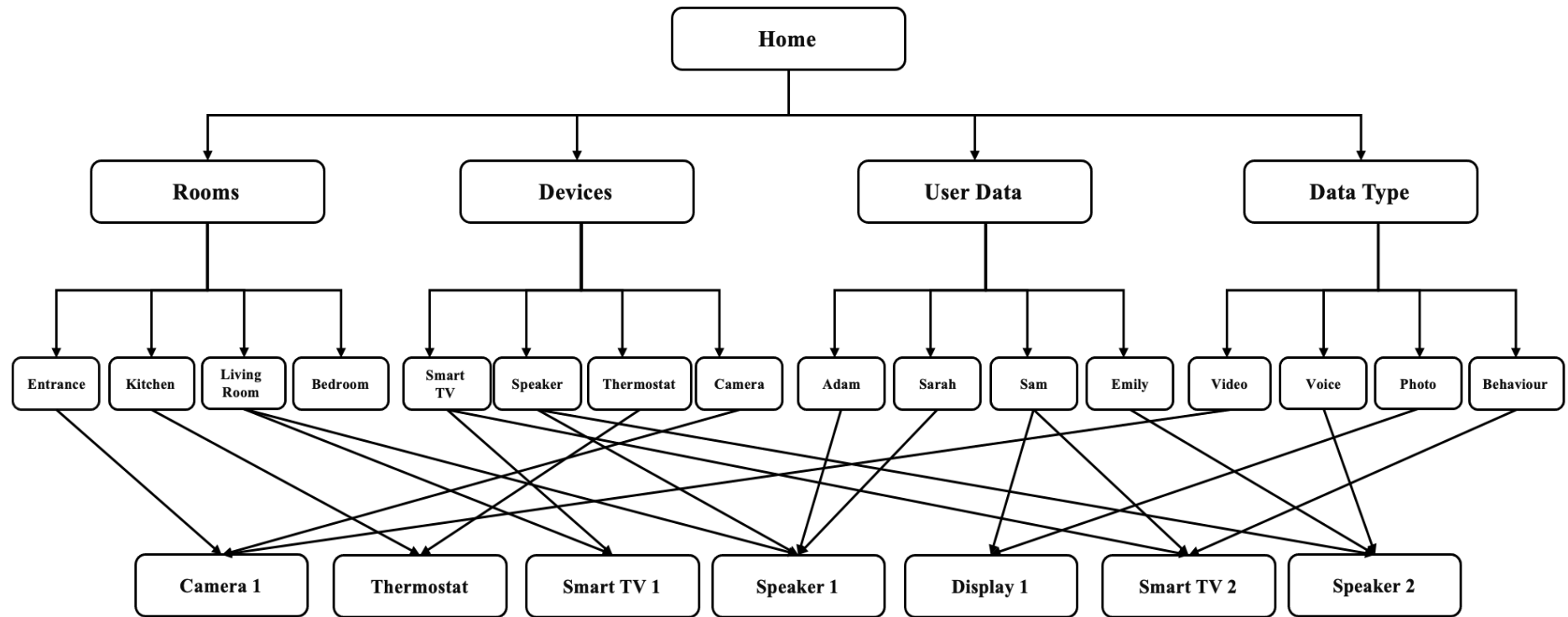


Figure 5.3: Dashboard Navigational Structure

5.4 Dashboard Architecture

This section introduces the architectural design of the proposed smart home dashboard, detailing how its key functionalities are organised to support a cohesive and user-centred interaction paradigm. The architecture is informed by the limitations identified in prior designs, particularly with respect to interface fragmentation and interaction complexity. By adopting a layered structure, the design seeks to enhance usability, minimise cognitive load, and provide users with a coherent overview of security and privacy across the smart home ecosystem.

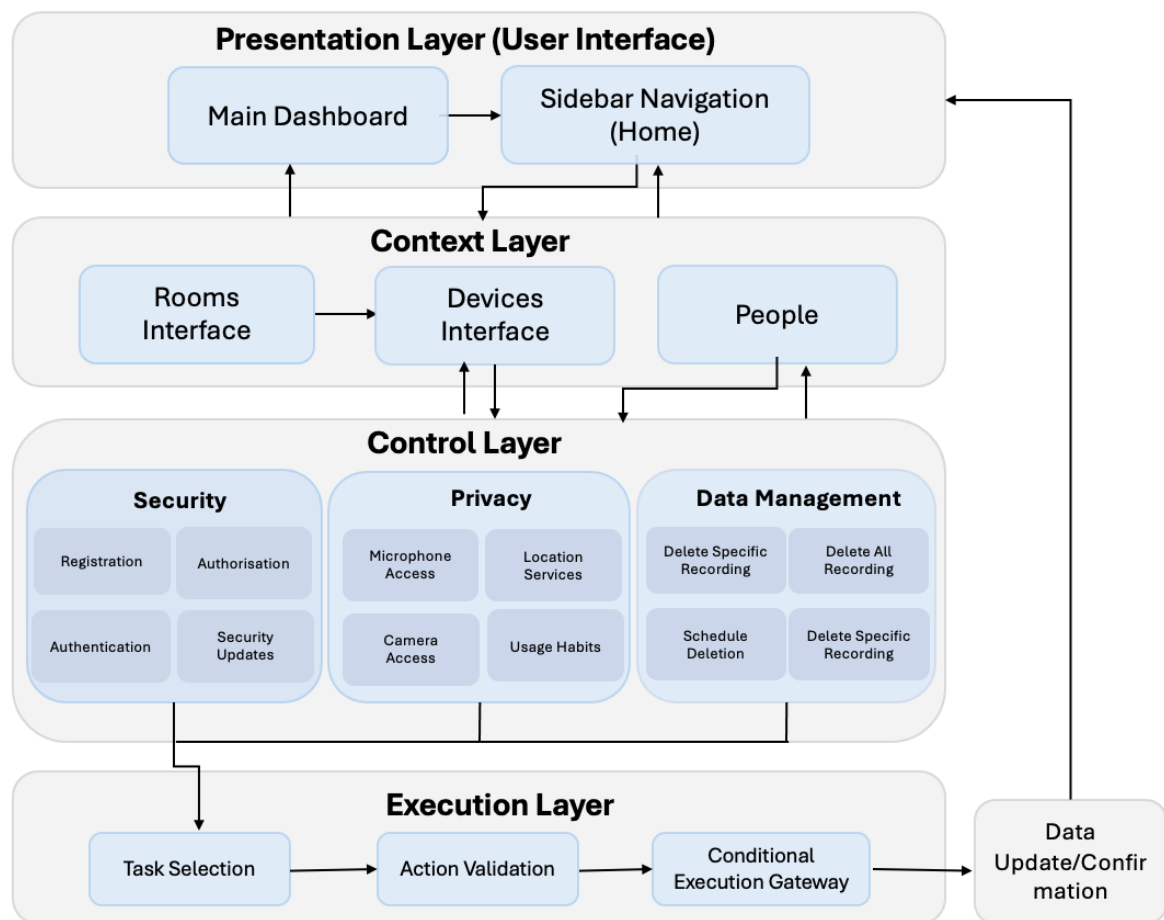


Figure 5.4: Conceptual Architecture of the Dashboard Prototype

Figure 5.4 illustrates the architecture of the proposed dashboard prototype, illustrating the conceptual organisation of the system and the distribution of its core functionalities across different levels of interaction. Rather than depicting a technical implementation, the figure

provides a high-level abstraction that reflects the underlying design rationale discussed throughout this chapter. The architecture is structured into four primary layers, as outlined below:

- **Presentation Layer (UI):** This layer represents the user-facing interface, including the main dashboard and sidebar navigation. It enables users to interact with the system, access different sections, and receive visual feedback regarding device status, security alerts, and privacy settings.
- **Context Layer:** This layer organises the smart home environment into meaningful perspectives, such as rooms, devices, and people. It enables users to navigate the dashboard based on their preferred view, whether by location, device type, or household member, thereby supporting intuitive and flexible interaction.
- **Control Layer:** This layer groups the core functional categories of the dashboard, including Security, Privacy, and Data Management. It provides structured access to key features such as authentication, security updates, and data handling operations, ensuring that all interactions are managed consistently across devices.
- **Execution Layer:** This layer represents how user actions are processed within the prototype. It includes task selection, action validation, and conditional execution, followed by data update or confirmation. This ensures that user actions are checked and confirmed before being applied, maintaining system reliability and user control.

Together, these layers provide a cohesive structure that supports clear interaction flow and enhances the overall usability of the dashboard. This layered organisation ensures that user actions are efficiently translated into system responses while maintaining clarity, control, and flexibility.

5.5 Usability Principles in Dashboard Design

To ensure that the Dashboard prototype met widely recognised usability standards, its design was evaluated against Nielsen's ten usability heuristics (Nielsen, 1994). These heuristics provide a comprehensive framework for user interfaces, addressing key aspects such as visibility, consistency, error prevention, and support for both novice and expert users.

This assessment aimed to bridge the gap between theory and practice by translating the usability and user-centred design principles discussed in Appendix A into specific design decisions. As a result of this process, several refinements were made to the Dashboard, ensuring that security and privacy information was presented in a manner that is not only accessible to non-technical users but also adheres to established HCI standards. Table 5.1 provides an overview of how each of Nielsen's heuristics was interpreted and operationalised within the Dashboard interface. It highlights the principles that have been successfully implemented while also identifying areas that still require further enhancement.

Table 5.1: Mapping Nielsen's Usability Principles to the Dashboard Design

Heuristic	Description	Application in Dashboard Design	Applied in Dashboard
1. Visibility of System Status	The system should always keep users informed about what is going on through appropriate feedback.	Implemented via Health Status icon, Software Update and Security Notifications that inform users about device security updates, data tracking, and privacy risks in real-time.	Fully applied.
2. Match Between System and Real World	The system should speak the users' language, with words, phrases and concepts familiar to the user, rather than system oriented terms. Follow real-world conventions, making information appears natural logical order.	Familiar labels like "Rooms", "Devices", "Data Types", and "User Data" are used, along with intuitive icons such as home, people, and settings, which align with common smart home terminology. This approach follows real-world patterns, ensuring that information appears in a natural and logical order for users, thereby reducing the learning curve and promoting intuitive navigation.	Fully applied.
3. User Control and Freedom	Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state	Provided continuous navigation flexibility through a persistent sidebar and breadcrumb links, enabling users to easily move between sections without relying on a traditional back button. Additionally, confirmation prompts	Fully applied.

Heuristic	Description	Application in Dashboard Design	Applied in Dashboard
	without having to go through an extended dialogue. Support undo and redo.	appear before any irreversible actions, such as deleting a specific recording, ensuring that users maintain control over important decisions.	
4. Consistency and Standards	Users should not have to wonder whether different words, situations, or actions mean the same thing.	Maintain a consistent vertical arrangement of navigation icons on the left side of all screens, along with an appropriate colour scheme that features a light background with grey and black accents. Additionally, implement a standardised navigation flow. This design approach enables predictability and minimises cognitive effort when users are finding and utilising the functions on the Dashboard.	Fully applied. Fixed icon placement and uniform visual standards across all screens
5. Error Prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. Either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.	Confirmation dialogs are displayed before all critical actions, such as delete or reset, with clear and descriptive labels to minimise the risk of accidental clicks.	Fully applied.
6. Recognition Rather than Recall	Minimize the user's memory load by making objects, actions, and options visible. users should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable.	Grouped related items (Rooms, Devices, User Data (Data Type) are visibly on the main interface, ensuring that users can select options directly without needing to recall details from previous interactions. This design approach minimises cognitive load and supports efficient navigation.	Fully applied.
7. Flexibility and Efficiency of Use	Accelerators unseen by the novice user may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.	The Dashboard employs a simple navigation structure that supports novice users by minimising complexity and providing clear access to essential functions. Although advanced shortcuts, such as a search bar or customisable quick actions, were not included in this version to prioritise clarity and reduce cognitive load for initial testing, the design framework is flexible enough to incorporate these enhancements in future updates, improving efficiency for experienced users	Partially applied . Shortcuts planned for future.
8. Aesthetic and Minimalist Design	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.	The Dashboard adopts a clean and uncluttered layout, using a light off-white background, minimal text, and essential icons to reduce cognitive load and direct attention to key interactive elements. Visual hierarchy is maintained through balanced spacing, consistent iconography, and selective use of colour highlights, ensuring that	Fully applied.

Heuristic	Description	Application in Dashboard Design	Applied in Dashboard
		only relevant information is presented on each screen.	
9. Help Users Recognise, Diagnose, and Recover from Errors	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.	Basic confirmation messages and notifications are provided to help users recognise potential errors before they occur. However, the prototype does not currently include detailed error diagnosis or guided recovery mechanisms due to the limited scope of this iteration. These capabilities are identified as important enhancements for future development to provide comprehensive support in error management.	Partially applied. Basic error recognition provided; detailed diagnosis and recovery planned for future versions.
10. Help and Documentation	It may be necessary to provide help and documentation. Any information should be easy to search, focused on the user's task, list steps to be carried out and not be too large.	The Dashboard features a comprehensive Information Page that offers various help resources. This includes instructions for using the Dashboard, frequently asked questions (FAQs), multilingual device tutorials, and access to a support centre. These resources provide immediate, context-relevant assistance, allowing users to find help without leaving the Dashboard environment. Although a fully searchable knowledge base was not included due to the prototype's scope, the available resources still offer substantial support for users onboarding and troubleshooting.	Partially applied. Help resources included via the Information Page; a full, detailed user manual was not developed as it was beyond the aims of this prototype.

The Dashboard design addressed nearly all of Nielsen's heuristics, as shown in Table 5.1. Some heuristics were fully implemented, such as visibility of system status, consistency and standards, and error prevention. Others were partially incorporated, including advanced flexibility for expert users, comprehensive error diagnosis, and extended help documentation. The primary focus was on developing a straightforward, intuitive, and privacy-centred interface for the non-technical user. Nonetheless, these elements remain significant considerations for future iterations, as they could further enhance efficiency.

The heuristic evaluation confirmed that the Dashboard aligned well with established usability standards while maintaining a strong focus on user comprehension and control. Given the

Dashboard's consideration of security and privacy, it is also essential to evaluate how effectively it communicates concepts of protection, trust, and decision support to users. Therefore, the following section extends this analysis by applying principles from Human–Computer Interaction for Security (HCISec), which specifically address the unique usability challenges faced by security-oriented systems.

5.6 HCISec Principles Relevant to Security Dashboards

In addition to Nielsen's general usability heuristics, this study also considered principles specific to Human–Computer Interaction for Security, which address unique challenges encountered in security-oriented systems. Prior studies highlight several factors particularly relevant to security dashboards (Ibrahim et al., 2010; Johnston et al., 2003). These principles were incorporated to ensure the prototype not only adhered to standard usability norms but also communicated security and privacy information effectively for both technical and non-technical users.

- **Visibility of Security Status**

Users must maintain an ongoing understanding of the current security status of their devices and data, which includes health indicators and real-time security notifications.

- **Minimal Use of Jargon**

Avoid technical or ambiguous terminology and providing plain-language alerts to make security concepts accessible to all users.

- **Support for Decision-Making**

Providing contextual information within security prompts, to enable informed decisions without overwhelming the user.

These HCISec-specific considerations complement Nielsen's heuristics by addressing the intersection of usability and security. Their incorporation ensures that the design of the

Dashboard not only provides a clear and intuitive interface but further supports users in managing their security and privacy-related tasks.

Building on the usability heuristics and HCI-Sec principles outlined above, the subsequent section details how these guidelines were operationalised within the Dashboard prototype. Subsequent interfaces illustrate the application of these principles in practice, demonstrating how security and privacy information was harmonised and presented to users across different interaction points such as rooms, devices, user data, and data types

5.7 Dashboard Interfaces

This section provides a comprehensive overview of the primary interfaces of an interactive prototype designed to function as a security and privacy dashboard for smart homes. The prototype, currently optimised for tablet use, was developed using the Figma design tool, which is a cloud-based collaborative platform that enables the creation of high-fidelity user interface mock-ups and interactive prototypes. Figma was chosen because it supported real-time collaboration, interactive prototyping, and precise control over layout and visual hierarchy. These features were essential for accurately simulating the dashboard's realistic interaction flow. The primary purpose of the dashboard is to provide users with an intuitive, functional way to manage the security and privacy of their smart home devices.

Figure 5.5 provides an overview of the entire Figma workspace. This screenshot illustrates the full scope of the design work, showing the interconnections between all dashboard interfaces and the navigation flow across the prototype. It demonstrates the complexity and scope of the design development undertaken during this research, highlighting the comprehensive structure established for the Smart Home Security and Privacy Dashboard. This detailed overview ensured that the entire dashboard structure was prepared for user testing as a complete and functional system. The details in the figure are not meant to be legible; rather, the illustration

is intended to convey the overall scope and complexity of the completed design work. For readers interested in a more in-depth exploration of the design, more detailed and readable versions of the dashboard interfaces can be found in Appendix D.

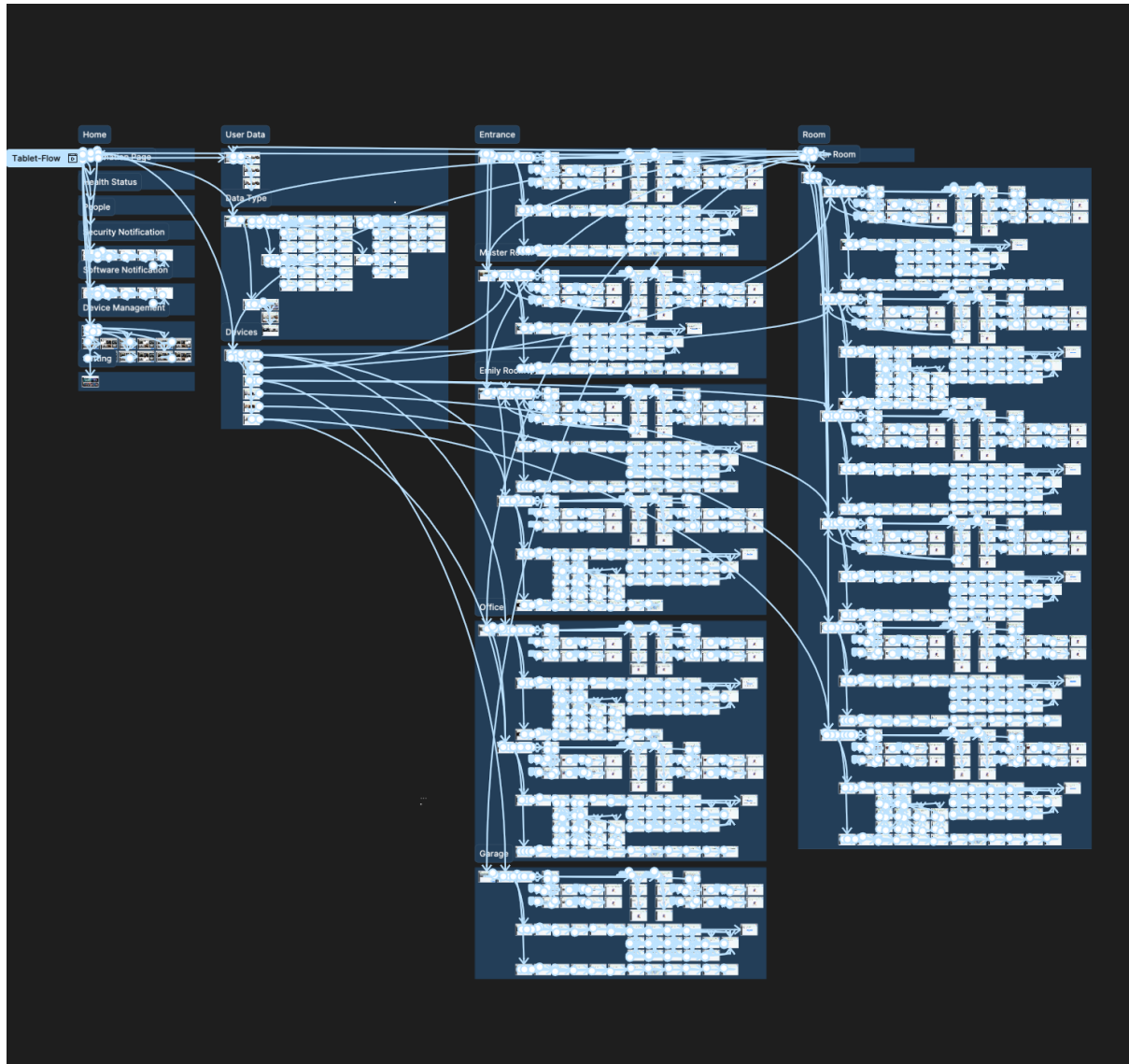


Figure 5.5: Full Figma Workspace Showing Dashboard Flow

During the design phase of the Dashboard interfaces, numerous aspects were considered, including the “What You See Is What You Get” (WYSIWYG) principle (Singapore et al., 1995). Accordingly, the research aimed to achieve the notion that users should see what they expect to see on the interface without any hidden functionality or connotations. This ensures

transparency, simplicity, and user-friendliness of the interface. Additionally, according to Wen (2021), designers must exercise careful consideration in selecting colour schemes, particularly concerning text information, because the text is the foundation of the entire interface and must be easily legible, with a high degree of contrast from its background colour. This is crucial to enable users to promptly discern the unique application characteristics and functions of software upon their initial reading. Moreover, the colours employed must be conducive to guiding the user in operating the software with ease. As part of our design approach, we have deliberately implemented a light gradient background, inspired by the white backgrounds frequently utilised in User Interface (UI) design. This decision ensures that other interface elements are more prominent, creating a clean and minimalist aesthetic.

Furthermore, it is recommended to use a consistent colour scheme for a light gradient background dashboard to ensure a uniform and recognizable look (Bryson, 2023). For this reason, the selection of black, dark grey, and light green thus was based on their complementary contrast with the light gradient background, which results in clear and legible text. This choice was conceptualised to enhance readability and provide ease of use to the user.

In situations where the design complexity is considerable, it can be challenging to capture the user's attention effectively (Wen, 2021). As such, during the interface design process, we employed custom images for each button, which effectively enhances the user interface's appeal and ensures it is easy to use.

During the design of the interface, ease of access to all available features was prioritised. Implementing grouping mechanisms in the centralised interface was a significant step. Consequently, grouping mechanisms were designed for rooms, devices, user data, and data types. The following subsection will describe each group in detail.

5.7.1 Home Interface

The initial conceptual illustration of the dashboard's interface, depicted in Figure 5.8, presents a straightforward design that provides users with an efficient means to manage their smart home devices from different perspectives. Therefore, the interface includes four categories, namely rooms, devices, user data, and data types, making it easier for users to browse and display the information. These four categories serve as optimal access points due to their direct relevance to users' primary concerns within a smart home environment. While the interfaces illustrate general navigation within the smart home, specific attention to security/privacy issues could be enhanced by implementing a dedicated Security and Privacy button: integrating a conspicuous icon or button on the main interface, specifically highlighting security and privacy concerns. Selecting this feature could lead to a comprehensive overview or checklist to address potential issues.

The interface comprises six key icons placed on the left-hand side of the screen, each serving distinct functions essential to user navigation and management:

1. **Home:** This icon functions as an entry point, directing users to the main interface, as depicted in Figure 5.6.
2. **Information:** Designed to offer guidance, this icon serves as an informational resource, detailing the dashboard's functionality and elucidating the purpose of each category within.
3. **Health Status:** This icon serves a critical role by displaying the security and privacy status of the devices linked to the system. Factors influencing this status may include tracking devices or the duration for which data has been unremoved.
4. **People:** Representing House members, this icon combines pertinent information such as their names, email addresses, and contact numbers for user reference and communication purposes.

5. **Security Notification:** to notify the users about vital updates such as software updates, security patches, and other critical alerts. Its prominence ensures the user remains informed about crucial device security and privacy.
6. **Device Management:** Enables administrators to control connected devices, manage permissions for different user roles, and adjust device-specific settings, ensuring secure and appropriate access.
7. **Settings:** This icon grants users' access to the general settings, containing language preferences, Wi-Fi settings, and other configurable parameters. Time settings are synchronized with the IP address location derived from the connected Wi-Fi network, ensuring accurate time representation.

Each icon serves a specific and pivotal purpose, contributing to the interface's functionality and user experience and facilitating seamless navigation and control over essential system elements.

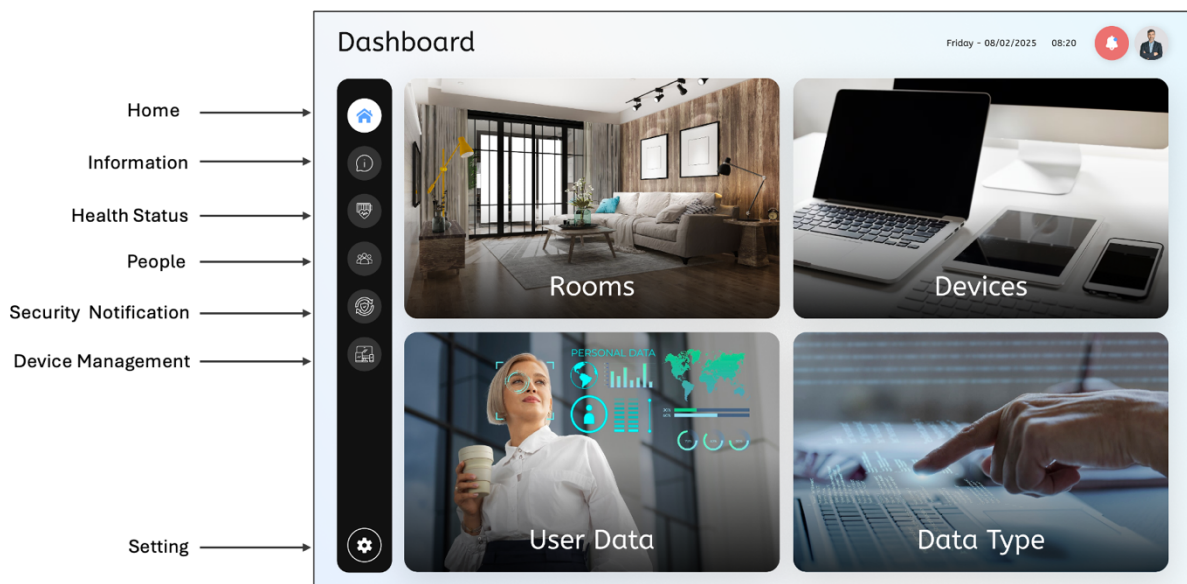


Figure 5.6: Home Interface

After providing a brief overview of the icons on the left side, the following section provides a detailed description of the Home, Information, Health Status, People, Security Notification,

Device Management, and Settings interfaces, highlighting their functional scope and key user interface elements.

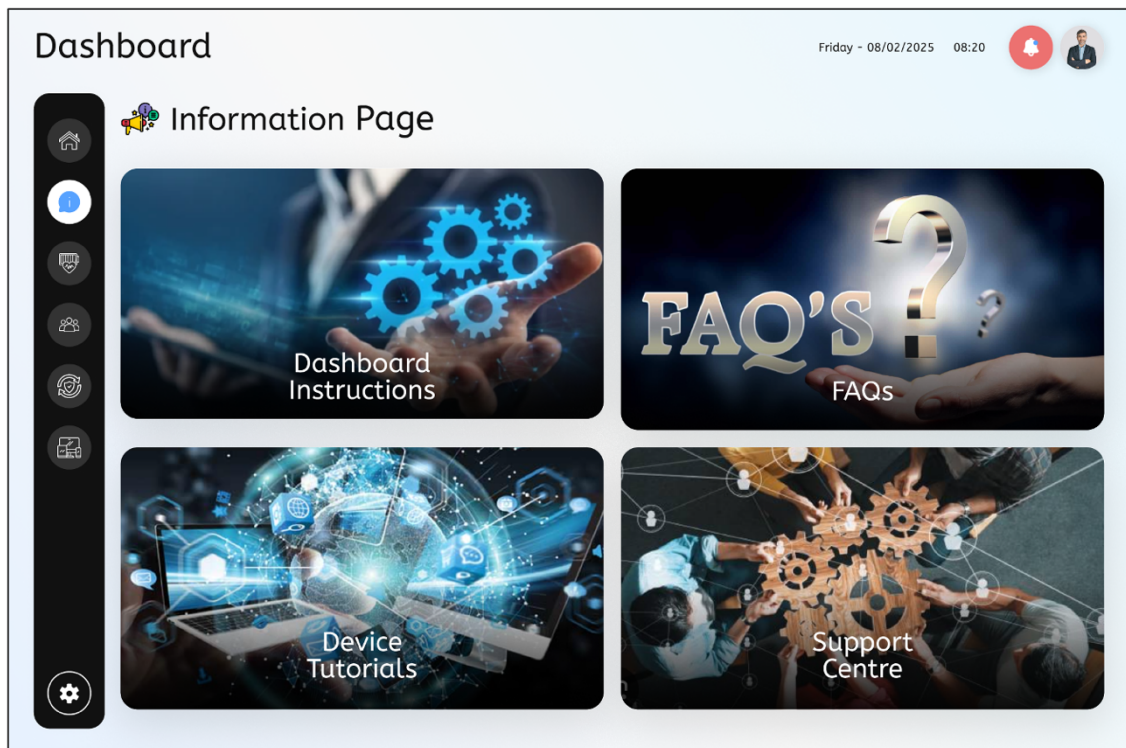


Figure 5.7: Information Page Interface

As shown in Figure 5.7, the Information Page contains essential support resources within the Dashboard. It provides direct access to four key sections, which are the Dashboard itself, Instructions for guided feature usage, a FAQs section that addresses common queries, and Device Tutorials available in multiple languages to meet diverse user needs. Additionally, there is a Support Centre for more specialised assistance. This structure ensures help is readily accessible, reducing cognitive load and facilitating user onboarding and troubleshooting.

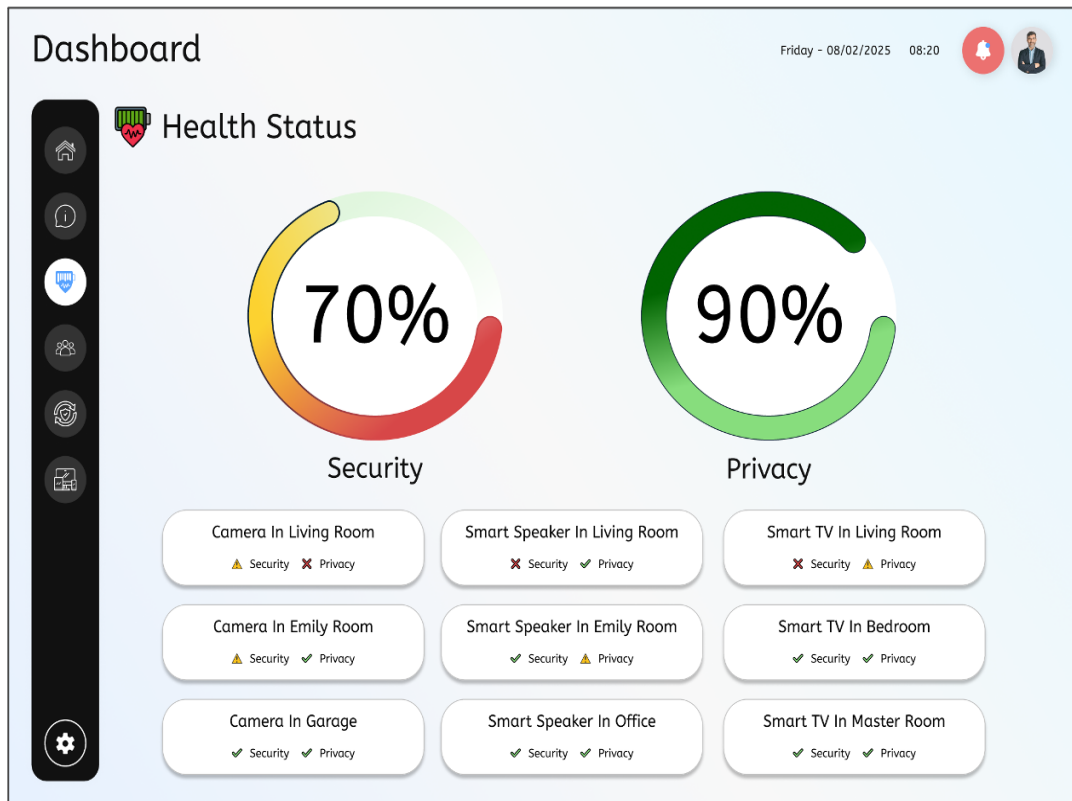


Figure 5.8: Health Status Interface

As illustrated in Figure 5.8, the page displays the household's overall security and privacy health status through two percentage-based gauges. Higher percentages, shown in green, indicate a stronger security or privacy posture. As the percentage decreases, the colour shifts to orange and then to red, signalling increased levels of risk.

A comprehensive list of devices is displayed under the gauges, with each smart device featuring individual security and privacy indicators. The status is shown using:

- ✔ (green check) – compliant and secure.
- ⚠ (yellow warning) – potential issue requiring attention.
- ✖ (red cross) – critical problem needing immediate action.

This design enables users to quickly diagnose system health, prioritise interventions, and maintain optimal protection across their smart home ecosystem.

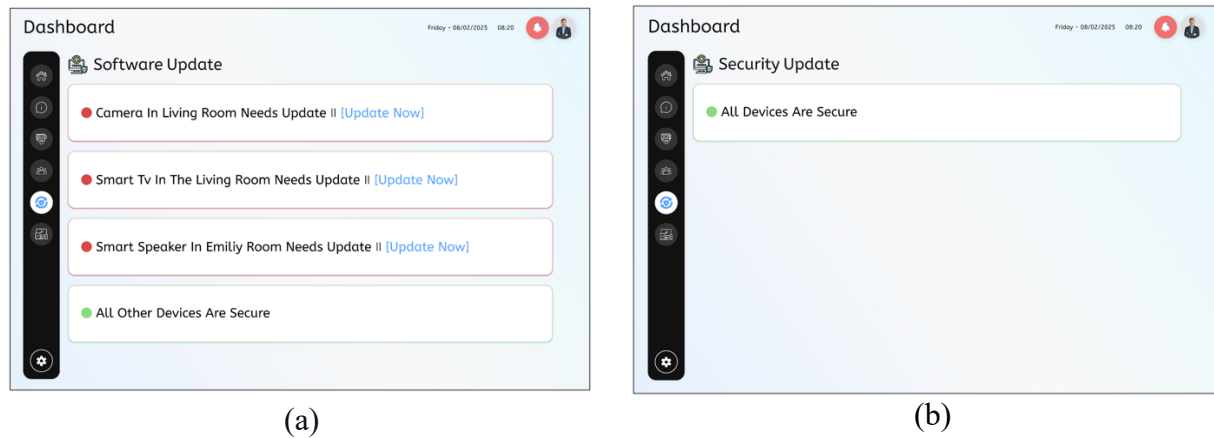


Figure 5.9: Software Update Interfaces

Figure 5.9 presents the Software Update interfaces, designed to provide a brief overview of the update status for all connected smart home devices.

In Figure 5.9(a), the interface displays a list of devices requiring immediate updates, identified by red status indicators, with an “Update Now” link to facilitate immediate user action. In contrast, Figure 5.9(b) is displayed only when all devices are fully updated and secure, presenting a single green status message.

This conditional display ensures that users see only the most relevant information. When an action is required, a detailed list is shown; when the system is fully secure, a simplified confirmation view appears. This approach reduces unnecessary cognitive load and enhances user focus.

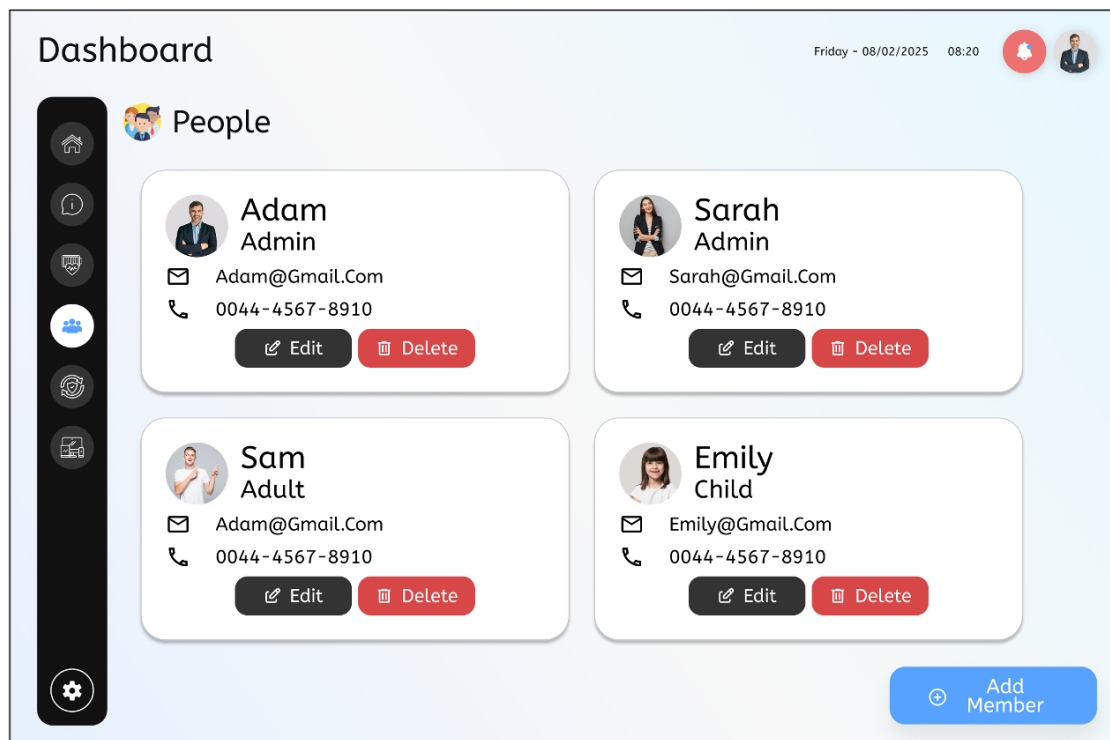


Figure 5.10: People Interface

The People interface, as shown in Figure 5.10, acts as a centralised platform for managing all authorised household members, categorising them according to predefined user roles, which are Admin, Adult, Child, and Guest. Each member's core contact details, such as email addresses and phone numbers, are prominently displayed alongside a profile image, which helps in quick identification.

The interface includes role-based controls directly within each user entry. These controls allow for the editing of personal details and permissions, as well as options for account deletion. Additionally, an "Add Member" button located at the bottom of the interface simplifies the process of adding new users, facilitating immediate role assignment from the start.

From a critical perspective, the separation of user role administration into a reliable interface is instrumental in reducing the complexity associated with device-level permissions management. This design choice enhances the transparency of the system for both administrators and regular users.

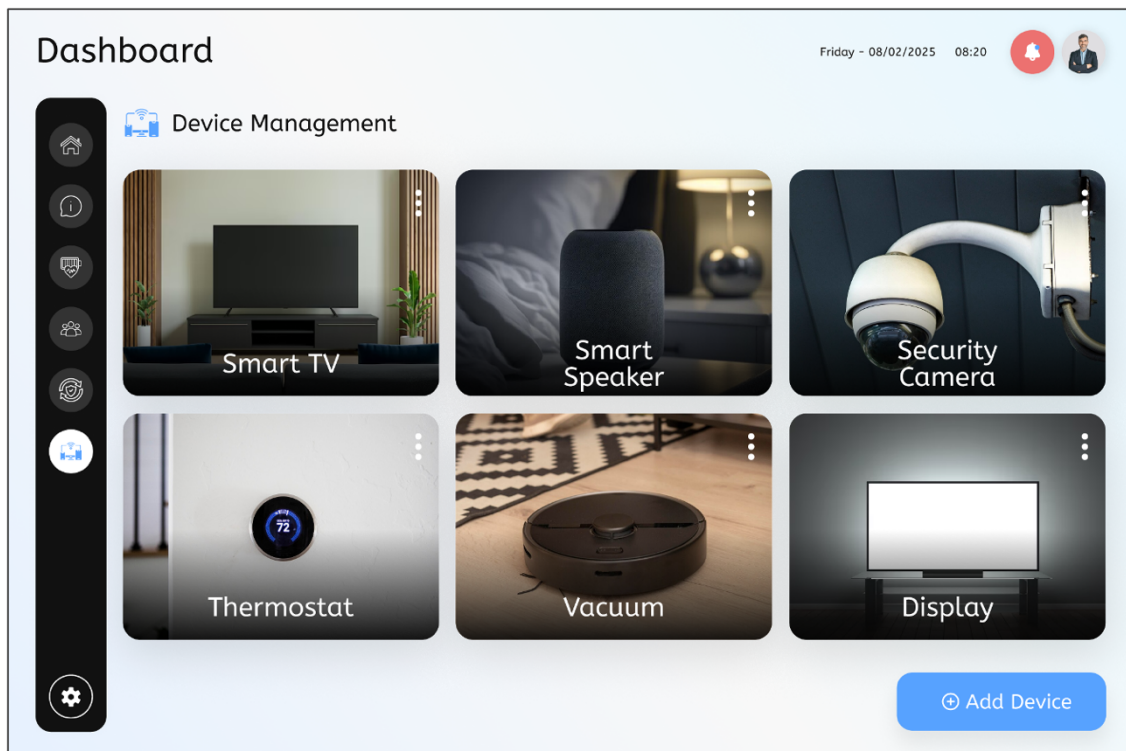


Figure 5.11: Device Management Interfaces – Device Overview

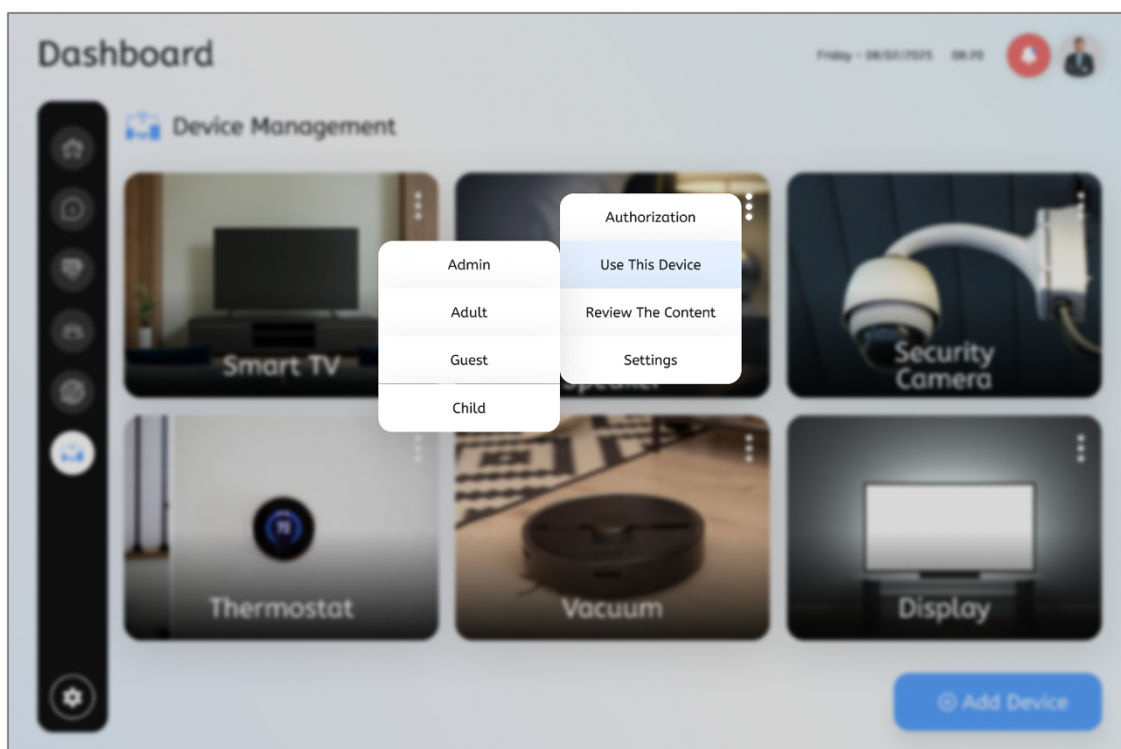


Figure 5.12 : Device Management Interfaces – Role-Based Permissions

The Device Management interfaces, as presented in Figure 5.11 and Figure 5.12 enables the administration of all smart devices within the household, including televisions, smart speakers, security cameras, thermostats, robotic vacuums, and displays. Devices can be added via the Add Device button, while the right-hand options panel provides granular, role-sensitive controls. Depending on the user's assigned role, available actions may include giving Authorisation, allowing Use of This Device, enabling Review of the Content, or accessing Settings.

Critically, permission allocation within this interface is exclusively reserved for admin users, ensuring that device access aligns strictly with security policies and the role definitions established in the People interface. By embedding permission management within the device view, the interface supports the principle of least privilege, enabling tight control over device access.

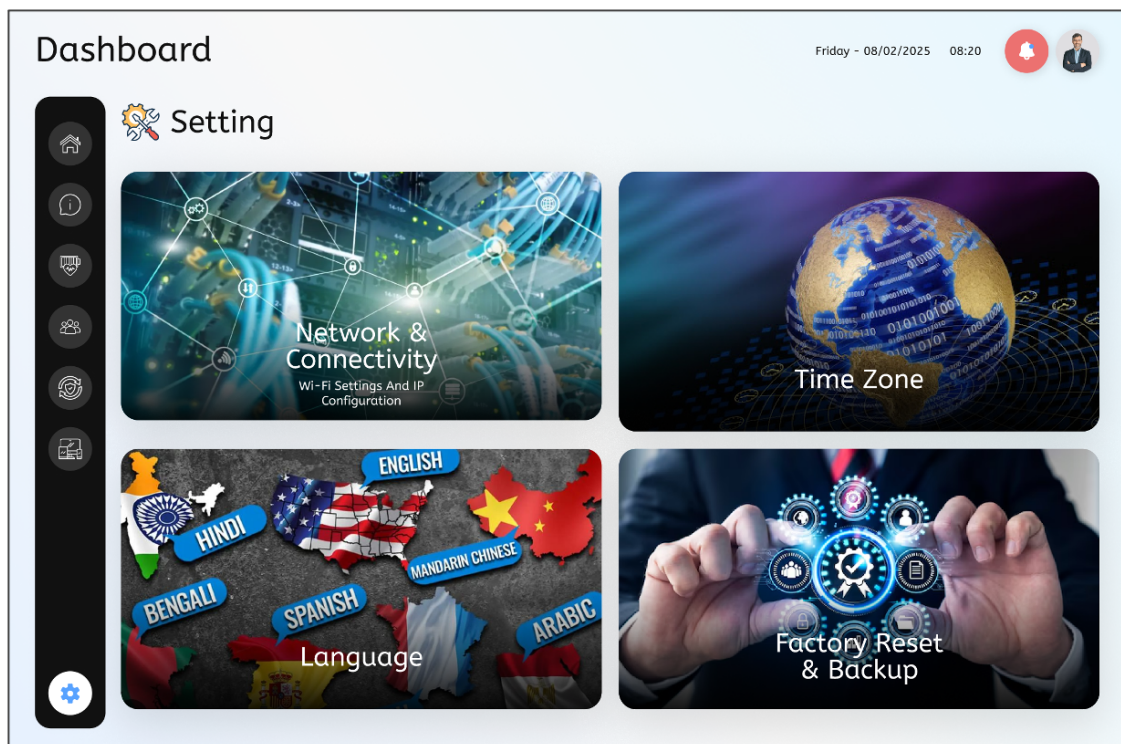


Figure 5.13: Setting Interface

Figure 5.13 presents the Settings Interface, which provides centralised access to essential configuration options within the smart home dashboard. The interface includes modules for managing Wi-Fi settings and IP configuration through the Network and Connectivity option, adjusting system time via the Time Zone feature, selecting preferred languages to enhance accessibility, and performing factory resets or backups to preserve or restore system data. Each module is visually represented by a large, clearly labelled tile accompanied by an illustrative image, enabling quick recognition and facilitating intuitive navigation.

Additionally, the main interface buttons are explained in detail in separate sections. Section 5.7.2 outlines the user's expectations when selecting the Room Button, while Section 5.7.3 clarifies what the user should expect to see when selecting the Devices button. User data is explained in Section 5.7.4, and Data Type is covered in Section 5.7.5.

5.7.2 Rooms Interfaces

When the user clicks the Rooms button, they will be taken through a series of interfaces, as shown in Figure 5.14. The interfaces will guide the user from the top level (Figure 5.14a) to the Privacy button for a specific smart speaker in the living room (Figure 5.14f).

For clarification, the Room Button allows the user to access all the rooms in the house, as shown in Figure 5.14a. From there, they can add or delete rooms, as shown in Figure 5.16b. By clicking on a specific room, such as the living room, the user can view the existing smart devices and add new ones, as shown in Figure 5.14b. Clicking on the "Add Room" button takes the user to a panel where they can enter the name of a new room. Popov et al. (2021) suggested separating the rooms into different buttons and an option for room management.

Moreover, clicking on a specific smart device, such as the Smart Speaker in the living room (Figure 5.14c). The Data Management category includes features such as deleting specific or

all recordings, scheduled deletions, and usage history, which are essential for effectively managing user data (Figure 5.14d). The Security category includes registration, authorisation, authentication, and security updates, which are crucial for protecting user data (Figure 5.14e). The Privacy category includes the microphone, location services, and camera usage. As mentioned in section 4.4, the smart speaker tracks the user via microphone and location (Figure 5.14f).

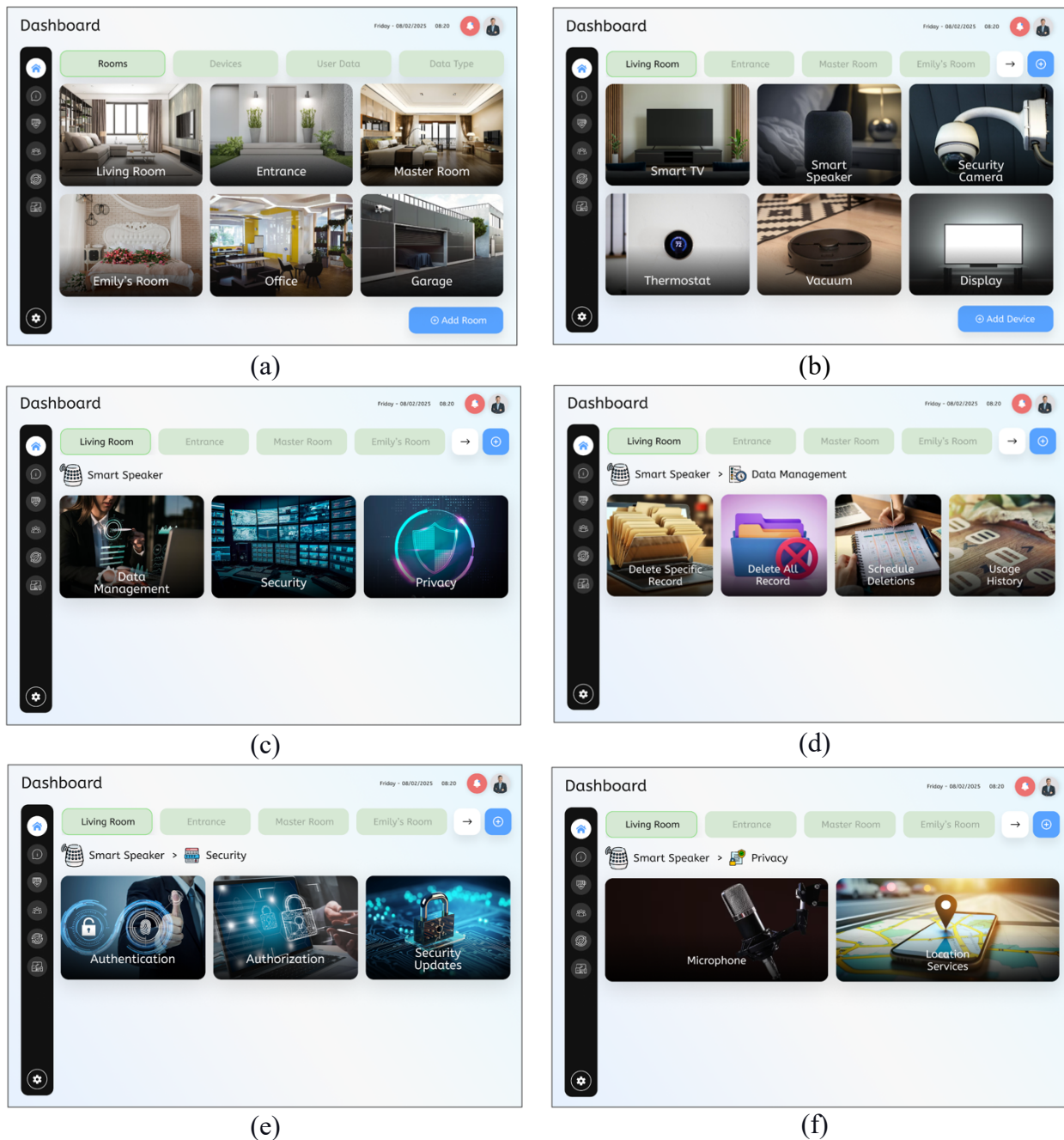


Figure 5.14: Rooms Interfaces

5.7.3 Devices Interfaces

A dedicated button was implemented that facilitates browsing and reviewing all devices within a smart home. This button, as shown in Figure 5.15a, allows users to select a specific device type, such as a speaker, which will subsequently display all rooms containing such devices. For instance, selecting a speaker device presents the user with all rooms with a speaker device installed. In Figure 5.15b, we illustrate an example where the house has three smart speakers in the living room, Emily's room, and the office. Suppose the user chooses to view the speaker in the living room; in that case, all three main categories, Data Management, Security, and Privacy, will be displayed in a similar manner as presented in Figures 5.14c-5.14f.

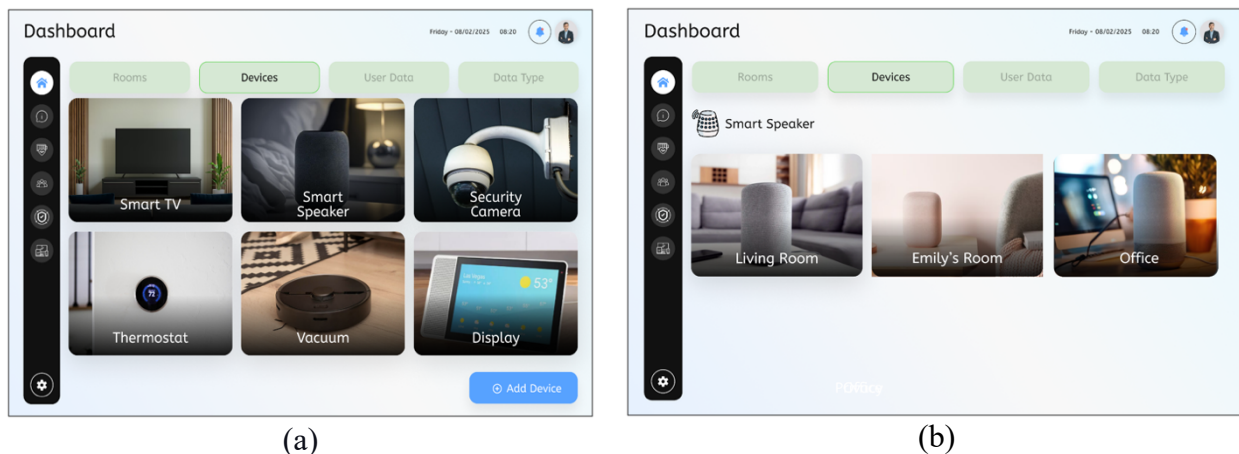


Figure 5.15: Devices Interfaces

5.7.4 User Data Interfaces

Given the widespread use of smart home devices, it is important to acknowledge that such devices invariably collect and record user data. To facilitate user access to this data, we have designed a dashboard that includes a dedicated button for user data display. This interface is designed to display all members of a household (Figure 5.16a). Once a user selects a particular household member, for instance, Emily, all her recordings will be displayed. Notably, as illustrated in Figure 5.16b, Emily's audio and video recordings will be displayed. Consequently,

Emily can easily peruse or delete the data within the smart devices that contain her personal information.

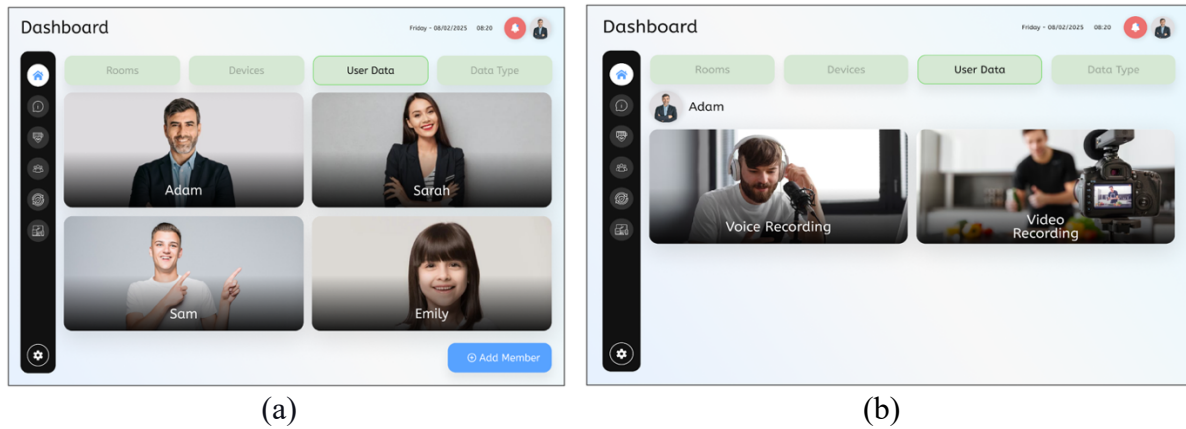
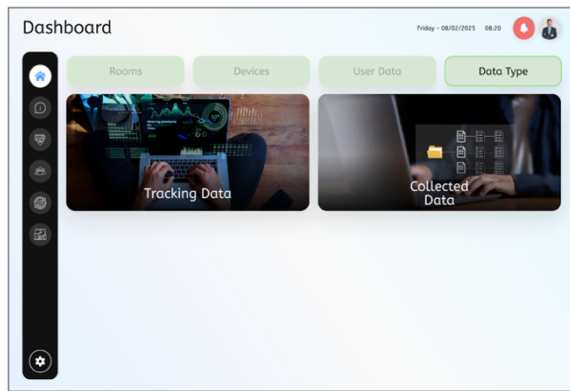


Figure 5.16: User Data Interfaces

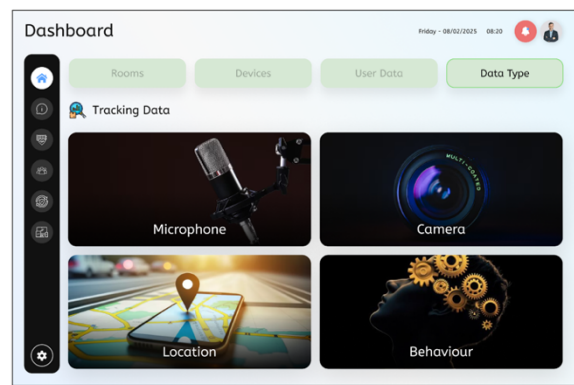
5.7.5 Data Type Interfaces

The design of a smart home dashboard must account for the type of data collected by smart devices and how they track users. To facilitate user review of this data and to enable them to determine whether they are being tracked, a categorization of data was employed in the form of tracking data and collected data, as illustrated in Figure 5.17a.

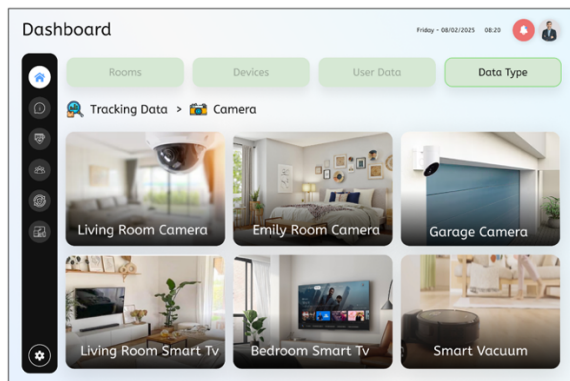
Tracking data refers to all smart devices that track user activity via cameras, location tracking, microphones, or TV usage, as displayed in Figure 5.17b. By selecting the camera button from the Tracking Data (Figure 5.17c), users can access detailed information about all smart devices equipped with cameras, enabling them to manage and control such devices effectively. Conversely, the collected data option displays all recorded data categories, such as voice and video recordings and recording content, along with the smart devices where such recordings are contained (Figure 5.17d). This allows users to modify or delete these recordings as necessary easily.



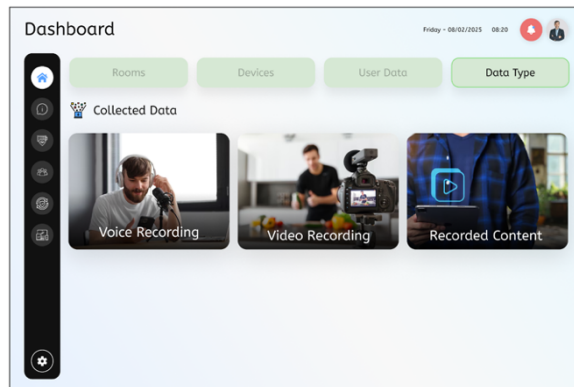
(a)



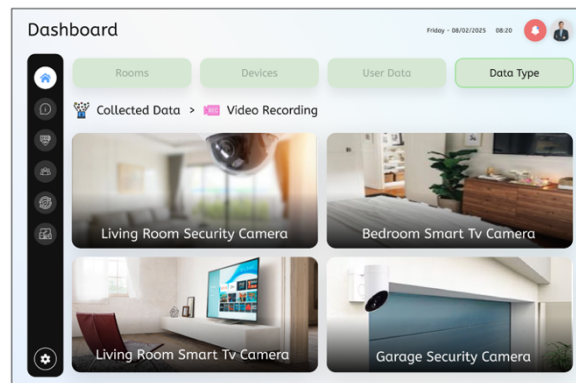
(b)



(c)



(d)



(e)

Figure 5.17: Data Type Interfaces

5.8 Summary

This chapter outlines the design and development of the proposed smart home security and privacy Dashboard, detailing its evolution from concept to final high-fidelity prototype in Figma. The structure of the Dashboard was designed to offer a unified platform for managing devices, monitoring security and privacy, and accessing essential system settings.

This chapter also presents the conceptual architecture of the proposed dashboard, which organises the system into four distinct layers: presentation, context, control, and execution. This layered approach provides a structured and unified framework that supports intuitive interaction, enhances transparency, and improves user control over security and privacy functionalities.

In addition, Nielsen's usability heuristics were applied throughout the design process to enhance clarity, consistency, and ease of use, ensuring that both novice and experienced users could navigate and operate the Dashboard effectively. Likewise, each interface was presented in detail, explaining its purpose and role within the overall Dashboard. These design decisions collectively contributed to a Dashboard that supports informed decision-making, reduced cognitive load, and improves the user's ability to maintain security and privacy in a smart home environment.

The next chapter presents an evaluation of the Dashboard through user testing and expert reviews, assessing its usability, functionality, and overall effectiveness in meeting the research objectives.

Chapter Six

User Evaluation of the Dashboard Prototype

This chapter presents the user evaluation of the smart home security and privacy Dashboard developed in this research. The first section outlines the methodology used in this evaluation, including the experimental design, participant recruitment, task scenarios, usability metrics, and data analysis procedures. Furthermore, the subsequent section reports the analysis and results, including quantitative measures such as task completion times, click counts, success rates, and System Usability Scale (SUS) scores, as well as qualitative insights from participant feedback. Together, these sections offer a comprehensive assessment of the Dashboard's performance in comparison to existing commercial platforms, namely Google Home, Amazon Alexa, and Apple HomeKit.

6.1 Methodology

This section describes the methodology used to evaluate the usability and effectiveness of the proposed smart home Dashboard in comparison to three existing platforms. The goal of the evaluation was to assess how efficiently and effectively users could complete common tasks across these platforms, as well as to evaluate their overall satisfaction with the interaction. By employing a combination of quantitative performance metrics, subjective satisfaction scores, and qualitative insights, the evaluation provided a comprehensive view of the user experience.

The methods utilised in this study were based on recognised usability evaluation frameworks and principles from Human-Computer Interaction research (Brooke, 1996; Sauro and Lewis, 2016). The study was designed as a task-based user experiment, in which participants were observed while interacting with each platform to complete comparable tasks. A detailed description of the study design, participant recruitment, evaluation procedures and performance measures is provided in the following sections.

6.1.1 Study Design and Context

The evaluation took place in quiet and distraction-free areas, either in a university room or in participants' homes. To ensure realism, we purchased and set up actual smart devices for each of the three main platforms: a smart security camera and a smart speaker for Amazon Alexa, Apple HomeKit, and Google Nest. This ensured that they functioned fully with their respective apps. The smart devices were connected, tested, and loaded with realistic data like video recordings, voice recordings, and privacy settings. This way, participants used real devices and apps instead of mock-ups, making the simulation more realistic. The same task scenarios were used for each platform to enable direct comparison of performance and usability.

The Dashboard is structured around four core views: Devices, Rooms, Data Type, and User Data. Accordingly, the evaluation scenarios were also organised to reflect these four views, with specific tasks designed under each view to simulate realistic user interactions. In total, sixteen scenarios were developed and subsequently classified into three categories: high, medium, and low priority, based on their importance to the study objectives, the estimated time required for completion, and their relevance to testing key features such as multi-device management, security, and privacy controls.

The task-based approach was chosen because it was a recognised and widely used approach in the usability research domain, providing a formalised method for measuring effectiveness, efficiency, and user satisfaction as users performed predefined scenarios. It was chosen over the use of self-reported methods by alone, as it enables the measurement of direct interaction and quantifiable performance. Google, Amazon, and Apple were selected as points of reference due to their market leadership in the smart home industry and their primary role as platforms through which users gain access. Comparing the Dashboard to these platforms ensured that the

analysis is grounded in real-world practice and revealed to what extent the proposed solution addresses recognised gaps in usability and management.

To provide clarity, three categories of scenarios will be described below:

- **High-Priority Scenarios**

These are essential to the study and focus on core functions such as security alerts, privacy controls across multiple smart devices, and centralised data management. All participants completed these tasks, as they were critical for evaluating the Dashboard's ability to provide integrated control and support efficient management of multiple devices.

- **Medium-Priority Scenarios**

These involved specific but narrower functions, for example adjusting settings for a single device or reviewing data logs for one category of information. A subset of participants tested these tasks when time and system conditions allowed. Although informative, they were secondary to the main goal of assessing cross-device management and security.

- **Low-Priority Scenarios**

These covered less common or peripheral tasks, such as individual customisation features. They were included to provide completeness but were not central to evaluating the Dashboard's primary objectives.

Table 6.1: Summary of Dashboard Evaluation Scenarios

	Features	Scenario	Objective	Steps	Compare System	Time Estimated	Importance	Priority
Devices	Security Notification Update	You have received an email about a critical security vulnerability affecting your smart home devices.	Evaluate the alert system for security updates.	1. Navigate to the Security Notification page. 2. Check the devices 3. Apply the update.		5-7 minutes	Essential for managing security across all devices	High
	Checking Software Updates	Ensure all your smart devices are running the latest software update to avoid any potential issues.	Ensure devices are up to date for security.	1. Select Devices. 2. View update status for each device.	- Apple HomeKit	5-7 minutes	Critical for maintaining system security	High
	Managing Smart Speaker Recordings	Review and delete some voice recordings from your smart speaker in the office for privacy reasons.	Review and delete voice recordings for privacy control.	1. Select Devices. 2. Select Smart Speaker 3. Review and delete recordings.	- Google Nest - Amazon Alexa	4-6 minutes	Important for privacy control across devices.	High
	Automatic Data Deletions	Schedule regular data deletions for a smart security camera in the living room to protect privacy.	Schedule regular deletions for a smart camera.	1. Set up a deletion schedule. 2. Confirm schedule setup.	- Google Nest - Amazon Alexa	5 minutes	Critical for data management.	Medium
Rooms	Unusual Activity in Living Room	You noticed some unusual activity in your living room at night and want to check the security status	Check security status after noticing unusual activity	1. Select Living Room. 2. View device statuses.	- Google Nest - Amazon Alexa - Apple HomeKit	5-6 minutes	Useful for monitoring specific events but not central to multi-device control.	Low
	Ensuring Privacy During a Meeting	Ensure the smart speaker's microphone in the Office is turned off for privacy.	Mute microphone in the office for privacy.	1. Navigate to Office. 2. Select Smart speaker 3. Mute microphone.	- Google Nest - Amazon Alexa - Apple HomeKit	6-8 minutes	Although it's for one device but, it's important for maintaining privacy during sensitive tasks.	High
	Disabling Location Services	You want to turn off location services for a smart speaker in Emily's room to ensure privacy.	Turn off location in Emily's room for privacy.	1. Select Emily's Room. 2. Select Smart Speaker 3. Disable location services.	- Google Nest - Amazon Alexa - Apple HomeKit	4-5 minutes	Useful for privacy, but specific to individual devices.	Medium
	Limiting Camera Usage	You have guests staying in your home, and you want to ensure the cameras in the living room is disabled to respect their privacy.	Disable living room camera usage.	1. Select Living Room. 2. Select Camera 3. Adjust camera settings.	-Google Nest (activity zones) - Amazon Alexa - Apple HomeKit	5-7 minutes	Useful for privacy but specific to individual devices.	Medium
	Managing Video Recordings	You want to review and delete video recordings from Security Camera 1 to free up storage space.	Review and delete camera videos.	1. Select Data type. 2. Select Video Recordings. 3. Play and delete as needed.	- Google Nest - Ring with Alexa - Apple HomeKit	5-7 minutes	Important for managing video data.	Medium

	Features	Scenario	Objective	Steps	Compare System	Time estimated	Importance	Priority
Data Type	Reviewing Security Camera Footage	Your neighbour mentions seeing a suspicious person near your house last night, and you want to check the security camera video recording for any unusual activity.	Check footage after a suspicious event.	1. Access recordings by date. 2. Play relevant footage.	- Google Nest - Amazon Alexa - Apple HomeKit	8-10 minutes	Essential for reviewing security events across multiple cameras.	High
	Turning of Location Services in all Devices	You want to disable location services for all smart home devices to protect your privacy.	Disable location services to protect privacy.	1. Open Data Type 2. Select Tracking Data. 3. Select Location 2. Delete selected recordings.	- Apple HomeKit	4-5 minutes	Useful for privacy management.	High
	Reviewing Usage History	You want to check when a smart speaker in your office was last activated to confirm if it was triggered accidentally.	Access the dashboard's log of device and data access.	1. Navigate to Usage History. 2. Review access logs.	- Google Nest - Amazon Alexa	4-5 minutes	Important for transparency but secondary to core security tasks.	Medium
User Data	Reviewing Voice Recording for One User	Joy wants to review and delete voice stored by any smart speaker in the house to protect his privacy.	Check voice recordings for specific users.	1. Select User Data. 2. Select User (Joy) 3. Review voice recordings. 4. Delete as needed.	- Google Nest - Amazon Alexa	4-5 minutes	Useful for one user households but not critical to core tasks.	Low
	Managing Data for Multiple Users	Joy wants to review and delete video recording for all house member stored by security camera.	Review and manage video recording for each household member.	1. Select User Data. 2. Select User (one user at a time) 3. Review video recordings. 4. Delete as needed.	- Google Nest - Amazon Alexa - Apple HomeKit	8-10 minutes	Useful for multi-user households but not critical to core tasks.	Low
	Data Sharing Permissions	You want to adjust data-sharing settings for a new smart doorbell to ensure only necessary information is shared.	Adjust data sharing permissions with third parties.	1. Go to Data Sharing Permissions. 2. Set permissions for each user.	- Google Nest - Amazon Alexa - Apple HomeKit	4-5 minutes	Important for privacy control but focused on external data sharing.	Medium
	Family Account Privileges	You want to set up a family account, giving your child access to their room's devices but restricting security controls.	Assign different permissions to family members.	1. Navigate to Devices 2. Set access levels for each user.	- Google Nest - Amazon Alexa - Apple HomeKit	8-10 minutes	Useful for multi-user control but not critical to security and privacy.	Low

While the full set of sixteen scenarios provided comprehensive coverage of security, Privacy, and data management tasks, the evaluation focused specifically on the high-priority scenarios, as these represented the most critical functionalities for assessing the Dashboard's usability. A total of six high-priority scenarios were identified; however, one of them could not be applied consistently across all three commercial platforms and was therefore excluded to maintain comparability. This refinement resulted in five core scenarios, which were used in the main study to ensure both methodological accuracy and fairness in comparing platforms.

The five scenarios included in the evaluation were:

1. Checking Software Updates

- Ensuring that all smart devices were running the latest software to maintain system security.
- This scenario was selected because keeping devices updated demonstrated a proactive security measure that shows users' awareness of system maintenance.

2. Managing Smart Speaker Recordings

- Reviewing and deleting stored voice recordings for privacy protection.
- This task was included to assess users' capability to manage personal data while ensuring voice privacy.

3. Ensuring Privacy During a Meeting

- Muting the microphone of a smart speaker in a specific room to maintain confidentiality.
- This scenario was chosen because it illustrated situational privacy management, one of the most realistic privacy behaviours in smart home contexts.

4. Reviewing Security Camera Recording

- Accessing and analysing recorded footage following a reported security incident.
- This task showed users' capability to manage incident response activities and review evidence following a potential security event.

5. Turning Off Location Services Across All Devices

- Disabling location services features across all devices.
- This scenario was selected to evaluate users' control over location-based privacy, which was essential for safeguarding personal data in smart home environments.

The five scenarios were intentionally selected to reflect the most critical and expected interactions that occurred when users manage security and privacy in smart home environments. Each scenario corresponded to a distinct aspect of the broader challenges in managing connected smart home devices, including system maintenance, privacy management, and incident response. By containing both proactive tasks, such as keeping software up to date, and reactive ones, such as reviewing security footage after an incident, the selection ensured a holistic assessment of user engagement with security and privacy controls. Moreover, these scenarios were validated through prior user studies and analysis of commercial smart home platforms, confirming their applicability to real-world user behaviour and their suitability for evaluating the effectiveness and usability of the proposed dashboard.

6.1.2 Participants

A total of 16 participants took part in this experiment. This sample size was selected based on established usability guidelines, which suggest that between 12 and 20 participants are typically sufficient for identifying most usability issues and drawing meaningful conclusions from user testing (Nielsen, 2000; Virzi, 1992). Participants were required to own at least two smart home

devices such as smart TV, smart speaker, or security camera, and have basic proficiency in English to understand task instructions and complete the post-task questionnaire.

Participants represented a range of digital literacy levels and backgrounds, reflecting a realistic user base. They joined the study by signing up after seeing a digital advertisement shared at the university and in local community areas. This method allowed us to include not only students and staff, but also members of the public with experience using smart home devices. The advertisement included brief study details, session length, and contact information. A sample of the recruitment advertisement is included in the Appendix E.

6.1.3 Pilot Study

Before launching the full evaluation, a pilot test was conducted with two participants. This pilot served primarily as a training opportunity for the researcher to test the clarity of task instructions and familiarity with session logistics. While no major revisions were required, minor adjustments were made to improve the clarity and flow of task wording. For example, a few task prompts were simplified to ensure all participants interpreted them consistently.

The pilot also helped estimate task durations, allowing the researcher to anticipate average session lengths and adjust breaks and transitions accordingly. Importantly, the pilot did not require any structural changes to the scenarios or evaluation flow.

6.1.4 Evaluation Procedure

Each participant conducted a one-to-one session in a quiet room. The setting was kept steady and distraction-free to create a controlled research environment. Each participant conducted the experiment using an iPad provided by the researcher. The device was an iPad (10th Generation)

with a 10.9-inch display, and all sessions were conducted in landscape orientation to ensure a consistent and optimal view of the dashboard interface across participants. The iPad came set up with the Dashboard prototype and three apps: Google Home, Amazon Alexa, and Apple HomeKit. They were also connected to real smart devices, such as cameras and speakers described above. All tasks in the evaluation were completed on this device. This ensured that all participants were under the same conditions, allowing for comparability among platforms and reducing interference from extraneous variables.

The experimental procedure consisted of four distinct phases:

1. Briefing

Participants were provided with an overview of the study objectives and introduction to the platforms as well as completed consent forms.

2. Task Performance

Participants completed five scenarios on each of the four platforms. The order of platform exposure was counterbalanced to control for learning effects.

3. Post-Task Assessment

Participants rated the difficulty of each task on a five-point scale ranging from Very Difficult to Very Easy for each platform. Upon completion of all tasks, participants completed the System Usability Scale for each platform.

4. Qualitative Feedback

Semi-structured interviews were conducted to gather information regarding usability, security attitudes, and comparative evaluations of the platforms.

All study materials referenced in the above phases, including the consent documentation, task-based scenarios, SUS forms, and post-task interview questions, are provided in Appendix F.

During task performance, the completion time, the number of clicks required to complete each task, and the navigation pathways were measured. Moreover, participants engaged in a think-aloud protocol, providing contextual feedback on their decision-making processes and areas where they encountered difficulties. Each experimental session lasted between 60 and 90 minutes, with brief pauses between the platforms used.

6.1.5 Usability Measurements

According to International Organization for Standardization (ISO) 9241-11, usability is defined as the degree to which specified users can utilise a product to achieve designated goals with effectiveness, efficiency, and satisfaction within a particular context of use (ISO, 2018). This framework highlights three essential dimensions: efficiency, effectiveness, and satisfaction. Efficiency concerns the resources and effort expended in relation to this achievement. Effectiveness refers to the completeness and accuracy with which users complete their goals. Satisfaction reflects the comfort and acceptability of the experience, ensuring that the system is perceived as pleasant and non-burdensome to use. Notably, ISO also emphasises that usability must always be interpreted in relation to the intended users, their goals, and the context of use.

This study adopted the following usability measurements as the basis for evaluating the Dashboard.

- **Efficiency** was measured by average task completion time and the number of clicks or actions required. These indicators are standard in usability testing, as they directly reflect how easily users navigate an interface to achieve their goals (Nielsen, 1994; Sauro and Lewis, 2016).
- **Effectiveness** was assessed by direct observation, with each task categorised as either successfully completed or not.

- **Satisfaction** was measured using the System Usability Scale (SUS), a method developed by Brooke (1996). SUS is calculated by assigning a score to each of the ten items, with responses ranging from 1 (Strongly Disagree) to 5 (Strongly Agree). For odd-numbered items, the score contribution is calculated by subtracting 1 from the user's response, while for even-numbered items, the contribution is obtained by subtracting the response from 5. The individual scores are then summed and multiplied by 2.5 to obtain a final SUS score ranging from 0 to 100. The SUS provides a reliable measure of perceived usability, allowing comparison across different systems. A score above 68 is generally considered above average, while scores above 80 indicate a high level of usability and user satisfaction. Lower scores suggest potential usability issues that may require further investigation. The SUS questionnaire is provided in Appendix F.

These metrics provided a balanced framework, combining objective performance measures with subjective user experience assessments. Moreover, this procedure enabled a structured and comparable evaluation of the Dashboard prototype and the three commercial platforms.

6.1.6 Data Analysis

Data were analysed using Microsoft Excel, selected for its suitability for performing descriptive statistical analysis and generating visualisations. Although inferential statistics such as ANOVA or t-tests were considered, they were not applied. Given the relatively small sample size, the analysis employed descriptive rather than inferential statistics to identify evident patterns of usability across platforms, consistent with prior usability research (Nielsen, 1994; Virzi, 1992).

Satisfaction was measured by the SUS, which is a ten-item tool scored on a five-point Likert scale. Scores were then converted into a single usability score for each participant, according to standard calculation (Brooke, 1996):

$$\text{SUS Score} = [(\sum (\text{odd items} - 1) + \sum (5 - \text{even items}))] \times 2.5$$

Task completion time and click counts were used to determine efficiency. Effectiveness was established through direct observation of whether a task was completed or not and documented. All three variables had their respective mean and standard deviation calculated across platforms to capture both central tendency and distribution of variation. The following statistical formulas were utilised:

Mean Calculation:

$$\bar{x} = \sum x_i / n$$

Standard Deviation Calculation:

$$SD = \sqrt{(\sum (x_i - \bar{x})^2 / (n - 1))}$$

Because the study involved a relatively small number of participants, the analysis was limited to descriptive statistics, including means, standard deviations, and visualisations. This approach aligns with usability research, which suggests that small sample sizes can be sufficient to uncover major usability patterns (Nielsen, 1994; Virzi, 1992; Lewis, 1994).

6.1.7 Ethical Considerations

The School of Computer Science Research Ethics Committee formally approved the study, confirming it met all ethical standards. Participants received a detailed information sheet explaining the study's purpose, procedures, and what their involvement would entail. This enabled

participants to make an informed decision about joining. After reading the information, participants signed a consent form to show they agreed to take part voluntarily.

One of the main priorities in this study was to protect the privacy and confidentiality of everyone who took part. All collected data was anonymised to ensure that no personal information was recorded. This step helped keep participants safe and showed our commitment to ethical research. The data were also stored securely and followed strict rules to prevent any unauthorised access.

Furthermore, the research emphasised the principles of voluntary participation and transparency throughout the entire study. Participants were assured that their involvement was entirely voluntary and that they had the right to withdraw from the study at any time without any repercussions. This commitment to ethical standards was a fundamental aspect of the research design and implementation.

For those interested in further details regarding the ethical considerations of this study, the relevant supporting materials are provided in Appendix G. These include the Ethical Approval Form (G.1), the Consent to Participate (G.2), and the Data Management Plan (G.3).

6.2 Results and Analysis

This section presents the results of the user evaluation and analyses the findings. The outcomes are reported in terms of efficiency, effectiveness, and satisfaction. Demographic context and user feedback are included to facilitate a comparison between the Dashboard and the three commercial platforms.

6.2.1 Participant Demographics

Demographic information helps provide context for understanding the study results. Table 6.1 shows the participants' gender, age, education, experience with smart home systems, first exposure to the platform, and how many smart home devices they own. This range of backgrounds helps the study reflect different user perspectives.

As outlined in the methodology, all participants owned at least two smart devices, ensuring a baseline level of familiarity with smart home technology. Particular attention was given to gender balance, with an equal distribution of eight males and eight females participants. Maintaining parity was important, as previous research has shown that gender imbalance in HCI studies can limit the generalizability of findings and introduce bias (Ofenwanger et al., 2021).

Table 6.2: Participant Demographic Information

Participant ID	Gender	Age	Education	Experience	Start with	Smart Devices
P1101	Male	26–35	Postgraduate	Basic	Google	2
P1102	Male	18–25	High School	Basic	Dashboard	4
P1103	Male	18–25	College/University Degree	Intermediate	Google	4
P1104	Female	46–55	College/University Degree	Intermediate	Google	6
P1105	Male	46–55	College/University Degree	Advanced	Dashboard	6
P1106	Female	36–45	Postgraduate Degree	Intermediate	Google	5
P1107	Male	18–25	College/University Degree	Basic	Google	5
P1108	Male	18–25	Postgraduate Degree	Intermediate	Dashboard	4
P1109	Female	26–35	Postgraduate Degree	Basic	Google	3
P1110	Female	26–35	Postgraduate Degree	Basic	Dashboard	4
P1111	Male	36–45	Postgraduate Degree	Advanced	Dashboard	6
P1112	Female	26–35	Postgraduate Degree	Advanced	Dashboard	8

P1113	Female	18–25	College/University Degree	Intermediate	Google	5
P1114	Female	18–25	College/University Degree	Basic	Dashboard	5
P1115	Male	36–45	Postgraduate Degree	Advanced	Dashboard	8
P1116	Female	26–35	Postgraduate Degree	Advanced	Google	5

As shown in Figure 6.2, the sample primarily consisted of younger adults. The largest group, with 6 participants falling within the 18–25 age range, followed by 5 participants in the 26–35 age group, 3 participants in the 36–45 range, and 2 participants in the 46–55 range. This age distribution suggests that the study's results mainly reflect the experiences and expectations of younger individuals who are familiar with technology. While this provides ecological validity for those who grew up with technology, it may limit the applicability of the findings to older adults or those who engage less with technology.

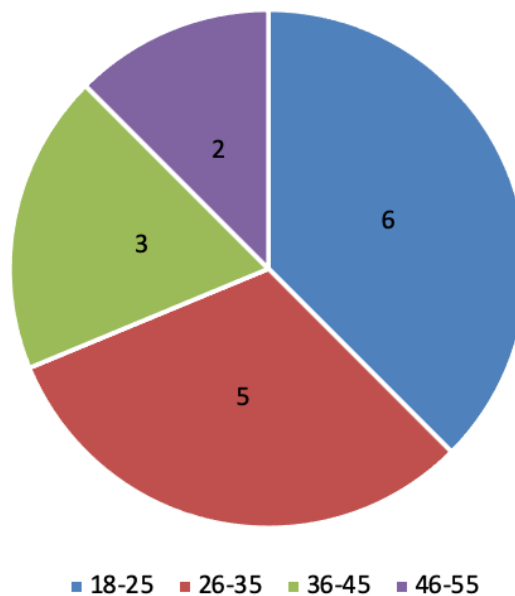


Figure 6.1: Age Group Distribution of Participants

Educational achievement was notably high, with nine participants holding postgraduate degrees, six holding undergraduate degrees, and one having completed high school education. This academic background is significant; participants with advanced education may be more familiar with analytical and digital problem-solving tasks, which may influence interaction with system interfaces. Nevertheless, this may also introduce limitations because the sample may not include individuals with little formal education who might utilise digital systems differently.

As shown in Figure 6.2, participants reported their experiences level with the smart home devices at different levels .The distribution among participants was relatively even, with six recognising themselves as basic experience users, five as intermediate users, and five as advanced users. This balance allows the study to capture a range of usability insights, particularly about perceived system complexity and ease of use across different skill levels.

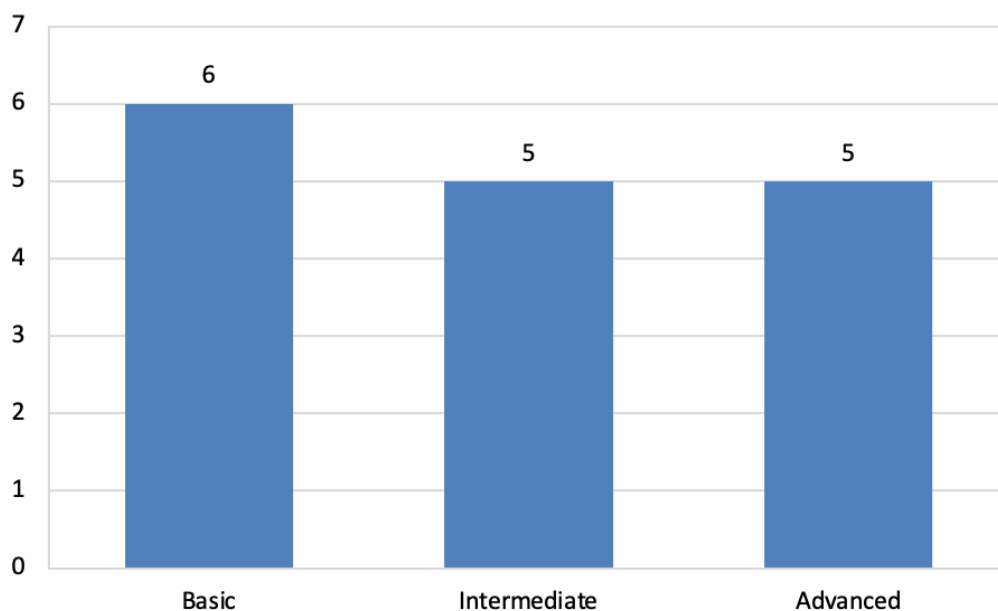


Figure 6.2: Experience Level Distribution

Most participants reported owning between four and six smart devices, with a few owning as many as eight. This high level of device ownership indicates that they interact regularly with smart home devices. As a result, their expectations regarding functionality, interface responsiveness, and interoperability are likely to be influenced.

To address practice effects and evaluation differences, Participants were evenly split into two counterbalanced groups regarding the order of system exposure during the experiment session. One group began with the Google system and proceeded through Amazon, Apple, and finally the Dashboard. The second group began with the Dashboard and followed the reverse sequence. This counterbalancing was critical to minimise bias due to order effects, such as learning, fatigue, or increasing familiarity with the task environment. This process of trial and evaluation of the platforms helped ensure that any differences in user experience metrics were due to the platforms and not the order of use.

The decision to initiate the trial with either Google or the designed Dashboard was strategically organised to establish a clear distinction in terms of system familiarity and evaluation, thereby addressing possible order effects. Google provided a highly familiar user experience, whereas the Dashboard represented an entirely novel interface. Amazon and Apple, positioned as intermediate in familiarity, were deliberately placed in the middle tier to mitigate possible carryover effects and ensure a more equitable comparison. This methodological choice enhanced the internal validity of the study by systematically varying the participants' initial exposure.

In summary, this diverse participant sample was carefully selected to encompass a range of ages, genders, educational levels, experience levels, and ownership of smart home devices. This

diversity enhances the study by ensuring that the findings reflect different user perspectives and contexts.

6.2.2 Efficiency Metrics

Measuring efficiency was important for evaluating how easily and quickly users can complete tasks on different platforms. These insights help identify where designs support smooth interaction and where they might create obstacles. This section examines how efficiently users were able to complete tasks on each platform. Moreover, it includes details on task completion time and the number of clicks per task, broken down by overall averages, user experience levels, gender, and initial platform exposure. At the conclusion of this section, participants' qualitative feedback on efficiency will be provided.

6.2.2.1 Task Completion Time

Task completion times were analysed across platforms, experience levels, gender, and initial starting systems to evaluate efficiency.

- ***Overall Comparison***

Figure 6.3 visualises the mean task completion times across the four digital platforms, including their standard deviations using error bars.

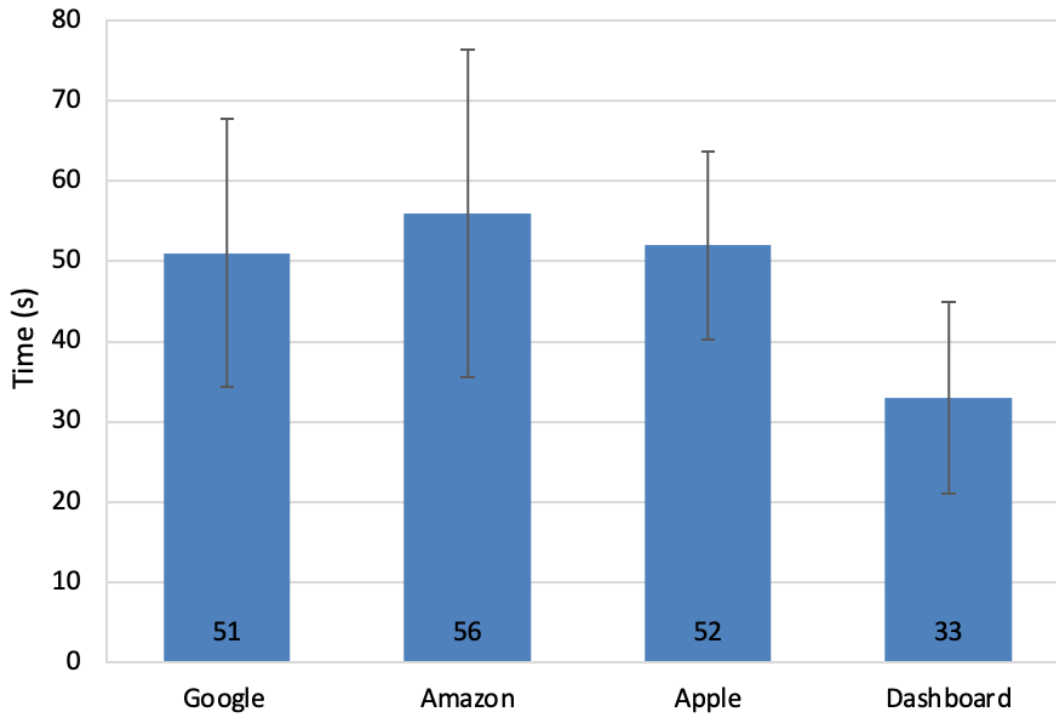


Figure 6.3: Mean of Task Completion Time with Standard Deviation

Google recorded a mean task completion time of 51 seconds ($\sigma = 17$), reflecting moderate speed with noticeable variability. Amazon was the slowest and most inconsistent platform, averaging 56 seconds with the highest standard deviation ($\sigma = 20$), suggesting extended task durations and wide variation in user performance.

Apple maintained a stable position, with an average of 52 seconds and the lowest variability ($\sigma = 12$). Although not the fastest, this consistency indicates predictable user performance. The Dashboard achieved the best results, with a mean completion time of 33 seconds. Despite having the same standard deviation as Apple ($\sigma = 12$), being 19 seconds faster demonstrates the Dashboard's capacity for quicker task execution while maintaining stability.

In summary, the Dashboard clearly recorded the lowest average completion times and highest consistency across participants compared to the other platforms. By contrast, Amazon imposed

the greatest temporal demands and exhibited the widest variability, highlighting potential efficiency issues. These overall differences provide the foundation for further examining the influence of user experience level on task performance.

▪ ***Average Task Completion Time by User Level Experience***

An analysis of average task-completion time across the three self-reported user experience levels, which were Basic, Intermediate, and Advanced, revealed clear patterns of efficiency gains with increasing proficiency. These patterns are visually summarised in Figure 6.4.

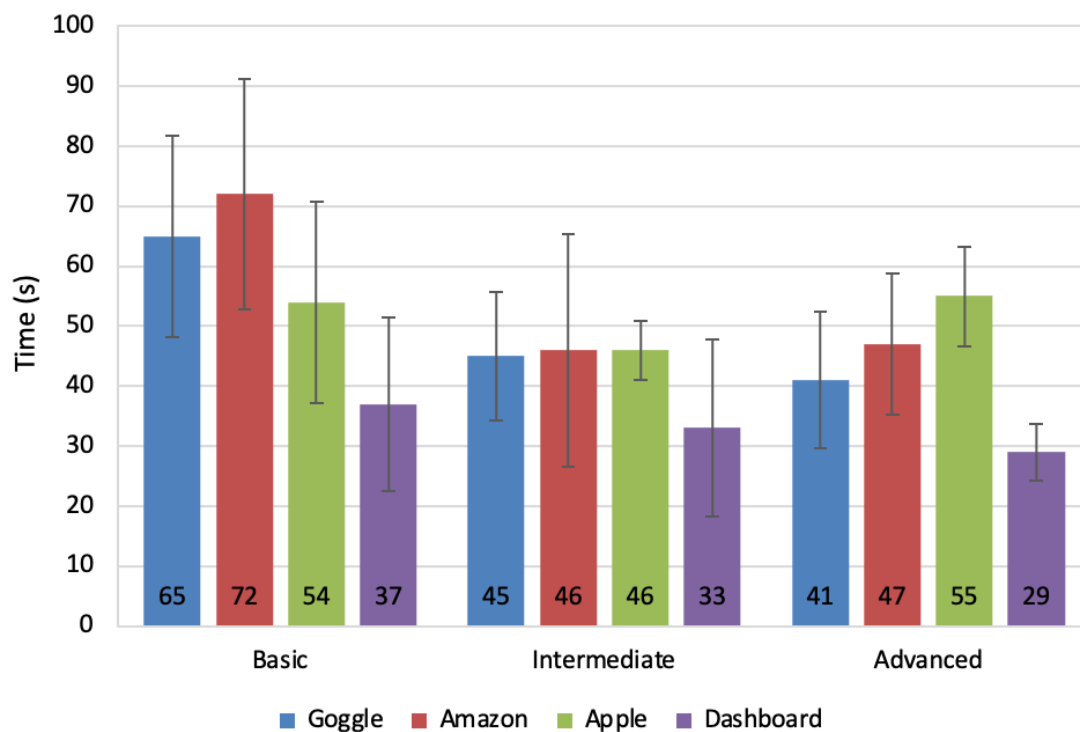


Figure 6.4: Mean Task Completion Time with Standard Deviation by Experience Level

In terms of Google, Basic users recorded the slowest performance at 65 seconds per task ($\sigma = 17$). Moreover, intermediate users showed substantial improvement, completing tasks in 45

seconds ($\sigma = 11$). Additionally, Advanced users achieved faster performance at 41 seconds, demonstrating an inverse relationship between experience and completion time.

For the Amazon platform, Basic users had the longest average task completion time at nearly 72 seconds ($\sigma = 19$). Intermediate users completed tasks more quickly, averaging 46 seconds, but their performance was highly variability ($\sigma = 19$). Moreover, Advanced users had a similar average time of 47 seconds with lower variability ($\sigma = 12$), indicating more reliable performance.

Regarding Apple, the participants' actions diverged from those observed with Google and Amazon. Basic and advanced users had comparable performance, averaging approximately 54 and 55 seconds, respectively. Intermediate users demonstrated greater speed, averaging 46 seconds with the lowest variability ($\sigma = 5$). This illustrates that individuals with moderate expertise are more familiar with the Apple Home app.

The Dashboard interface showed excellent performance across users of all experience levels. Advanced users had the fastest average completion time at 29 seconds ($\sigma = 5$). Intermediate users followed with an average of 33 seconds ($\sigma = 15$), while Basic users had an average time of 37 seconds ($\sigma = 14$). Although there was expected variation among less experienced users, the consistently low average times across all groups highlight the Dashboard's high usability and ease of adoption (see Figure 6.4).

Overall, the Dashboard was clearly the fastest and most consistent for everyone, no matter their experience level. This shows the value of a well-designed interface that keeps things simple and reduces effort for all users.

- *Average Task Time by Gender*

The statistical data for task completion time, categorised by gender, are visualised in Figure 6.5. The figure highlights both similarities and differences in user performance across platforms, offering insights into efficiency patterns related to gender.

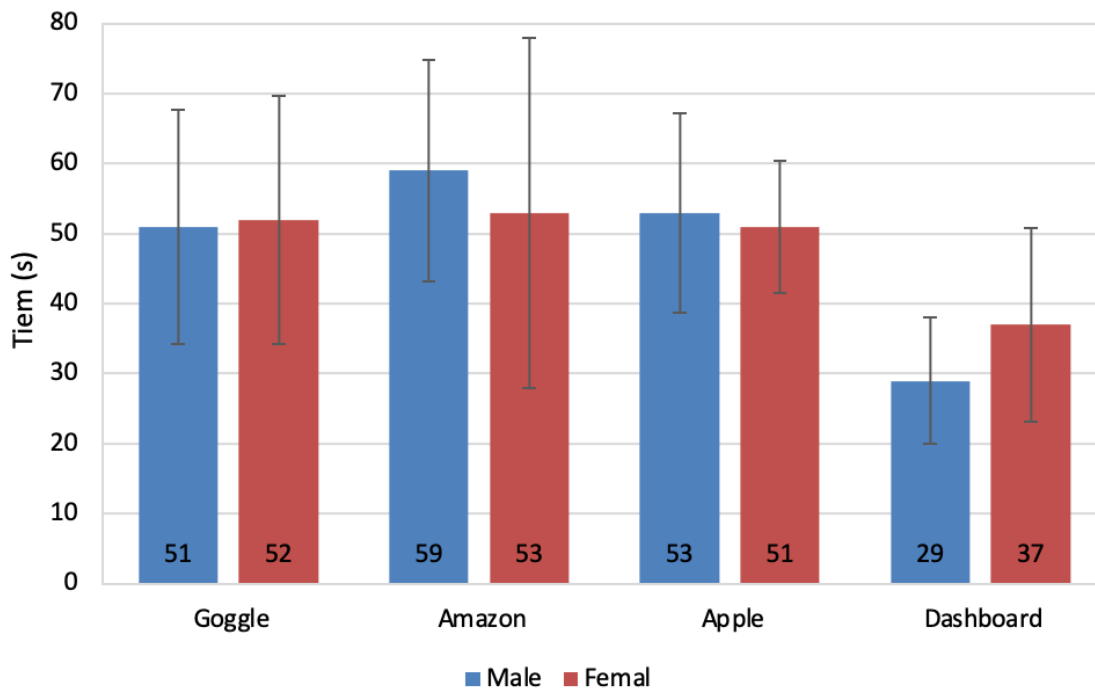


Figure 6.5: Mean Task Completion with Standard Deviation Time by Gender

In terms of the Google platform, task completion times were virtually identical across genders, with females averaging 52 seconds and males at 51 seconds. However, as shown in Figure 6.5, females exhibited slightly higher standard deviation ($\sigma = 18$) compared to males ($\sigma = 17$).

In the Amazon platform, gender differences were more noticeable. Males' users required an average of 59 seconds per task, which is 6 seconds longer than that of female participants at

53 seconds. However, it is worth noting that the overall performance variability for females was higher, with a standard deviation of 25 seconds compared to 19 seconds for males.

In Apple, mean task times converged for both males and females, with males averaging 53 seconds and females 51 seconds. However, variability was lower among females ($\sigma = 9$) than males ($\sigma = 14$), indicating more consistent performance.

The Dashboard was the fastest system for both genders. males achieved 29 seconds ($\sigma = 9$), while females averaged 37 seconds ($\sigma = 14$), reflecting both higher speed and greater consistency among male participants.

Overall, gender differences across platforms were modest, except on Amazon, where variability was greatest. The Dashboard consistently exceeded all systems, particularly for males who demonstrated the fastest and most reliable interaction.

- ***Average Task Completion by Initial Platform***

Figure 6.6 illustrates the mean task completion times and standard deviation for each platform. The data is categorised by the initial interface that participants engaged with. The results indicate that the choice of starting platform had an impact on performance, with noticeable differences observed between the two groups.

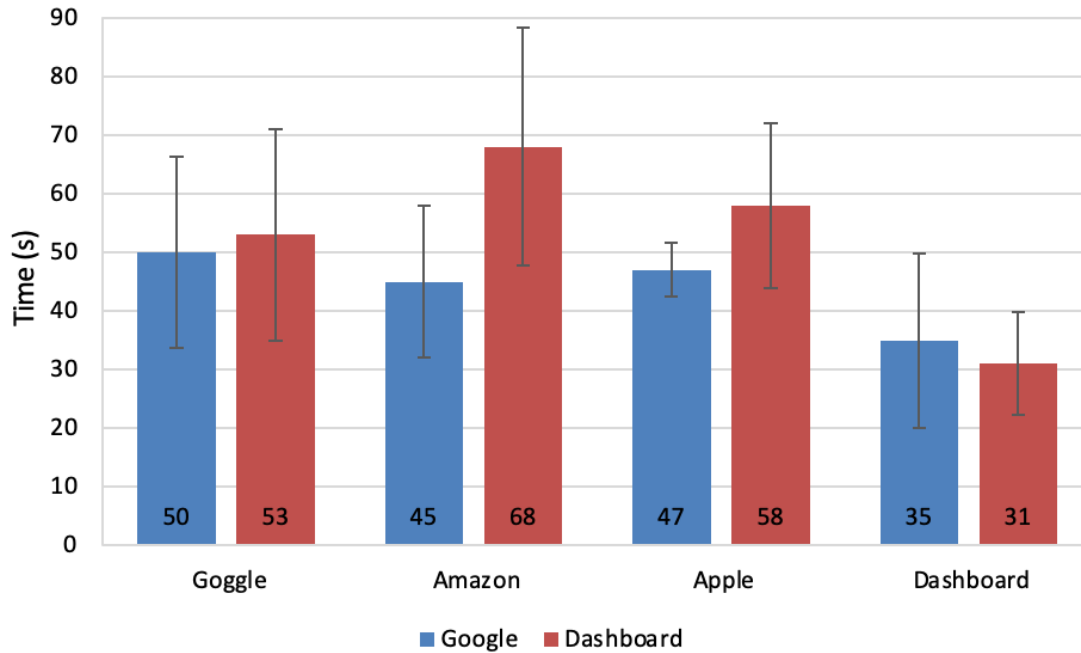


Figure 6.6: Mean Task Completion Time with Standard Deviation by Initial Platforms

- ***Dashboard First Start***

This group consisted of eight participants: four Advanced users, three Basic users, and one Intermediate user. As shown in Figure 6.6, participants completed Dashboard tasks most rapidly, with a mean of 31 seconds ($\sigma = 9$). The low mean indicates the influence of highly skilled users, whose proficiency reduces both average time and inconsistency, clearly demonstrating how experience shapes performance distribution. In contrast, Amazon was the slowest platform for this group, averaging 68 seconds ($\sigma = 20$). This higher average is mainly due to the longer task times recorded by Basic and Intermediate participants, which counterbalanced the faster performance of the Advanced users. Moreover, Google and Apple occupied intermediate positions at approximately 53 seconds and 58 seconds, respectively. Both showed substantial variability ($\sigma = 18$ for Google and $\sigma = 14$ for Apple).

This indicated that participants faced challenges adjusting from the simplified Dashboard to these more complex platform designs, leading to greater variability in performance.

- ***Google First Start***

This group comprised eight participants: three are Advanced users, three are Basic users, and two are Intermediate users who demonstrated an efficient approach. As shown in Figure 6.6, participants who initiated their tasks with Google completed them in a mean time of 50 seconds ($\sigma = 16$). Importantly, this group maintained relatively strong performance across subsequent platforms. For clarification, Amazon task time dropped to a mean of 45 seconds with a relatively moderate standard deviation of 13 seconds. Moreover, Apple had better performance, with a mean of 47 seconds and an extraordinarily low variability which ($\sigma = 5$). For the Dashboard, although the mean time for completing tasks remained competitive at 35 seconds, the standard deviation was higher at approximately 15 seconds compared to the Dashboard first-start group. This reflects mixed proficiency as these participants encountered the bespoke interface without prior practice with it.

As illustrated in Figure 6.6, the initial platform significantly influences both task efficiency and consistency. Starting with Google appears to promote adaptable interaction strategies, allowing users to perform more quickly and uniformly across subsequent systems. In contrast, starting with the Dashboard provides only localised benefits. While users remain extremely fast and consistent, their performance on more demanding commercial interfaces deteriorates, particularly among less experienced participants, resulting in elevated mean times and greater variance. These findings emphasise the importance of sequencing in usability studies, as the initial platform can significantly influence subsequent interaction patterns.

6.2.2.2 Clicks Per Task

This section analyses the number of clicks needed to complete tasks as a measure of interaction efficiency. It includes an overall comparison of different platforms and examines variations based on user experience level, gender, and initial system order. By evaluating mean click counts and standard deviation, this section aims to determine how interface design and user characteristics influence efficiency and consistency.

- **Overall Comparison**

Figure 6.7 presents the mean number of clicks per task, together with standard deviations, across all four platforms. This comparison highlights differences in interaction efficiency and consistency, with initial results suggesting notable variation between platforms.

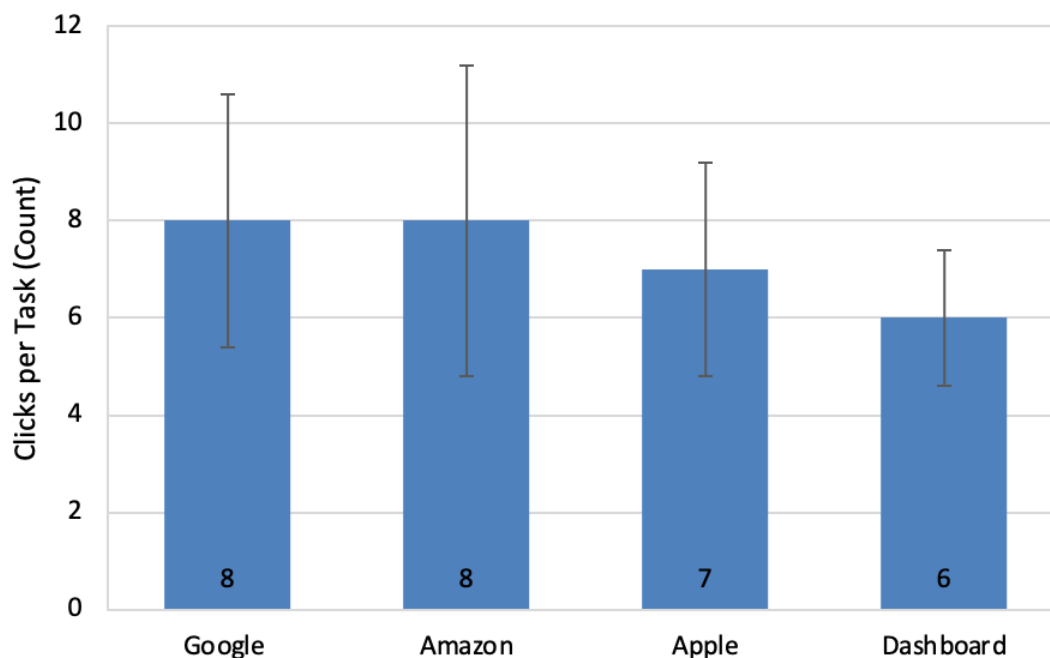


Figure 6.7: Mean Clicks per Task with Standard Deviation for all Platforms

As shown in Figure 6.7, the Dashboard was the most efficient platform, requiring an average of 6 clicks to complete each task. Moreover, the Dashboard showed the smallest standard deviation. This demonstrates a highly consistent and streamlined workflow. Additionally, Apple participants exhibit a slightly higher number of clicks, averaging seven clicks per task, with relatively low variability ($\sigma = 2$ clicks). Moreover, Google and Amazon exhibit the highest interaction patterns; participants required an average of 8 clicks to complete each task on Google platforms.

Generally, these results demonstrate that Dashboard provided the most efficient and consistent user experience, requiring the smallest number of steps required to complete each task and showed the least variability across users. In contrast, Amazon's high click demands, and inconsistency suggest a need for substantial design refinement to streamline tasks and make the experience more predictable.

- ***Average Clicks Per Task by User Level Experience***

Figure 6.8 presents the average number of clicks per task for users categorized into three self-reported experience levels: Basic, Intermediate, and Advanced. These visuals also include measures of standard deviation, enabling an analysis of how increasing familiarity and proficiency affect interaction patterns and efficiency across varying levels of expertise.

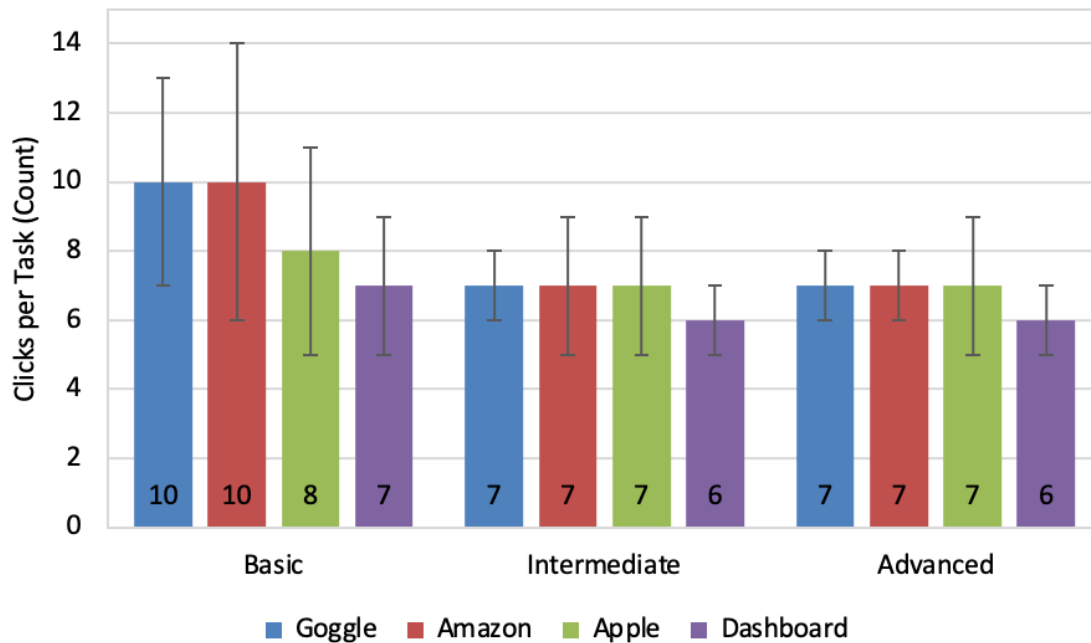


Figure 6.8: Mean Clicks per Task with Standard Deviation by User Experience Level

As illustrated in Figure 6.8, basic users consistently required the most clicks, with means around 10 for Google and Amazon, and higher standard deviation indicating more inconsistent performance. Apple was slightly better for this group, while Dashboard remained the most efficient and consistent, even for novices, averaging seven clicks with low variance.

Intermediate and Advanced users completed the task with a better average of seven clicks across Google, Amazon, and Apple platforms, indicating more consistent interaction patterns. However, advanced users showed the lowest variance, as displayed in Figure 6.8. Moreover, in terms of the Dashboard platforms, intermediate and advanced users have developed highly efficient workflows that require fewer steps, specifically six clicks. These patterns illustrate how users' experiences can affect both effort and variability to achieve better results, while also highlighting the Dashboard's advantage in supporting efficient use across all skill levels.

- ***Average Clicks Per Task by Gender***

Figure 6.9 displays the average number of clicks per task broken down by gender, along with a standard deviation to illustrate variability in interaction patterns.

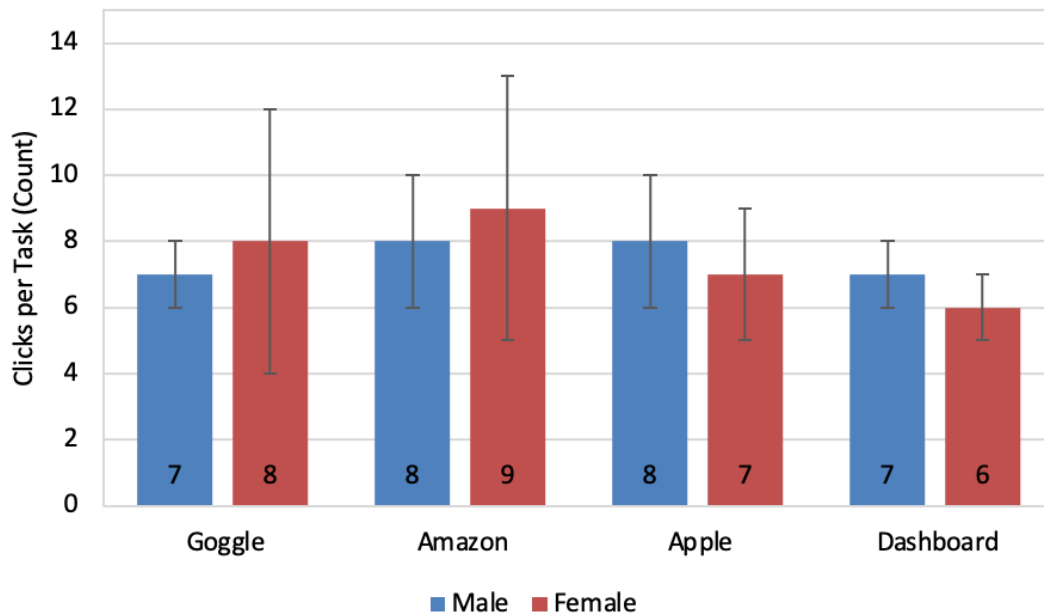


Figure 6.9: Mean Clicks per Task with Standard Deviation by Gender

On the Google platform, female participants averaged eight clicks, while men averaged seven. However, females exhibited much higher variability, with a standard deviation of 4 clicks, compared to men, who had a standard deviation of 1 click. This indicates that while many female participants navigated the platform efficiently, some required significantly more steps to reach their destination. A similar pattern appeared on Amazon, with females averaging nine clicks compared to eight for men, and a larger standard deviation of four among females, compared to two among men. The pattern at Apple is more equitable. On average, females clicked seven times, while men clicked eight times. Both genders showed similar variability, with a standard deviation of 2 clicks. This shows that the interaction was more uniform, and

the design may support consistent performance among users more effectively. On the Dashboard, both genders performed efficiently. female participants averaged six clicks and men seven, with equally low variability ($\sigma = 1$). This consistency suggests that the custom design supported streamlined workflows regardless of gender.

Overall, gender differences were more obvious in terms of variability than in mean click counts. Female participants tended to show greater variation on more complex platforms such as Google and Amazon. At the same time, the simpler and more guided designs of Apple and the Dashboard reduced these differences and, in some cases, gave female participants a slight efficiency advantage.

- ***Average Clicks Per Task by Initial Platform***

Figure 6.10 summarises the average number of clicks per task based on the initial platform sequence. This comparison reveals potential order effects on interaction efficiency and consistency, offering insights into how familiarity and learning shape overall performance.

- ***Dashboard First Start***

Participants who started with the Dashboard interface needed the fewest clicks, averaging six with a standard deviation of two. Moreover, when participants moved to commercial platforms, their average clicks rose to eight on Google and Amazon, and seven on Apple. The standard deviation increased to about two or three clicks, which suggests users tried different approaches as they adjusted from the simple Dashboard to the more complex commercial platforms.

- ***Google First Start***

Users who started with Google needed, on average, one additional click when they later used the Dashboard, resulting in an average of seven clicks with a standard deviation of one click. In contrast, users on commercial platforms had results that closely matched those of the Dashboard first-start group, averaging eight clicks on Google and Amazon, and seven clicks on Apple. The variability remained consistent, with standard deviations ranging from two to three.

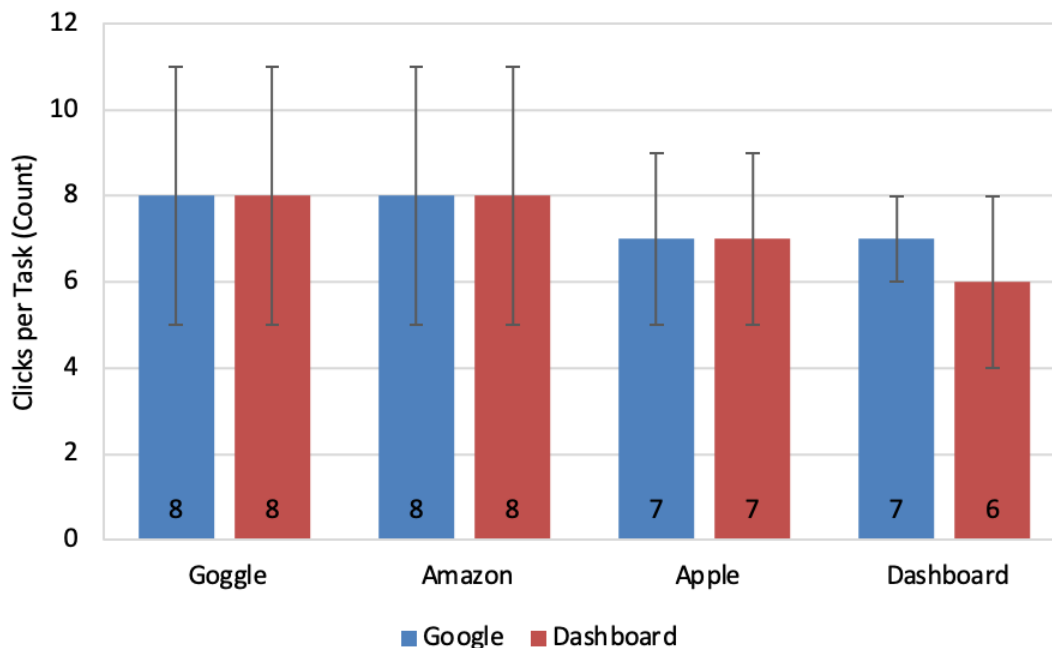


Figure 6.10: Mean Clicks per Task with Standard Deviation by Initial Platform

Generally, the choice of starting interface had only a modest impact on average click counts. Both groups converged at around eight clicks on the Apple, Amazon and Google platforms and between six and seven clicks on the Dashboard platform. This shows that the Dashboard's simple design helped users interact more efficiently, while commercial systems led to more varied ways of getting things done.

Quantitative analyses showed measurable aspects of efficiency, like task time and interaction effort. To add context, the next section looks at users' feedback to show how participants viewed the Dashboard's efficiency compared to other platforms.

6.2.2.3 Qualitative Feedback on Efficiency

Efficiency is defined as the ease and speed of task completion, clarity of navigation, and adequacy of features for streamlined use. This section summarises qualitative feedback from participants P1101 to P1116 regarding the efficiency of the Dashboard, compared with Apple, Amazon, and Google platforms.

- ***Task Difficulty***

Participants overwhelmingly described the Dashboard as easy to use, with minimal learning requirements and reduced effort. For example, P1101 described it as "smooth and very straightforward", while P1115 noted it was "very easy and has no complications." P1102 called it "very easy and understandable", and P1108 highlighted it as "very positive compared with others", enabling the completion of all tasks. P1105 summarised it as "easy to use and save my time," and P1111 noted it was "simple and easy to understand".

This pattern suggests that the Dashboard's design effectively supports intuitive use and reduces cognitive load. However, minor learning challenges were reported in the first experience. For instance, P1116 said, "I did not know how to return to the previous page", while P1114 recommended clearer labelling of fields and icons. P1112 noted, "It would be very easy once users become familiar with the application, as the first time is not clear". These observations highlight opportunities to further improve first-time usability without undermining overall simplicity.

By contrast, Apple, Amazon, and Google were described as significantly more difficult. P1101 reported Google was “very complicated” and admitted to giving up after multiple attempts. P1103 similarly said, “I give up.” P1105 described Apple settings as confusing (“I did not know”), while P1107 found Amazon privacy settings “not clear” and also gave up on Google’s recordings task. These comments underscore the Dashboard’s relative advantage in reducing user effort and frustration.

- ***Navigation Issue***

Navigation was widely identified as one of the Dashboard's strengths. Participants appreciated its clarity, simplicity, and multiple access routes. P1105 described it as "not complicated" and noted the ease of finding features. P1115 praised the ability to reach the same setting from different paths and called the use of images to clarify choices "a smart idea". P1107 described it as "the most intuitive" due to labelled options at each stage, noting it was "faster, easier to use and looked nicer." P1103 concluded, "There is no difficult task."

Despite the overall positive feedback, several participants suggested minor improvements to navigation. P1116 proposed adding a clearer back button, while P1114 and P1113 reported confusion about returning to previous pages. P1112 recommended making the icons on the left side clearer. These suggestions present opportunities to refine the interfaces and improve the overall experience. In contrast, navigation in Apple, Amazon, and Google was frequently described as confusing or inefficient. P1111 noted that Apple's settings were "not obvious" and P1103 described it as "more complicated". Amazon was criticised for requiring repeated steps, with P1109 noted that the participant repeated the same steps many times, then said, "I give up", and P1105 remarked "It needs time". Google was similarly problematic, with P1101, who tried many times, eventually gave up.

- *Missing Features*

When asked about missing or inadequate features, most participants reported no significant gaps. P1102, P1103, P1105, P1106, P1107, P1108, P1109, P1110, and P1111 explicitly answered "Nothing" or "No", indicating that the core feature set effectively met the primary user needs.

However, some participants proposed advanced improvements. P1101 suggested adding voice commands and cloud support for file backup. P1115 recommended an advanced settings option for more choices, quick actions for frequent tasks, and a dedicated back button. P1114 proposes group control for managing multiple smart devices simultaneously, along with a display indicator (green/red light) to indicate device status. Even though only a few people made these suggestions, they point out ways we could make things better for advanced users while still keeping everything simple.

Overall, participants found the Dashboard more efficient than those from Apple, Amazon, and Google. They highlighted how easy it was to use, with straightforward task flows and clear navigation. While some small changes were suggested, most feedback showed that the Dashboard meets user needs without adding extra complexity.

After evaluating efficiency in terms of task time and number of clicks, it is essential to assess how effectively users were able to complete tasks across all four platforms. The following section will analyse participants' success rates of the Smart Home Dashboard in comparison to those of Apple, Amazon, and Google.

6.2.3 Effectiveness Metrics

Measuring effectiveness was necessary for assessing how effectively participants achieved their goals in each platform. This analysis helps to understand whether interfaces supported users in completing tasks accurately and consistently. The analysis reports overall averages and examines differences by user experience, gender, and initial platform exposure. Qualitative feedback on effectiveness is also presented in the following section.

6.2.3.1 Task Completion Rate

This section analyses task completion rate as a core measure of effectiveness, assessing how successfully participants completed required security and privacy tasks across platforms. By examining average completion rates and variability, the analysis provides insight into overall system support for reliable and consistent task success.

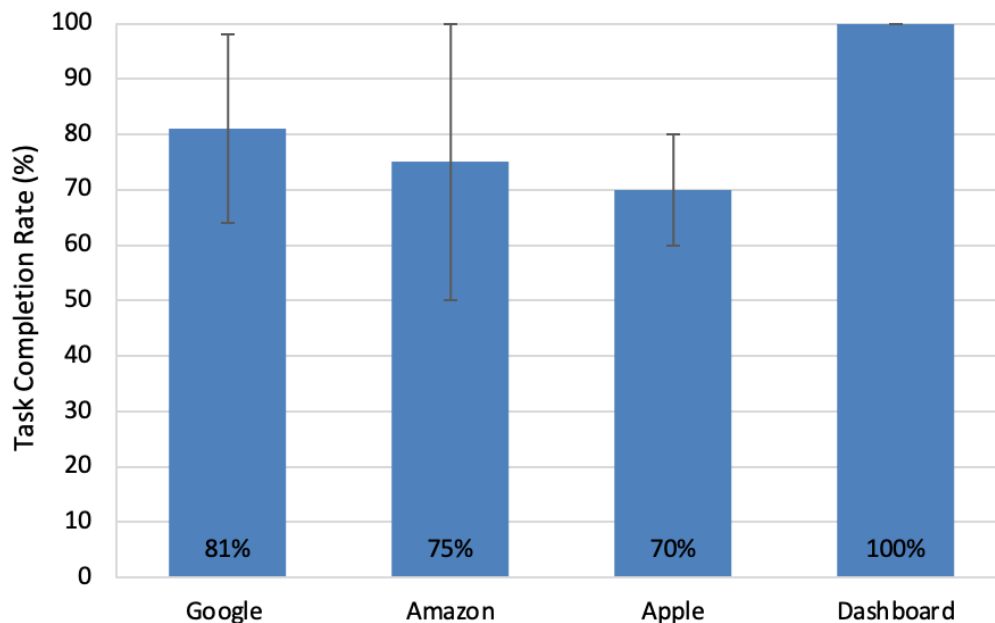


Figure 6.11: Mean Task Completion Rate with Standard Deviation

- ***Overall Comparison***

Figure 6.11 illustrates the mean task completion rate, highlighting the differences among all four applications.

Participants using Google achieved an average task completion rate of 81%, with a standard deviation of 17%, signifying moderate variability. Although most users completed the majority of tasks, some encountered difficulties, suggesting inconsistent navigation issues or unclear steps. Amazon had a lower rate of 75% and showed the highest variation in results, with a standard deviation of 26%. In comparison, Apple averaged 70% with a standard deviation of 10, indicating more consistent but generally lower performance, possibly due to shared interface issues. In contrast, all participants in the Dashboard completed all tasks without any issues, resulting in a perfect completion rate of 100%. This demonstrates the effectiveness of the design, which enables all types of users to complete tasks successfully.

In general, completion rates decline as the interface becomes more complex, making it more difficult for participants to complete tasks, and thus their completion rates decrease. In terms of Google, participants performed well, but with significant variation. Amazon shows a lower average, with a significant difference, indicating a complex design that leads to inconsistent experiences. Apple delivers slightly lower but more consistent results, while Dashboard achieves optimal and consistent success across tasks for everyone.

- ***Average Task Completion Rate by User Level Experience***

Figure 6.12 illustrates the mean task completion rate, highlighting the differences among all four applications.

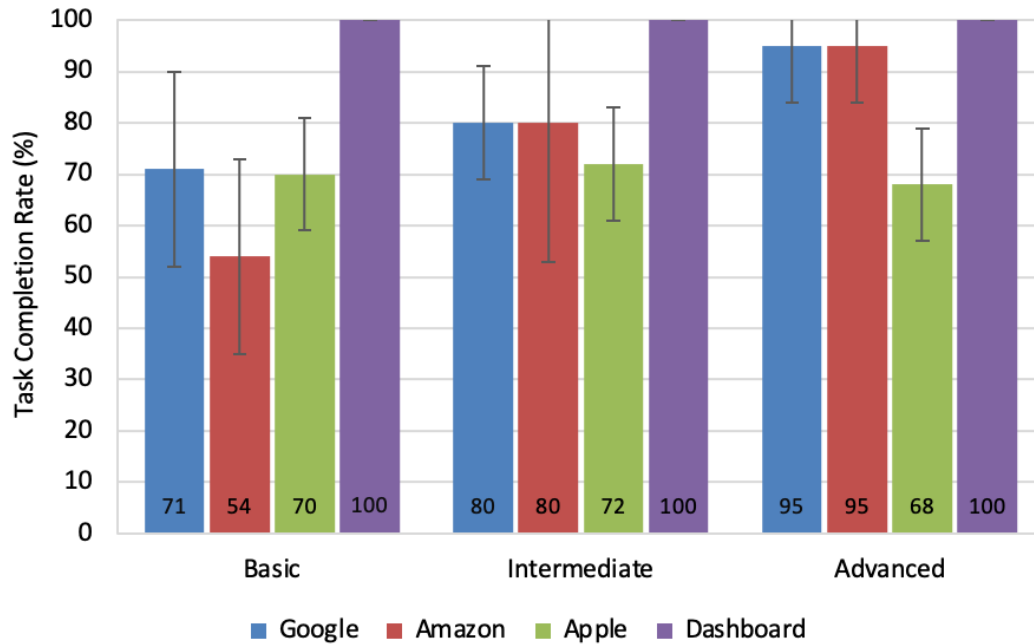


Figure 6.12: Mean Task Completion Rate with Standard Deviation by User Experience Level

As presented in Figure 6.12, advanced users generally showed strong task completion rates, with averages of 95% on both Google and Amazon, whereas performance on Apple was somewhat lower at 68%. Moreover, it is essential to note that advanced participants still demonstrated consistently low variability, with a standard deviation of 11% across all three platforms.

On the other hand, Basic users recorded lower rates, with 71 % on Google and only 54 % on Amazon, which was the lowest among all groups. Apple was higher at 70%. There was more variability ($\sigma = 19\%$ for Google and Amazon), showing that less experienced participants had more inconsistent results.

Intermediate participants typically had a mean completion rate between that of the basic and advanced groups, with an average of approximately 80% on both Google and Amazon, and 72% on Apple. While this positioning might seem predictable, it is noteworthy that their results

on Amazon exhibited significant variability, as indicated by a high standard deviation of 27%. This spread shows that although many users completed the tasks well, some struggled significantly. This may be due to parts of Amazon's interface that are less intuitive and require more careful navigation, particularly for users who have some experience but lack full confidence.

Across all experience levels, the Dashboard performance remained consistently high. This pattern highlights the design's strength in supporting users of all skill levels equally well. By offering clear, streamlined workflows that minimise confusion and effort, it enables even less experienced participants to complete tasks reliably and confidently.

- ***Average Task Completion Rate by Gender***

Figure 6.13 shows task completion rates by gender, enabling analysis of potential differences in performance and variability between males and females participants.

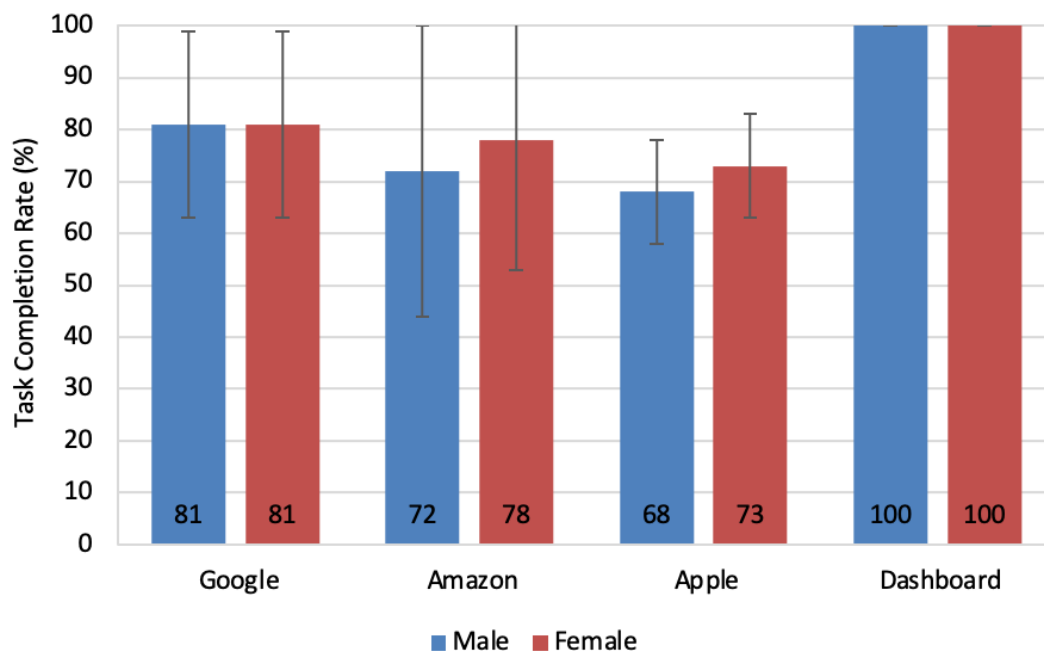


Figure 6.13 Mean Task Completion Rate with Standard Deviation by Gender

On Google, the mean task completion rate is identical for both genders at 81 ($\sigma = 18$), indicating similar and moderately consistent performance. On the other hand, results from Amazon reveal a notable gender disparity in performance, with females performing more efficiently than men. On average, females score 78% ($\sigma = 25$) and men averaged 72% ($\sigma = 28$). Both groups had a wide range of results, suggesting that Amazon's interface led to uneven success, with men being slightly less successful overall. On Apple, average task completion rates are similar, with females achieving an efficient completion rate of 73% and men achieving 68%, (both $\sigma = 10$). Results were steady but lower overall, indicating common challenges with the platform. In comparison, everyone reached a 100% completion rate on the Dashboard, showing that it was clear and easy for all users.

To sum up, men and females did equally well on Google and the Dashboard, but females had higher completion rates than men on Amazon and Apple.

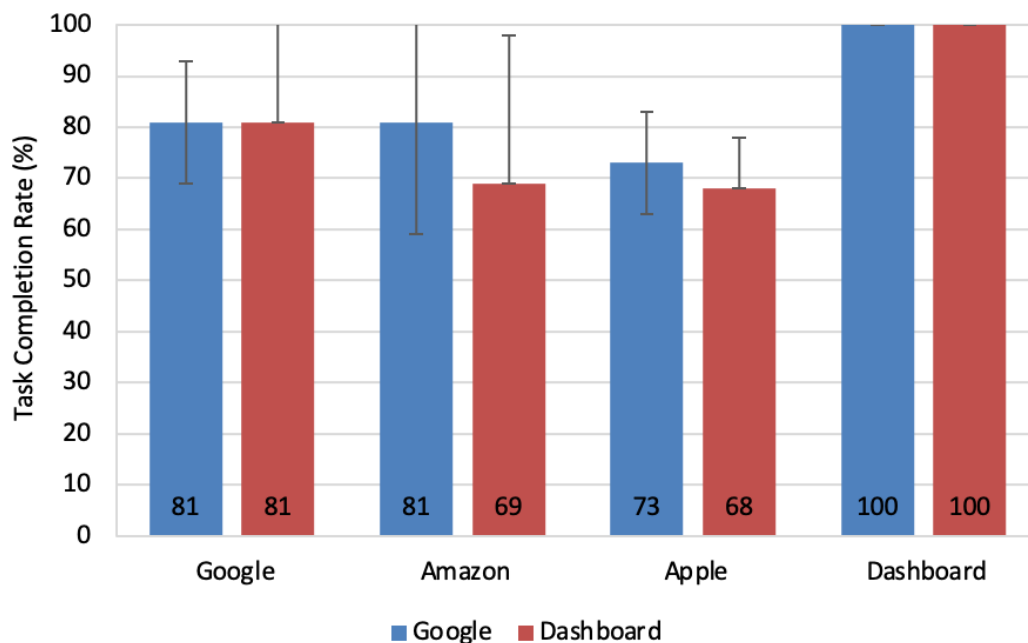


Figure 6.14: Mean Task Completion Rate with Standard Deviation by Initial Platform

- ***Average Task Completion Rate by Initial Platform***

Figure 6.14 shows task completion rates depending on which platform participants used first, exploring whether the order of exposure influenced task success and variability.

Participants who began on Google and those who started on the Dashboard both achieved identical results on Google itself, with an 81% completion rate and a standard deviation of 22%. Similarly, both groups performed equally well on the Dashboard, with no observed variability. This indicates that the starting interface had no impact on their eventual performance with these two platforms.

Clear differences emerge on Amazon and Apple platforms. For further clarification, on Amazon, participants who started with Google maintained a higher average completion rate of 81% ($\sigma = 22\%$), while those who began with the Dashboard dropped to 69% ($\sigma = 29\%$). Moreover, a similar, but smaller effect was observed on Apple. The Google-first group achieved 73 % completion ($\sigma = 10 \%$), while the Dashboard-first group averaged 68 % ($\sigma = 10 \%$).

The results suggest that users who started with a more complex system adapted better to other challenging interfaces. Those who began with a simpler system were less prepared. The Dashboard always led to perfect success, but commercial systems had lower and less consistent results. To complement these findings and gain a deeper understanding of users' perspectives on success, the following section presents qualitative feedback on effectiveness.

6.2.3.2 Qualitative Feedback on Effectiveness

This section presents and analyses qualitative feedback from participants P1101 to P1116 on the effectiveness of the smart home Dashboard, in comparison with Apple, Amazon, and Google

platforms. Effectiveness is examined in terms of users' ability to complete security and privacy tasks with minimal errors or obstacles, while also meeting their expectations for overall feature completeness.

- ***Task Completion Success***

Participants' comments on task success reveal how effectively they were able to complete security and privacy tasks using each platform, highlighting differences in complexity and reliability.

Participants consistently reported 100% task success with the smart home Dashboard, rating all scenarios as Easy or Very Easy. Comments highlighted its intuitive design and suitability for managing security and privacy. For example, P1101 described it as "smooth and very straightforward," while P1105 summarised it as "user-friendly", and P1107 said it aligned "very well" with their expectations.

Moreover, participants praised the system's ability to integrate and control multiple smart devices from a single interface. P1116 described it as "easy to link all the devices in one control environment," and P1115 appreciated having "all my devices in one app and easy to use." While overall ratings were very high, a few Neutral ratings were occasionally noted in specific contexts (e.g., privacy during meetings), reflecting minor complexity without resulting in task failure.

In contrast, Apple consistently demonstrated lower effectiveness, with frequent failures on critical privacy tasks, such as reviewing camera footage and managing recordings. Participants rated these scenarios as "Difficult" or "Very Difficult," citing the numerous steps and lengthy

times, for example P1102 reported 19 actions and over 90 seconds. P1114 called Apple "difficult" due to "too many steps," and P1110 described repeated failures in privacy tasks.

Amazon showed mixed success. While some tasks were completed, managing recordings and ensuring privacy during meetings often failed or were rated Very Difficult. Participants frequently cited confusing navigation and excessive steps as issues. P1109 noted repeated failures, and P1108 described giving up entirely on certain privacy tasks.

Google also demonstrated limited effectiveness in privacy management. Although basic tasks often succeeded, managing recordings and ensuring privacy during meetings were repeatedly rated as 'Difficult' or 'Very Difficult', with high action counts and long durations. For example, P1103 described managing recordings as "Very Difficult" with 12 actions and over 100 seconds of time. P1106 also highlighted failures with high time-on-task.

These consistent differences underscore the Dashboard's advantage in supporting successful and smooth task completion with less complexity compared to commercial platforms.

- ***Feature Completeness and Expectations***

Participants' feedback on feature completeness indicates how well each platform met their expectations for supporting security and privacy management, while also revealing areas for potential improvement. More specifically, most participants stated the Dashboard fully met their expectations for managing security and privacy. Common responses included "Very well" P1102, P1108, "Excellent" P1105, and both P1112 and P1116 stated that it "met my expectations". Moreover, P1109 described it as "aligns very well with my expectations to protect my data and privacy," and P1113 called it "higher than my expectations."

In comparison, participants identified several shortcomings in the commercial platforms. They noted that Apple had too many steps and unclear icons, Amazon had fragmented privacy settings and inconsistent labelling, and Google had settings that were not intuitive and required multiple steps. Due to these recurring issues, participants viewed the Dashboard as a more unified and dependable option for managing security and privacy.

To sum up, participants found the Dashboard to be very effective for managing security and privacy, especially when compared to those of Apple, Amazon, and Google. They highlighted its ability to deliver 100% task success with minimal complexity, intuitive navigation, and strong feature completeness, all of which aligned with user expectations. While some participants suggested improvements, such as advanced settings, group controls, or clearer icons, these were mostly preferences from power users, rather than major issues.

In contrast, commercial platforms were consistently associated with task failures, excessive steps, or unclear settings. These limitations supported the Dashboard's position as a more reliable and comprehensive solution for managing smart home security and privacy.

6.2.4 Satisfaction Metrics

Measuring satisfaction is crucial for evaluating users' feelings about a system, interface, or overall user experience. This assessment is based on personal perceptions, including ease of use, system integration, complexity and learnability. Moreover, users often determine their level of satisfaction through methods such as questionnaires such as SUS, interviews, or open-ended comments. This section presents user satisfaction across four different platforms using the SUS, analysing individual SUS responses and participants' qualitative feedback.

6.2.4.1 System Usability Scale (SUS) Results

This section reports users' perceptions of overall system usability using SUS. It analyses average SUS scores and their variability across platforms, while also examining differences based on user experience level, gender, and starting condition in the experiment.

All descriptive and comparative analyses in this section were based on participants' individual SUS ratings across the four platforms. Table 6.3 presents the individual SUS scores for each participant across the four evaluated platforms. Participant IDs correspond to those listed in Table 6.2, which provides demographic details.

Table 6.3: SUS Scores for All Participants

Participant ID	SUS Google	SUS Amazon	SUS Apple	SUS Dashboard
P1101	30	25	25	77.5
P1102	62.5	27.5	42.5	90
P1103	70	72.5	62.5	80
P1104	55	35	60	72.5
P1105	65	55	55	95
P1106	60	30	42.5	80
P1107	25	30	45	77.5

Participant ID	SUS Google	SUS Amazon	SUS Apple	SUS Dashboard
P1108	50	20	30	87.5
P1109	47.5	32.5	42.5	95
P1110	25	27.5	60	90
P1111	57.5	65	50	77.5
P1112	67.5	62.5	57	92.5
P1113	52.5	60	60	95
P1114	35	37.5	42.5	77.5
P1115	67.5	45	45	95
P1116	72.5	72.5	57.5	85

As summarised in Table 6.2, the participants' SUS ratings varied across the four platforms. The following subsection further examines these variations to identify significant usability trends.

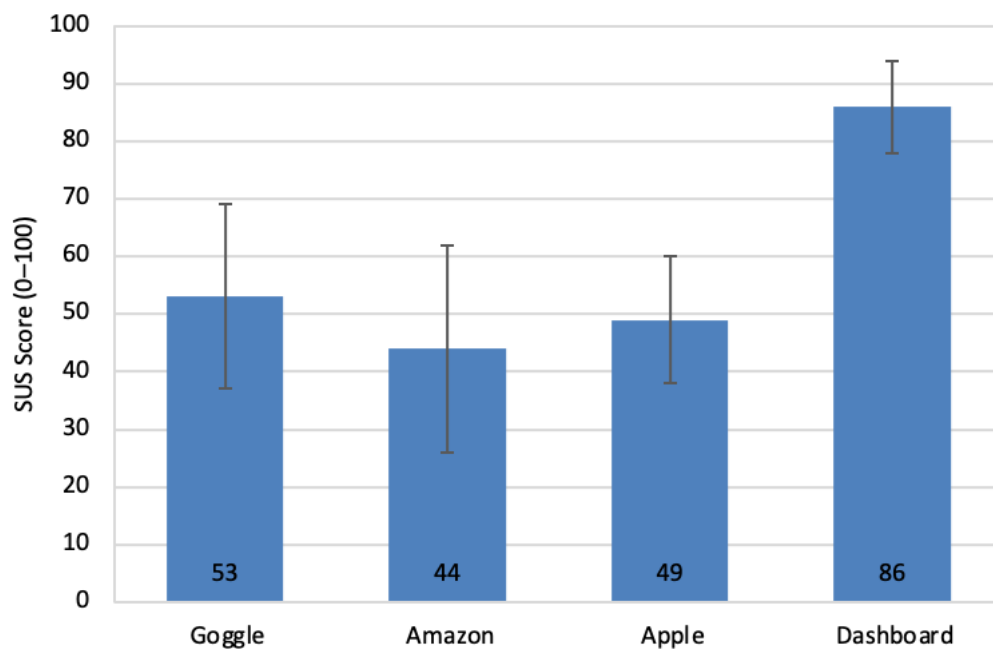


Figure 6.15: Mean SUS with Standard Deviation

▪ ***Overall Comparison***

An evaluation of the SUS scores for four platforms reveals a clear hierarchy in perceived usability as shown in Figure 6.15.

Among the four platforms, Dashboard demonstrates the highest perceived usability, with a mean SUS score of 86. This is notably higher than the other platforms and is accompanied by the smallest standard deviation, at 8, indicating both high usability and a strong consensus among participants. The relatively short error bar reinforces this interpretation, signifying consistent user feedback.

In contrast, Amazon records the lowest mean SUS score at 44 and exhibits the highest standard deviation of 18. These values suggest a generally negative perception of usability and considerable variability in user responses. The corresponding error bar in the chart is the tallest among all products, highlighting the wide dispersion of scores and suggesting inconsistent user experiences.

Google achieves a moderate mean score of 53, which is higher than Amazon and Apple but remains below Dashboard. The relatively high standard deviation of 16 indicates a wide range of user opinions. This suggests that while some users found the interface to be reasonably usable, others rated it poorly.

Apple occupies an intermediate position in terms of a mean score of 49 and is distinguished by its relatively low standard deviation of 11, which reflects a more uniform user perception. This consistency is visually represented by a shorter error bar in the chart, although the average score still suggests only moderate usability.

To sum up, the Dashboard is the only platform that combines high average usability with consistent user ratings. Amazon needs the most improvement in usability. Google and

Apple are in the middle, with Apple being more consistent but only moderate in usability, and Google showing more mixed user experiences.

▪ *SUS by User Level Experience*

An analysis of SUS scores stratified by participants' self-reported experience levels, which are Basic, Intermediate, and Advanced, reveals a consistent and meaningful pattern across the four evaluated platforms: Google, Amazon, Apple, and Dashboard. As illustrated in Figure 6.16, the results present both the mean SUS scores and the corresponding variability, represented by standard deviations, across different experience groups.

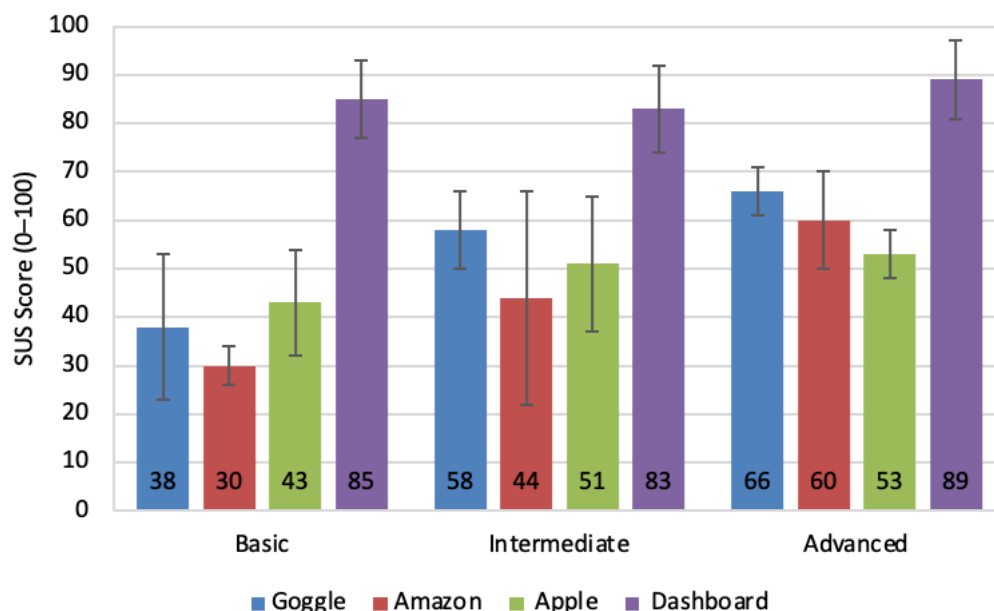


Figure 6.16: Mean SUS Score with Standard Deviation by Experience Level

Across all platforms, participants with greater prior experience consistently reported higher SUS scores, suggesting a positive relationship between familiarity with a digital interface and perceived usability. Additionally, standard deviations tended to decrease with increasing experience, indicating that advanced users rated the systems more favourably and did so with greater consensus.

For the Google interface, the mean SUS score rose substantially with experience, increasing from 38 for Basic users to 58 for Intermediate users and reaching 66 for Advanced users. Notably, standard deviation decreased from 22 to 5 as experience level increased, reflecting a convergence in user opinions.

Amazon followed a similar trajectory, with an increase in usability scores from 30 for Basic users to 60 for Advanced users. The Intermediate group showed the most variability, with a standard deviation of 22, highlighting the diverse experiences among users in this cohort. This suggests that moderate familiarity may lead to varied evaluations as users navigate and adapt to usability challenges in innovative ways.

Apple's usability ratings increased more gradually, rising from 43 among Basic users to 53 among Advanced users. Standard deviation remained similar overall for Basic and Intermediate users but dropped significantly in the Advanced group to 5, reflecting more homogeneous perceptions of usability at higher experience levels.

The Dashboard interface consistently achieved the highest SUS scores across all user experience levels, with scores of 85 for Basic users, 83 for Intermediate users, and 89 for Advanced users. While its standard deviation was not always the lowest, it remained relatively small, ranging from 8 to 9, indicating consistently positive evaluations. These findings reinforce the Dashboard's status as the most usable and reliably rated platform, regardless of the user's level of experience.

These findings highlight the significant impact of user experience on perceptions of usability. As users become more familiar with a platform, their views on usability improve considerably, resulting in more consistent evaluations. This direction is particularly apparent in both the Google and Dashboard interfaces. Google demonstrates a remarkable learning curve, while Dashboard offers high usability right from the start, making it an

excellent choice for novice users and ensuring a seamless experience for everyone, regardless of their level of expertise.

▪ *SUS by Gender*

A gender-stratified analysis of SUS scores reveals slight differences in user perceptions across the four platforms. As shown in Figure 6.17, the mean usability ratings were broadly comparable between males and females participants, with few differences exceeding ten points.

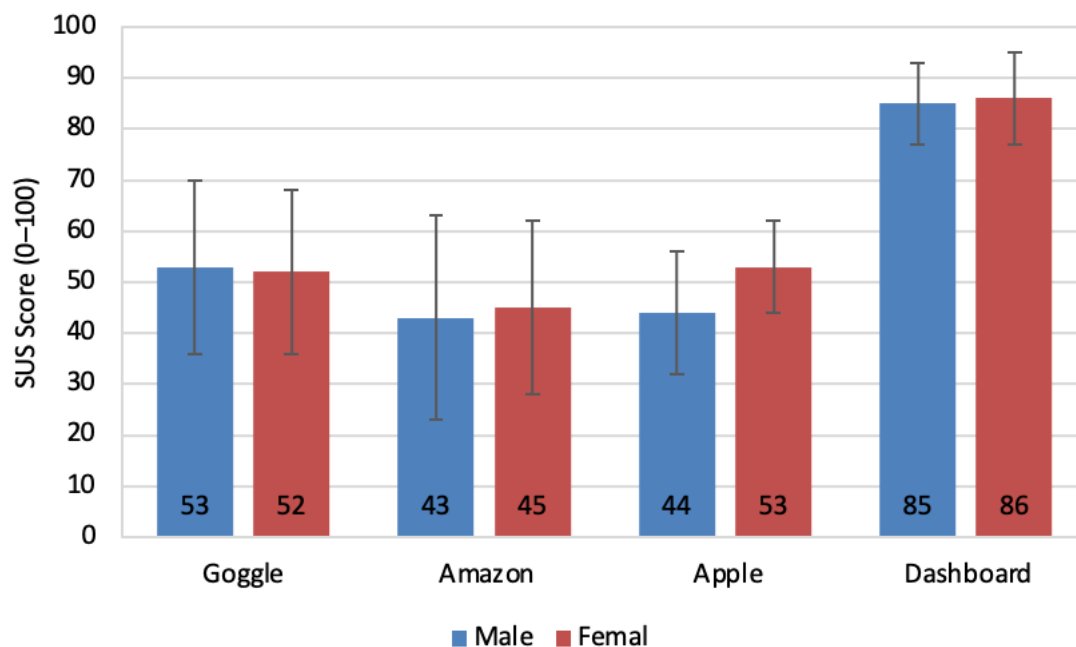


Figure 6.17: Mean SUS Score with Standard Deviation by User Gender

In the Google interface usability study, males reported an average SUS score of 53, which was slightly higher than the score of 52 reported by females, with similar standard deviations of 17 and 16 respectively. These findings indicate that men and females have nearly identical perceptions of usability.

On Amazon, female users rated the platform slightly higher (45) than males (43), with a standard deviation of 17, while males rated it an average of 43, with a standard deviation

of 20. The greater variability in ratings among male users indicates that they have more diverse experiences with the platform.

The clearest gender difference was observed in the Apple interface. Female participants rated it notably higher, at 53 ($\sigma=9$), compared to 44 ($\sigma=12$) for males, indicating both a more positive and more consistent perception among females.

For the Dashboard, both groups achieved high SUS scores, with 86 for females and 85 for males, and identical low standard deviations of 9, indicating strong agreement across genders.

Overall, the gender-based differences in SUS scores were modest; however, consistent patterns were observed on certain platforms, particularly Apple, where female participants reported higher scores with lower standard deviations. These findings highlight the importance of considering gender as a factor when evaluating user experience and interpreting usability outcomes.

- ***SUS by Initial Platform***

An analysis of the SUS outcomes, categorised by participants' initial platform, revealed subtle yet consistent patterns in usability perceptions. Participants were divided into two groups: those who began the evaluation using the Google interface and those who started with the Dashboard. Descriptive statistics and the corresponding visual summary can be found in Figure 6.18.

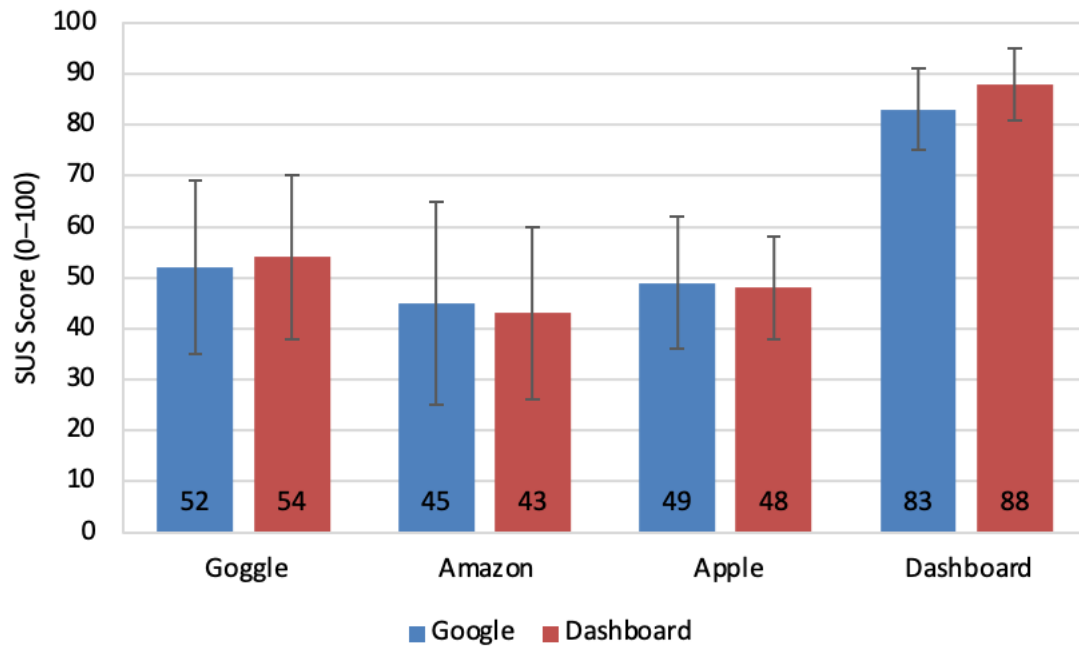


Figure 6.18: Mean SUS with Standard Deviation by Initial Platform

For the Google interface, participants who began with the Dashboard reported a slightly higher mean SUS score of 54 ($\sigma = 16$), compared to 52 ($\sigma = 17$) among those who started with Google. Although the difference in scores is minor, the standard deviations indicate that both groups displayed similar levels of agreement in their ratings.

A similar trend was observed on the Amazon platform. Users who began with Google assigned it a mean score of 45 ($\sigma = 20$), while those who started with the Dashboard gave it a mean score of 43 ($\sigma = 17$). Although the average scores are close, both groups exhibited relatively high standard deviations, with users who started with Google showing slightly more variability. This high variability may reflect the complexity of the Amazon interface itself, resulting in mixed user experiences regardless of their starting point.

In the Apple interface, Google starters reported a slightly higher mean SUS score of 49 ($\sigma = 13$) compared to 48 ($\sigma = 10$) for Dashboard starters. The one-point difference is minimal, and both groups exhibited lower standard deviations than those observed for Google and Amazon, suggesting more consistent perceptions.

The clearest difference appeared in evaluations of the Dashboard interface. Participants who started with this platform rated it higher, with a mean SUS score of 88 ($\sigma = 7$) compared to 83 ($\sigma = 8$) for those who began with Google. While the difference is modest, it suggests that first exposure to a highly usable interface may slightly enhance later evaluations of that same platform. Overall, the starting context had only a limited influence on usability perceptions across platforms; however, Dashboard consistently achieved the highest and most consistent scores, regardless of the sequence.

This analysis of the SUS indicates considerable differences in perceived usability across various platforms and user groups. The Dashboard consistently receives high scores with low variability, indicating overall strong and stable user satisfaction. While these aggregate scores provide helpful insights, a more detailed understanding requires a closer examination of individual SUS questions. The following section addresses this by analysing the ratings for each question to identify specific usability strengths and weaknesses for each platform.

6.2.4.2 SUS Questions Analysis

This section provides a detailed analysis of participant responses to each SUS question across all platforms. This comprehensive view highlights specific usability strengths and weaknesses that may not be apparent in the overall SUS scores.

Q1. I think that I would like to use this platform frequently (Frequent Use)

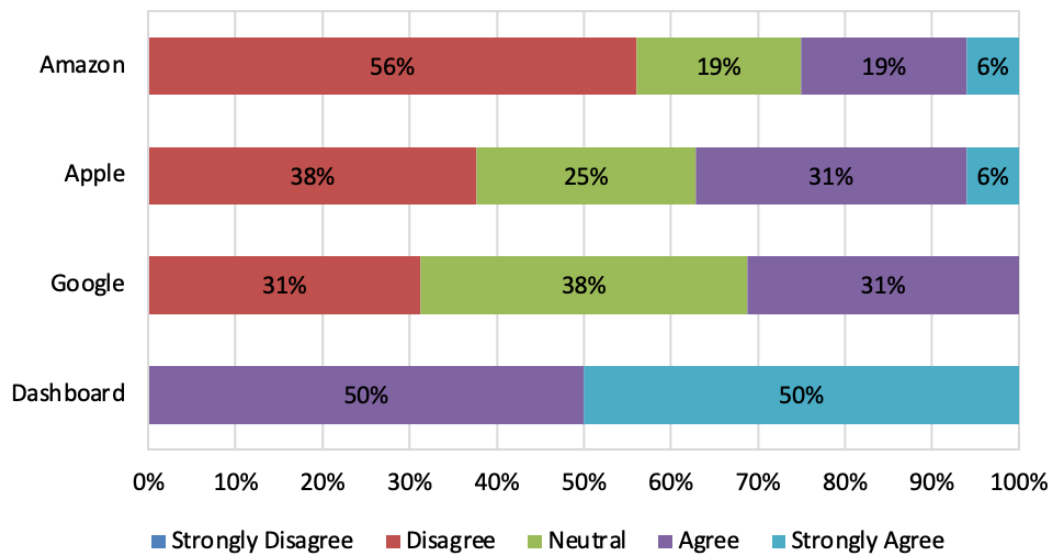


Figure 6.19: Q1. I think that I would like to use this platform frequently

Figure 6.19 shows the distribution of responses across platforms. The Dashboard received overwhelmingly positive ratings, with all participants selecting “Agree” or “Strongly Agree,” indicating strong willingness for frequent use. In contrast, Amazon had the most negative responses (56 % “Disagree”), suggesting low appeal for repeated use. Google responses were mixed, but leaned negative, with high counts of Neutral and Disagree. Apple performed slightly better than Amazon and Google but still showed substantial “Neutral” and “Disagree” responses.

These results suggest that the Dashboard’s design successfully supports frequent use by providing a clear and user-friendly experience, whereas other platforms face adoption challenges due to perceived complexity or inconsistency.

Q2. I found the platform unnecessarily complex (Complexity)

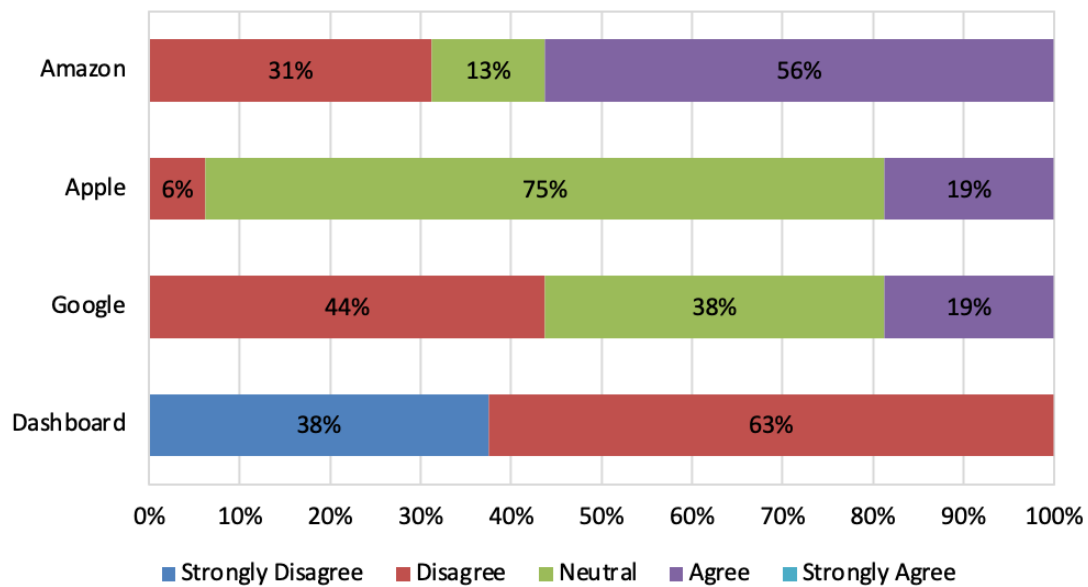


Figure 6.20: Q2. I found the platform unnecessarily complex

As shown in Figure 6.20, the Dashboard was perceived as the least complex platform, with 100% of participants selecting "Disagree" or "Strongly Disagree", indicating clear confidence in its simplicity. Google performed moderately well, with 44% of users rejecting unnecessary complexity, although 38% remained Neutral, suggesting some uncertainty about its ease of use. Apple had the most Neutral responses (75%), suggesting many users were unsure about its complexity. In contrast, Amazon showed the highest complexity concern, with 56% of participants agreeing that it felt unnecessarily complex.

These results highlight Dashboard's success in minimising perceived cognitive load, while suggesting that Amazon and, to a lesser extent, Apple and Google could benefit from design improvements to reduce complexity and increase user confidence.

Q3. I thought the platform was easy to use (Ease of Use)

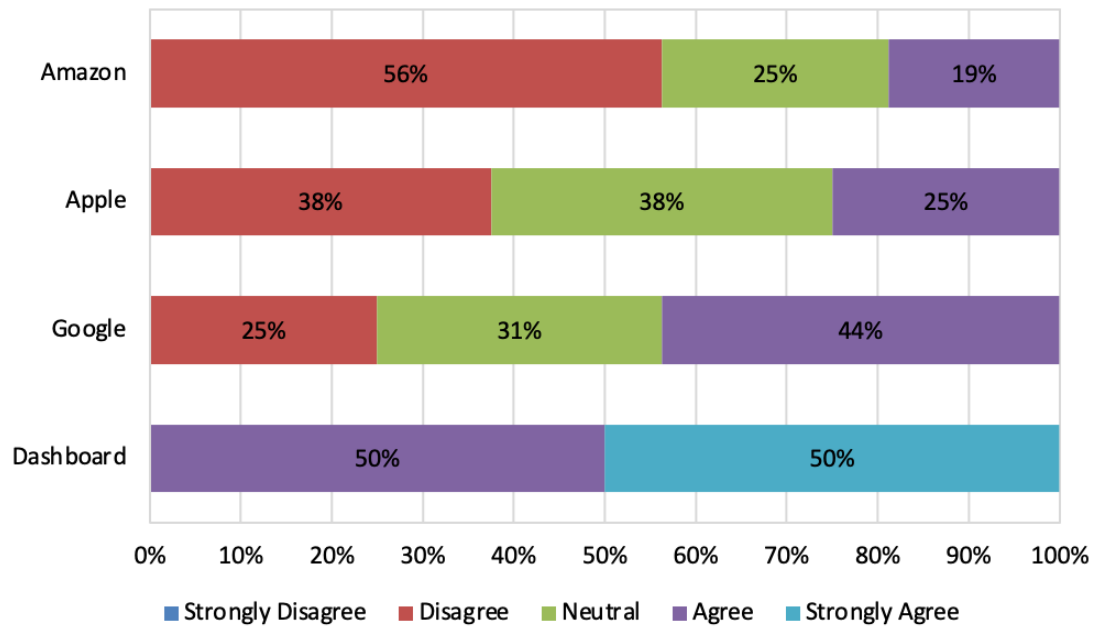


Figure 6.21: Q3. I thought the platform was easy to use

As illustrated in Figure 6.21, the Dashboard received perfect ratings, with 100% of participants selecting either 'Agree' or 'Strongly Agree,' indicating an outstanding perceived ease of use. In contrast, Google had a more mixed response, with 44% of responses indicating ease, but also recorded 31% as Neutral and 25% expressing disagreement, suggesting a mixed experience with significant uncertainty.

Apple's performance was less favourable, with only 25% of participants reporting ease of use. Moreover, 38% of participants responded Neutral, and another 38% of users expressed disagreement, indicating considerable variability in perceived usability. Amazon received the lowest ease-of-use ratings, with only 19% of participants indicating agreement, while a significant 56% of users selected 'Disagree', highlighting substantial challenges regarding intuitive use. These results underscore the Dashboard's significant usability advantages and identify clear opportunities for design enhancements in the other platforms.

Q4. I think that I would need the support of a technical person to be able to use this platform.

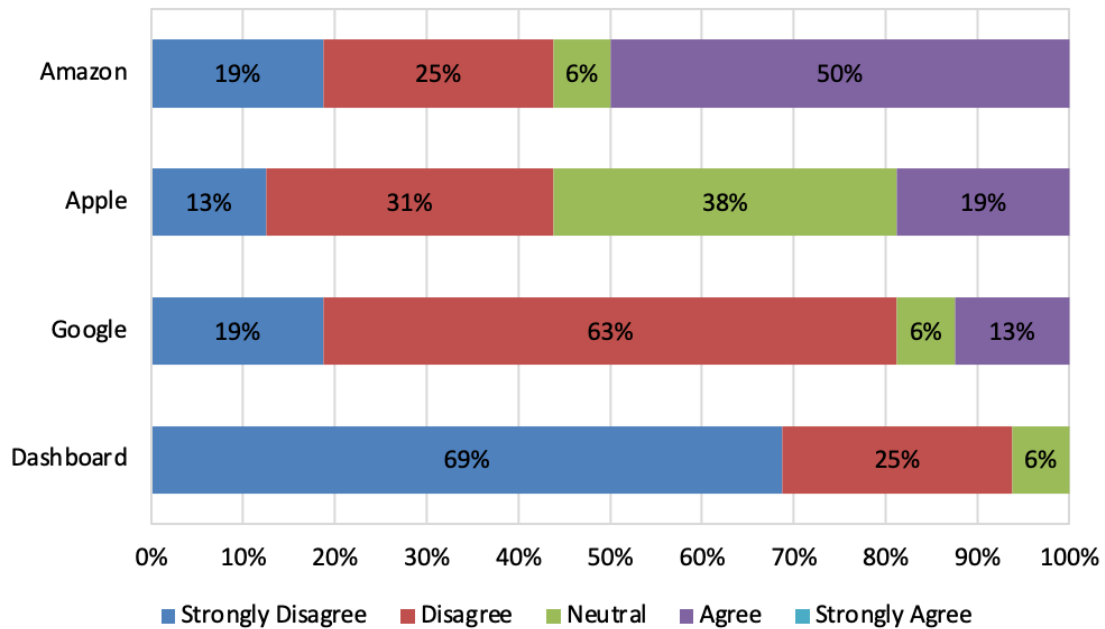


Figure 6.22: Q4. I think that I would need the support of a technical person to be able to use this platform

As presented in Figure 6.22, the Dashboard received the strongest indication of independent usability, with 94% of participants selecting "Disagree" or "Strongly Disagree," suggesting that users felt fully capable of using it without technical support. Google also performed well in this regard, with 81% rejecting the need for assistance. In contrast, Apple and Amazon were seen as more complex, with only 44% of participants saying they wouldn't need help to use them. Notably, half of Amazon's users agreed they'd need support, suggesting real concerns about how easy it is to use independently. These findings indicate that while Dashboard and Google support intuitive, self-guided interaction, Apple and Amazon may require design improvements to reduce reliance on external help.

Q5. I found the various functions in this platform were well integrated

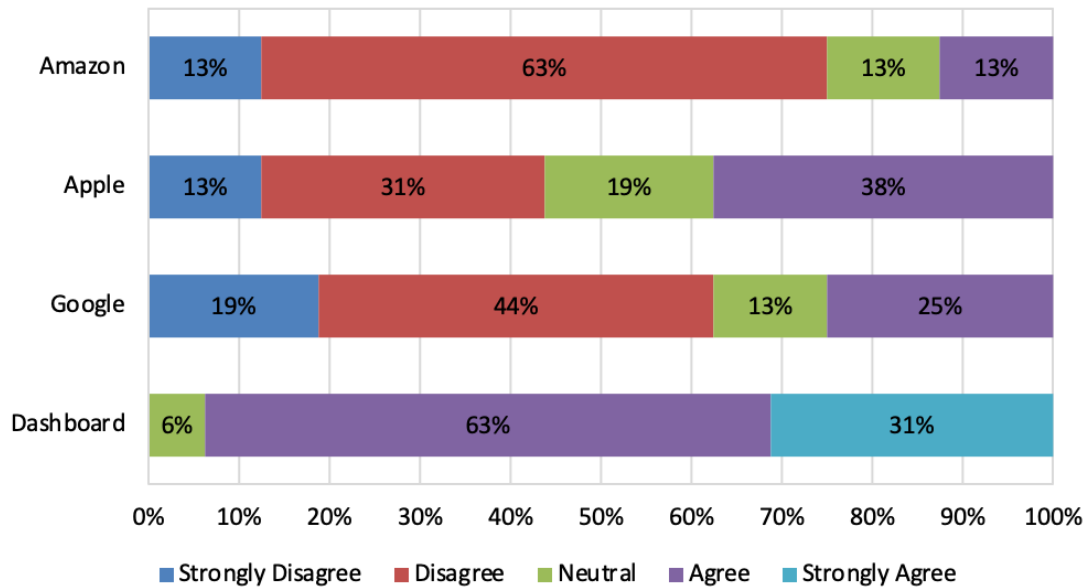


Figure 6.23: Q5. I found the various functions in this platform were well integrated

As displayed in Figure 6.23, the Dashboard achieved the strongest ratings for integration, with 94% of participants selecting 'Agree' or 'Strongly Agree', indicating highly cohesive and intuitive functionality. Apple showed a moderate level of positive responses with 38% of participant selecting Agree but also had 44% of participants selecting Disagree or Strongly Disagree, suggesting mixed perceptions of integration. Moreover, Google's results were less positive, with only 25% of participants selecting Agree and 63% selecting Disagree, suggesting clear issues with how well its features integrate. Similarly, Amazon performed the worst, with only 12.5% of users choosing Agree and 75% of users choosing either disagree or 'Strongly Disagree, highlighting serious concerns about fragmented and poorly integrated functionality. These findings suggest that while Dashboard offers seamless integration, the other platforms, especially Amazon, may need significant design enhancements to provide a more harmonious user experience.

Q6. I thought there was too much inconsistency in this platform

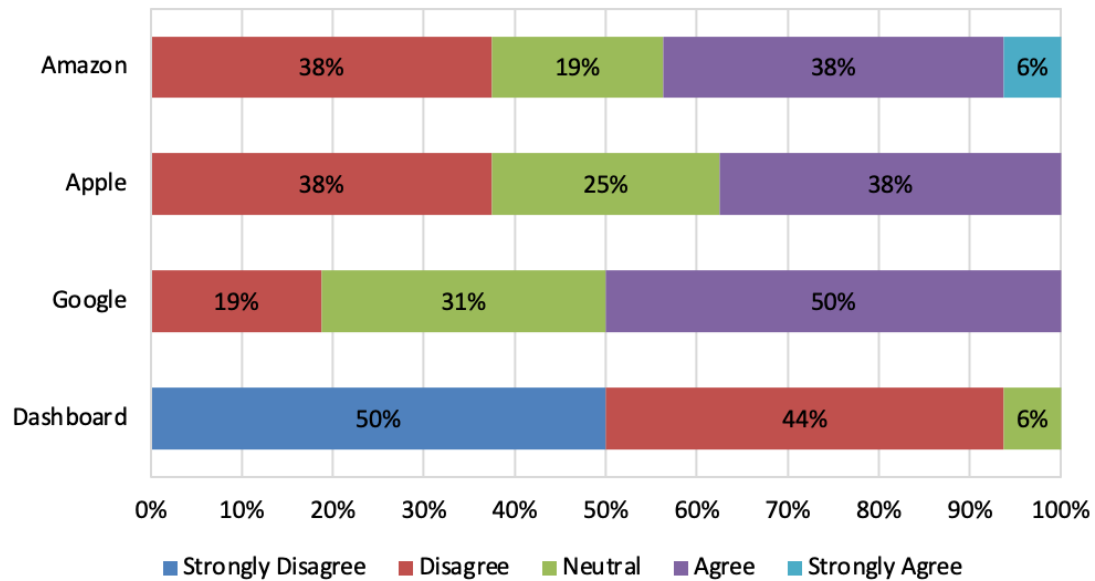


Figure 6.24: Q6. I thought there was too much inconsistency in this platform

As illustrated in Figure 6.24, the Dashboard received the most favourable ratings in terms of consistency, with 94% of participants selecting 'Strongly Disagree' or 'Disagree' when asked whether the interface felt inconsistent. Therefore, many participants found the Dashboard easy to follow, with a clear and consistent structure that made interaction feel natural and straightforward.

Alternatively, Google raised the most concern among participants, with half of them agreeing that the interface felt inconsistent. Nearly a third selected the neutral option, while fewer than 20% disagreed, showing a noticeable split in perception. Such results suggest that some users may have struggled with varying layouts or unpredictable elements while navigating the system.

Moreover, Amazon also received less favourable feedback, with 44% of participants agreeing or strongly agreeing that the experience felt inconsistent. Users may have

encountered disjointed workflows or scattered navigation, which can make the system feel harder to follow and mentally demanding.

Conversely, Apple's ratings were relatively more favourable, though they still exhibited a degree of inconsistency. Approximately 38% of participants agreed with the statement, indicating moderate concerns regarding the uniformity of the user experience. While the issues were not as pronounced as those observed with Google or Amazon, these results suggest that users still perceived variations in design or interaction patterns, which could disrupt their overall workflow.

Altogether, these findings support the Dashboard's strength in delivering a harmonious and seamless experience, while emphasising the need for other platforms to improve interface consistency and reduce conflict in the user journey.

Q7. I would imagine that most people would learn to use this platform very quickly

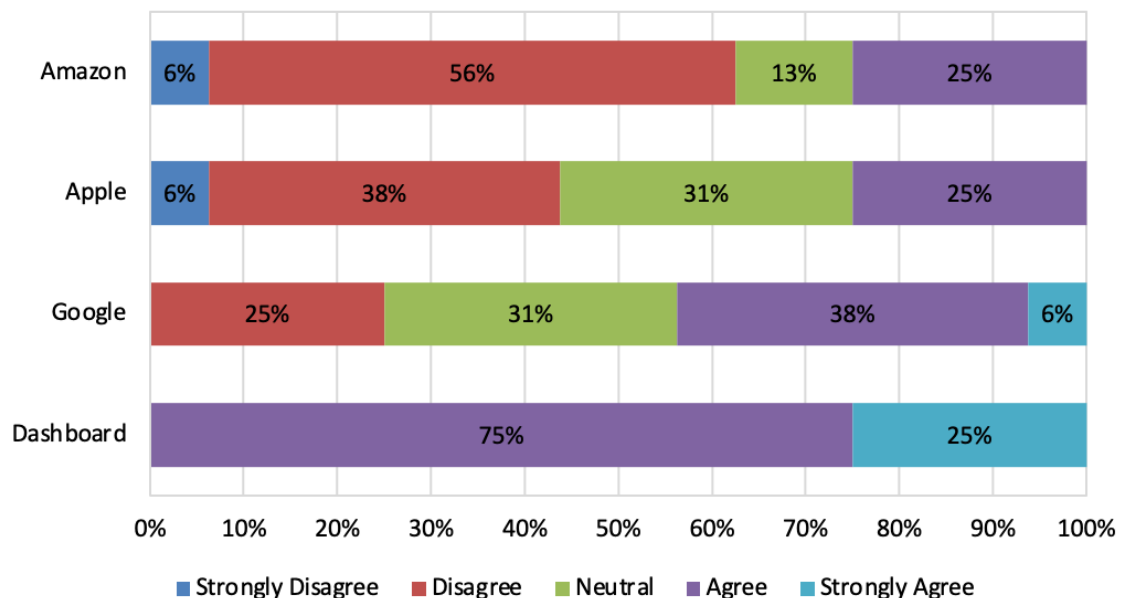


Figure 6.25: Q7. I would imagine that most people would learn to use this platform very quickly

As shown in Figure 6.25, the Dashboard emerged as the best platform in this question, with all participants agreeing that most individuals would be able to learn how to use it quickly. This finding points to an interface that is significantly intuitive and user-friendly. On the other hand, Google garnered mixed feedback. Concurrently, 44% of users believed it would be easy to learn, a noteworthy quarter expressed disagreement, and many remained neutral, suggesting some level of uncertainty regarding its learning curve.

Apple's feedback was even more divided between participants, with only 25% of users rating it as easy to learn. On the other hand, 44% felt that the system might be challenging, indicating that it could require more time to master. Ultimately, Amazon performed the least favourably compared to the others. For more classifications, only 25% of users perceived it as easy to learn, while a striking 63% believed it would pose difficulties for most users. These findings underscore the Dashboard's strength in facilitating quick user onboarding, whereas the commercial platforms, particularly Amazon, need a study of their designs to enhance their learnability.

Q8. I found the platform very cumbersome to use.

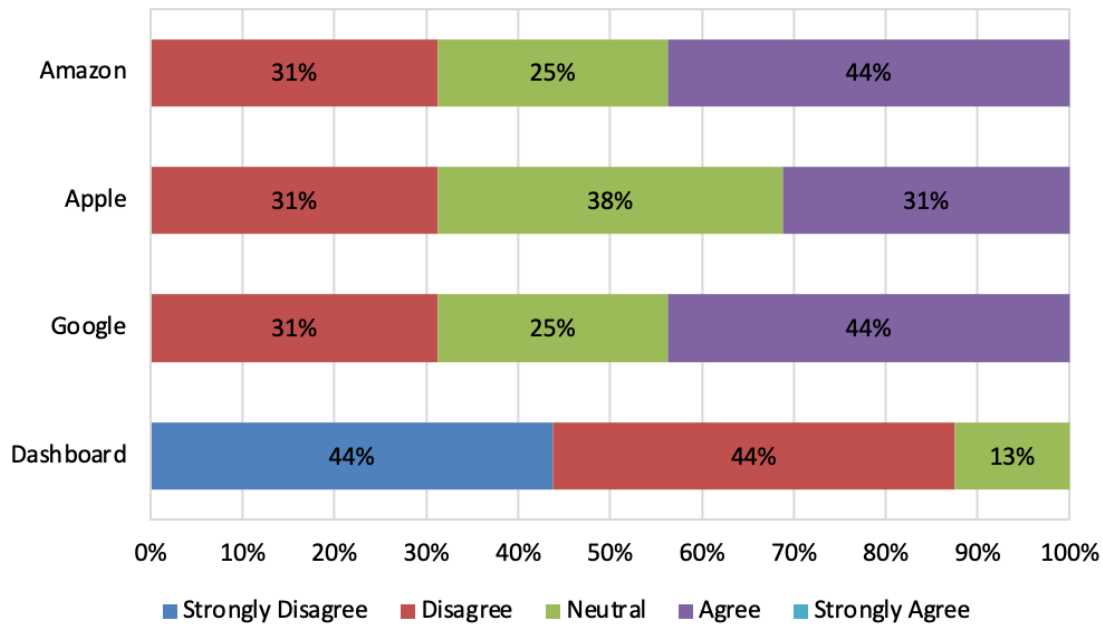


Figure 6.26: Q8. I found the platform very cumbersome to use

As presented in Figure 6.26, the Dashboard received the highest ratings for ease of use, with 88% of participants indicating they "Strongly Disagree" or "Disagree" with the notion that it is cumbersome. This demonstrates that users found it easy to navigate without unnecessary steps or complications. Alternatively, both Google and Amazon faced considerable challenges in this area, with 44% of participants describing their platforms as cumbersome. This indicates that many users felt these platforms were too demanding or had complicated workflows.

Apple's ratings were relatively higher; however, they still raised some concerns. Specifically, 31% of participants described the experience as cumbersome, and a considerable number remained neutral, indicating some uncertainty regarding its ease of use. These findings underscore the Dashboard's strong performance in providing a streamlined experience, while also highlighting the need for commercial platforms, especially Google and Amazon, to simplify their designs and reduce user effort.

Q9. I felt very confident using the platform

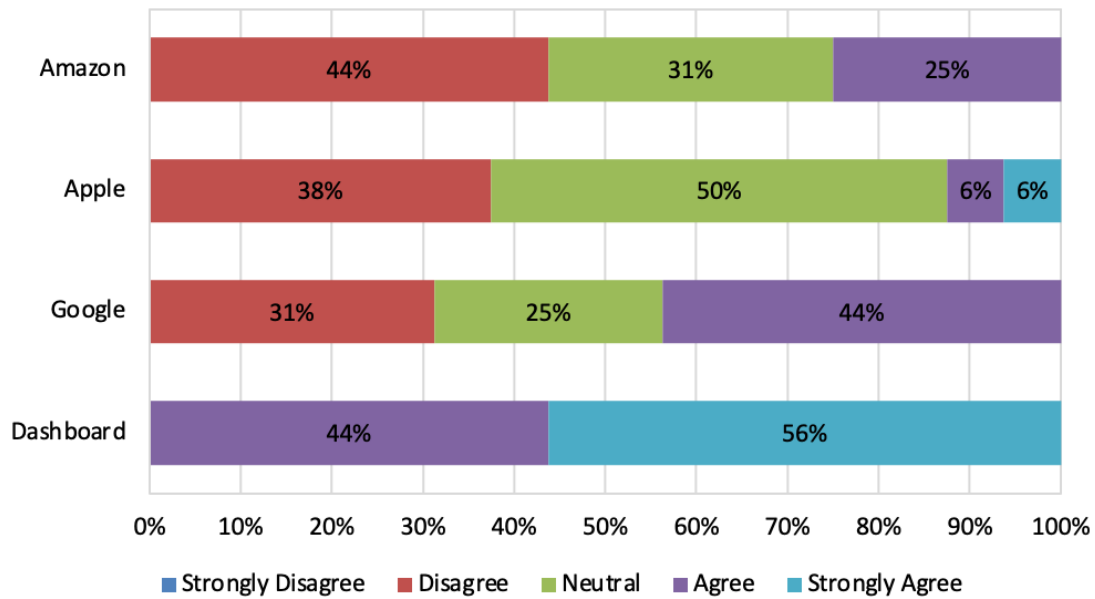


Figure 6.27: Q9. I felt very confident using the platform

As illustrated in Figure 6.27, participants expressed confidence in navigating the Dashboard interfaces; all selected Agree or Strongly Agree in response to the confidence question. In contrast, Google displayed varied results; 44% of participants reported feeling confident using the platform, while a significant number remained neutral or disagreed, highlighting an inconsistent user experience. Amazon's performance was even less favourable, with only 25% of participants expressing confidence, while many others conveyed uncertainty or a lack of assurance when using the platform. Apple received the lowest confidence ratings, as only 12.5% of participants agreed or strongly agreed that they felt in control. Additionally, half of the participants selected the neutral option, indicating that they may have encountered difficulties in navigating and feeling comfortable with the interface.

These findings emphasise the Dashboard's significant advantage in building user confidence. At the same time, commercial platforms, such as Apple and Amazon, need substantial improvements to ensure users feel secure and competent in their interactions.

Q10. I needed to learn a lot of things before I could get going with this system

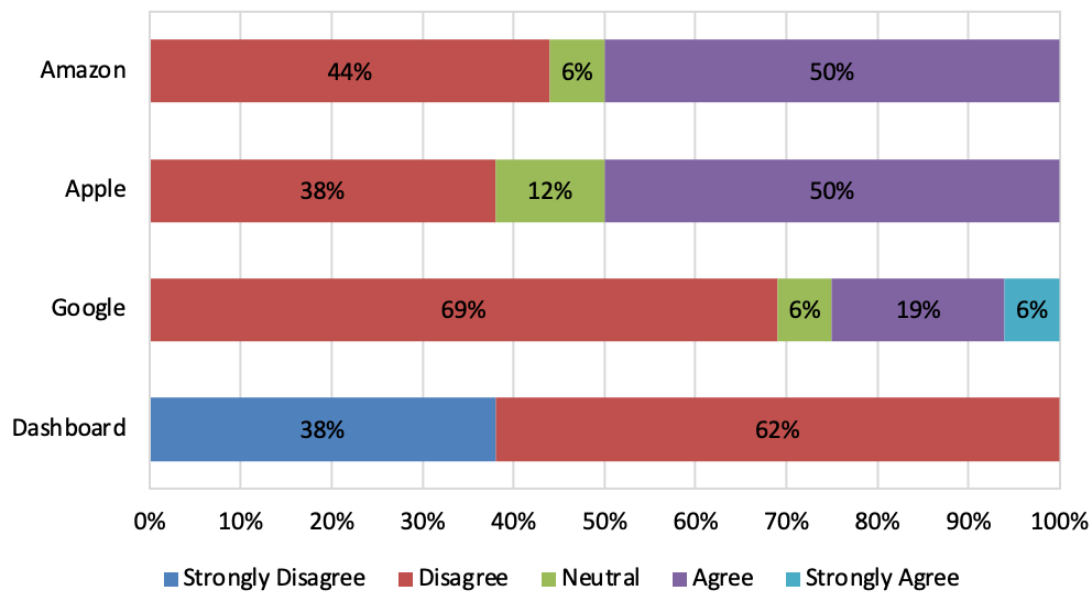


Figure 6.28: Q10. I needed to learn a lot of things before I could get going with this system

As shown in figure 6.28, the Dashboard performed best on this question, as all participants selected Strongly Disagree or Disagree. To clarify, users can start using it immediately without needing to learn additional steps or concepts. Google also performed well, with 69% of participants disagreeing that much learning was needed. However, around a quarter indicated that it did require some learning, suggesting a minor level of complexity for certain tasks. In contrast, both Amazon and Apple exhibited clear issues here, with half of the participants indicating that they needed to learn a lot before getting started. Therefore, complex interfaces can complicate the onboarding experience for new users. The success of Dashboard in delivering an immediately usable experience suggests that both Amazon and Apple could benefit from simplifying their initial learning processes.

The item-level analyses of the SUS highlight consistent patterns in perceived usability strengths and weaknesses across different platforms. The Dashboard was found to have clearer, simpler, and more predictable design features. In contrast, competing systems received higher ratings for unnecessary complexity, inconsistency, and a lack of user confidence.

While the SUS scores and item-level ratings provide detailed quantitative perspectives on user satisfaction, the following section focuses on Qualitative Feedback on Satisfaction to capture participants' own words, reflections, and contextual insights about their experiences with the platforms.

6.2.4.3 Qualitative Feedback on Satisfaction

This section summarises qualitative feedback from participants P1101 to P1116 regarding their overall satisfaction with the smart home Dashboard, compared with Apple, Amazon, and Google platforms. Satisfaction here refers to users' subjective impressions of ease of use, enjoyment, attractiveness of design, perceived intuitiveness, and their willingness to recommend the system to others. This analysis offers a deeper understanding of not only what participants thought, but also why they perceived the Dashboard as superior to alternatives.

- ***Overall Impressions***

Participants consistently described the smart home Dashboard as easy to use, intuitive, and user-friendly, frequently contrasting it with the greater complexity of Apple, Amazon, and Google. For example, P1101 described it as "smooth and very straightforward," while P1108 characterised it as very positive and mentioned that "it is much better designed than other apps". Many highlighted its clarity and the convenience of having all settings and devices in one place. P1107 praised it as "a lot easier to use and learn than the manufacturer's apps". P1116 commented that it was "attractive even for kids" and "easy to

link all the smart devices in one control environment", reflecting strong appeal across different user types.

- ***Intuitiveness***

Participants also emphasised the system's intuitiveness and accessible design. P1110, who described having no technical background, explained: " I prefer using the dashboard. I do not have a technical background, but I found it easy to use", adding, "I never felt lost while using it". Similarly, P1102 noted that " all ages could understand it well". These comments highlight how the system's design facilitates understanding across varying levels of experience and fosters confidence in managing privacy settings.

- ***Comparison with Apple, Amazon, and Google***

While the Dashboard was generally praised, participants contrasted it directly with competing systems, highlighting key shortcomings in those alternatives. In contrast, Apple, Amazon, and Google received lower satisfaction ratings across participants. Comments highlighted unclear icons, excessive steps, fragmented privacy settings, and confusing navigation paths. For example, P1114 criticised "Apple's icon not clear" and complex flows, while P1109 described Amazon as "unnecessarily complex" with "many repeated steps." Google was most often described as the least satisfying, with participants reporting that they gave up on tasks due to confusing settings structures and extended times. Such critical comparisons underscore why users preferred the Dashboard, linking satisfaction not only to positive features but to relief from frustrations experienced with other systems.

- ***Recommendations***

While overall satisfaction was high, participants offered targeted suggestions for improvement. Common recommendations focused on navigation clarity and personalisation options, such as adding a back button (P1101, P1104, P1105, P1116) and clearer or larger icons (P1111, P1112, P1107). Several participants proposed advanced or power-user features, including authentication and 2FA (P1101), advanced settings and quick actions (P1115), group control for multiple smart devices with a display indicator (P1114), live camera views (P1108), and additional notification features (P1106). Notably, some suggestions, such as adding a back button, address both navigation improvements and feature completeness, indicating that users often view these aspects as interconnected. Despite these suggestions, many participants considered the Dashboard sufficient as it is, with responses such as P1110 said "None, I believe the dashboard is sufficient as it is" and P1102 said "Nothing" when asked about improvements. Despite these improvement suggestions, overall confidence in the Dashboard remained strong, with most users seeing it as ready for daily use.

- ***Recommendation Dashboard to Others***

An important indicator of satisfaction was participants' willingness to recommend the Dashboard to others. Nearly all participants expressed strong endorsement, with P1105 replying "Yes", P1107 describing it as "much better than the device's native application," and P1109 emphasising that it was so clear "even someone who has no experience in technology can use it." P1115 stated: "I highly recommend it, all the smart devices in one platform and easy to control", while P1116 described it as "easy, even for kids". Such consistent willingness to recommend the Dashboard highlights its perceived value and appeal across diverse user groups. These qualitative insights reinforce the Dashboard's

strong perceived value and suggest clear design strategies for maintaining high user satisfaction.

- ***Summary***

Overall, participants found the smart home Dashboard to be highly satisfying compared to Apple, Amazon, and Google, highlighting its ease of use, intuitive design, and strong alignment with their expectations. While minor improvements were suggested, the feedback demonstrates the Dashboard's potential as a user-friendly, reliable, and recommendable solution for smart home privacy management.

Having presented detailed results on efficiency, effectiveness, and satisfaction separately, it is valuable to synthesise these findings. The next section presents an integrated comparative analysis to highlight the relative strengths and weaknesses of smart home dashboards in context.

6.2.5 Comparative Analysis

This concluding section synthesizes findings from the metrics of efficiency, effectiveness, and user satisfaction. It provides a comparative analysis that integrates quantitative and qualitative results across all platforms, allowing the identification of patterns, differences, and both strengths and weaknesses in design. By integrating these insights, the analysis offers a comprehensive overview of usability and provides recommendations for enhancing the user experience.

- ***Efficiency Comparison***

Quantitative data consistently demonstrated that the smart home Dashboard recorded the fastest completion times and the lowest number of clicks required per task across participants compared to the other platforms. Users completed tasks on the Dashboard in

an average of approximately 33 seconds, compared to 51 to 56 seconds on other platforms. Additionally, the average number of clicks per task was approximately six on the Dashboard, while it ranged from seven to eight on the others. The variance in performance was also lower for the Dashboard, indicating consistent results across various user groups, experience levels, and genders.

Qualitative feedback supported these findings. Participants described the Dashboard as “smooth,” “straightforward,” and “very easy to use,” while they frequently criticised Apple, Amazon, and Google for their confusing paths, unclear icons, and multi-step processes. Suggestions for minor efficiency improvements, such as adding a back button, focused on fine-tuning rather than addressing significant flaws. In contrast, the commercial platforms received repeated complaints regarding unnecessary complexity and steep learning curves, particularly from less experienced users. Overall, these patterns indicate that the smart home Dashboard offers a notably more efficient interaction design, reducing cognitive load and the time spent on tasks, while also facilitating rapid learning.

▪ ***Effectiveness Comparison***

Effectiveness results, measured by task completion rates, strongly favoured the Dashboard, which achieved consistently higher completion rates than commercial platforms. In contrast, Google, Amazon, and Apple had average success rates ranging from 70% to 81%, with higher variability indicating inconsistent performance. Amazon, in particular, showed significant variability, revealing design issues that posed challenges for less experienced users. Qualitative data further supported these findings. Participants noted that the Dashboard facilitated confident and error-free task execution, even in privacy scenarios.

In comparison, Apple, Amazon, and Google often struggled with tasks such as managing recordings or controlling privacy during meetings, leading some users to abandon these

tasks altogether. Users described the Dashboard as consistently meeting their expectations by seamlessly integrating multiple smart devices within a single environment. Feedback on feature completeness indicated that the Dashboard largely addressed user needs, although it also prompted advanced suggestions, such as voice commands, cloud backup, and enhanced settings. Importantly, many suggestions linked navigation and feature completeness (such as requests for a clearer back button), highlighting the relationship between design clarity and functionality.

▪ **Satisfaction Comparison**

The SUS results demonstrated a clear trend, with the smart home Dashboard achieving the highest mean score of approximately 86, accompanied by the lowest standard deviation. This indicates both high user satisfaction and strong consensus regarding its usability. In contrast, Amazon received the lowest score, around 44, while Google and Apple had moderate but varied ratings ranging from 49 to 53. These trends were consistent across different experience levels, genders, and starting conditions, with advanced users rating all platforms higher but still showing a distinct preference for the Dashboard. An analysis of the SUS questions revealed that the Dashboard excelled in all areas, including perceived ease of use, feature integration, consistency, and learnability. Participants strongly disagreed with statements suggesting that the platform was cumbersome or inconsistent, and nearly all felt confident using it without technical assistance.

In comparison, Amazon and Apple often received neutral or negative ratings on these aspects, highlighting ongoing usability challenges. Qualitative feedback on user satisfaction further reinforced these findings. Participants described the Dashboard as intuitive, visually appealing, and easy to navigate, praising its design for consolidating smart home management in one place. Many explicitly stated they would recommend it to

others, in stark contrast to the frequent frustration, confusion, and abandonment experienced with the commercial platforms.

▪ ***Integrated Insights and Implications***

The results present a strong case for the superior usability of the smart home Dashboard across all key areas. Its design enables faster, simpler, and more reliable task flows, ensuring consistent success even for less experienced users. High SUS scores and participants' willingness to recommend the Dashboard indicate strong perceived value and potential for adoption.

However, advanced users pointed out opportunities for improvement. Suggestions such as incorporating voice commands, quick action buttons, and advanced settings highlight the need to strike a balance between simplicity and flexibility for power users. Minor navigation enhancements, including clearer back buttons and better icon labelling, could further improve the experience for first-time users.

In contrast, Google, Amazon, and Apple face challenges with inconsistent navigation, unclear labelling, and fragmented settings, which increase task duration, variability, and error rates, particularly in privacy management. These issues emphasize the difficulty in balancing robust functionality with clarity and ease of use.

Overall, the success of the smart home Dashboard illustrates the importance of user-centred design in providing an efficient, effective, and satisfying experience for managing smart home security and privacy.

6.3 Summary

This chapter presented a comprehensive evaluation of the smart home Dashboard, assessing its usability, efficiency, and effectiveness in comparison with three leading commercial platforms: Google Home, Amazon Alexa, and Apple HomeKit. Using a task-based experimental design, the study measured objective performance metrics such as completion time, click count, and success rate alongside subjective satisfaction through the SUS and qualitative feedback.

The findings consistently demonstrated that the Dashboard achieved excellent results across all metrics. It enabled faster task completion, fewer interaction steps, and complete task success while also receiving the highest SUS ratings with minimal variability. Participants described it as intuitive, cohesive, and significantly more straightforward to use than commercial alternatives, particularly in managing security and privacy tasks across multiple devices.

These results confirm that the Dashboard's user-centred design effectively simplifies smart home management while enhancing user confidence and satisfaction. The insights gained from this evaluation directly inform the following chapter, which explores the design implications, technical feasibility, and overall contribution of the proposed Dashboard within the context of smart home security and privacy management.

Chapter Seven

Implications and Further Implementation

Building on the evaluation results presented in Chapter 6, this chapter discusses their implications for smart home interface design, focusing on how the harmonized dashboard addresses the usability gaps identified in other smart home devices. This chapter also considers technical feasibility and outlines recommendations for future improvements.

7.1 Key Findings

The evaluation compared the smart home Dashboard with Google Home, Amazon Alexa, and Apple HomeKit applications. The findings of this study demonstrate that the Dashboard prototype achieved better results than the other platforms in terms of efficiency, effectiveness, and user satisfaction.

In terms of efficiency, the Dashboard enabled participants to complete tasks in significantly less time and with fewer clicks. Specifically, the average completion time was approximately 33 seconds, in contrast to the 51 to 56 seconds range observed on other platforms. This significant difference highlights the platform's efficiency. Furthermore, the Dashboard users required fewer interactions, averaging around six clicks per task. The Dashboard also showed lower variability in performance among users from diverse backgrounds. These outcomes align with established usability principles, which recognise time on task and interaction effort as key indicators of efficiency (Nielsen, 1994; Sauro and Lewis, 2016).

Regarding effectiveness, the Dashboard achieved a perfect 100% task completion rate across all scenarios. In contrast, Google, Amazon, and Apple reported lower and more variable completion rates, ranging from 70% to 81%. Participants frequently reported leaving tasks on these applications due to unclear navigation, fragmented settings, or excessive steps. Similar usability barriers in IoT platforms have been reported in prior studies, where users expressed frustration with hidden or inconsistent privacy controls (Zeng et al., 2017).

Moreover, the satisfaction scores further confirmed these results. The participants gave the Dashboard prototype a mean SUS score of 86, which is well above the high usability benchmark of 80 (Brooke, 1996). In contrast, the other platforms scored between 44 and 53 on the SUS. Additionally, participants provided positive feedback about the Dashboard, describing it as intuitive and user-friendly. They also highlighted its capability to manage smart home devices through a single interface. Many participants expressed a willingness to recommend the Dashboard to others, highlighting its value and usability.

Qualitative feedback provides additional depth to these findings. For example, participants often described Apple, Amazon, and Google as complex, inconsistent, or unclear, indicating that these observations are consistent with prior research on fragmented IoT privacy interfaces (Emami-Naeini et al., 2020). Conversely, some participants described the Dashboard as "smooth", "straightforward", and "easy to use". Although some suggestions were made for refining the Dashboard, such as a clearer back button, improved icon labelling, and advanced settings, these were relatively minor and did not significantly compromise the design's overall usability.

Altogether, the findings demonstrate that the smart home Dashboard not only addresses recognised gaps in commercial applications but also delivers a more efficient, reliable, and satisfying solution for managing smart home security and privacy.

7.2 Implications for Design

The evaluation results provide important insights for designing an effective smart home Dashboard.

First, the findings highlight the importance of simplicity and clarity in navigation. Participants consistently expressed appreciation for the Dashboard's streamlined task flows, while some

noted the unnecessary complexity of other applications. This feedback aligns with previous research in HCI, which indicated that minimising unnecessary steps and providing clear labelling can significantly enhance learnability and reduce cognitive load (Norman, 2013; Sweller, 1988). Based on this insight, designers should focus on creating intuitive interfaces that establish straightforward pathways for users to complete tasks effectively.

Second, the evaluation highlights the need for a centralised and harmonised approach for managing security and privacy in smart home devices. Unlike other platforms, where privacy features are scattered across multiple menus, the Dashboard consolidated security notifications, software updates, and data management into a single interface. This integrative approach directly addresses earlier findings that IoT users struggle with fragmented privacy information and desire clearer, unified management tools (Emami-Naeini et al., 2020; Zeng et al., 2017).

Third, the results underscore the value of consistency and predictability for users. The uniform design of the Dashboard enabled all participants, regardless of their experience level, to complete their tasks. In contrast, inconsistent workflows on other platforms often led to participants making errors or abandoning their tasks. This supports Norman's (2013) point that predictable interfaces facilitate user interaction with platforms and enhance their confidence.

Fourth, participants' feedback reveals opportunities for personalisation and advanced features. While most users appreciated the simplicity of the Dashboard, advanced users expressed a desire for additional functionalities, such as quick actions and group controls. To address this, implementing a layered design could enhance navigation for both security and privacy features, making them accessible to all users. At the same time, expert users could access advanced features, encouraging broader adoption without sacrificing usability. This distinction in perspectives based on users' experience levels is supported by Emami-Naeini et al. (2020), who found that privacy expectations differ significantly between basic and advanced users.

Ultimately, the results emphasise the crucial connection between trust and usability as key design objectives. Participants often linked the clarity and ease of use of the Dashboard to their confidence in managing their data. On the other hand, the complexity of commercial systems decreased trust and made users less willing to engage with privacy settings. Previous research has demonstrated that enhancing usability directly improves users' ability to understand and effectively utilise privacy controls (Emami-Naeini et al., 2020; Zeng et al., 2017).

Even though these applications were not specifically designed as privacy or security management tools, the evaluation revealed that many participants struggled to complete basic security and privacy-related tasks. For example, some participants were unable to complete certain tasks on their applications, such as turning off the microphone on the smart speaker or deleting video clips from the security camera. These challenges underscore how fragmented or inadequately designed interfaces can hinder users' ability to manage their data effectively. This highlights the fact that, regardless of a platform's initial design intentions, usability is a critical factor in ensuring that users can effectively manage their security and privacy features.

Beyond these design implications, the findings of this study contribute a novel perspective by demonstrating that usability challenges in smart home environments are not solely the result of technical limitations but are significantly influenced by how security and privacy features are structured and presented to users. While prior research has highlighted issues such as user awareness and privacy concerns, this study extends that understanding by providing empirical evidence of how fragmented interfaces, inconsistent navigation, and directly impacts user performance and decision-making.

This shifts the focus from improving individual features to rethinking the overall design of smart home systems as unified and user-centred environments. From a design perspective, this

implies the need for integrated dashboard structures, consistent navigation models, and the consolidation of security, privacy, and data management into a single, coherent interface.

As such, the contribution of this work lies not only in identifying design improvements, but in reframing security and privacy as interaction design problems that require integrated and user-centred solutions that bring together security, privacy, and data management in a clear and accessible way.

In summary, the findings of this study highlight simplicity, centralisation, consistency, flexibility, and trustworthiness as essential design priorities for smart home dashboards. These principles collectively support the development of more effective, user-centred systems that enhance usability and accommodate the diverse needs of smart home users.

7.3 Technical Feasibility

To demonstrate the feasibility of implementing a smart home Dashboard, a parallel bachelor's dissertation was carried out alongside this PhD research (Rowey, 2025). The undergraduate study was intentionally supervised as part of the broader research design, ensuring alignment with the technical objectives of this thesis. As a result, the dissertation demonstrated the possibility of integrating various smart home devices into a unified dashboard.

At the same time, the primary aim of this PhD research is to create a dashboard that harmonises information from smart home devices, enhancing user understanding and facilitating control over security and privacy features.

The bachelor's thesis addressed the complementary challenge of technical interoperability by developing a solution that enabled platform-agnostic communication between a central application and multiple smart home ecosystems, including Amazon Alexa, Ring, Samsung SmartThings, and Apple HomeKit.

At a high level, the approach focused on enabling communication between a central application and these ecosystems, demonstrating that it was technically feasible to consolidate fragmented device environments into a unified dashboard. The system adopted a modular architecture that supported interoperability across communication protocols such as REST APIs, Bluetooth Low Energy (BLE), and Wi-Fi, providing a scalable and flexible foundation for integrating diverse smart devices.

Accordingly, the undergraduate work is referenced here only as a supporting proof-of-concept, establishing the technical feasibility of integrating fragmented smart home ecosystems within a unified environment.

7.4 Summary

In summary, this chapter examined the implications of the evaluation results, demonstrating how the proposed dashboard addresses key security and privacy gaps identified in existing smart home systems. It also highlighted key design principles, including simplicity, consistency, and centralisation, which contribute to improved user trust and interaction.

In addition, the chapter considered the technical feasibility of the proposed approach, supported by a complementary undergraduate project, confirming that the solution is both practical and implementable.

Collectively, these findings provide a foundation for the final chapter, which presents the overall contributions, limitations, and future directions of this research.

Chapter Eight

Conclusions

This chapter concludes the thesis by summarising its main achievements, underlining the study's challenges and limitations, and outlining future research directions. Additionally, it discusses the broader implications of security and privacy in smart homes, providing closure while highlighting opportunities for further development.

8.1 Achievements

This thesis has made several significant achievements in the area of smart home security and privacy. The central contribution lies in the design and development of a harmonised Dashboard that brings together fragmented and inconsistent security and privacy controls across different smart home devices. By consolidating these controls, the research has demonstrated that it is possible to simplify complexity and provide users with a more coherent and transparent way to manage security and privacy in smart home devices. In line with the aims and objectives stated in Chapter 1, all research goals were successfully achieved, as outlined in the following points:

1. The research investigated the extent to which security and privacy issues are made apparent to users of smart home devices by conducting a qualitative content analysis of product documentation, user manuals, online FAQ pages, and online resources. This analysis revealed significant inconsistencies, limited transparency, and major gaps in the way essential information is communicated to smart device users. Following this stage, the study evaluated how easily users could access and control security and privacy features in practice, thereby assessing the accessibility of these features and the overall user experience. Using smart speakers as a case study, a comparative evaluation of Apple, Amazon, and Google revealed that users may encounter challenges, such as complex navigation paths and inconsistent terminology, which hinder their ability to manage security and privacy effectively.

It is worth noting that the core findings from Chapter 3 were published as a peer-reviewed paper and presented at the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023), held in Lisbon, Portugal. This external validation highlights the originality and relevance of the work, as well as its contribution to the broader academic and professional community.

2. The research expanded its evaluation to include a broader range of smart home devices, covering five categories from three different manufacturers. This included smart speakers, thermostats, cameras, and robotic vacuums. The comparative analysis assessed the consistency of security, privacy, and data management features, as well as their availability and accessibility across these categories. The findings revealed significant differences in how manufacturers implement these security and privacy features, highlighting the lack of standardisation within the industry.
3. Building upon these insights, the research proposed and implemented a harmonised Dashboard as a practical solution to address the identified issues. The prototype consolidated fragmented controls into a unified and transparent interface. Moreover, the design was developed and guided by usability and HCISec principles prioritised clarity, accessibility, and meaningful interaction, ensuring a genuine improvement over existing fragmented solutions.

It is essential to highlight the key findings from Chapters 4 and 5, which were published as a peer-reviewed paper and presented at the 2024 HCI International Conference. This publication, titled "*Towards a Harmonised Approach for Security and Privacy Management in Smart Home Contexts*", further supports this research's contribution and highlights its significance in human–computer interaction and smart home security.

4. The proposed Dashboard was further validated through comparative evaluation with three leading platforms which are Google Home, Amazon Alexa, and Apple HomeKit. The results confirmed the feasibility of the proposed Dashboard and demonstrated measurable improvements in effectiveness, efficiency, and user satisfaction.

These findings indicated that the Dashboard not only addresses the limitations of existing fragmented interfaces but also provides a meaningful enhancement to users' ability to understand and manage security and privacy in smart home environments.

8.2 Thesis Contributions

This thesis makes several key contributions to the field of usable security and privacy in smart home environments, addressing limitations related to fragmentation, lack of transparency, and usability challenges identified in existing systems.

1. Comparative Analysis Contribution

While prior research has highlighted security and privacy challenges in smart home ecosystems, particularly due to device heterogeneity and fragmented platforms (Gavra et al., 2020; Geneiatakis et al., 2017). These studies have largely focused on technical vulnerabilities rather than how such fragmentation affects user interaction.

This thesis contributes a comparative analysis of smart home platforms, including 15 smart home devices across five categories, highlighting the extent of variation across platforms and focusing on how security, privacy, and data management features are presented and accessed from a user perspective. The findings demonstrate that inconsistencies in interface design, navigation structures, and terminology significantly hinder users' ability to understand and manage security and privacy settings effectively.

By explicitly evidencing how fragmentation manifests in real user interactions, this contribution identifies a critical usability gap that has been underexplored in the literature.

2. Design Contribution

Existing research has proposed various dashboards to enhance privacy awareness and security in smart homes, such as SaferHome (Windl et al., 2022) and Peekaboo (Jin et al., 2022). However, these solutions remain fragmented, often focusing on specific aspects such as data visualisation or awareness without providing integrated control. In addition, numerous smart home dashboards have been developed with goals such as energy efficiency, environmental monitoring, and household convenience. However, these dashboards primarily focus on energy and environmental data, with limited attention to how users manage security and privacy within the same interface. For instance, examples include Smart Electricity Dashboards (Jing et al., 2022) and Home Energy Management Systems (Zafar et al., 2020).

To address this limitation, this thesis proposes a unified smart home dashboard that integrates security, privacy, and data management into a single, coherent interface. The proposed Dashboard introduces a centralised interaction model that allows users to access features through multiple perspectives, including Rooms, Devices, User Data, and Data Types. It also organises functionalities into three core domains: Security, Privacy, and Data Management. The design introduces a structured interaction model that improves visibility, consistency, and user control, and is grounded in usability and Human-Computer Interaction (HCI) principles.

This contribution offers a novel design approach that translates identified usability challenges into a practical and integrated solution for smart home management.

3. Evaluative Contribution

Previous studies evaluating smart home privacy and security solutions have often relied on small-scale samples or a limited number of participants (Worthy et al., 2016; Udoh and Alkharashi, 2017), limiting their ability to assess usability in realistic scenarios.

This research addresses this gap through a controlled comparative user study evaluating the proposed dashboard against leading platforms, including Google Home, Amazon Alexa, and Apple HomeKit. The study involved 16 participants from diverse backgrounds and educational levels, with varying levels of experience in using smart home devices.

The results demonstrate significant improvements in efficiency, effectiveness, and user satisfaction, as evidenced by faster task completion, higher success rates, and improved SUS scores.

This contribution provides robust empirical evidence that a unified, design-driven approach can substantially enhance security and privacy in smart home environments.

4. Conceptual Contribution

Prior research has largely approached smart home security and privacy as technical challenges, focusing on solutions such as authentication protocols and network-based protections (Kotz et al., 2009; Garfinkel, 2014). However, these approaches often overlook how such mechanisms are presented to end users, and studies have shown that users frequently struggle to understand and manage privacy and security settings (Jacobsson and Davidsson, 2015; Zheng, 2017; Wash and Rader, 2015), thereby increasing potential risks, as a lack of understanding can limit users' ability to protect their data effectively.

This research advances understanding by demonstrating that security and privacy challenges in smart home environments are not solely technical issues but are strongly shaped by how these features are presented, structured, and accessed within user interfaces.

By linking technical security solutions with user-centred interaction design, this research reframes smart home security and privacy as usability and interaction design problems, rather than purely technical concerns.

This contribution emphasises the importance of clarity, consistency, and transparency in interface design, demonstrating that improving how security and privacy features are organised can simplify complexity and support more effective user decision-making, aligning with prior work highlighting the role of user awareness and interaction in managing smart home risks.

8.3 Challenges and Limitations

Although this research successfully achieved its objectives and made valuable contributions, several challenges and limitations must be acknowledged. These factors do not diminish the importance of the findings but instead highlight the practical and academic boundaries of the study. The main limitations are summarised as follows:

1. Controlled Testing Environment

The prototype was implemented and evaluated within a simulated and controlled environment rather than in fully operational households. Whilst this approach enabled systematic observation and reduced extraneous variables, it inevitably restricted the ecological validity of the findings. It limited the extent to which real-world complexities could be captured.

2. Time and Resource Constraints

Given the timeframe and resources available to a single doctoral researcher, it was beyond the scope of this study to develop and deploy a fully functional application. Instead, a high-fidelity prototype was developed and evaluated within this research, while a separate proof-of-concept implementation, developed as part of a parallel bachelor's project, demonstrated the technical feasibility of the proposed approach

3. Sample Size Limitations

The experimental evaluation involved a reasonably small number of participants. Although the number of participants was sufficient to identify key usability issues and to allow for meaningful comparison of initial findings, the overall sample size was relatively small. This limitation inevitably constrains the extent to which the results can be generalised across broader populations and different household contexts. To enhance the validity and applicability of the findings, future research should involve larger and more diverse participant groups, preferably through longitudinal studies.

4. Challenges in Accessing Security and Privacy Features

Obtaining information on how to control security, privacy, and data management features in smart home devices proved to be a significant challenge, as not all smart device manufacturers provide consistent or dedicated user pages that clearly explain how to configure these features.

5. Restricted Scope of Devices

The investigation focused on a specific subset of smart home devices, which included smart TVs, speakers, thermostats, cameras, and robotic vacuums. While these categories are significant within the consumer market, the rapid evolution of smart home technology means that the findings may not apply uniformly to emerging or less common device types.

6. Simulated Integration with Commercial Platforms

The prototype demonstrated the feasibility of integration with platforms such as Amazon Alexa and Apple HomeKit in a simulated environment. However, achieving full real-world integration would require substantial additional engineering and development efforts.

In summary, the challenges and limitations identified in this research highlight both the academic scope and practical limitations of implementing a harmonised Dashboard in real-world settings. While these issues do not reduce the contributions made, they highlight the complexity of the smart home ecosystem and the challenges of achieving interoperability, scalability, and long-term adoption. Recognising these limitations is crucial for guiding future research, particularly in large-scale evaluations, technical integration, and strategies to enhance user trust. These factors define the boundaries of the current work while also paving the way for future research, which will be discussed in the next section.

8.4 Future Research Directions

This thesis has laid the groundwork for harmonising security and privacy management in smart homes, yet several areas remain open for future exploration.

First, future studies should evaluate the dashboard in real household environments instead of controlled settings. While the prototype has demonstrated its feasibility for managing various smart home devices, testing it in actual homes will yield valuable insights into long-term usability and any unexpected challenges that may arise. Additionally, it would be beneficial to involve a larger and more diverse sample of participants to improve the generalizability of the findings and to capture the perspectives of users from different backgrounds, levels of technical expertise, and cultural contexts.

Second, future research should consider expanding the dashboard's scope beyond security and privacy. Future research should examine how the harmonisation approach can address additional areas of smart home management, such as energy efficiency, automation routines, accessibility, and user comfort. This would position the dashboard as a central hub for managing all smart home functions.

Third, future research should focus on making the dashboard more intelligent and adaptive. By integrating machine learning with automation, the dashboard could evolve to be more than just a display and control interface for security and privacy features. It would be capable of proactively detecting new risks, automatically adjusting privacy settings, and providing personalised advice to users. This way, the dashboard would function not only as a management tool but also as an intelligent assistant. Such enhancements would reduce the cognitive load on users while simultaneously strengthening the overall security of smart homes.

Fourth, future work should investigate how a wider range of smart home devices can be integrated into the dashboard. As the smart home ecosystem continues to expand with heterogeneous smart devices, further studies are needed to determine how different device categories interact with the system and how interoperability can be improved.

In summary, extending this study requires not only technical development and larger-scale evaluation but also careful attention to user adoption, device diversity, and collaboration with the wider smart home ecosystem.

8.5 The Future of Security and Privacy in Smart Homes

Security and privacy will continue to be significant challenges as smart homes grow in scale, complexity, and integration with our daily lives. The rapid increase in interconnected smart devices, along with advancements in artificial intelligence and automation, will undoubtedly

expand the potential for cyberattacks and introduce new risks associated with data misuse, surveillance, and system vulnerabilities. These developments underscore the urgent need for effective, transparent, and user-friendly strategies to manage security and privacy in the smart home environment.

In the coming years, harmonising security and privacy features will be essential to overcoming fragmentation across manufacturers and ecosystems. Without such unification, users will continue to face inconsistent, complex, and sometimes unclear controls that undermine trust in innovative technologies. Efforts to embed clarity, interoperability, and user empowerment into design processes will therefore shape the direction of the smart home industry.

At the same time, the future of security and privacy in smart homes will depend not only on technological innovation but also on regulatory frameworks and industry collaboration. Therefore, governments, manufacturers, and standardisation bodies must work together to establish guidelines and shared practices that protect users while enabling innovation. This collaboration will ensure that solutions like harmonised dashboards are not isolated prototypes but scalable foundations for real-world adoption.

Ultimately, the future of smart homes depends on creating environments that are trusted, resilient, and inclusive, where security and privacy are considered essential values rather than optional features. By integrating these principles into the core of design and governance, smart homes can transform into safe and empowering spaces that improve the quality of life while protecting the rights and interests of their users.

Overall, this research contributes to the field of smart home security and privacy by proposing a harmonised, user-centred dashboard design. The developed high-fidelity prototype demonstrates how complex security and privacy configurations can be translated into a more

accessible and comprehensible experience for all smart home users, regardless of their level of experience. This lays a foundation for future implementations and studies in this domain.

References

- Abbott, J., Dev, J., Kim, D., Gopavaram, S., Iyer, M., Sadam, S., Mare, S., Ringenberg, T., Andalibi, V., & Camp, L. (2023). Kids, Cats, and Control: Designing Privacy and Security Dashboards for IoT Home Devices. *Ndss-Symposium.Org* J Abbott, J Dev, DI Kim, SR Gopavaram, M Iyer, S Sadam, S Mare, T Ringenberg, V Andalibi Proceedings 2023 Symposium on Usable Security. Internet Society, 2023•ndss-Symposium.Org. <https://doi.org/10.14722/usec.2023.236290>
- Abdi, N., Such, J., & Ramokapane, K. (2019). More than Smart Speakers: Security and Privacy Perceptions of Smart Home Personal Assistants. *Usenix*. www.usenix.org/conference/soups2019/presentation/abdi
- Abrishamchi, M., Zainal, A., Ghaleb, F., Qasem, S., & Albarrak, A. (2022). Smart Home Privacy Protection Methods against a Passive Wireless Snooping Side-Channel Attack. *Sensors (Basel, Switzerland)*, 22(21). <https://doi.org/10.3390/S22218564>
- Acar, Y., Stransky, C., Wermke, D., Mazurek, M., & Fahl, S. (2017). End User Security and Privacy Concerns with Smart Homes. *Uesnix*, 65–80. <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/acar>
- Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM*, 42(12), 40–46. <https://doi.org/10.1145/322796.322806>
- Ahmed, F., & Ko, Y. B. (2016). Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks. *Security and Communication Networks*, 9(18), 5143–5154. <https://doi.org/10.1002/SEC.1684>
- Al-Ali, A., Zualkernan, I., Rashid, M., Gupta, R., & Alikarar, M. (2017). A Smart Home Energy Management System Using IoT and Big Data Analytics Approach. *IEEE Transactions on Consumer Electronics*, 63(4), 426–434. <https://doi.org/10.1109/TCE.2017.015014>
- Apthorpe, N., Reisman, D., & Feamster, N. (2017). A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic. <https://doi.org/10.48550/arxiv.1705.06805>
- Ashari, A., Shouran, Z., & Kuntoro, T. (2019). Internet of Things (IoT) of Smart Home: Privacy and Security. *Article in International Journal of Computer Applications*, 182(39), 975–8887. <https://doi.org/10.5120/ijca2019918450>
- Augusto-Gonzalez, J., Collen, A., Evangelatos, S., Anagnostopoulos, M., Spathoulas, G., Giannoutakis, K., Votis, K., Tzovaras, D., Genge, B., Gelenbe, E., & Nijdam, N. (2019). From internet of threats to internet of things: A cyber security architecture for smart

- homes. *IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks, CAMAD, 2019-September*.
<https://doi.org/10.1109/CAMAD.2019.8858493>
- Bai, X., Xing, L., Zhang, N., Wang, X., Liao, X., Li, T., & Hu, S. (2016). Staying Secure and Unprepared: Understanding and Mitigating the Security Risks of Apple ZeroConf. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 655–674.
<https://doi.org/10.1109/SP.2016.45>
- Balta-Ozkan, N., Amerighi, O., & Boteler, B. (2014). A comparison of consumer perceptions towards smart homes in the UK, Germany and Italy: reflections for policy and future research. *Https://Doi.Org/10.1080/09537325.2014.975788*, 26(10), 1176–1195.
<https://doi.org/10.1080/09537325.2014.975788>
- Balta-Ozkan, N., Davidson, R., Bicket, M., & Whitmarsh, L. (2013). Social barriers to the adoption of smart homes. *Energy Policy*, 63, 363–374.
<https://doi.org/10.1016/J.ENPOL.2013.08.043>
- Baudier, P., Ammi, C., & Deboeuf-Rouchon, M. (2020). Smart home: Highly-educated students' acceptance. *Technological Forecasting and Social Change*, 153, 119355.
<https://doi.org/10.1016/J.TECHFORE.2018.06.043>
- Beautement, A., Sasse, M. A., & Wonham, M. (2009). The compliance budget: Managing security behaviour in organisations. *Proceedings New Security Paradigms Workshop*, 47–58. <https://doi.org/10.1145/1595676.1595684>
- Bitdefender. (2017). Remote Exploitation of the NeoCoolcam IP Cameras and Gateway. Szeno. <http://www.szneo.com>
- Bos, B., Calzada, V., Puri, R., & Mare, S. (2024). Exploring Usability of Data Flow Visualizations in a Privacy-focused Smart Home Dashboard. *CPSIoTSec 2024 - Proceedings of the 6th Workshop on CPS and IoT Security and Privacy, Co-Located with: CCS 2024*, 111–117. <https://doi.org/10.1145/3690134.3694823>
- Brooke, J. (1996). SUS-A quick and dirty usability scale. *Taylorfrancis.Com*, 207–212.
<https://doi.org/10.1201/9781498710411-35/SUS-QUICK-DIRTY-USABILITY-SCALE-JOHN-BROOKE>
- Bryson, M. (2023). *Principles of Color in UI Design*. UX Planet.
<https://uxplanet.org/principles-of-color-in-ui-design-43708d8512d8>
- Bugeja, J., Jacobsson, A., & Davidsson, P. (2017). On Privacy and Security Challenges in Smart Connected Homes. *Proceedings - 2016 European Intelligence and Security Informatics Conference, EISIC 2016*, 172–175. <https://doi.org/10.1109/EISIC.2016.044>

- Bugeja, J., Jönsson, D., & Jacobsson, A. (2018). An Investigation of Vulnerabilities in Smart Connected Cameras. *FTC*. <https://www.ftc.gov/news-events/press-releases/2013/09/marketer-internet->
- 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. <https://doi.org/10.1016/j.chb.2023.107770>
- Carlini, N., Mishra, P., & Vaidya, T. (2016). Hidden voice commands. *Usenix.Org*. <https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/carlini>
- Carminati, B., Colombo, P., Ferrari, E., & Sagirlar, G. (2016). Enhancing user control on personal data usage in internet of things ecosystems. *Proceedings - 2016 IEEE International Conference on Services Computing, SCC 2016*, 291–298. <https://doi.org/10.1109/SCC.2016.45>
- Cate, F. (2010). The Limits of Notice and Choice. *IEEE Security and Privacy*, 8(2), 59–62. <https://doi.org/10.1109/MSP.2010.84>
- Chan, M., Campo, E., Estève, D., & Fourniols, J. (2009). Smart homes — Current features and future perspectives. *Maturitas*, 64(2), 90–97. <https://doi.org/10.1016/J.MATURITAS.2009.07.014>
- Chen, J., Xu, F., Dong, S., Sun, W., & Zhang, K. (2024). Authorisation inconsistency in IoT third-party integration. *IET Information Security*, 16(2), 133–143. <https://doi.org/10.1049/ISE2.12043>
- Colnago, J., Feng, Y., Palanivel, T., Pearman, S., Ung, M., Acquisti, A., Cranor, L., & Sadeh, N. (2020). Informing the Design of a Personalized Privacy Assistant for the Internet of Things. *Conference on Human Factors in Computing Systems - Proceedings*. <https://doi.org/10.1145/3313831.3376389>
- Conti, M., Nati, M., Rotundo, E., & Spolaor, R. (2016). Mind The Plug! Laptop-User Recognition Through Power Consumption. *Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security*, 37–44. <https://doi.org/10.1145/2899007>
- Coskun, A., Kaner, G., & Bostan, İ. (2018). Is Smart Home a Necessity or a Fantasy for the Mainstream User? A Study on Users' Expectations of Smart Household Appliances Design for healthy hydration View project Sustainability in the Hospitality Sector View project. *International Journal of Design*, 12(1). www.ijdesign.org

- Cui, A., & Stolfo, S. (2010). A Quantitative Analysis of the Insecurity of Embedded Network Devices: Results of a Wide-Area Scan. *Proceedings of the 26th Annual Computer Security Applications Conference on - ACSAC '10*. <https://doi.org/10.1145/1920261>
- Davis, B., Mason, J., & Anwar, M. (2020). Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal*, 7(10), 10102–10110. <https://doi.org/10.1109/JIOT.2020.2983983>
- Demiris, G., & Hensel, B. (2008). Technologies for an aging society: a systematic review of “smart home” applications. *Yearbook of Medical Informatics*, 17(01), 33–40. <https://doi.org/10.1055/S-0038-1638580/ID/JR1638580-31>
- Duezguen, R., & Mayer, P. (2021). How to Increase Smart Home Security and Privacy Risk Perception. *Ieeexplore.Ieee.OrgR Duezguen, P Mayer, B Berens, C Beckmann, L Aldag, M Mossano, M Volkamer, T Strufe2021 IEEE 20th International Conference on Trust, Security and, 2021•ieeexplore.Ieee.Org*. https://ieeexplore.ieee.org/abstract/document/9724299/?casa_token=uOIVa7xHOM4AA AAA:ef5miHpPU5TpDJUD7h7ZbdoR0ir5fQo-9i-moWdpO8S0xio38S9oHQBdJJ4Cjkc8l3Azaul
- Edu, J., Such, J., & Suarez-Tangil, G. (2020). Smart Home Personal Assistants: A Security and Privacy Review. *ACM Computing Surveys (CSUR)*, 53(6). <https://doi.org/10.1145/3412383>
- Emami-Naeini, P., Agarwal, Y., Faith Cranor, L., & Hibshi, H. (2020). Ask the experts: What should be on an IoT privacy and security label? *Proceedings - IEEE Symposium on Security and Privacy, 2020-May*, 447–464. <https://doi.org/10.1109/SP40000.2020.00043>
- Emami-Naeini, P., Dixon, H., Agarwal, Y., & Cranor, L. (2019). Exploring How Privacy and Security Factor into IoT Device Purchase Behavior. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, 12(2019). <https://doi.org/10.1145/3290605>
- Emoncms. (n.d.). *OpenEnergyMonitor*. Home Open Energy Monitor. Retrieved September 19, 2025, from https://openenergymonitor.org/?utm_source=chatgpt.com
- Fabian, B., Ermakova, T., & Lentz, T. (2017). Large-scale readability analysis of privacy policies. *Proceedings - 2017 IEEE/WIC/ACM International Conference on Web Intelligence, WI 2017*, 18–25. <https://doi.org/10.1145/3106426.3106427>
- Fahrurozi, M., Tarigan, S., Tanjung, M., & Mutijarsa, K. (2020). The Use of ISO/IEC 27005: 2018 for Strengthening Information Security Management (A Case Study at Data and Information Center of Ministry of Defence). *ICITEE 2020 - Proceedings of the 12th*

- International Conference on Information Technology and Electrical Engineering*, 86–91. <https://doi.org/10.1109/ICITEE49829.2020.9271748>
- Fernandes, E., Rahmati, A., & Jung, J. (2017). Security implications of permission models in smart-home application frameworks. *Ieeexplore.Ieee.Org*, 15(2), 24–30. https://ieeexplore.ieee.org/abstract/document/7891524/?casa_token=_glmSxIa-wgAAAAA:4gzRcIRu9b-ww02cFXtnQ40U3gEOvXwgJymIzq0JFcaFFXXyqXRwpZcJ-YL2GV24v5lxQfM3
- Ford, R., Pritoni, M., Sanguinetti, A., & Karlin, B. (2017). Categories and functionality of smart home technology for energy management. *Building and Environment*, 123, 543–554. <https://doi.org/10.1016/J.BUILDENV.2017.07.020>
- Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, 31(8), 983–988. <https://doi.org/10.1016/J.COSE.2012.08.004>
- Furnell, S., Jusoh, A., Katsabas, D., & Dowland, P. (2006). Considering the Usability of End-User Security Software. *IFIP International Federation for Information Processing*, 201, 307–316. https://doi.org/10.1007/0-387-33406-8_26
- Furnell, S. M., Katsabas, D., Dowland, P. S., & Reid, F. (2007). A Practical Usability Evaluation of Security Features in End-User Applications. *IFIP International Federation for Information Processing*, 232, 205–216. https://doi.org/10.1007/978-0-387-72367-9_18
- Gavra, V. D., Dobra, I. M., & Pop, O. A. (2020). A Survey on Threats and Security Solutions for IoT. *Proceedings of the International Spring Seminar on Electronics Technology, 2020-May*. <https://doi.org/10.1109/ISSE49702.2020.9120977>
- Garfinkel, S. (2014). Usable Security: History, Themes, and Challenges. *IEEE Security & Privacy*, 12(5), 52–58. <https://doi.org/10.1109/MSP.2014.88>
- Geneiatakis, D., Kounelis, I., Neisse, R., Nai-Fovino, I., Steri, G., & Baldini, G. (2017). Security and privacy issues for an IoT based smart home. *2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2017 - Proceedings*, 1292–1297. <https://doi.org/10.23919/MIPRO.2017.7973622>
- Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*, 29(7), 1645–1660. <https://doi.org/10.1016/J.FUTURE.2013.01.010>

- Gupta, B. B., Arachchilage, N. A. G., & Psannis, K. E. (2018). Defending against phishing attacks: taxonomy of methods, current issues and future directions. *Telecommunication Systems*, 67(2), 247–267. <https://doi.org/10.1007/S11235-017-0334-Z/FIGURES/13>
- Han, J., Jeon, Y., & Kim, J. (2015). Security considerations for secure and trustworthy smart home system in the IoT environment. *Ieeexplore.Ieee.Org*, 1116–1116. https://ieeexplore.ieee.org/abstract/document/7354752/?casa_token=Y5qH2OGVxbsAAA:AAA:eS1tr9-jPmLcd0DJUwmb8yOQRpAwMRLeylelnEUMatcgL4cd2M5NEU2oU9louvvX-j3LPjvk
- Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., & Sikdar, B. (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. *IEEE Access*, 7, 82721–82743. <https://doi.org/10.1109/ACCESS.2019.2924045>
- Hatzivasilis, G., Ioannidis, S., Smyrlis, M., Spanoudakis, G., Frati, F., Goeke, L., Hildebrandt, T., Tsakirakis, G., Oikonomou, F., Leftheriotis, G., & Koshutanski, H. (2020). Modern Aspects of Cyber-Security Training and Continuous Adaptation of Programmes to Trainees. *Applied Sciences 2020, Vol. 10, Page 5702*, 10(16), 5702. <https://doi.org/10.3390/APP10165702>
- He, W., Golla, M., Padhi, R., Ofek, J., Dürmuth, M., Fernandes, E., & Ur, B. (2018). Rethinking Access Control and Authentication for the Home Internet of Things. In *Proceedings of the 27th USENIX Security Symposium*. <https://www.usenix.org/conference/usenixsecurity18/presentation/he>
- Hernandez, G., Arias, O., Buentello, D., & Jin, Y. (2015). Smart nest thermostat: A smart spy in your home. *Blackhat.Com*. <https://blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home-WP.pdf>
- Home Assistant. (n.d.). Home Energy Management. HA. Retrieved September 19, 2025, from <https://www.home-assistant.io/home-energy-management>
- Horcher, G. (2018). Woman Says Amazon Alexa Recorded Her Private Conversation, Sent Audio to Random Contact. The Daily Beast. <https://www.thedailybeast.com/woman-says-amazon-alexa-recorded-her-private-conversation-sent-audio-to-random-contact>
- Horton, H. (2018). Amazon Alexa recorded owner’s conversation and sent to “random” contact, couple complains. Telegraph. <https://www.telegraph.co.uk/news/2018/05/25/amazon-alexa-recorded-owners-conversation-sent-random-contact/>

- Hu, W., Chang, C., Sengupta, A., & Bhunia, S. (2020). An overview of hardware security and trust: Threats, countermeasures, and design tools. *Ieeexplore.Ieee. Org*, 40(6), 1010–1038.
- Hubert, M., Blut, M., Brock, C., Zhang, R. W., Koch, V., & Riedl, R. (2019). The influence of acceptance and adoption drivers on smart home usage. *European Journal of Marketing*, 53(6), 1073–1098. <https://doi.org/10.1108/EJM-12-2016-0794/FULL/PDF>
- Ibrahim, T., Furnell, S. M., Papadaki, M., & Clarke, N. L. (2010). Assessing the Usability of End-User Security Software. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6264 LNCS, 177–189. https://doi.org/10.1007/978-3-642-15152-1_16
- Islam, K., Shen, W., & Wang, X. (2012). Security and privacy considerations for Wireless Sensor Networks in smart home environments. *Proceedings of the 2012 IEEE 16th International Conference on Computer Supported Cooperative Work in Design, CSCWD 2012*, 626–633. <https://doi.org/10.1109/CSCWD.2012.6221884>
- ISO 9241-210. (2019). Ergonomics of human-system interaction: Human-centred design for interactive systems. *ISO*. <https://www.iso.org/obp/ui/#iso:std:iso:9241:-210:ed-2:v1:en>
- Itair, M., Shahrour, I., & Hijazi, I. (2023). The use of the smart technology for creating an inclusive urban public space. *Mdpi.Com*. <https://www.mdpi.com/2624-6511/6/5/112>
- Jackson, C., & Orebaugh, A. (2018). A study of security and privacy issues associated with the Amazon Echo. *International Journal of Internet of Things and Cyber-Assurance*, 1(1), 91. <https://doi.org/10.1504/IJITCA.2018.090172>
- Jacobsson, A., & Davidsson, P. (2015). Towards a model of privacy and security for smart homes. *IEEE World Forum on Internet of Things, WF-IoT 2015 - Proceedings*, 727–732. <https://doi.org/10.1109/WF-IOT.2015.7389144>
- Jin, H., Liu, G., Hwang, D., Kumar, S., Agarwal, Y., & Hong, J. I. (2022). Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes (Extended Technical Report). *ArXiv*. <https://arxiv.org/pdf/2204.04540>
- Jing, C., Guo, S., Zhang, H., Lv, X., & Wang, D. (2022). SmartEle: Smart Electricity Dashboard for Detecting Consumption Patterns: A Case Study at a University Campus. *ISPRS International Journal of Geo-Information 2022, Vol. 11, Page 194, 11(3)*, 194. <https://doi.org/10.3390/IJGI11030194>
- Johnson, A. (2021). How to securely store passwords – tips for managing and storing passwords. Norton. <https://us.norton.com/blog/how-to/how-to-store-passwords>

- Johnston, J., Eloff, J. H. P., & Labuschagne, L. (2003). Security and human computer interfaces. *Computers and Security*, 22(8), 675–684. [https://doi.org/10.1016/S0167-4048\(03\)00006-3](https://doi.org/10.1016/S0167-4048(03)00006-3)
- Kainda, R., Flechais, I., & Roscoe, A. (2010). Security and Usability: Analysis and Evaluation. *Oxford University Computing Laboratory*.
- Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. *Sensors 2020, Vol. 20, Page 4806*, 20(17), 4806. <https://doi.org/10.3390/S20174806>
- Kanchi, S., & Karlapalem, K. (2021). A Multi Perspective Access Control in a Smart Home. *CODASPY 2021 - Proceedings of the 11th ACM Conference on Data and Application Security and Privacy*, 321–323. https://doi.org/10.1145/3422337.3450324/SUPPL_FILE/CODASPY21-CODAS08P.MP4
- Karimi, K., & Atkinson, G. (2013). *What the Internet of Things (IoT) needs to become a reality*. Freescale Semiconductor. <https://www.nxp.com/docs/en/white-paper/IOT-NEEDS-WP.pdf>
- Kapucu, N., & Bilim, M. (2023). Internet of Things for Smart Homes and Smart Cities. *Power Systems, Part F1423*, 331–356. https://doi.org/10.1007/978-3-031-38506-3_13
- Karayiannis, K. (2023). User Interface Designs for Smart Home Device Security. *The University of Nottingham*.
- Katsabas, D., & Furnell, S. (2005). Using Human Computer Interaction Principles to Promote Usable Security. *Books.Google.Com*. <https://books.google.com/books?hl=en&lr=&id=t9zOAwwAAQBAJ&oi=fnd&pg=PA235&dq=Using+human+computer+interaction+principles+to+promote+usable+security&ots=FdQgUEQ1oi&sig=uZ2gp4x8hTaehdnf9ptOcANZEtw>
- Kelley, P. G., Consolvo, S., Cranor, L. F., Jung, J., Sadeh, N., & Wetherall, D. (2012). A conundrum of permissions: Installing applications on an android smartphone. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 7398 LNCS, 68–79. https://doi.org/10.1007/978-3-642-34638-5_6/COVER
- Keshavarz, M., & Anwar, M. (2019). The Automatic Detection of Sensitive Data in Smart Homes. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 11594 LNCS, 404–416. https://doi.org/10.1007/978-3-030-22351-9_27/COVER/

- Khalil, I., Zahoor, K., & Amber, S. (2018). Human Computer Interaction and Security (HCI-Sec). *International Journal of Scientific & Engineering Research*, 9(4).
<http://www.ijser.org>
- Khan, A., Javaid, N., & Khan, M. (2018). Time and Device Based Priority Induced Comfort Management in Smart Home Within the Consumer Budget Limitation. *Sustainable Cities and Society*, 41, 538–555. <https://doi.org/10.1016/J.SCS.2018.05.053>
- Kobialka, D. (2014). *HP: 70% of IoT Devices Vulnerable to Attack*. 2014.
<https://www.channelfutures.com/cloud/hp-70-of-iot-devices-vulnerable-to-attack>
- Kotz, D., Avancha, S., & Baxi, A. (2009). A privacy framework for mobile health and home-care systems. *Proceedings of the ACM Conference on Computer and Communications Security*, 1–12. <https://doi.org/10.1145/1655084.1655086>
- Koupaei, D., Song, T., Cetin, K., & Im, J. (2020). An Assessment of Opinions and Perceptions of Smart Thermostats Using Aspect-Based Sentiment Analysis of Online Reviews. *Building and Environment*, 170, 106603.
<https://doi.org/10.1016/J.BUILDENV.2019.106603>
- Krishnan, N., & Cook, D. (2014). Activity Recognition on Streaming Sensor Data. *Elsevier*, 138–154.
- Laricchia, F. (2022). *Smart speakers - Statistics & Facts*. Statista.
<https://www.statista.com/topics/4748/smart-speakers/>
- Lau, J., Zimmerman, B., & Schaub, F. (2018). Alexa, Are You Listening? Privacy Perceptions, Concerns and Privacy-seeking Behaviors with Smart Speakers. *DL.Acm.Org*, 2(CSCW).
<https://doi.org/10.1145/3274371>
- Lei, X., Tu, G., Liu, A., Li, C., & Xie, T. (2018). The insecurity of home digital voice assistants - Vulnerabilities, attacks and countermeasures. *2018 IEEE Conference on Communications and Network Security, CNS 2018*.
<https://doi.org/10.1109/CNS.2018.8433167>
- Leo Gorski, P., Lo Iacono, L., Wermke, D., Stransky, C., Moeller, S., Acar, Y., & Fahl, S. (2018). *Informal Support Networks: an investigation into Home Data Security Practices*.
www.usenix.org/conference/soups2018/presentation/gorski
- Li, Q., Feng, X., Zhao, L., & Sun, L. (2017). A Framework for Searching Internet-Wide Devices. *IEEE Network*, 31(6), 101–107. <https://doi.org/10.1109/MNET.2017.1700034>
- Liu, P., Ji, S., Fu, L., Lu, K., Zhang, X., Qin, J., Wang, W., & Chen, W. (2023). How IoT Re-using Threatens Your Sensitive Data: Exploring the User-Data Disposal in Used IoT

- Devices. *Proceedings - IEEE Symposium on Security and Privacy, 2023-May*, 3365–3381. <https://doi.org/10.1109/SP46215.2023.10179294>
- Liu, X. (2021). *Ethical Hacking of a Smart Video Doorbell*. School of Electrical Engineering and Computer Science.
- Lu, Y., & Xu, L. (2018). Internet of Things (IoT) cybersecurity research: A review of current research topics. *Ieeexplore.Ieee.Org*.
https://ieeexplore.ieee.org/abstract/document/8462745/?casa_token=C_O5zFS9uS0AAA:YK_-xssWgzA37X_sCp7BNQauFDC9uOhUyCkOLnyPCGTFX1l24u5ejTwwPuYRUs8HU-tD5-Ww
- Ly, P., Lai, H., Hsu, W., & Shih, Y. (2018). Fuzzy AHP analysis of Internet of Things (IoT) in enterprises. *Technological Forecasting and Social Change, 136*, 1–13.
<https://doi.org/10.1016/J.TECHFORE.2018.08.016>
- Madakam, S., & Ramaswamy, R. (2014). Smart homes (conceptual views). *2nd International Symposium on Computational and Business Intelligence . IEEE.*, 63–66.
https://ieeexplore.ieee.org/abstract/document/7119535/?casa_token=USwjL5qPIsAAAA:AA:eehs-Wa6x3slqqpiPzDM_is09hiDphr28jMXeourtYglzOzAQirkVT1U6_ZOAgDUHJd7I3uT
- Malkin, N., Deatrck, J., & Tong, A. (2019). Privacy attitudes of smart speaker users. *Par.Nsf.Gov*. <https://par.nsf.gov/biblio/10109137>
- Mcreynolds, E., Hubbard, S., Lau, T., Saraf, A., Cakmak, M., & Roesner, F. (2017). Toys that Listen: A Study of Parents, Children, and Internet-Connected Toys. *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*.
<https://doi.org/10.1145/3025453>
- Meng, Y., Zhang, W., & Zhu, H. (2018). Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures. *Ieeexplore.Ieee.Org*, 25(6), 53–59.
https://ieeexplore.ieee.org/abstract/document/8600778/?casa_token=cOwVKbZ9-K0AAAAA:ZtA1Yt8Kb3HCMPfPBFOUeF6nSIqhzLBkFoaZJ3ItY4Bz-lgjuptl5RwIBrmVQSjDg8oF97xb
- Michele, B., & Karpow, A. (2014). Demo: Using malicious media files to compromise the security and privacy of smart TVs. *Demo*, 1144–1145.
<https://doi.org/10.1109/CCNC.2014.6940494>
- Mohammad, Z., Qattam, T., & Saleh, K. (2019). Security weaknesses and attacks on the Internet of Things applications. *Ieeexplore.Ieee.Org*, 431–436.

https://ieeexplore.ieee.org/abstract/document/8717411/?casa_token=AlnsZehga7sAAAAA:cZcIzHfvPnQouBdVcpo38d2uDgkXNIgMJiJB2Rk0NHn7fGPeuubFd2ed3SxdF9XpIZ6cl43S

Mukherjee, T., & Nath, A. (2016). Securing Human Computer Interaction, *Current Trends in Technology and Science*.

https://www.researchgate.net/publication/299438178_Securing_Human_Computer_Interaction

Muller, H. (2022). How to Ensure that the Smart Home Doesn't Jeopardize Data Privacy?.

Help Net Security. <https://www.helpnetsecurity.com/2022/05/20/smart-home-data-privacy/>

Munshaw, J. (2022). Vulnerability Spotlight: Vulnerabilities in Anker Eufy Homebase could lead to code execution, authentication bypass. 2022.

<https://blog.talosintelligence.com/vuln-spotlight-anker-eufy-homebase/>

Naeini, E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L., Sadeh, N., Emami-Naeini, P., & Cranor, F. (2017). *Privacy Expectations and Preferences in an {IoT} World*. <https://www.usenix.org/conference/soups2017/technical-sessions/presentation/acar>

Ndaguba, E., Cilliers, J., Ghosh, S., & Herath, S. (2023). Operability of smart spaces in urban environments: a systematic review on enhancing functionality and user experience.

Mdpi.Com E Ndaguba, J Cilliers, S Ghosh, S Herath, ET Mussi *Sensors*, 2023•*mdpi.Com*. <https://www.mdpi.com/1424-8220/23/15/6938>

Nguyen, D., Kobsa, A., & Hayes, G. (2008). An Empirical Investigation of Concerns of Everyday Tracking and Recording Technologies. *University of California, Irvine*.

Nielsen, J. (1994). 10 Usability Heuristics for User Interface Design. *NN/G*.

<https://www.nngroup.com/articles/ten-usability-heuristics/>

Niemietz, M., Somorovsky, J., Mainka, C., & Schwenk, J. (2016). Not so Smart: On Smart TV Apps. *Proceedings - 2015 International Workshop on Secure Internet of Things, SIoT 2015*, 72–81. <https://doi.org/10.1109/SIoT.2015.13>

Norman, D. (2013). *The Design of Everyday Things*. *Mit Press*.

<https://mitpress.mit.edu/9780262525671/the-design-of-everyday-things/>

Ofenwanger, A., Milligan, A., Chang, M., Bullard, J., Yoon, D., & Yoon, W. (2021).

Diagnosing bias in the gender representation of HCI research participants: how it happens and where we are. *DL.Acm.Org*. <https://doi.org/10.1145/3411764.3445383>

- OpenHAB. (2024). *openHAB*. Empowering the Smart Home. Retrieved July 19, 2025, from <https://www.openhab.org/>
- Oser, P., Feger, S., Woźniak, W., Karolus, J., Spagnuolo, D., Gupta, A., Lüders, S., Schmidt, A., & Kargl, F. (2020). SAFER: Development and Evaluation of an IoT Device Risk Assessment Framework in a Multinational Organization. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 4(3). <https://doi.org/10.1145/3414173>
- Ouaddah, A., Mousannif, H., Abou Elkalam, A., & Ait Ouahman, A. (2017). Access control in the Internet of Things: Big challenges and new opportunities. *Computer Networks*, 112, 237–262. <https://doi.org/10.1016/J.COMNET.2016.11.007>
- Oulasvirta, A., Pihlajamaa, A., Perkiö, J., Ray, D., Vähäkangas, T., Hasu, T., Vainio, N., & Myllymäki, P. (2012). Long-term effects of ubiquitous surveillance in the home. *UbiComp'12 - Proceedings of the 2012 ACM Conference on Ubiquitous Computing*, 41–50. <https://doi.org/10.1145/2370216.2370224>
- Padmanaban, S., Sivaraman, P., & Sharmela, C. (2023). Artificial Intelligence-Based Smart Power Systems. In *Wiley*. https://books.google.com/books?hl=en&lr=&id=t6yeEAAQBAJ&oi=fnd&pg=PR15&dq=In+Artificial+Intelligence-Based+Smart+Power+Systems%3B+Wiley&ots=G1e1j5O8ED&sig=TBOE_Kkg4Y2Az8Dq90rG2hkK0mw
- Paetz, A., Dütschke, E., & Fichtner, W. (2012). Smart Homes as a Means to Sustainable Energy Consumption: A Study of Consumer Perceptions. *Journal of Consumer Policy*, 35(1), 23–41. <https://doi.org/10.1007/S10603-011-9177-2/TABLES/1>
- Pandya, S., Ghayvat, H., Kotecha, K., Awais, M., Akbarzadeh, S., Gope, P., Mukhopadhyay, S. C., & Chen, W. (2018). Smart Home Anti-Theft System: A Novel Approach for Near Real-Time Monitoring and Smart Home Security for Wellness Protocol. *Applied System Innovation 2018, Vol. 1, Page 42, 1(4)*, 42. <https://doi.org/10.3390/ASI1040042>
- Perera, C., McCormick, C., Bandara, A. K., Price, B. A., & Nuseibeh, B. (2016). Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. *Proceedings of the 6th International Conference on the Internet of Things*, 83–92. <https://doi.org/10.1145/2991561>
- Popov, A. A., Yakimov, S. P., Satsuk, M. M., & Artyshko, A. A. (2021). Conference Series PAPER • OPEN ACCESS To cite this article: A A Popov et al 2021. *Journal of Physics*, 32004. <https://doi.org/10.1088/1742-6596/2094/3/032004>

- Prathibha, L., & Fatima, K. (2018). Exploring security and authentication issues in Internet of Things. *Ieeexplore.Ieee.Org*, 673–678.
https://ieeexplore.ieee.org/abstract/document/8663111/?casa_token=Lpjf4OFspnQAAA:AA:8pduMEBWi87Ft5cJilA-3Wv3kdZGE1LQTRVR3xJHFiCtk7V4tm8Y6dj3f36a_TYQZqE8OSo
- Rani, S., Chauhan, M., Kataria, A., & Khang, A. (2023). IoT Equipped Intelligent Distributed Framework for Smart Healthcare Systems. *Studies in Big Data*, 137, 97–114.
https://doi.org/10.1007/978-981-99-6034-7_6
- Rodden, T., Fischer, J., Pantidi, N., Bachour, K., & Moran, S. (2013). At Home with Agents: Exploring Attitudes Towards Future Smart Energy Infrastructures. *Conference on Human Factors in Computing Systems - Proceedings*, 1173–1182.
<https://doi.org/10.1145/2470654.2466152>
- Rowey, E. (2025). Platform Agnostic Smart Home Device Manager. *The University of Nottingham*.
- Santoso, F., & Nicholase, C. (2015). Securing IoT for smart home system. *Ieeexplore.Ieee.Org*, 1–2.
https://ieeexplore.ieee.org/abstract/document/7177843/?casa_token=7bnJXXow7cUAAA:AAA:Q5dX7tbExzzzDAXWpwleNG9_srto0gJEkFf9dfJdbAs5gpz_XCD5cVhXpMu6sP_nrCYKnVrC
- Satpathy, L. (2006). Smart Housing: Technology to Aid Aging in Place - New Opportunities and Challenges. *Theses and Dissertations*. <https://scholarsjunction.msstate.edu/td/3967>
- Sauro, J., & Lewis, R. (2016). Quantifying the User Experience: Practical Statistics for User Research, Second Edition. *Quantifying the User Experience: Practical Statistics for User Research, Second Edition*, 1–350.
- ScienceDaily. (2020). Could your vacuum be listening to you? Researchers hacked a robotic vacuum cleaner to record speech and music remotely -- *ScienceDaily*. Science Daily.
<https://www.sciencedaily.com/releases/2020/11/201117210102.htm>
- 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>
- Singapore, S., Madrid, T., Juan, S., Seoul, P., Mexico, M., & Taipei, C. (1995). *Macintosh Human Interface Guidelines* (., Ed.). Apple.
- Smyrlis, M., Somarakis, I., Spanoudakis, G., Hatzivasilis, G., & Ioannidis, S. (2021). CYRA: A Model-Driven CYber Range Assurance Platform. *Applied Sciences* 2021, Vol. 11, Page 5165, 11(11), 5165. <https://doi.org/10.3390/APP11115165>

- Spring, T. (2020). Smart Doorbell Disaster: Many Brands Vulnerable to Attack. *Threatpost*.
<https://threatpost.com/smart-doorbell-vulnerable-to-attack/162527/>
- Sudharsan, B., Corcoran, P., & Ali, M. I. (2022). Smart speaker design and implementation with biometric authentication and advanced voice interaction capability. *CEUR Workshop Proceedings*, 2563, 305–316. <https://arxiv.org/pdf/2207.10811>
- Sweller, J. (1988). Cognitive Load During Problem Solving: Effects on Learning. *Cognitive Science*, 12(2), 257–285. https://doi.org/10.1207/S15516709COG1202_4
- Thielke, S., Harniss, M., Thompson, H., Patel, S., Demiris, G., & Johnson, K. (2011). Maslow’s Hierarchy of Human Needs and the Adoption of Health-Related Technologies for Older Adults. *Ageing International 2011* 37:4, 37(4), 470–488.
<https://doi.org/10.1007/S12126-011-9121-4>
- Tian, Y., Lin, Y., Wang, S., Zhang, N., Wang, X., Ur, B., Guo, X., & Tague, P. (2017). SmartAuth: User-Centered Authorization for the Internet of Things. *26th USENIX Security Symposium, Vancouver, BC, Canada, August 16-18, 2017.*, 361–378.
- Udoh, E., & Alkharashi, A. (2017). Privacy risk awareness and the behavior of smartwatch users: A case study of Indiana University students. *FTC 2016 - Proceedings of Future Technologies Conference*, 926–931. <https://doi.org/10.1109/FTC.2016.7821714>
- Umair, M., Cheema, M., Afzal, B., & Shah, G. (2023). Energy management of smart homes over fog-based IoT architecture. *Sustainable Computing: Informatics and Systems*, 39, 100898. <https://doi.org/10.1016/J.SUSCOM.2023.100898>
- Vardakis, G., Hatzivasilis, G., Koutsaki, E., & Papadakis, N. (2024). Review of Smart-Home Security Using the Internet of Things. *Electronics 2024, Vol. 13, Page 3343*, 13(16), 3343. <https://doi.org/10.3390/ELECTRONICS13163343>
- Velasco, J. (2020). Should You Be Worried About Cameras in Robot Vacuums? *Digital Trends*. <https://www.digitaltrends.com/home/security-cameras-robot-vacuums-feature-privacy-concerns/>
- Wang, D., Jiang, M., Chang, R., Zhou, Y., Hou, B., Luo, X., Wu, L., & Ren, K. (2021). A Measurement Study on the (In)security of End-of-Life (EoL) Embedded Devices. *Arxiv*. <https://arxiv.org/pdf/2105.14298>
- Wang, Q., Hassan, W., & Bates, A. (2018). Fear and Logging in the Internet of Things. *Par.Nsf.Gov*. <https://doi.org/10.14722/ndss.2018.23282>
- Wash, R., & Rader, E. (2015). Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium On Usable Privacy and Security (SOUPS 2015)* (pp. 309-325).

- Wen, G. (2021). Research on Color Design Principles of UI Interface of Mobile Applications Based on Vision. *2021 IEEE International Conference on Advances in Electrical Engineering and Computer Applications, AEECA 2021*, 539–542.
<https://doi.org/10.1109/AEECA52519.2021.9574226>
- Whitten, A., & Tygar, J. (1999). Why Johnny Can't Encrypt: A Usability Evaluation. In .
- Williams, M., Nurse, J., & Creese, S. (2016). The perfect storm: The privacy paradox and the Internet-of-things. *Proceedings - 2016 11th International Conference on Availability, Reliability and Security, ARES 2016*, 644–652. <https://doi.org/10.1109/ARES.2016.25>
- Wilson, C., Hargreaves, T., & Hauxwell-Baldwin, R. (2017). Benefits and risks of smart home technologies. *Energy Policy*, 103, 72–83.
<https://doi.org/10.1016/J.ENPOL.2016.12.047>
- Windl, M., Hiesinger, A., Welsch, R., Schmidt, A., & Feger, S. (2022). SaferHome: Interactive Physical and Digital Smart Home Dashboards for Communicating Privacy Assessments to Owners and Bystanders. *Proceedings of the ACM on Human-Computer Interaction*, 6(ISS), 680–699. <https://doi.org/10.1145/3567739>
- Worthy, P., Matthews, B., & Viller, S. (2016). Trust me: Doubts and concerns living with the internet of things. *DIS 2016 - Proceedings of the 2016 ACM Conference on Designing Interactive Systems: Fuse*, 427–434. <https://doi.org/10.1145/2901790.2901890>
- Yaqoob, I., Ahmed, E., & Hashem, I. (2017). Internet of things architecture: Recent advances, taxonomy, requirements, and open challenges. *Ieeexplore.Ieee.Org*, 24(3), 10–16. https://ieeexplore.ieee.org/abstract/document/7955906/?casa_token=fa-o0Rocb_YAAAAA:9KzR44nXbkDhgWf0zOTfilQTVgIpxwBFZdXeMIYhwqLYSkOxe5j5VyA3Fs06zsLl1QMd-Znu
- Yee, K. (2002). User Interaction Design for Secure Systems. *University of California*.
- Zafar, U., Bayhan, S., & Sanfilippo, A. (2020). Home Energy Management System Concepts, Configurations, and Technologies for the Smart Grid. *IEEE Access*, 8, 119271–119286.
<https://doi.org/10.1109/ACCESS.2020.3005244>
- Zeng, E., Mare, S., Roesner, F., & Allen, P. (2017). End User Security and Privacy Concerns with Smart Homes End User Security & Privacy Concerns with Smart Homes. *USENIX*.
<https://www.usenix.org/conference/soups2017/technical-sessions/presentation/zeng>
- Zeng, E., Roesner, F., & Allen, P. (2019). Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. *USENIX*, 159–176. <https://www.usenix.org/conference/usenixsecurity19/presentation/zeng>

- Zhang, G., Yan, C., Ji, X., Zhang, T., Zhang, T., & Xu, W. (2017). DolphinAttack: Inaudible Voice Commands. *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*. <https://doi.org/10.1145/3133956>
- Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., & Qian, F. (2019). Dangerous skills: Understanding and mitigating security risks of voice-controlled third-party functions on virtual personal assistant systems. *Proceedings - IEEE Symposium on Security and Privacy, 2019-May*, 1381–1396. <https://doi.org/10.1109/SP.2019.00016>
- Zhao, Y., Zhang, X., & Crabtree, J. (2016). Human-Computer Interaction and User Experience in Smart Home Research: A Critical Analysis. *Issues in Information Systems, 17*, 11–19.
- Zheng, S. (2017). User Perceptions of Privacy in Smart Homes. *Princeton University, Computer Science*. <https://dataspace.princeton.edu/handle/88435/dsp01kd17cw477>
- Zhu, P., Hu, J., Li, X., & Zhu, Q. (2023). Using Blockchain Technology to Enhance the Traceability of Original Achievements. *IEEE Transactions on Engineering Management, 70*(5), 1693–1707. <https://doi.org/10.1109/TEM.2021.3066090>

Appendix A: Usability and User-Centred Design Principles

The growing integration of smart home technologies into daily life has changed how individuals interact with connected devices. However, as highlighted in previous sections, smart homes face ongoing security and privacy challenges from complex configurations, unclear permissions, and limited user awareness. Addressing these challenges requires more than technical enforcement; it means designing systems that are understandable, manageable, and responsive to users' needs. This section discusses how principles from Human–Computer Interaction (HCI) and User-Centred Design (UCD) can improve the usability, security, and privacy of smart home systems.

A.1 The Role of HCI in Enhancing Security and Privacy

Human–Computer Interaction examines the design, implementation, and evaluation of interactive computing systems for human use (Khalil et al., 2018). It studies the relationship between people, computers, and the processes through which they interact. With the rapid advancement of digital environments, HCI has evolved beyond efficiency and aesthetics to include *security* and *privacy* as fundamental dimensions of user experience (Zhao et al., 2016).

HCI aims to enhance communication between humans and systems by creating interfaces that are efficient, effective, and secure. However, many security threats arise because connected systems rely heavily on the Internet (Mukherjee and Nath, 2016). Devices remain vulnerable when users do not understand how to navigate or configure their security features. Studies show that many users particularly those less experienced with technology, accept default settings and fail to review permissions (Katsabas and Furnell, 2005). Software developed by technical specialists often assumes a technically skilled audience, resulting in interfaces that are unnecessarily complex for ordinary residents.

Improving HCI design in IoT applications can therefore make it easier for households to apply and maintain appropriate security settings. Striking a balance between usability and protection produces systems that are both *robust* and *reliable*. Understanding how users interact with devices and how they perceive privacy risks is essential. Devices such as cameras and microphones (Krishnan & Cook, 2014) are frequently seen as intrusive, especially in private areas (Naeini et al., 2017). Even non-visual sensors such as thermostats can reveal sensitive behavioural patterns, including occupancy and sleep routines (Hassija et al., 2019). However, traditional HCI research has tended to focus on performance and efficiency metrics rather than on users' privacy expectations. This limitation highlights the need to embed security and ethical awareness into interaction design itself, rather than treating protection as a separate technical function. These challenges highlight why the next section turns to user-centred design frameworks that explicitly prioritise human needs and behaviour.

A.2 Usability and User-Centred Design Concepts

Building on the discussion in the previous section, usability is essential for ensuring that the security and privacy mechanisms in smart home environments are both accessible and easy to understand for users. Although strong security controls are necessary, they become ineffective if users cannot easily locate, interpret, or manage them (Adams and Sasse, 1999; Beauteument et al., 2009). Research consistently indicates that poor usability can lead to unsafe behaviours, such as ignoring alerts, disabling notifications, or keeping insecure default settings. Therefore, achieving usable security requires a balanced design in which protection is integrated into everyday interactions, rather than placed as an additional technical burden.

According to (ISO 9241-210, 2019), usability refers to how well specific users can achieve their goals effectively, efficiently, and satisfactorily in a given context of use. This definition highlights that the users themselves influence usability, the tasks they are performing, and the

conditions they are in. In smart home environments, these contexts can vary significantly, as household members can differ in age, technical skills, and privacy awareness. Designing with this diversity in mind promotes inclusivity. Moreover, it enhances users' sense of control, which in turn helps different groups of smart home users to build trust and encourages the adoption of the system.

Nielsen (1994) developed ten usability heuristics that continue to be among the most widely used frameworks for evaluating interface quality. These heuristics include principles such as visibility of system status, user control and freedom, consistency and standards, and error prevention. Their structured nature provides designers with a validated set of guidelines for identifying usability issues early in the development process. However, several researchers argue that general usability heuristics, such as those commonly used in productivity user interfaces, are not sufficient on their own for security or privacy critical systems. Instead, specialised principles and evaluation methods are necessary for secure interaction design (Kainda et al., 2010; Whitten and Tygar, 1999; Yee, 2002). When applied to systems that handle sensitive data, these principles require contextual adaptation to address user perceptions of trust, control, and risk.

Recognising this limitation, researchers have extended traditional usability approaches through frameworks like Human–Computer Interaction for Security (HCISec), which integrate human factors into the design of secure systems. HCISec focuses on bridging usability and security by ensuring that interfaces communicate protection clearly and transparently, without relying on technical jargon or complex configuration steps. As highlighted in prior studies (Ibrahim et al., 2010; Johnson, 2021), these research emphasises several recurring principles that enhance user understanding and engagement with security features. It stresses the importance of maintaining the visibility of the system and privacy status so that users remain continuously aware of how

their data and devices are being protected. Additionally, clarity and the use of plain language are also considered essential for helping non-technical users analyse and manage security and privacy features confidently, replacing complex terminology with intuitive and straightforward expressions. Moreover, HCISec highlights the value of decision support, where systems provide contextual explanations and feedback that enable users to make informed and confident choices regarding their security and privacy preferences. Collectively, these principles contribute to creating interfaces that foster transparency, trust, and informed user control qualities that are particularly important in smart home environments, where users interact with multiple interconnected devices and need to manage security and privacy settings across diverse contexts.

The UCD framework complements theoretical principles by providing a practical, iterative process for incorporating user needs throughout system development. UCD involves understanding users, their contexts, and their goals; defining user and organisational requirements; producing and refining design solutions; and evaluating outcomes through user testing and feedback. This iterative cycle ensures that usability and functional requirements evolve together through continuous evaluation.

In this research context, the UCD framework serves not only as a theoretical foundation but also as a methodological approach that structured the design of the smart home security and privacy dashboard. The process began by analysing user needs identified in the literature and translating them into design requirements. This was followed by prototype creation, user evaluation, and refinement based on feedback. This approach aligns with ISO 9241-210's (2019) emphasis on iterative design and sustained user involvement.

This research combines Nielsen's heuristics, HCISec principles, and the UCD methodology to create a comprehensive framework for developing a dashboard interface that is usable,

transparent, and trustworthy. By integrating these frameworks, usability is prioritised as a fundamental aspect of secure interaction design rather than an afterthought. As discussed in Chapter 6, these principles are put into practice to enhance user control over privacy and security settings in smart homes, effectively translating theoretical insights into a functional, user-friendly design.

A.3 Usable Security and Privacy in Smart Homes

In the context of usable security and privacy, researchers point out that strong technical measures alone are not enough; users also need to understand and manage these systems. Furnell et al., 2006) explain that many systems still expect users to have advanced technical skills, which can discourage people from engaging and reduce overall protection. Similarly, (Furnell et al., 2007) show that when a system is complex to use, people may be unable to complete even simple security tasks, thereby making technical protections less effective. Building on this, (Furnell & Clarke, 2012) highlight that improving the usability and accessibility of security interfaces enhances users' willingness and ability to follow security practices, ultimately supporting more effective protection.

Real-world cases such as unauthorised access to home cameras or the misuse of voice-assistant recordings show that poor interface feedback can erode users' trust. These situations make it clear that improving technology alone is not enough for security and privacy. Users need information that is clear, relevant, and easy to act on. With this in mind, the dashboard developed in this project uses usability and user-centred design to help smart home residents stay security and privacy in their daily lives. Instead of hiding controls in technical menus, the interface gives clear, context-based feedback so users can see, change, and track how their devices behave in ways that make sense to them.

With this approach, the dashboard lets users take an active role in protecting their information, rather than relying only on built-in protections. This shift aligns with a broader move toward integrating security into daily routines, not treating it as something separate. The system aims to make security and privacy clear and easy to understand, so users feel confident and in control.

Appendix B: Evaluating Provision of Information

This appendix provides an extended analysis of the results presented in Chapter 3, Section 1. It examines the availability of privacy-related information on the official websites of the selected smart devices. The findings offer a deeper understanding of how each company presents and communicates its privacy policies to users.

1.Evaluation Questions

In this research, we evaluated what users could find out about the devices from online sources and the extent to which users are presented with this information as part of the standard user guidance, etc. The first three questions motivate why/whether users need to be told something about security and privacy. The last two questions then determine the extent to which they may then find related information, in terms of whether these aspects are headlined in relevant places such as users' manuals and privacy policy pages.

1. What type of information does each device collect, including personal information, home location, and body-related information?

- **Personal Information**

This question specifies the type of personal information gathered by each device, as mentioned on the product's privacy policy webpage. Personal information may include name, date of birth, and contact details.

- **Body-related information**

This represents users' bodies and distinguishes personal characteristics, for instance, heart rates, fingerprints, and voices. Many smart home devices also gather sensitive user data such as sleep patterns and stress levels.

- **Home location**

This section was inducted in this review because several smart home devices provide the location of users' homes, so we will evaluate whether the selected device will provide the location of the user's home.

2. Do devices share users' information with a third party, and if so, for what purpose?

Smart home device companies may share their users' data with third- parties for several reasons and outcomes, such as advertisements or to improve their services, but this sharing is considered a violation of users' privacy. Therefore, this question is to elucidate whether the companies share their users' data with a third party.

3. Does the device and its application have the potential to invade the user's privacy?

This assessment examines whether smart home devices have the potential to invade the user's privacy. Moreover, it reviews the device site as well as the Apple Store or Google Play Store. This is vital because examining permission asked of each application may involve specifying whether the device and its applications utilized a camera, microphone, or location tracking.

4. How much privacy-related information is presented on the E manual webpage?

This question considers the company's manual page of the smart home device to note if any information useful to users has been mentioned or clarified to protect their data.

5. How easy it was to find the information in the privacy policy pages?

This review has provided this question to consider how easy it is to find clear and easy-to-understand information about the privacy policies of smart home devices. Multiple companies take the form of long privacy policies, which usually include legal jargon and are difficult for users to read (Fabian et al., 2017). Moreover, privacy policies are usually absent (Cate, 2010), difficult to find and challenging to understand (Kelley et al., 2012), making it cumbersome, if not inconceivable, for users to use and control their data effectively.

Robotic Vacuums

This assessment examined devices from four companies: Eufy, Ecovacs Deebot, Wyze, and iRobot.

1. Eufy Robotic Vacuum

Eufy vacuum does not have a built-in camera; it maps and navigates houses utilizing nine sensors. Generally, Sensors are more secure than the vacuum that comes with the camera ([Velasco,2020](#)).

- **What type of information does the Eufy Robotic Vacuum collect?**

- Name, Email.

- **Do devices share users' information with a third party, and if so, for what purpose?**

This vacuumed mentioned privacy policy and collecting user data in their website.

- This policy does not involve information gathered by third-party sites.
- They mentioned they have no control over no liability or responsibility for any third-party use, collection, retention, and disclosure of user data and that use, collection, retention, and disclosure are not subject to their policy.
- The user can access and correct some of his personal information
- Eufy may process personal user data on servers not in his country.
- Eufy uses the data collected via cookies, device identifiers, log files, and location information for many purposes, such as monitoring aggregate metrics such as usage, the real number of visitors, and demographic designs on their services.

- **How usable for users to control their data?**

- Eufy Vacuum supplies users with the capability to check, control or delete their data.

- **How much privacy-related information is presented on E manual webpage?**

- Not presented

- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	No	Yes
Application	No	No	Yes

- **Is it easy for users to read the privacy policy?**

- No, it's around 1500 words

- **Does Eufy Vacuum have a privacy policy web page?**

- [Privacy policy web page](#)

2. Ecovacs Deebot Vacuum

Ecovacs Deebot vacuums have a built-in camera, room-mapping sensors, microphones, and LiDAR lasers. Cameras on robot vacuums increase noticeable security and privacy concerns such as getting hacked and spying on the user's own home ([Velasco,2020](#)).

- **What type of information does the Ecovacs Deebot Vacuum collect?**
 - The username, gender, age, phone number.
 - location if the user gives the permission.
- **Do devices share users' information with a third party, and if so, for what purpose?**
 - Yes
 - They mentioned they could reveal users' data to third-party for aims such as marketing.
- **How usable for users to control their data?**
 - Users can update their private data straight from their account settings.
 - Ecovac mentioned that users have the right to demand to delete their personal information in certain circumstances.
- **How much privacy-related information is presented on E manual webpage?**
 - Not presented
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Cannot determine
Application	No	No	Yes
- **Is it easy for users to read the privacy policy?**
 - No, it's too long around 5500 words
- **Does Ecovacs Deebot Vacuum have a privacy policy web page?**
 - Yes
 - [Privacy Policy web page](#)
 - [E manual Page](#)
 - <https://www.ecovacs.com/uk/deebot-robotic-vacuum-cleaner/t8-aivi>
 - <https://www.ecovacs.com/uk/support/faqs>

3. Wyze Vacuum

Wyze vacuum comes with a lidar scanner and a laser on the top of the vacuum to scan and map the house. Wyze vacuum doesn't provide a built-in camera, and these are typically securer than other vacuums that comes with cameras ([Velasco,2020](#)). Nevertheless, researchers discovered that LIDAR vacuums could be hacked, and then the hacker spied on voice conversations in the smart home even without a microphone ([ScienceDaily,2020](#)).

- **What type of information does the Wyze Vacuum collect?**
 - The username, gender, birthday.
- **Do devices share users' information with a third party?**
 - Yes
- **How usable for users to control their data?**
- Users can delete their account information by contacting Wyze support to request to delete their account.
- **How much privacy-related information is presented on E manual webpage?**
 - Not presented
 - [User Manuals](#)

6. Do the device and its application have the potential to invade the user's privacy?

	Camera	Microphone	Track Location
Device	No	No	No
Application	No	Yes	Yes

- **Is it easy for users to read the privacy policy?**
 - No, it's around 1900 words
- **Does Wyze Vacuum have a privacy policy web page?**
 - Yes
 - [Wyze Privacy Statement](#)
 - <https://support.wyze.com/hc/en-us/sections/360006246811-General-FAQ>
 - <https://www.wyze.com/products/wyze-robot-vacuum>

4. iRobot Vacuum

In the last few years, iRobot company got its reputation affected because it appears they were mapping users' houses using their robot vacuums with probability plans to sell the user data (Astor 2017).

- **What type of information does the iRobot Vacuum collect?**
 - The username, phone number, email, and address.
- **Do iRobot Vacuum share user's information with a third party?**
 - Yes
 - They mentioned they could reveal users' data to third-party to develop tools and applications that interact with their Service.
- **How usable for users to control their data?**
 - Users can prevent mapping data from being transmitted to the iRobot company.
- **How much privacy-related information is presented on E manual webpage?**
 - Not presented
 - [Manual Page](#)

7. Do the device and its application have the potential to invade the user's privacy?

	Camera	Microphone	Track Location
Device	Yes	No	No
Application	No	No	Yes

- **Is it easy for users to read the privacy policy?**
 - No, it's too long around 9100 words
- **Does iRobot Vacuum have a privacy policy web page?**
 - Yes
 - [Privacy Policy web page](#)
 - https://www.irobot.co.uk/en_GB/irobot-roomba-s9plus-braava-m6-h1-handheld/EMEA_S9plus-M6B-H1.html

Smart Speakers

This assessment evaluates Google Nest, Amazon Echo Dot, and Apple HomePod

1. Google Nest Smart Speaker

The Google Nest Smart Speaker comes with features called "Smart Sound" to adjust the volume to be ideal for the size of the room. Moreover, it is equipped with three built-in microphones so that it can listen to all user commands

- **What type of information does the Google Nest collect?**
 - Personal data, such as name, email, phone number, and address.
 - Audio recordings.
- **Do Google Nest Speaker share user's information with a third party?**

No, however, it shares voice recordings with partners working on analysing the audio
- **How usable for users to control their data?**
 - Google delivers diverse privacy controls, available through Google Privacy setting. Moreover, many defined methods are available to users to delete personal information, such as removing a complete Google Account or deleting voice recording using Nest Hup application.
 - The timer can be set up automatically for three or eighteen months to delete the recording voice.
- **How much privacy-related information is presented on E manual webpage?**
 - They mentioned how to turn off the microphone.
 - [E-manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	Yes
Application	Yes	Yes	Yes
- **Is it easy for users to read the privacy policy?**
 - It's provided with many pictures; however, it's too long and difficult to find.
- **Does Google Nest Speaker have a privacy policy web page?**
 - [Nest Privacy Web Page](#)
 - https://store.google.com/product/nest_wifi?hl=en-GB
 - <https://support.google.com/googlenest/answer/7029281?hl=en-GB>

2. Amazon Echo Dot Speaker

Amazon smart speakers that are Alexa-powered have become the most popular. Amazon smart speakers can do various tasks such as making phone calls, turning on the lights, playing music, reading the news, reporting the weather, and purchasing online.

- **What type of information does the Amazon Echo Speaker Dot collect?**

Many types of information Amazon smart speaker's device collects, such as

- Personal data, such as name, email and phone number, and postal address.
- A third-party payment processor gathers and holds payment data, such as name, card, and security code.
- The geolocation of the user's smartphone device if the user has permission to collect this information.
- Voice recordings.

- **Do Amazon Echo Dot Speaker share user's information with a third party?**

- They mentioned they could reveal users' data to various third parties for aims such as marketing and improving the voice functionally.

- **How usable for users to control their data?**

- Users can delete their voice recordings from amazon smart Speakers anytime by accessing their account. Moreover, they can turn off the microphone to prevent Alexa from listening. However, it costs losing some features.

- **How much privacy-related information is presented on E manual webpage?**

- No
- [E-manual Page](#)

- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	Yes
Application	Yes	Yes	Yes

- **Is it easy for users to read the privacy policy?**

- No, more than 3400 words.

- **Does Amazon Echo Dot Speaker have a privacy policy web page?**

- Yes
- [Amazon.com Privacy Notice](#)
- [Alexa Device FAQs](#)
- [Questions About Alexa Privacy](#)

3. Apple HomePod Speaker

The Apple HomePod speaker is provided with four built-in smart microphones in five colours that listen to all "Hey Siri" requests by the user.

- **What type of information does the Apple HomePod Speaker collect?**
 - Personal data, such as name, email, phone number, and address.
 - Audio recordings.
- **Do Apple HomePod Speaker share user's information with a third party?**
 - No
 - Apple states it will not transfer its customer information data to any third parties for marketing or commercial aims.
- **How usable for users to control their data?**
 - Users can delete their voice recordings from Apple HomePod Speakers anytime. Moreover, they can turn off the microphone to prevent Siri from listening. Furthermore, they can turn off the location services and avoid track locations.
- **How much privacy-related information is presented on E manual webpage?**
 - Yes
 - [E-manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	Yes
Application	NA	Yes	Yes
- **Is it easy for users to read the privacy policy?**
 - It's provided with many pictures; however, it's too long
- **Does Apple HomePod Speaker have a privacy policy web page?**
 - Yes
 - [Apple Privacy Policy](#)
 - [Privacy Statement](#)
 - <https://www.apple.com/uk/homepod-mini/>
 - <https://support.apple.com/en-gb/homepod>

1. Smart Displays

This assessment evaluates Google Nest Hub, Amazon Echo Show, and Facebook Portal.

1. Google Nest Hub Smart Display

This smart display permits the user to watch YouTube, view their photos, listen to podcasts, and maintain the lights with their voice, but it does not have a video camera that monitors the users. Google added features that utilize motion and sound to monitor users' sleep.

- **What type of information does the Google Nest Hub Smart Display collect?**
 - Personal data, such as name, email and phone number, and address.
 - Audio recordings.
- **Does Google Nest Hub Smart Display share user's information with a third party?**
 - No
- **How usable for users to control their data?**
 - Google delivers diverse privacy controls, available through Google Privacy setting. Moreover, many defined methods are available to users to delete personal information, such as removing a complete Google Account or removing information from the Nest Hub application.
 - An automatic timer can be set up for three months or eighteen months. Details of retention are also included on the privacy policy web page.
- **How much privacy-related information is presented on E manual webpage?**
 - Not Presented

- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	Yes
Application	No	Yes	Yes

- **Is it easy for users to read and understand the privacy policy?**
 - It's provided with many pictures, however it's too long
- **Does Google Nest Hub have a privacy policy web page?**
 - Yes
 - [Nest Privacy Web Page](#)

2. Amazon Echo Show Smart Display

The Amazon Echo Show allows users to use basic voice commands and connect to smartphones to control different smart home devices. The device-specific features are web browsing, photo/video recording, video calling, streaming video content, and using Alexa for Echo Show Smart Display.

- **What type of information does the Amazon Echo Show collect?**

Many types of information Amazon smart speaker's device collects, such as

- Personal data, such as name, email and phone number, and postal address.
 - A third-party payment processor gathers and holds payment data, such as name, card, and security code.
 - The geolocation of the user's smartphone device if the user has permission to collect this information.
 - Voice recordings.
 - Contacts which is optional to make calls.
- **Do Amazon Echo Show share user's information with a third party?**
 - They mentioned they could reveal users' data to various third parties for aims such as marketing and improving the voice functionally.
 - **How usable for users to control their data?**
 - Users can delete their voice recordings from Amazon Echo Show anytime by accessing their account. Moreover, the user can configure auto-deletion to delete recordings in three or eighteen months. Furthermore, the user can choose not to save any recordings, but this comes at the expense of some features.
 - **How much privacy-related information is presented on E manual webpage?**
 - **Not Presented**
 - [Amazon Echo Show E manual Page](#)
 - **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	No
Application	Yes	Yes	Yes
 - **Is it easy for users to read the privacy policy?**
 - No, more than 3400 words.
 - **Does Amazon Echo Show have a privacy policy web page?**
 - [Amazon.com Privacy Notice](#)
 - [Alexa Device FAQs](#)
 - [Questions About Alexa Privacy](#)

3. Facebook Portal Smart Display

The Facebook Portal Smart Display is a video calling hub. The Facebook Portal's primary function is to make video calls to family and friends using Facebook Messenger's built-in video calling service, but it also includes Alexa smart assistant functionality. Users can activate the smart display by saying "Hey Portal," followed by the command they want it to execute.

- **What type of information does the Facebook Portal collect?**
 - Personal data, such as name and email.
 - Video Recording.
 - Social Contact: Facebook Portal requires signing in with WhatsApp or Facebook account.
- **Do Facebook Portal share user's information with a third party?**
 - Facebook Portal shares data with various third parties, including advertisers, analytics services, and measurement partners.
- **How usable for users to control their data?**
 - The user can turn off the camera and the built-in microphone on the smart display by clicking the button on the device. A red light near the lens indicates that the microphone and camera are off.
- **How much privacy-related information is presented on E manual webpage?**
 - The mentioned how to turn off the camera and the microphone.
 - [Facebook Portal E manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	Yes
Application	Yes	Yes	Yes
- **Is it easy for users to read the privacy policy?**
 - It's provided with many pictures; however, it's too long
- **Does Facebook Portal have a privacy policy web page?**
 - [Meta Privacy Centre](#)
 - [Facebook Portal Privacy](#)
 - <https://www.meta.com/gb/portal/products/>

Smart Cameras

This assessment involves Amazon Ring Security Cameras, Google Nest Cameras, and Eufy Security Cameras

1. Amazon Ring Security Cameras

Amazon Ring's outdoor and indoor security cameras contain standard HD video, motion activation, and a night vision to put the user home under observation all day. Monitor video via the ring application on user smartphone or Amazon Echo Show home hub. Request Alexa to represent user what is happening in the user's backyard.

- **What type of information does the Amazon Ring Security Cameras collect?**
 - Many types of information this device collect such as
 - Personal data, such as name, email and phone number, and postal address.
 - Account data, such as an online password.
 - The geolocation of user smartphone device if user permission to the collection of this information.
 - Video and audio recordings of the body movement.
- **Does Amazon Ring Security Cameras share user's information with a third party?**
 - Yes, they mentioned they could reveal users' data to many third parties for aims such as marketing. However, in 2020 [EFF](#) showed that the Ring application transfers information with numerous different trackers did not say in their policy.
- **How usable for users to control their data?**
 - Users can delete their voice recordings from amazon smart Speakers anytime by accessing their account. Moreover, they can turn off the microphone to prevent Alexa from listening. However, it costs losing some features.
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Yes	Yes	Yes

- **Is it easy for users to read the privacy policy?**
 - No
- **Does Amazon Ring Security Cameras have a privacy policy web page?**
 - Yes
 - [Ring Privacy Notice](#) web page.
 - [Ring Privacy Pillars web page](#)

2. Google Nest Cameras

Google's outdoor and indoor Nest Cams provide 24/7 recording, HD video recording, microphones for noticing different noises, motion detection alerts, and intelligent alerts that distinguish between a person and a thing.

- **What type of information does the Google Nest Cam collect?**
 - Personal data, such as name, email, phone number, and address.
 - Face IQ.
 - Voice recording.
- **Do Google Nest Cam share user's information with a third party?**
 - Transcripts of user voice interactions may be used to personalize the advertisement, but home sensor reading, and voice recordings will not. According to Google, user personal information is never sold to third parties, and Google claims that video footage, audio recordings, and house environment sensor readings are preserved particularly from advertising and will not be used for ad personalization.
- **How usable for users to control their data?**
 - Google delivers diverse privacy controls, available through Google Privacy setting. Moreover, many defined methods are available to users to delete personal information, such as removing a complete Google Account or deleting voice recording using Nest Hub application.
 - Users can delete their historical data and should therefore delete their data regularly.
 - The timer can be set up automatically for 3 or 18 months to delete their data
- **How much privacy-related information is presented on E manual webpage?**
 - Not Presented
 - [Manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Yes	Yes	Yes
- **Is it easy for users to read the privacy policy?**
 - It's provided with many pictures; however, it's too long, complicated, and difficult to find.
- **Does Google Nest Cam have a privacy policy web page?**
 - [Nest Privacy Page](#).

3. Eufy Security Cameras

Eufy manufactures both outdoor and indoor security cameras to monitor users house and neighbourhood. They include the expected features such as live streaming, HD video, and night vision. Users can save his data on a microSD card and then live stream it to the user's phone via the Eufy application, which uses high-end encryption to secure the users' video.

- **What type of information does the Eufy Security Cams collect?**
 - Personal data, such as name, email.
 - If the user decides to allow biometric and imaging features, the **Eufy Security Cams will collect** Face images.
- **Do Eufy Security Cams share user's information with a third party?**
 - Yes
 - Sharing is restricted to information required by services. Users who utilize third-party services will be subject to third-party services terms and privacy policies.
- **How usable for users to control their data?**
 - Eufy Security Cams supplies users with the capability to check, control or delete their data.
- **How much privacy-related information is presented on E manual webpage?**
 - **Not Presented**
 - [Eufy Cams E manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Yes	Yes	Yes
- **Is it easy for users to read the privacy policy?**
 - No, more than 6800 words.
- **Does Eufy Security Cams have a privacy policy web page?**
 - Yes
 - [Efuy Privacy Page](#)

Smart Thermostats

This review examined the Netatmo smart thermostat and the Amazon smart thermostat.

1. Netatmo Smart Thermostat

This smart thermostat requires the user to determine when needs to get up, sleep, go out, and go home to operate at the right time.

- **What type of information does the Netatmo Smart Thermostat collect?**
 - Personal data, such as name and contact details.
 - Location using the application, which is an optional choice.
- **Does Netatmo Smart Thermostat share user's information with a third party?**
 - No
 - Their privacy policy seems to apply the strictest privacy regulations to all their data collection.
 - They are extremely careful about sharing the user's information.
- **How usable for users to control their data?**
 - The data is kept for the contract duration, which ends with sending a request to their e-mail asking to delete the account information.
 - After three years of inactivity, the company will delete the user account.
- **How much privacy-related information is presented on E manual webpage?**
 - Not Presented
 - [E manual webpage](#)

- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	No	No
Application	Yes	Yes	No

- **Is it easy for users to read the privacy policy?**
 - No
- **Does Netatmo Smart Thermostat have a privacy policy web page?**
 - Yes
 - [Privacy Policy Webpage](#)
 - [Netatmo Smart Thermostat FAQs](#)

2. Smart Thermostat by Amazon

Amazon collaborated with Honeywell to develop its smart thermostat. Moreover, when the user pairs a smart thermostat with another Alexa-controlled device in his house, Alexa will control almost everything. The user will need an Echo Dot speaker or something like use voice control Because the thermostat lacks a microphone and speaker.

- **What type of information does the Amazon Smart Thermostat collect?**
 - Personal data, such as name, email and phone number, and postal address.
 - Voice Recording
- **Do Amazon Smart Thermostat share user's information with a third party?**
 - They integrate the voice information with third-party data to train the speech recognition of Alexa and respond to user queries. The user has the option not to save any audio recordings, but this will cost losing some features.
- **How usable for users to control their data?**
 - Users can delete their voice recordings from amazon smart thermostat anytime by accessing their account.
 - The timer can be set up automatically for three or eighteen months to delete the recording voice.
- **How much privacy-related information is presented on E manual webpage?**
 - Not Presented
 - [Amazon Smart Thermostat Support](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	No	Yes	Yes
Application	Yes	Yes	Yes
- **Is it easy for users to read the privacy policy?**
 - No, more than 3500 words.
- **Does Amazon Smart Thermostat have a privacy policy web page?**
 - Just for Amazon
 - [Amazon Privacy Notice](#)
 - <https://www.amazon.com/Amazon-Smart-Thermostat/dp/B08J4C8871>

Smart Video Doorbells

This assessment examined Netatmo, Eufy and Ring smart video doorbells.

1. Smart Video Doorbells by Netatmo

The Smart Netatmo Video Doorbells alert the user if a person is approaching his house's door and allows the user to communicate with the person outside his house using the microphone. Moreover, Netatmo does not save videos to the Cloud storage, but the videos are saved locally to an encrypted MicroSD card, a great feature for privacy and security.

- **What type of information does the Netatmo Smart Video Doorbell collect?**
 - Personal data, such as name and contact details.
 - Location services using the application, which is an optional choice.
- **Do the Netatmo Smart Video Doorbell share user's information with a third party?**
 - No
 - Their privacy policy seems to apply the strictest privacy regulations to all their data collection.
 - They are extremely careful about sharing the user's information.
- **How usable for users to control their data?**
 - The data is kept for the contract duration, which ends with sending a request to their e-mail asking to delete the account information.
 - After three years of inactivity, the company will delete the user account.
- **How much privacy-related information is presented on E manual webpage?**
 - **Not Presented.**
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Cannot determine	Cannot determine	Yes

- **Is it easy for users to read the privacy policy?**
 - No, more than 18500 words.
- **Does the Netatmo Smart Video Doorbell have a privacy policy web page?**
 - Yes
 - [Privacy Policy Webpage](#)
 - [Netatmo Video Doorbell FAQ](#)

2. Eufy Smart Video Doorbell

Eufy smart video doorbell does not provide cloud repository subscriptions; instead, they only provide local storage, a great feature for privacy and security for users who want a video from their smart doorbell but do not want their videos kept in the cloud where hackers could access it. Eufy also allows users to access their locally stored footage from anywhere and protects it during transmission with strong encryption. However, these video doorbells perform the same functions as the others: motion detection, HD video, two-way audio, and compatibility with Google Assistant and Alexa.

- **What type of information does Eufy Smart Video Doorbell collect?**
 - Personal data, such as name, email.
 - If the user decides to allow biometric and imaging features, the **Eufy Security Cams will collect Face images.**
- **Do does Eufy Video Doorbell share user's information with a third party?**
 - Yes
 - Sharing is restricted to information required by services. Users who utilize third-party services will be subject to third-party services terms and privacy policies.
- **How usable for users to control their data?**
 - Eufy Security Cams supplies users with the capability to check, control or delete their data.
- **How much privacy-related information is presented on E manual webpage?**
 - **Not Presented**
 - [Eufy Video Doorbell manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Yes	Yes	Yes

- **Is it easy for users to read the privacy policy?**
 - No, more than 6800 words.
- **Does Eufy Smart Video Doorbell have a privacy policy web page?**
 - Yes
 - [Efuy Privacy Page](#)
 - <https://uk.eufy.com/collections/video-doorbell>

3. Ring Video Doorbell by Amazon

Ring video doorbells can capture video clips, detect movements, and talk in two directions. Moreover, they let the users identify who is standing at the door through their phone or smart display.

- **What type of information does the Ring Video Doorbell collect?**
 - Many types of information this device collect such as
 - Personal data, such as name, email and phone number, and postal address.
 - Video and audio recordings of the body movement.
- **Do Ring Video Doorbell share users' information with a third party?**
 - Yes, they mentioned they could reveal users' data to many third parties for aims such as marketing.
- **How usable for users to control their data?**
 - Users can delete their recording video from Ring Protect anytime by accessing their accounts.
- **How much privacy-related information is presented on E manual webpage?**
 - **Not Presented**
 - [Manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Yes	Yes	Yes

- **Is it easy for users to read the privacy policy?**
 - No
- **Does Ring Video Doorbell have a privacy policy web page?**
 - Yes
 - [Privacy Notice](#)
 - [Privacy Statement Webpage](#)
 - [FAQ Page](#)
 - <https://en-uk.ring.com/pages/doorbells>

Smart TVs

This review investigated the Sony and Samsung Smart TV

1. Sony Smart TV

- **What type of information does the Sony Smart TV collect?**
 - Sony Europe may collect data concerning the user in different forms, such as when users upload documents or text fields.
 - Some of Sony's services demand users to make an account, and they may ask users to provide many details about the users, such as name, date of birth, contact details, and interests.
 - When users purchase, register Sony TV, Sony may ask the user to provide details such as their contact details and payment information
 - When users use online services, Sony may obtain content that users decide to upload, such as product reviews, comments, photos, and details of user preferences.
- Information that Sony collect from different sources
 - If users use Sony's social network apps or use one of Sony's services that permit interaction with social networks, Sony may receive information connecting to the user accounts, for example If users log in to one of Sony's services utilizing their social network account, Sony obtains primary details from the user profile. The primary details rely on the users' privacy settings in his account. Nevertheless, they may contain user social network name, ID, profile picture, gender, and locale. Sony may also receive additional information from the user profile.
- **Do Sony Smart TV share users' information with a third party?**
 - Yes
- **How usable for users to control their data?**
 - Sony Smart TV provide privacy setting controls.
 - User can approve or disagree on the Sony TV privacy choices.
 - Failure to agree to the policy will negatively impact the user experience, disabling multiple Sony smart TV features, such as an automatic update.
- **How much privacy-related information is presented on E manual webpage?**
 - **Not Presented**
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Not Available	Not Available	Not Available
- **Is it easy for users to read the privacy policy?**
 - No

- **Does Sony Smart TV have a privacy policy web page?**
 - Yes
 - [Privacy Policy Web Page](#)
 - [Privacy policy Setting Option](#)
 - <https://www.sony.co.uk/electronics/support/televisions-projectors>
 - <https://www.sony.co.uk/electronics/support/articles/00166669>

2. Samsung Smart TV

- **What type of information does the Samsung Smart TV collect?**
 - Personal data, such as name and contact details.
 - contact details and payment information
 - Social Contact.
- **Do Sony Samsung Smart TV share users' information with a third party?**
 - Yes
 - The user's personal information may be shared with Samsung's subsidiaries and service providers. Moreover, it may share geolocation and personal information, such as personal identifiers, browsing history, and products purchased for business purposes.
- **How usable for users to control their data?**
 - User can approve or disagree on the Samsung privacy choices.
 - Samsung unable users to reject their agreements during setup, therefore users can't utilize the TV's streaming operations.
- **How much privacy-related information is presented on E manual webpage?**
 - They just mentioned to agree the privacy setting without explaining.
 - [Samsung Manual Page](#)
- **Do the device and its application have the potential to invade the user's privacy?**

	Camera	Microphone	Track Location
Device	Yes	Yes	Yes
Application	Not Available	Not Available	Not Available

- **Is it easy for users to read the privacy policy?**
 - No
 - Samsung TVs' privacy policy consists of the largest number of words compared to other smart TV, with more than 8,000 words. This makes it difficult for users to read all the privacy policy web pages, and therefore they accept them immediately.

- **Does Samsung Smart TV have a privacy policy web page?**
 - Yes
 - [Privacy Policy Web Page](#)
 - <https://www.samsung.com/uk/sustainability/security-and-privacy/>
 - https://www.samsung.com/uk/tvs/oled-tv/s95b-65-inch-oled-4k-smart-tv-ge65s95batxxu/?cid=uk_paid_ppc_google_4126821848_FF~Eval:Brand_TV_OLED_KS~BA_BS~VD_PR~CTV_SB~VDMUL_OB~SALES_FS~LHQ_AI~N_MT~EXA_CA~KEW_paid-cdm-ModernSearch_OLED+-+DSA&&msclkid=ce443b0844fc127d6d3b587a808e2af4&utm_source=bing&utm_medium=cpc&utm_campaign=FF~Eval%3ABrand_TV_OLED_KS~BA_BS~VD_PR~CTV_SB~VDMUL_OB~SALES_FS~LHQ_AI~N_MT~EXA_CA~KEW_paid-cdm-ModernSearch&utm_term=https%3A%2F%2Fwww.samsung.com%2Fuk%2Ftvs%2Foled-tv%2Fs95b-65-inch-oled-4k-smart-tv-ge65s95batxxu&utm_content=OLED%20-%20DSA&gclid=ce443b0844fc127d6d3b587a808e2af4&gclsrc=3p.ds

Appendix C: Evaluating the Accessibility of the Security and Privacy Features

This appendix provides an extended explanation of the results presented in Chapter 3, Section 2. It includes detailed step-by-step illustrations for the evaluated examples, showing how users can interact with privacy and security controls on different smart speaker platforms. These details complement the analysis by demonstrating the usability and accessibility of key privacy functions.

1. Mute the Microphone

The microphone on the smart speaker remains on to listen for the trigger phrases and words that permit users to utilize the device. This indicates that smart speakers are consistently listening to the users.

▪ Amazon Echo Speaker

Select the microphone button on the speaker device.

Press and hold the button until it converts to red.

Press and hold the button until it converts to blue to turn on the microphone again.

▪ Google Nest Speaker

Muting the microphone prevents the WIFI of the speaker from hearing or answering the users' queries. However, the users can utilize it as a speaker through Bluetooth or cast. Therefore, turn off the Google Nest microphone by switching the button on the back of the Nest WIFI. If the button is converted to orange, the microphone is off.

▪ Apple HomePod Speaker

The HomePod device does not have a physical button to mute the microphone. Therefore, the user has two choices to disable it:

1. The first is by speaking to Siri: "Hey Siri, stop listening."

To reactivate the feature, the user can press and hold the touch surface, as shown in figure C.1, then say, "Turn on Hey Siri" or "Start listening."

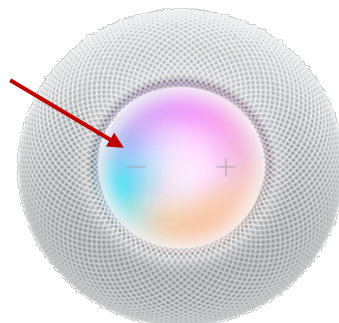


Figure C.1: Touch Surface in Apple HomePod

2. The second option is done through the application, as shown in the Figure C.2.

To evaluate the usability of muting the microphone in HomePod, the first choice to mute the microphone in Apple HomePod Speaker. Moreover, the second choice of using the application (Figure C.2)

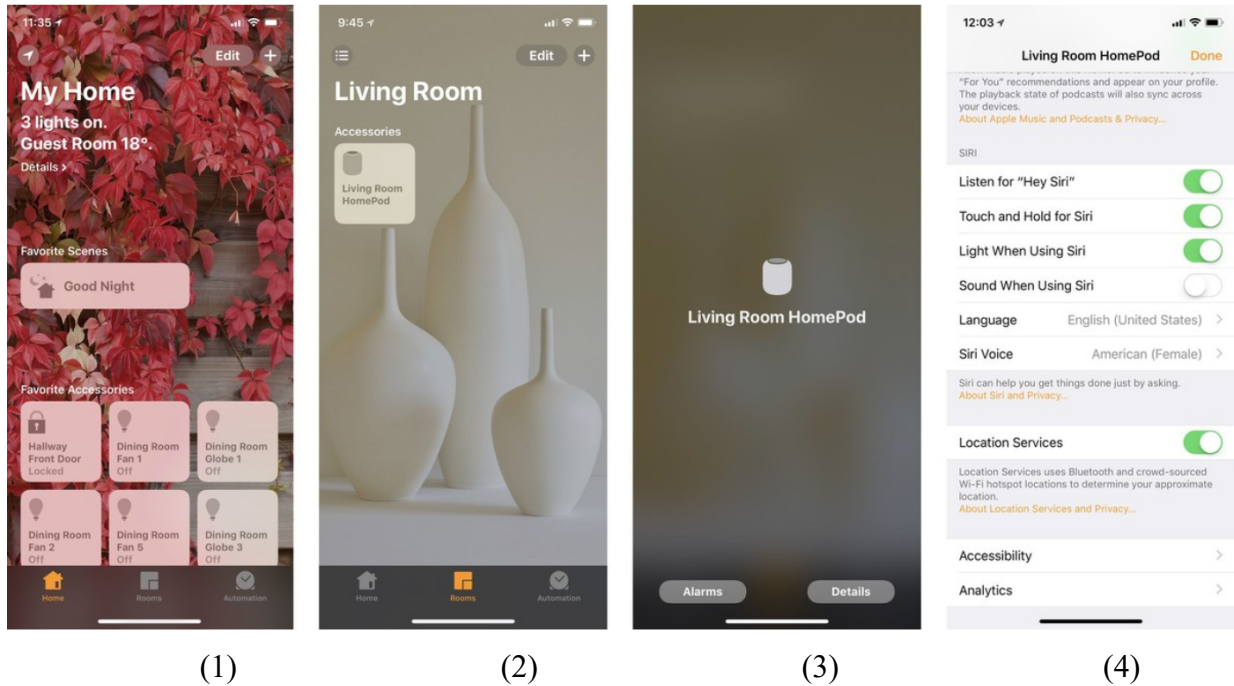


Figure C.2: Mute the Microphone of the Apple HomePod speaker

2. Delete a Specific Recording

▪ Amazon Echo Dot Speaker

The user can delete a particular recording by selecting the recording box that the user wants to delete. Then the user can choose Delete Recordings. However, as shown in Figure C.3, if the user wants to delete one voice recording, it requires to perform at least nine steps, and this indicates that deleting one recording is not easy, and from it, we conclude that the user may not easily know how to do these steps because various options which can be cumbersome. Moreover, if the user has 100 records and wants to delete 50 sensitive recordings, the user must select one record, select deleting the record, and press confirms. Therefore, the user must do these steps 50 times to delete 50 sensitive records.

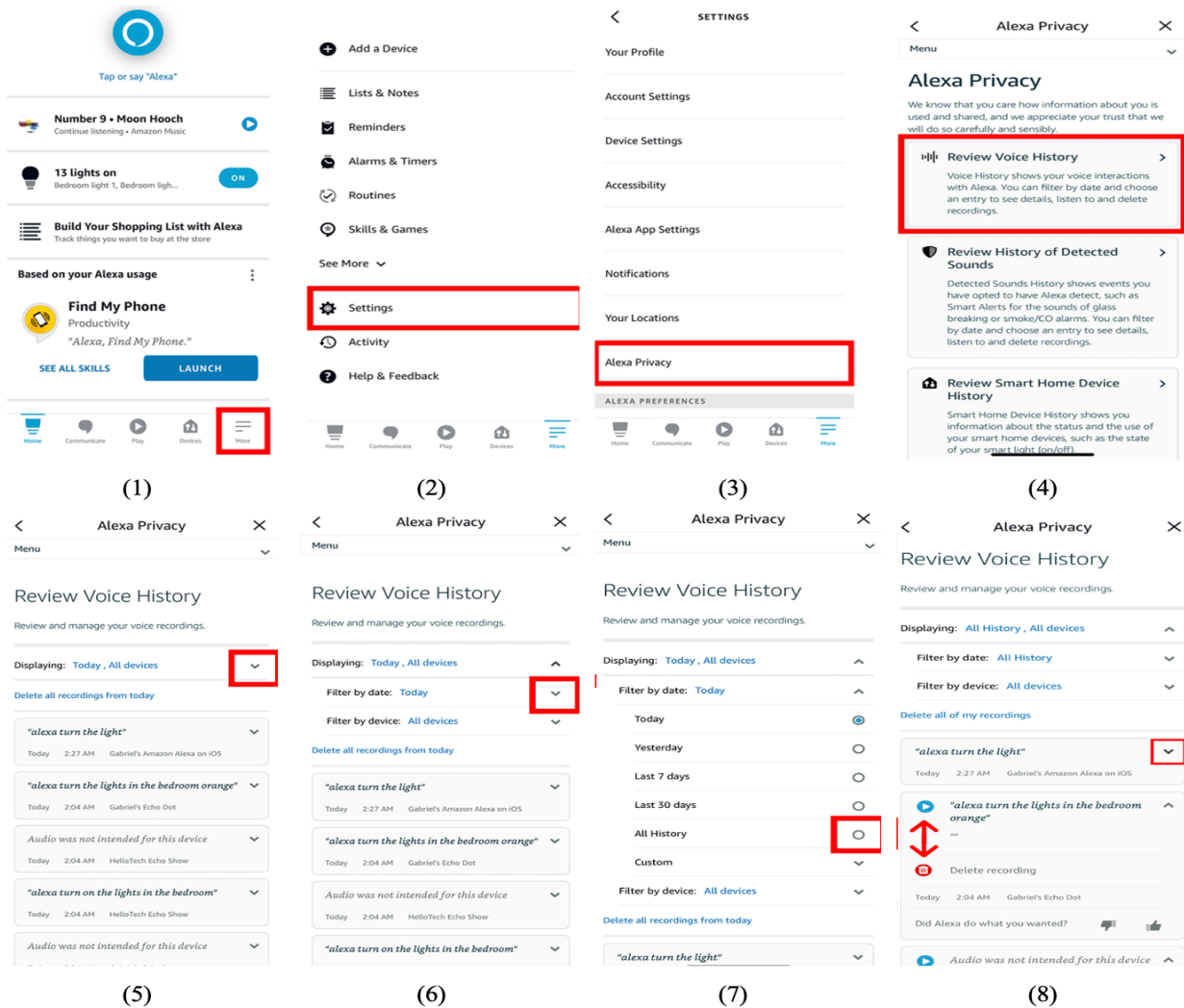


Figure C.3: Steps required to Delete Particular Voice Recording

■ Google Nest Speaker

The user can delete a specific recording manually from his Google Account by following several steps, as shown in Figure C.4. It illustrates that the user must select around nine options and scroll down via pages to find the Voice & Audio Activity page to delete one record. This indicates that deleting one recording is not easy, and from it, we conclude that the user may not easily know how to do these steps because of various choices, as well as scrolling down via pages. Moreover, the process is not straightforward, which leads to cumbersome. Furthermore, if the user has 100 records and wants to delete 50 sensitive recordings, the user must select one record, select deleting the record, and confirm to delete. Therefore, the user must do these steps 50 times to delete 50 sensitive records.

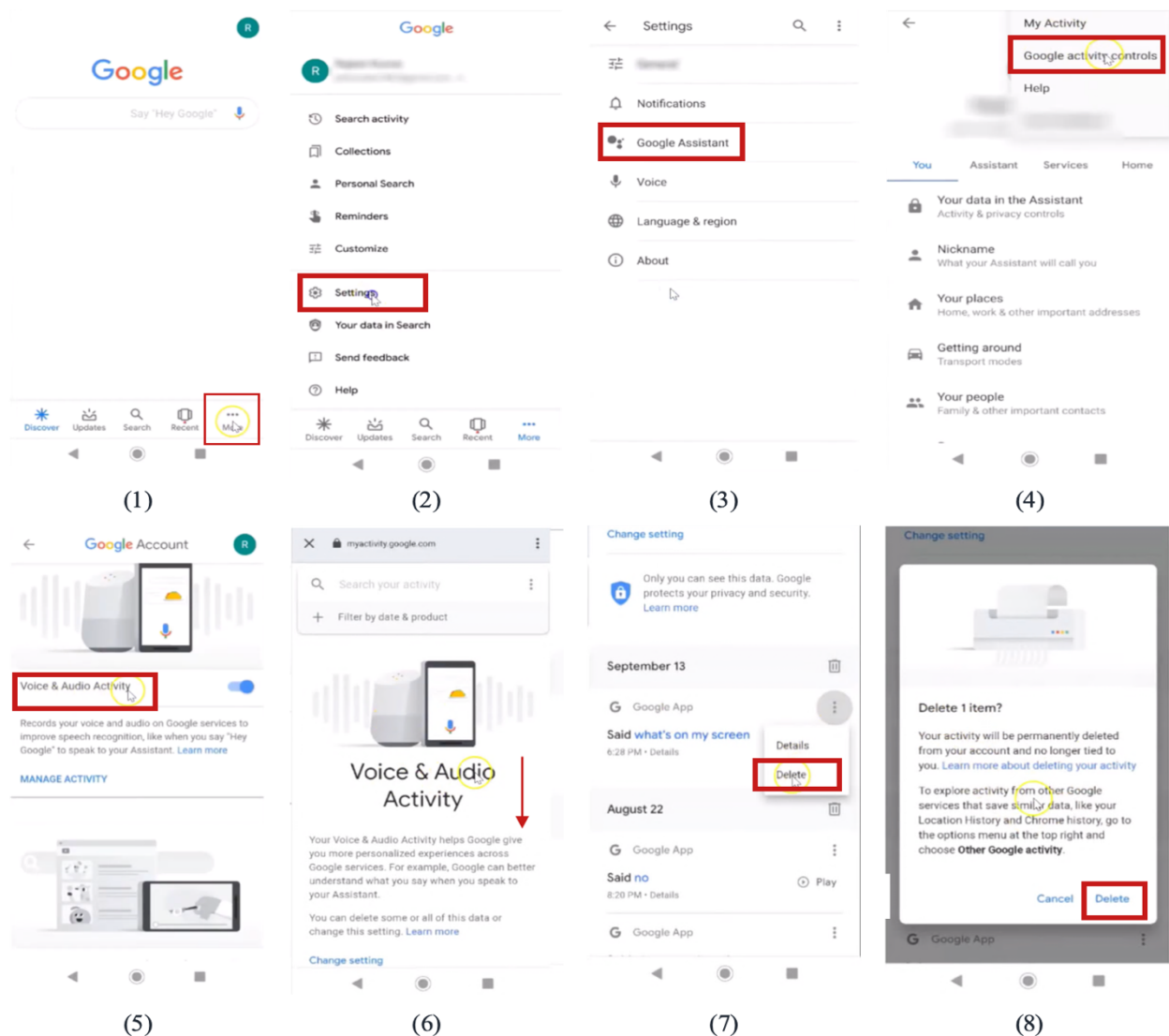


Figure C.4: Steps required to Delete a Specific Recording in Google Speaker

3. Delete all the Recording

■ Amazon Speaker

The user can delete recordings manually from the Amazon speaker device on the Alexa application setting, as shown in Figure C.5; if the user wants to delete all the recordings, the user must perform at least eight steps, which shows that deleting the recordings is not easy. From it, we conclude that the user may not easily know how to do these steps because of various options, which can be cumbersome.

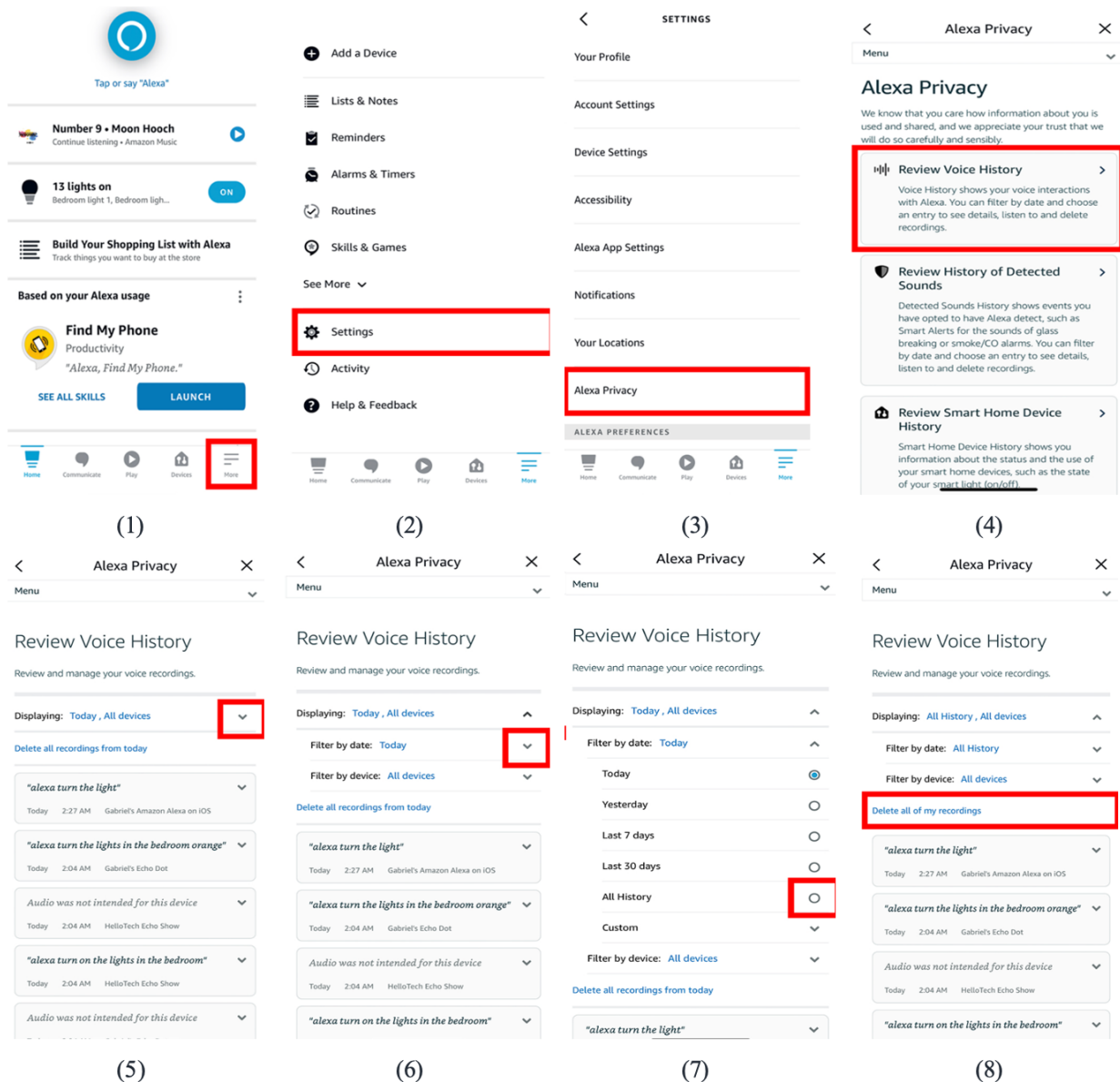


Figure C.5: Steps required to Delete all the Recording from Amazon Smart Speakers

■ Google Nest Speaker

The user can delete all records at once by doing from his Google Account by following several steps, as shown in Figure C.6. It shows that the user must select around ten options and scroll down via pages to find the **Voice & Audio Activity** page to delete all voice records. This indicates that deleting all voice recordings is not easy, and from it, we conclude that the user may not easily know how to do these steps because of various and unclear choices as well as scrolling down via pages, which can make the user try several options and undo them to reach the chosen option. For example, if the user opens the setting page, how will he know it requires him to open the **Google Assistant** option, not the **Voice** option? Therefore, the process is not straightforward, which leads to cumbersome.

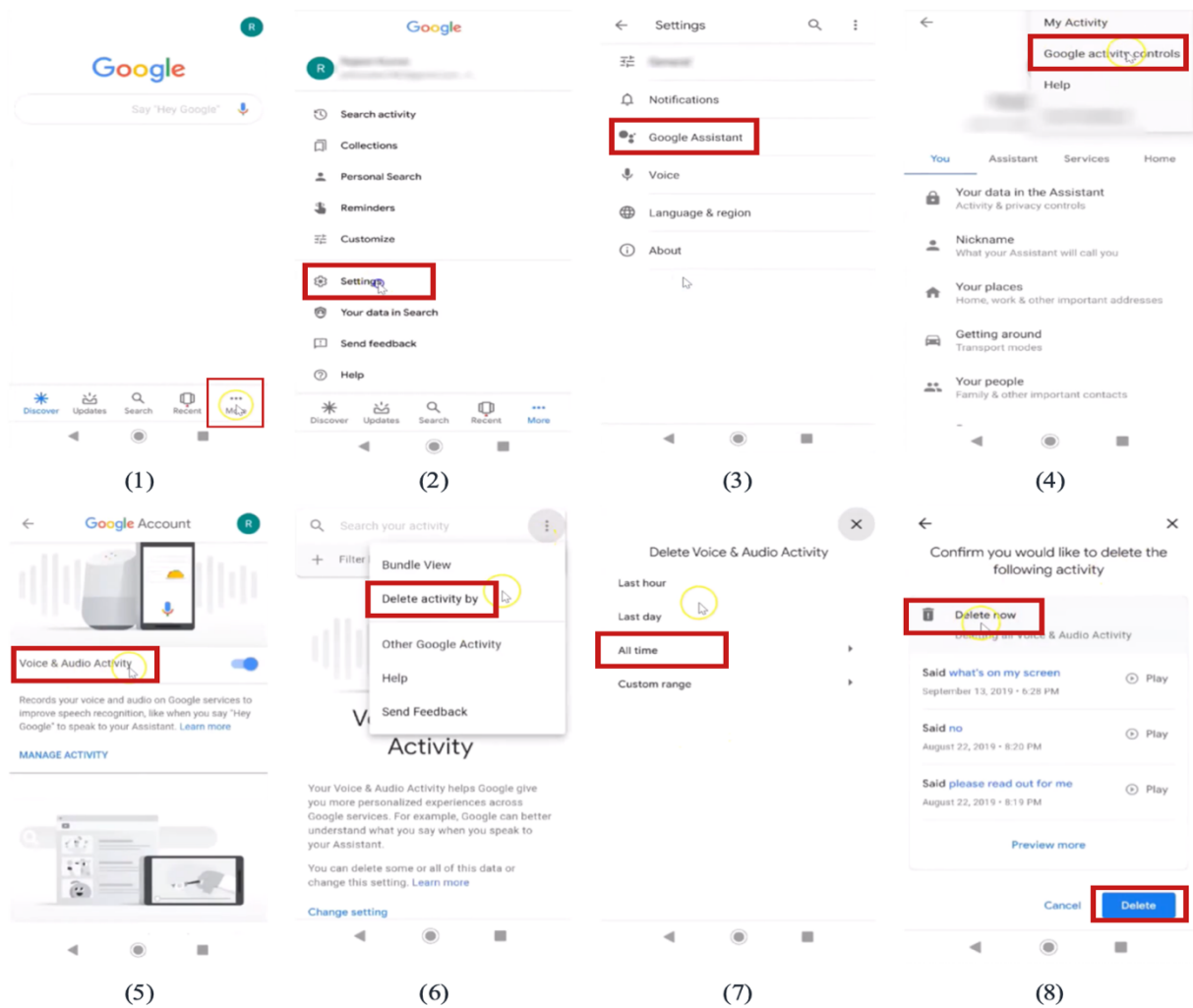


Figure C.6: Steps required to Delete all Records in Google Nest Speaker

■ Apple HomePod Speaker

The user can delete recordings from Home application by following several steps, as shown in Figure C.7. This indicates that the process could be more usable; however, it can be performed faster than other smart speakers.

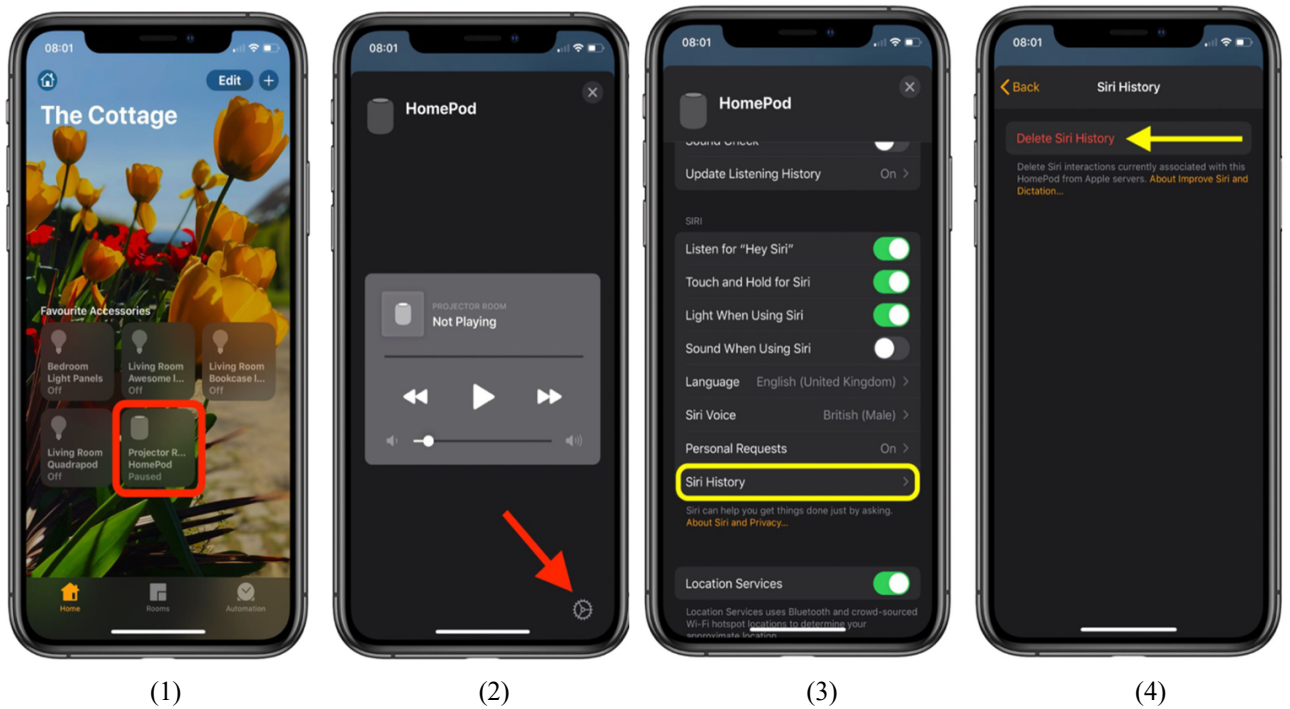


Figure C.7: Steps required to Delete Siri History from HomePod Application

4. Scheduling Deletions

■ Amazon Speaker

The user can organize deletions on the Amazon speaker by performing at least eight steps. As shown in Figure C.8, schedule deletions **are not easy** and we conducted that the user may not easily know how to do these steps because of various and unclear options, which can make the user try several options and undo them to reach the chosen option. For example, if the user opens the **Alexa Privacy page** (Step 4), how will the user know that it requires to choose to **Manage your Alexa Data** (Step 5)? Therefore, the users may take time and open different pages in the setting to finally reach the final steps, which can be cumbersome.

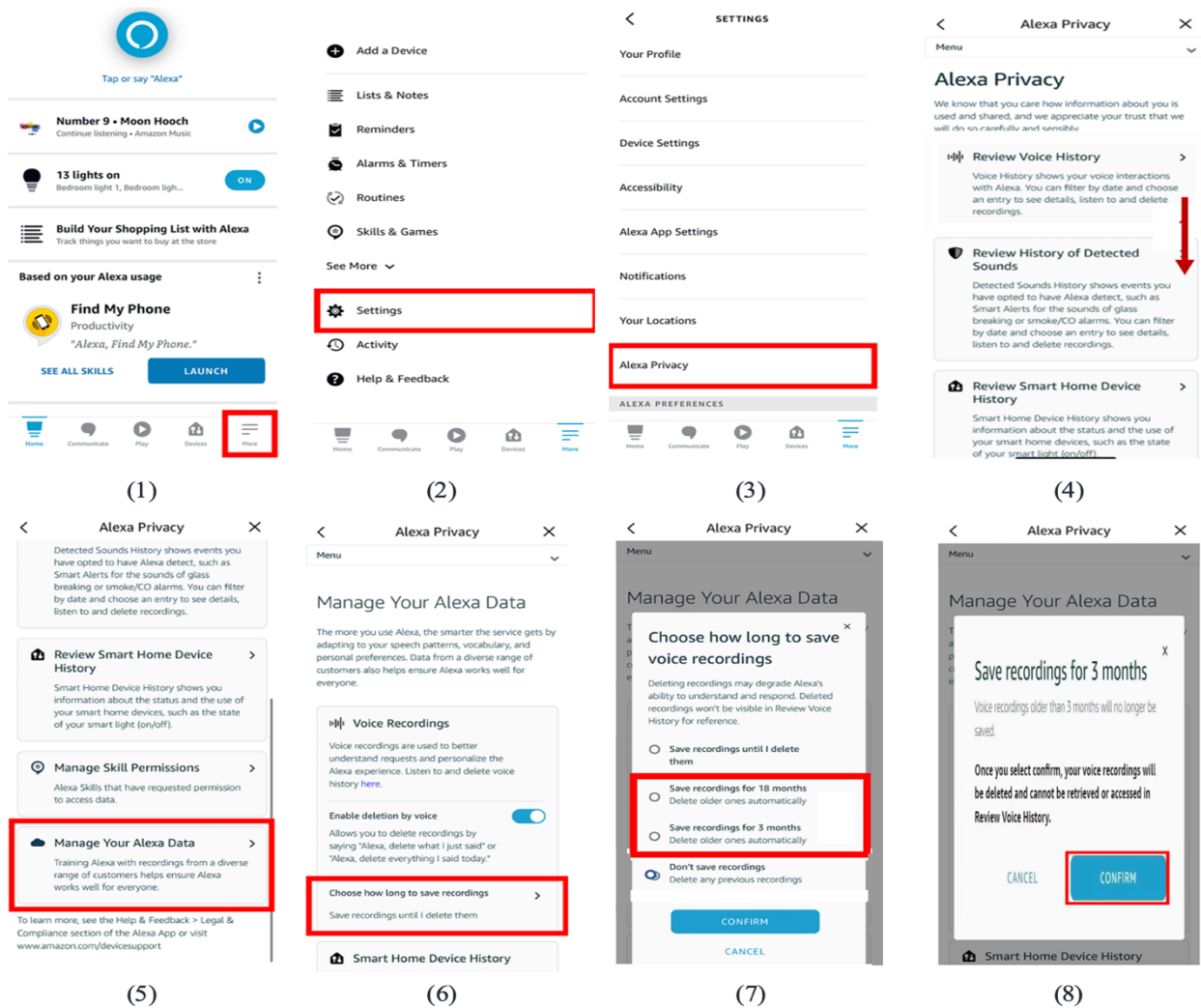


Figure C.8: Steps required to Schedule Deletions on Amazon Smart Speaker

■ Google Nest Speaker

The user should be careful because these steps will automatically delete all the activity items on the Web and Application, not only those with a voice recording. So, the user can automatically delete all the records at once by doing these steps on his Google account as follows:

- Select **Data & privacy**
- Select **Web & App Activity**, then **Manage activity** under the History setting.
- On the **Manage activity** page, select **More**, then select **Keep activity**.
- Determine the period to keep the record in the Google Account.
- **Press Confirm.**

Therefore, the user needs to perform different steps to reach various pages to **Schedule deleting the voice recording**, and we conclude that the user may not easily know how to do these steps because of various and unclear choices as well as scrolling down via pages, which can make the user try several options and undo them to reach the chosen option.

▪ Apple HomePod Speaker

Unlike Amazon Echo and Google Nest speakers, Apple HomePod Speaker will not allow users to schedule the records deletions; nevertheless, the history of voice recordings will be deleted automatically after six months. Furthermore, users will be able to delete the history of voice recordings. Moreover, Deletion options are limited in Apple HomePod speakers, unlike Google Nest and Amazon Echo Dot Speakers; the user can only delete all voice recordings in Siri history.

5. Turning off Audio Purchase

Turning off the audio purchase is most useful to sufficiently protect the user's finances and stop impulsive purchases from people in the user's home. Disabling voice purchase is provided by Amazon Echo Dot and Google Nest speakers. However, the Apple HomePod speaker does not provide disabled voice purchase.

▪ Amazon Echo Dot Speaker

The user can use turn off the Voice Purchasing from Alexa application by following several steps, as shown in Figure C.9. It shown that turning off the audio purchase can be done in around five steps.

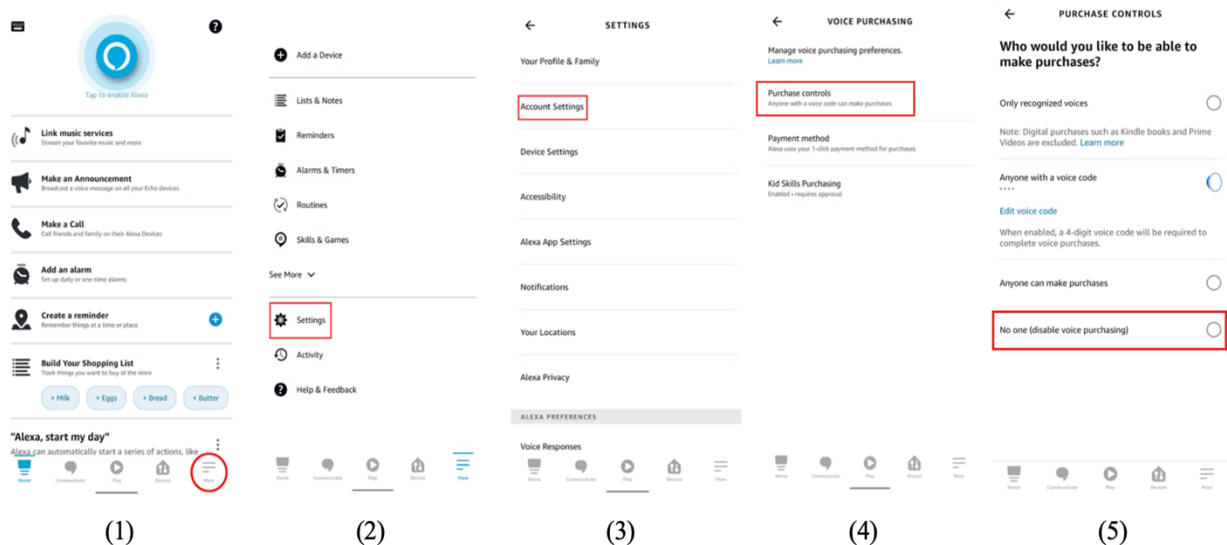


Figure C.9: Steps required to Turn off Audio Purchas in Amazon Eco Dot Speaker

6. Demand Code for Voice Purchases

■ Amazon Speaker

Requesting a 4 -digit code to complete a voice purchase increases the users' finances secure. The user can establish a 4-digit voice code to prevent unexpected orders or verify purchases. However, this feature is just available through Amazon Alexa. From Figure C.10, we can conclude that the user needs to do around seven steps to set up a 4-digit voice code.

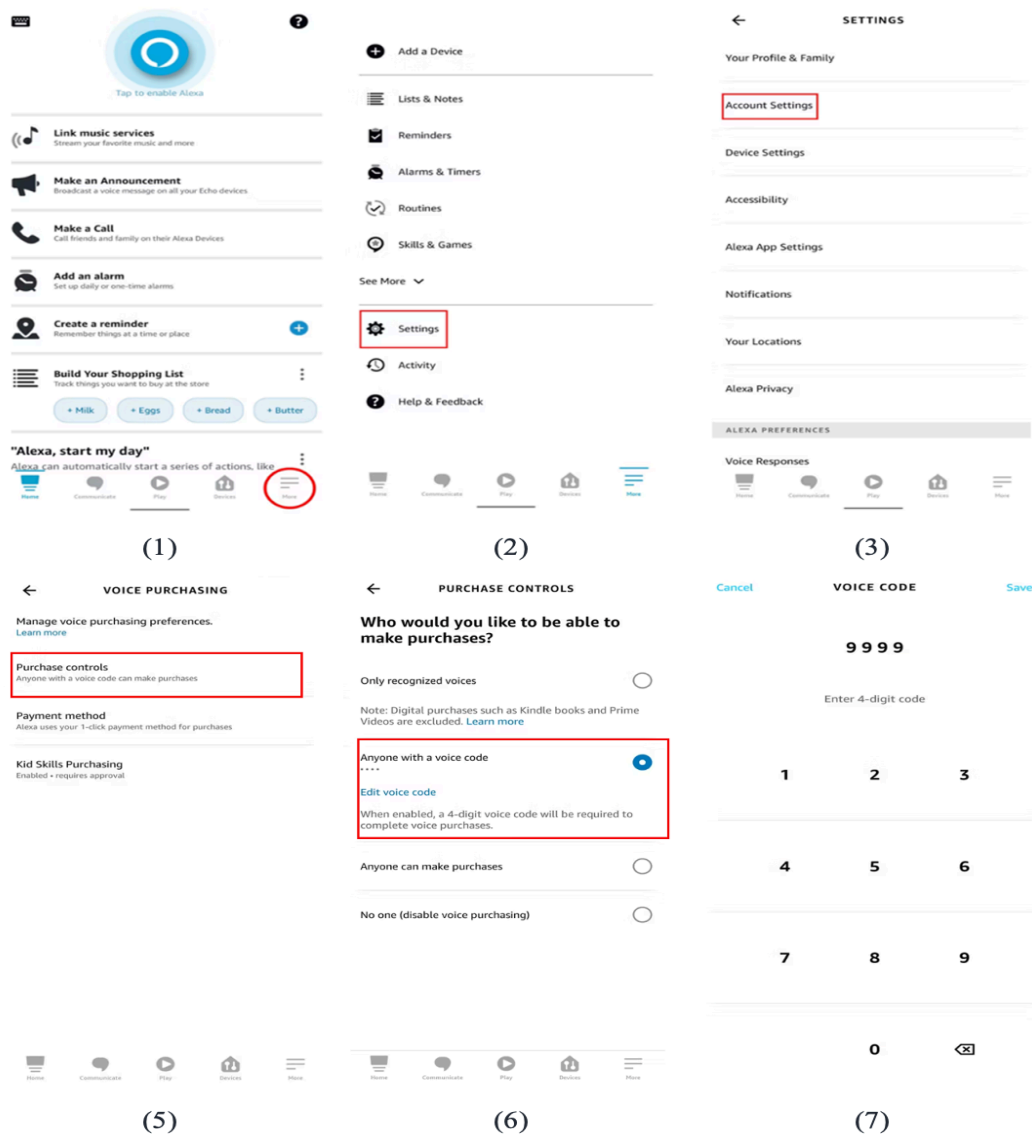


Figure C.10: Steps required to Demand Code for Voice Purchases in Amazon Speaker

7. Turning off the Location Assistance

Siri utilizes the location of the Apple HomePod speaker to provide regional news such as weather traffic and nearby businesses. Moreover, Location services settings will apply to all Apple HomePods speakers in the house. Therefore, the user should be careful with this service because it indicates the home location, which may violate the user's security and privacy. However, this feature is just available through Apple HomePod.

The user can control this feature by using the Home application and turning it off, as displayed in Figure C.11. Moreover, it shows that the user requires to choose around three choices to turn off the location services.

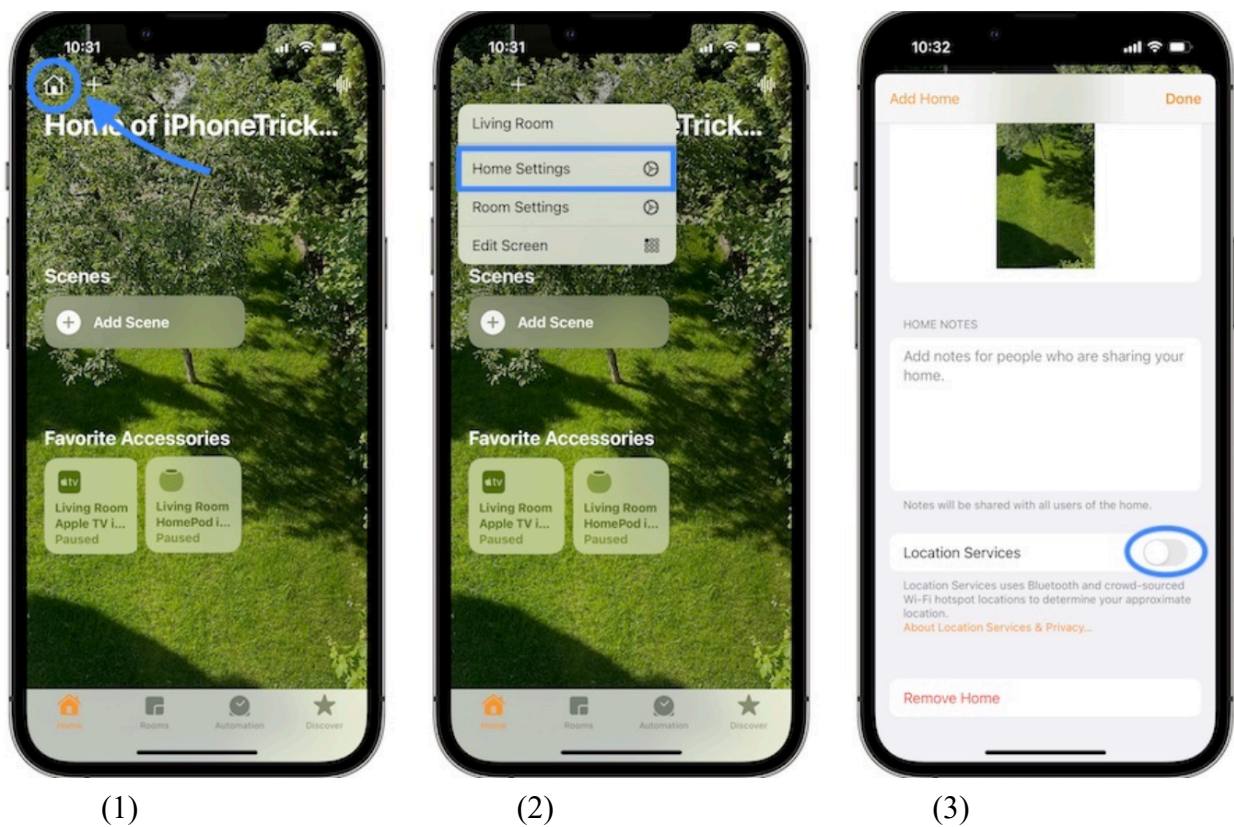


Figure C.11: Steps required to Turn off Location Services in Apple HomePod

8. Updating the Software

Updates are released regularly to improve the device's stability, adding new features, and closing security gaps. Therefore, the user needs to review the software version of his smart speaker device and compare it to the latest release version. It must be updated if a smart speaker device runs an outdated version. This section explains how to update the smart speaker software on each device.

■ Amazon Echo Dot Speaker

The user needs to follow these steps to update the Alexa software on Amazon Echo Dot smart speaker:

- Check that the device is turned on and connected to the WIFI network.
- Press the mute button until the light turns red.
- Wait between 30 minutes to one hour to enable Amazon Echo dot to update.
- The smart speaker device will reboot with the most recent firmware installed.

Therefore, the updating process in amazon Echo Speaker is easy and usable. However, it requires time to be done because the user needs to wait for a while and not use the smart speaker to update the software.

■ Google Nest Speaker

A semi-circle of white lights will appear on the top of the Google Nest speaker if it needs to update. Moreover, the update on Google Nest will be run automatically and take around ten minutes. Therefore, the updating process in Google Nest Speaker is easy and usable.

■ Apple HomePod Speaker

Updates are installed automatically on HomePod by default, but there is a way to force an update if new software is released. The software update can be done via the Home application, as shown in Figure C.12. It displays that updating the software is easy and usable and can be done quickly.

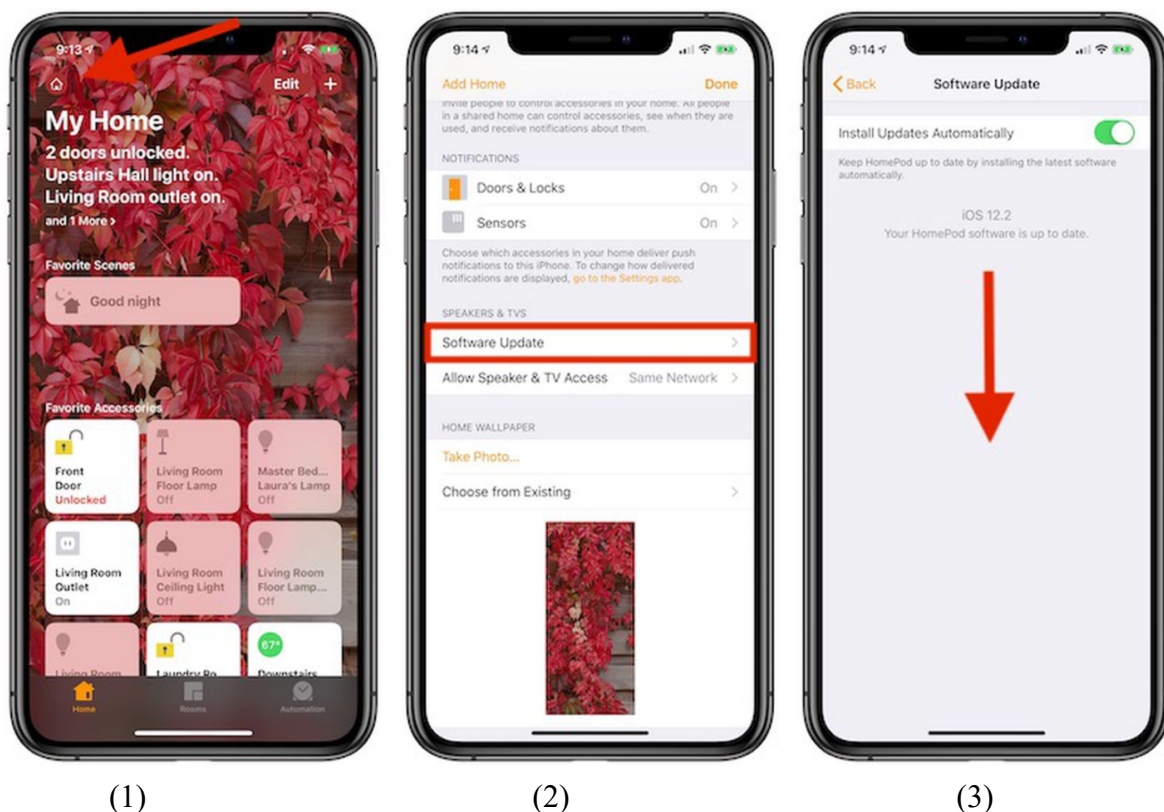


Figure C.12: Steps required to Update the Software in HomePod

4.3.5 Setting Up Voice Recognition

When a smart speaker shares with different people, the smart speaker can tell details that are not specific to the user, or it may share the user information with somebody else. Therefore, this can lead to weak authorisation security and privacy issue. In cases like this, the Voice match feature will allow the smart speaker to fetch the data specific to the user only if it hears the user's voice.

▪ Amazon Echo Dot Speaker

The user can create a voice profile using the Amazon application to recognize his voice as displayed in Figure C.13. The screen will then display instructions for creating the user Voice Profile. When the user asks Alexa to recognize his voice, she will ask the user to confirm his name and repeat ten different phrases. Therefore, we can conclude that the user requires to perform around seven options to create a voice profile in a smart speaker.

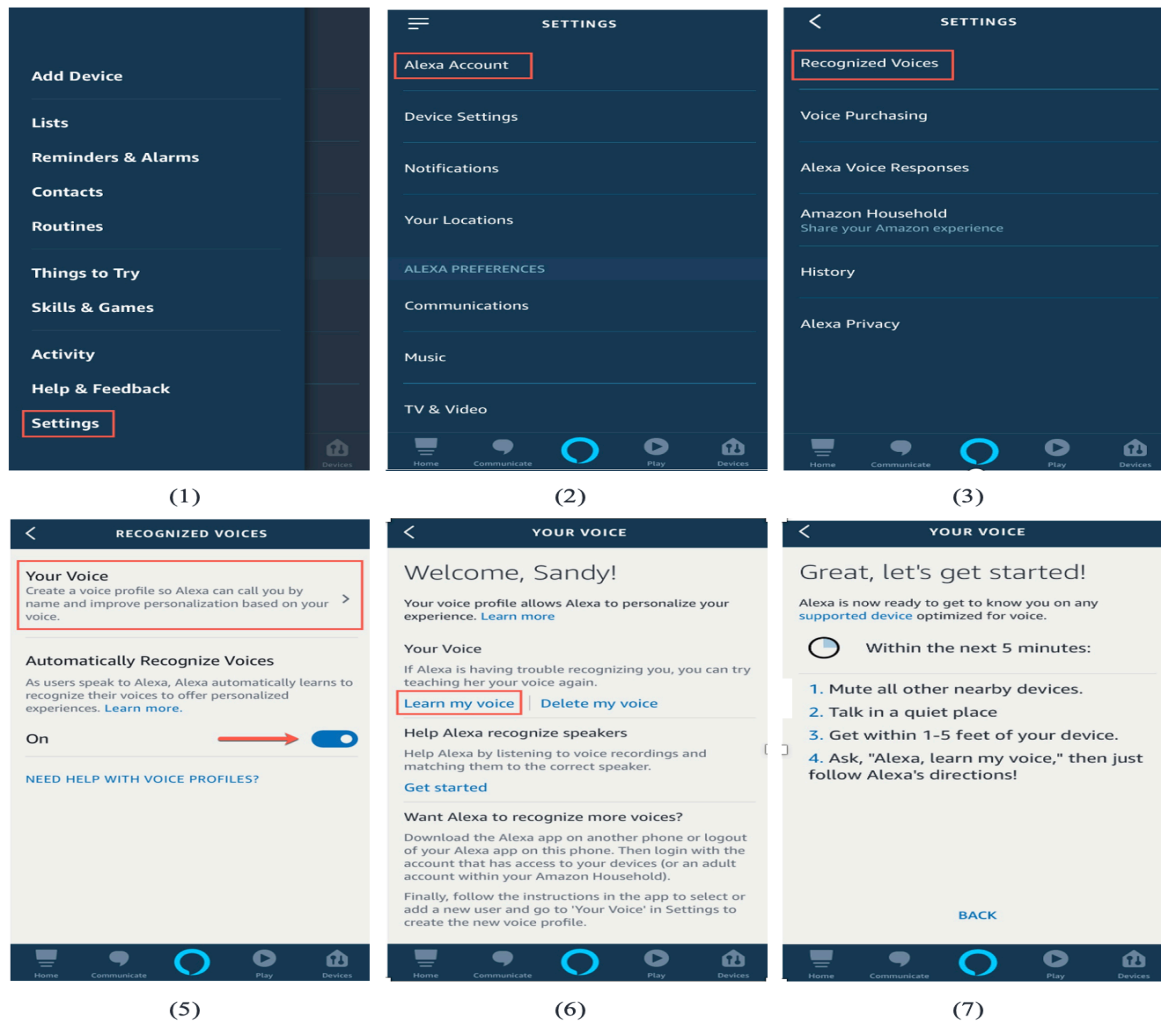


Figure C.13: Steps required to Create a Voice Profile using the Amazon

■ Google Nest Speaker

In Google Nest Speaker, this feature is called **voice match**. Therefore, the user can create a voice match using the Google Home application to recognize his voice, as displayed in Figure C.14. We can conclude that the user needs to perform more than eight steps to create a voice match in his smart speaker.

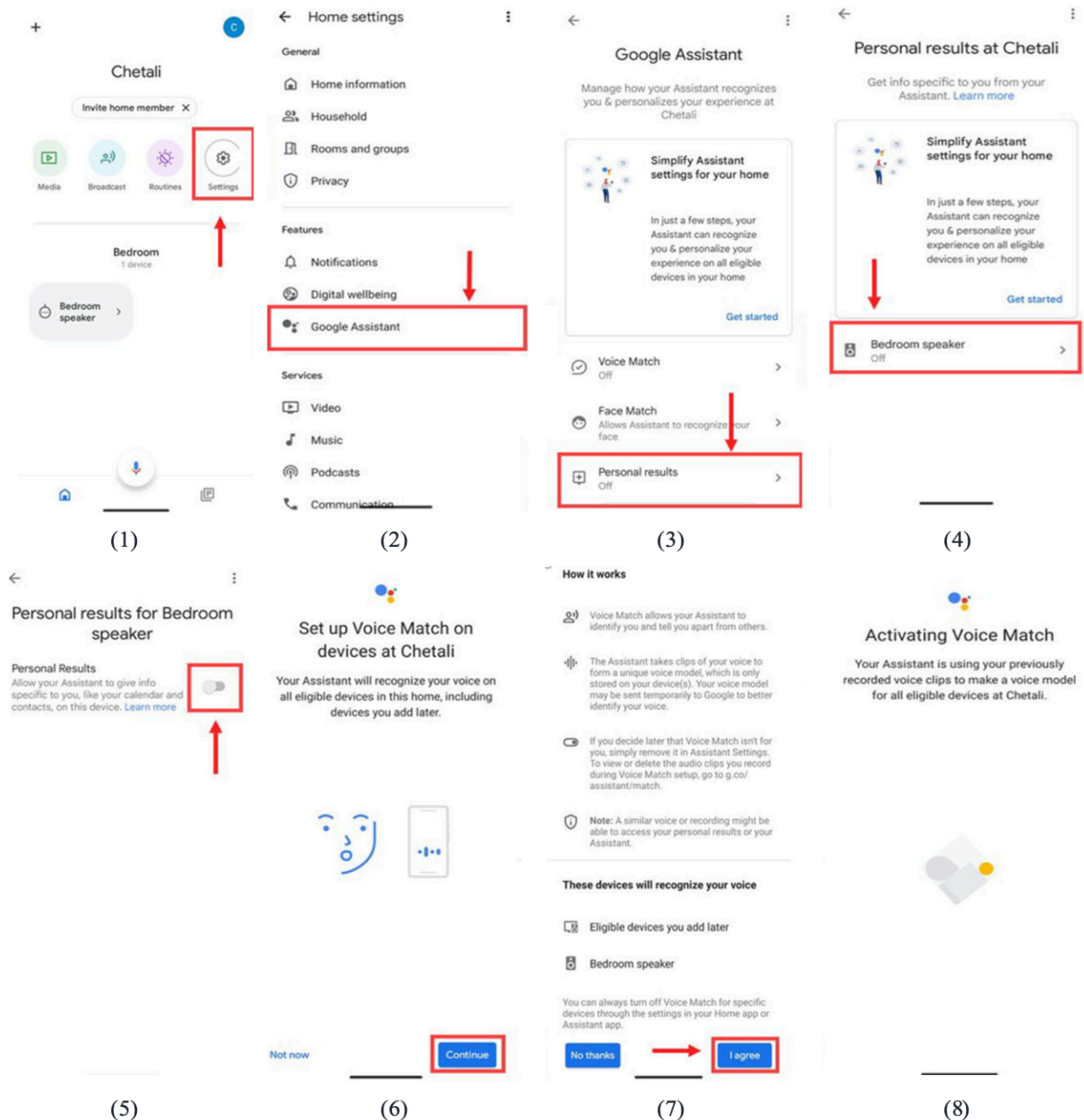


Figure C.14: Steps required to Create a Voice Match in Google Nest Speaker

▪ **Apple HomePod Speaker**

The user needs to turn on the following settings on the Home application to allow Siri to recognize who is speaking as follows:

Select Settings.

- Select Listen for Hey Siri.
- Under the *People* heading, the user needs to tap his name.
- Toggle Recognize My Voice
- Turn on Personal Requests.

The user requires to choose around five choices to create voice recognition.

Appendix D: Additional Dashboard Interfaces

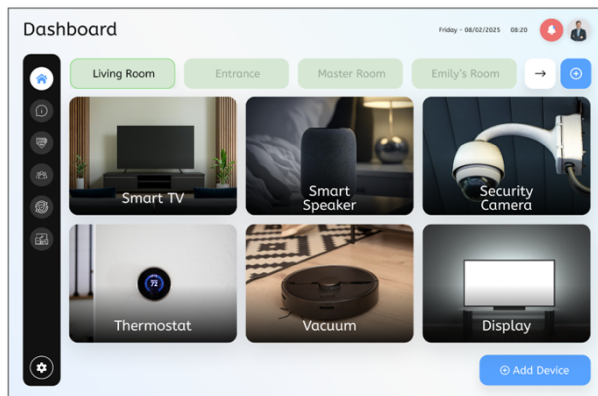
This appendix presents the supplementary interfaces developed as part of the Smart Home Security and Privacy Dashboard prototype but not included in the main body of Chapter 5. These interfaces further demonstrate the system's functional depth and navigation structure.

The following examples outline the general steps common to all devices integrated into the Smart Home Security and Privacy Dashboard. Although only representative examples are provided, the same sequence of actions, such as deleting or modifying privacy and security features, was consistently applied across all devices in the system. These examples illustrate the overall design and functional workflow of the dashboard.

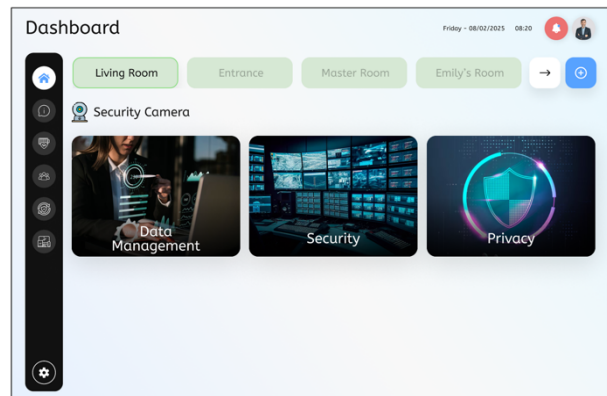
Example 1: Steps to Delete a Specific Recording in the Security Camera (Living Room)

1. Access Room Interface From the main dashboard, select Rooms and then choose the Living Room.
2. Select Device Choose the Security Camera device from the list of available smart devices.
3. Open Data Management Category: Click on Data Management to view available data-related actions.
4. Select Recording: Choose the specific recording you want to delete from the displayed list.
5. Confirm Deletion:
6. Click Delete and confirm the action in the pop-up dialog box.

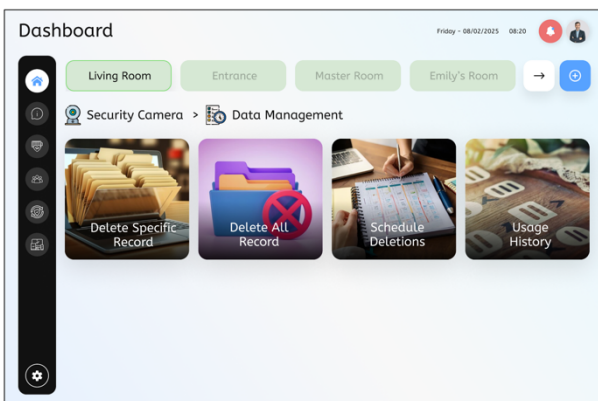
Figures D.1a–D.1f illustrate this process.



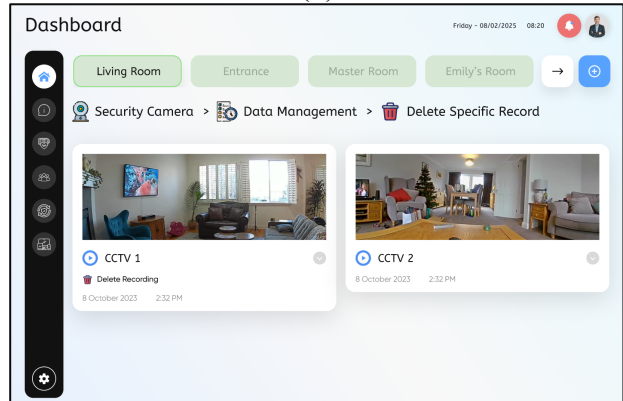
(a)



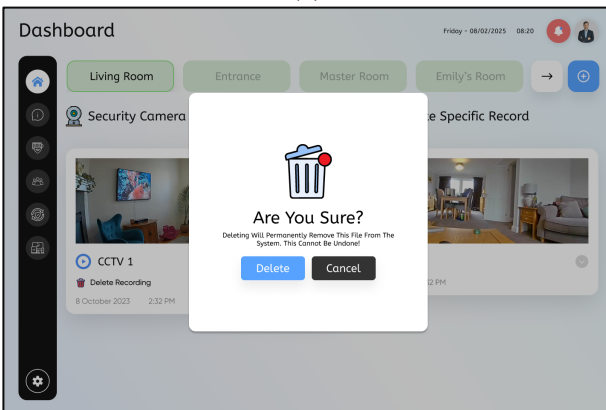
(b)



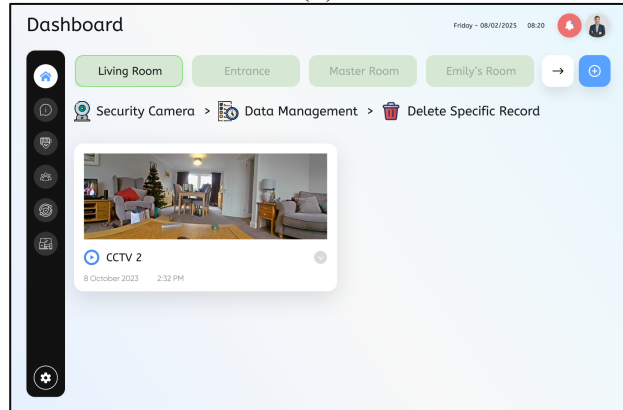
(c)



(d)



(e)



(f)

Figure D.1: Steps to Delete a Specific Recording in the Security Camera

Example 2: Steps to Delete All Recordings in the Security Camera (Living Room)

1. Navigate to Rooms > Living Room > Security Camera.
2. Open Data Management.
3. Select Delete All Recordings.

4. Confirm deletion in the confirmation window.
(Figures D.2a–D.2b.)

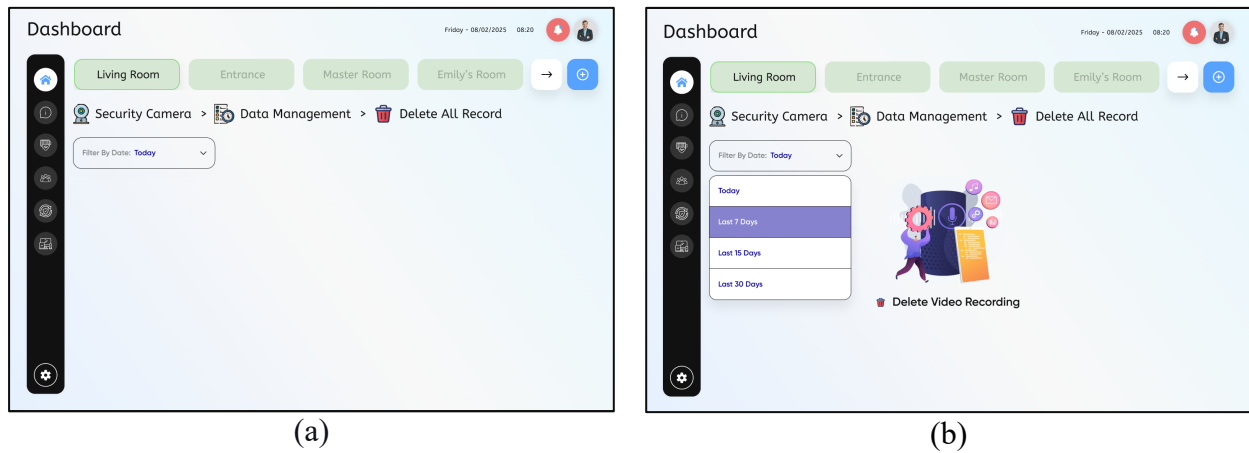


Figure D.2: Steps to Delete All Recording in the Security Camera

Example 3: Steps to Schedule Recording Deletion in the Security Camera (Living Room)

1. Go to Rooms > Living Room > Security Camera.
 2. Under Data Management, select Schedule Deletion.
 3. Set the desired frequency and duration.
 4. Click Confirm to save the schedule.
- (Figures D.3a–D.3b.)

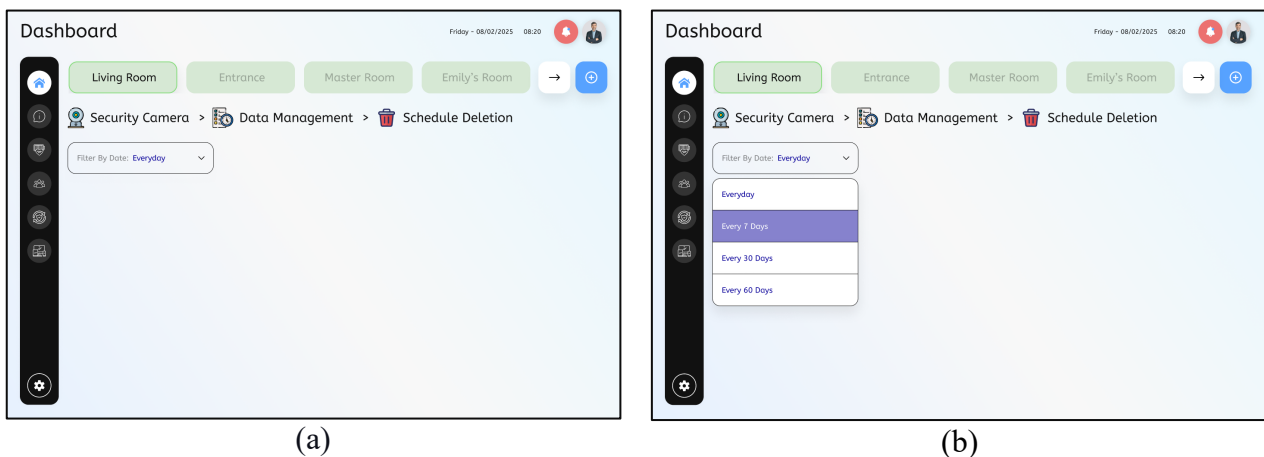
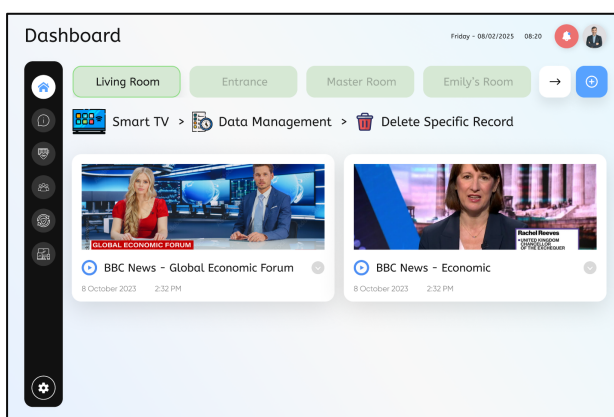


Figure D3: Steps to Delete All Recording in the Security Camera

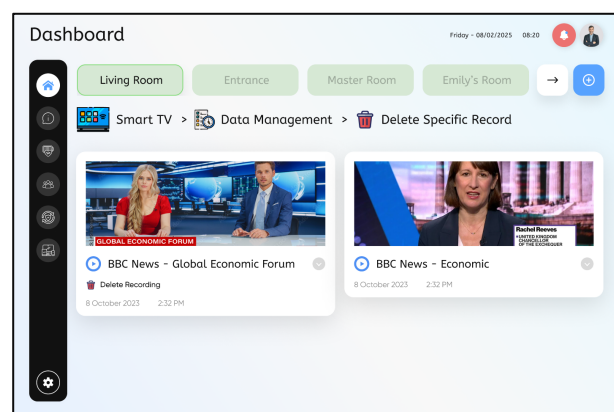
Example 4: Steps to Delete a Specific Recording in the Smart TV (Living Room)

1. Access Rooms > Living Room > Smart TV.
2. Choose Data Management.
3. Select the specific recording.
4. Click Delete and confirm.

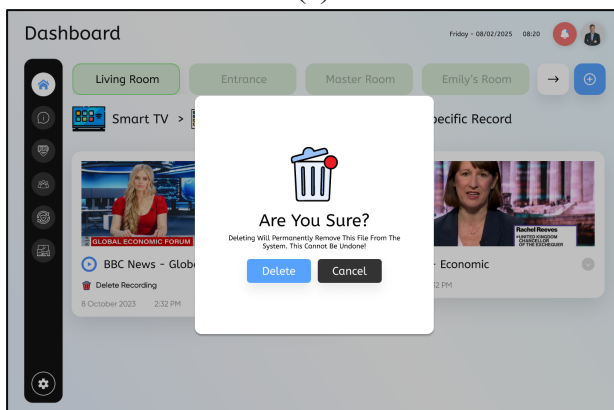
(Figures D.4a–D.4d.)



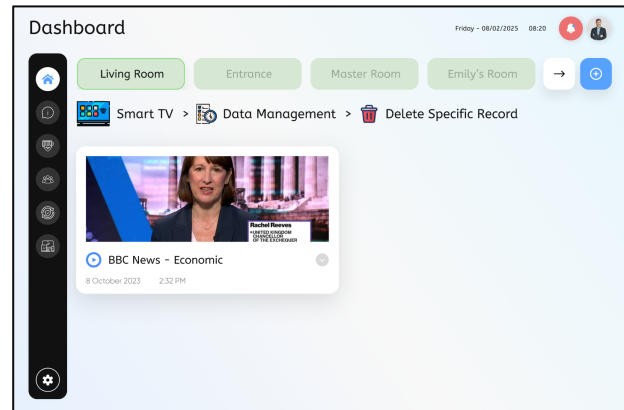
(a)



(b)



(c)



(d)

Figure D.4: Steps to Delete a Specific Recording in the Smart Tv

Example 5: Steps to Delete a Specific Recording in the Smart Speaker (Living Room)

1. Access Rooms > Living Room > Smart Speaker.
2. Choose Data Management.
3. Select the specific recording.
4. Click Delete and confirm.

(Figures D.5a–D.5d.)



Figure D.5: Steps to Delete a Specific Recording in the Smart Speaker

Example 6: Steps to Modify Authentication Settings in the Smart Speaker

1. Navigate to Rooms > Living Room > Smart Speaker.
2. Select Security category.
3. Choose Authentication Settings.

4. Update or modify the authentication method (e.g., password, voice ID).
5. Save changes.

(Figures D.6a–D.6d.)

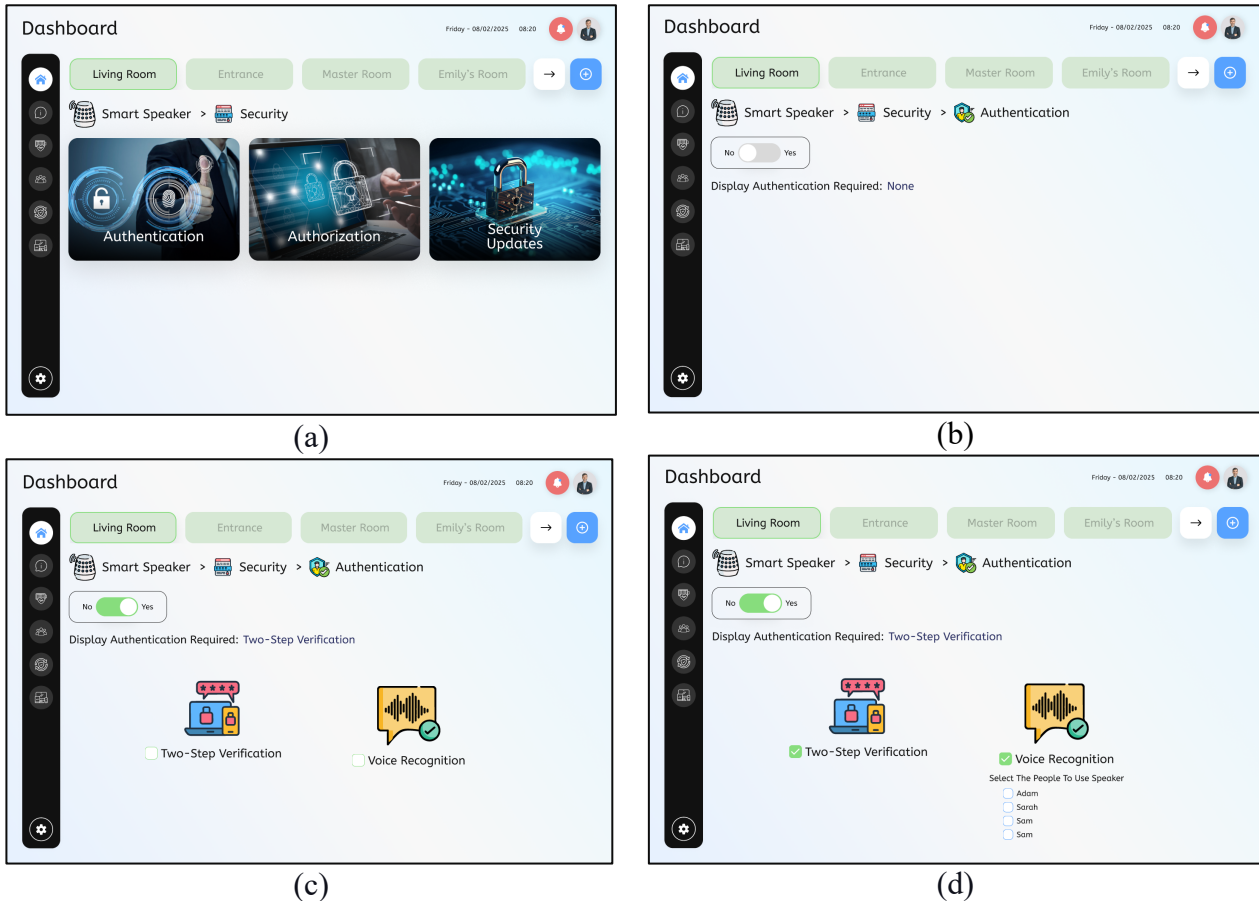


Figure D.6: Steps to Modify Authentication Settings in the Smart Speaker

Example 7: Steps to Modify Authorisation Settings in the Smart Speaker

1. Access Device Interface: from the main dashboard, select Rooms > Living Room > Smart Speaker.
2. Select Security Category: choose the Security section to view available options related to device protection.
3. Open Authorisation Settings: click on Authorisation to display the list of users authorized to access the smart speaker.
4. Modify Authorisation: enable or disable authorisation for specific users as required.

(Figures D.7a–D.7c illustrate this process.)

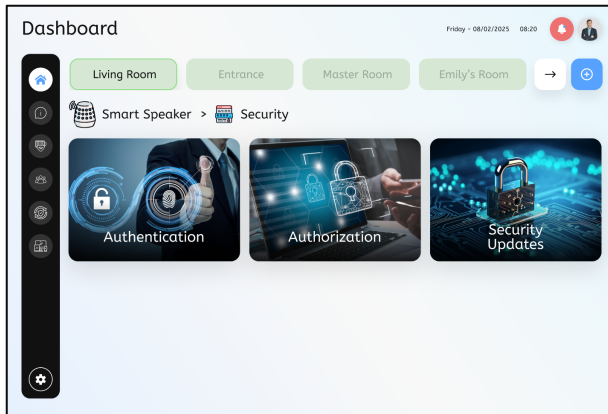


Figure D.7: Steps to Modify Authorization Settings in the Smart Speaker

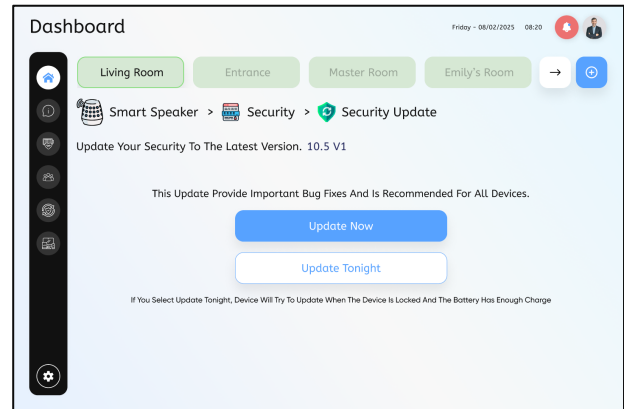
Example 8: Steps to Check Security Update Settings in the Smart Speaker

1. Access Smart Speaker Security Settings.
2. Navigate to Rooms > Living Room > Smart Speaker > Security.
3. Select Security Updates
4. Open the Security Updates section to review the latest system update information and available patches.

(Figures D.8a–D.8b.)



(a)



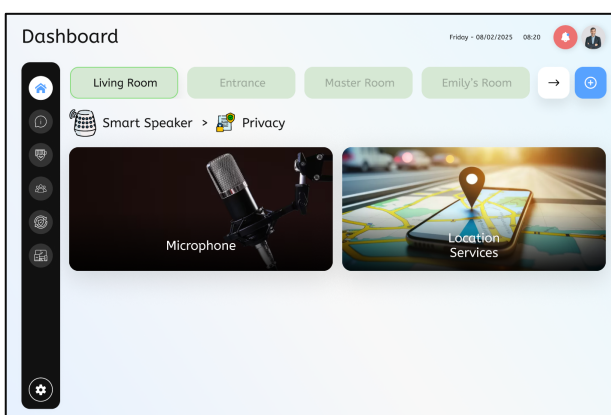
(b)

Figure D.8: Steps to Check Security Update Settings in the Smart Speaker

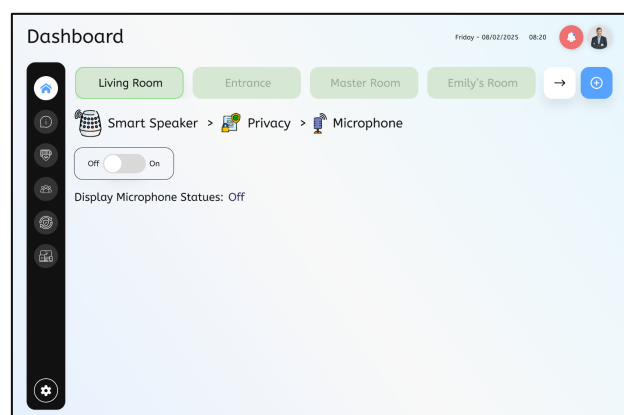
Example 9: Steps to Modify Microphone Settings in the Smart Speaker

1. Open Smart Speaker Privacy Category:
2. Go to Rooms > Living Room > Smart Speaker > Privacy.
3. Select Microphone Settings: Click on the Microphone option to view control options.
4. Adjust Settings: Choose to turn the microphone on/off or limit voice recording permissions.
5. Confirm Changes: Save the new settings to apply them.

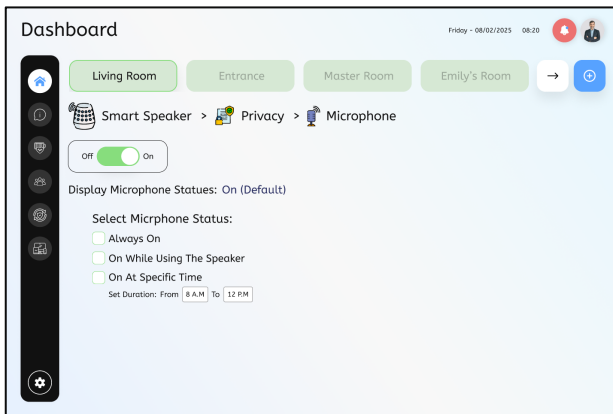
(Figures D.9a–D.9d.)



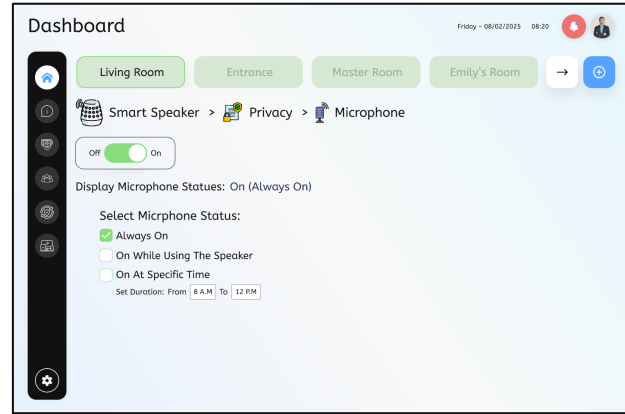
(a)



(b)



(c)



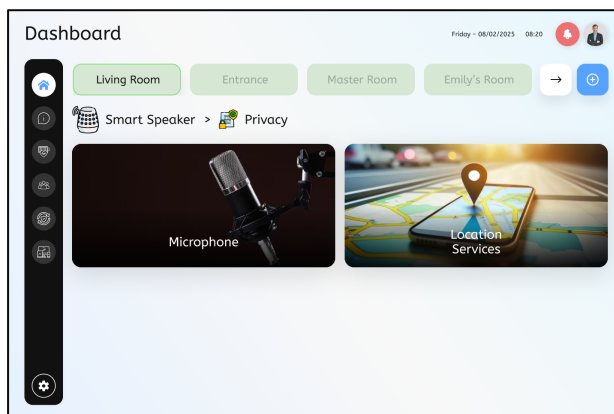
(d)

Figure D.9: Steps to Modify Microphone Settings in the Smart Speaker

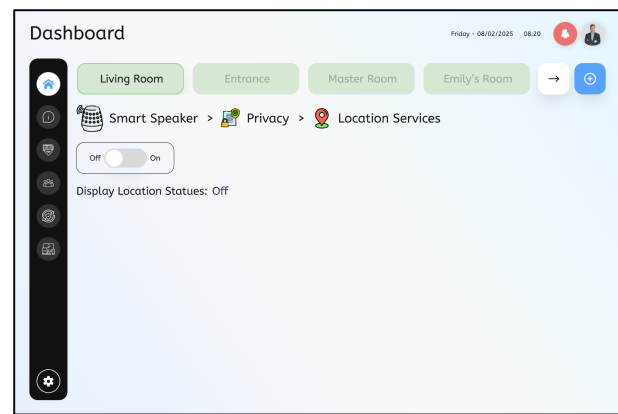
Example 10: Steps to Modify Location Settings in the Smart Speaker

1. Access Privacy Settings
2. Navigate to Rooms > Living Room > Smart Speaker > Privacy.
3. Select Location Services: Click on Location to view tracking and sharing options.
4. Adjust Permissions: Modify the access level for location data (e.g., enabled, disabled, or restricted).

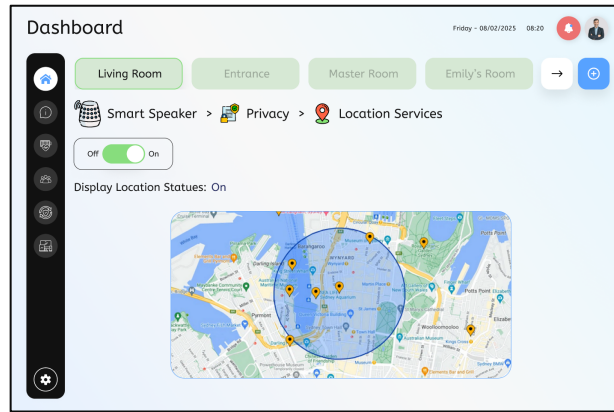
(Figures D.10a–D.10c.)



(a)



(b)



(c)

Figure D.10: Steps to Modify Location Settings in the Smart Speaker

Appendix E: Recruitment Advertisement Sample

This appendix presents the recruitment advertisement used to invite participants to the study. It includes the message content, participation details, and contact information.



University of Nottingham
UK | CHINA | MALAYSIA



**Do you own a Smart Home device?
Help us shape its Security and Privacy features**

We are looking for users with varying experience using smart home devices to participate in a research study to improve security and privacy management

What's Involved?

- Participate in usability testing & evaluation of a new **Smart Home Dashboard** and compare it to existing methods
- Share your feedback and suggest ideas for further enhancement

Session Details



60-90 minute session



In-person session



**Computer Science Building
Jubilee Campus**



Receive 10 as a thank-you for your time!

For more details, contact:
Samiah Alghamdi
samiah.alghamdi@nottingham.ac.uk

**Interested?
Please sign up!**



Appendix F: Participant Question Sheets

This appendix includes the questionnaires and evaluation materials provided to participants during the user study. It includes demographic questions, task-based scenarios, System Usability Scale (SUS) forms, and post-task interview questions to evaluate the usability and user experience of the Smart Home Dashboard compared with Google Home, Amazon Alexa, and Apple HomeKit.

Participant Number:

Questions:

1. Background and Demographics

- What is your gender? Male
- What is your age group?
 - 18–25
 - 26–35
 - 36–45
 - 46–55
 - 56–60
 - 61–65
 - 66–70
 - 71+
- What is your education level?
 - High School or Below
 - College/University Degree
 - Postgraduate Degree.
 - Other (Please specify).....
- Which of the following devices do you have and how frequently do you use each?
 - **Smart Thermostat** (e.g., Nest, Ecobee, Honeywell Home):
[Frequently / Regularly / Occasionally / Rarely / Not Applicable] []
 - **Smart Doorbell** ✓ (e.g., Ring, Google Nest, Arlo):
[Frequently / Regularly ✓ / Occasionally / Rarely / Not Applicable] []

- **Smart Display** (e.g., Google Nest Hub, Amazon Echo Show, Facebook Portal):
[Frequently / Regularly / Occasionally / Rarely / Not Applicable] [☐]
- **Smart Speaker** (e.g., Amazon Echo, Google Nest Audio, Apple HomePod):
[Frequently / Regularly / Occasionally / Rarely / Not Applicable] [☐]
- **Smart TV** ✓ (e.g., Samsung Smart TV, LG WebOS, Sony Bravia):
[Frequently / Regularly ✓ / Occasionally / Rarely / Not Applicable] [☐]
- **Smart Vacuum** (e.g., iRobot Roomba, Roborock, Dyson 360 Heurist):
[Frequently / Regularly / Occasionally / Rarely / Not Applicable] [☐]
- **Smart Security Cameras** (e.g., Arlo Pro, Nest Cam, Ring Stick Up Cam):
[Frequently / Regularly / Occasionally / Rarely / Not Applicable] [☐]
- **Other Smart Devices** (e.g., Washing mashein):
[Frequently / Regularly / Occasionally / Rarely / Not Applicable] [☐]

2. Expectations and Experience (Recording)

- **How experienced are you with managing smart home devices using apps (e.g., Alexa, Google Home, Apple HomeKit)?"**
 - Beginner (Never used any smart home apps)
 - Basic (Used a few times but not regularly) ✓
 - Intermediate (Comfortable managing multiple devices)
 - Advanced (Frequently use and configure settings)
 - Expert (Highly knowledgeable, troubleshoot, and set up automations)

- **How do you typically manage privacy and security settings for your smart home devices?**

- **Do you have any concerns when using smart home devices (e.g., privacy, data security, ease of use)?**

Google						
Task	Scenario	Task-Level Satisfaction Rating	Task Success Rate	Comments	Click Count/Number of Actions	Time on Task (Seconds)
Checking Software Updates	Ensure all your smart devices are running the latest software update to avoid any potential issues.					
Managing Smart Speaker Recordings	Review and delete some voice recordings from your smart speaker in the living room for privacy reasons.					
Ensuring Privacy During a Meeting	Ensure the smart speaker's microphone in the Office is turned off for privacy.					
Reviewing Security Camera Footage	Your neighbour mentions seeing a suspicious person near your house last night, and you want to check the camera video recording for any unusual activity.					
Turning of Location Services in all Devices	You want to disable location services for all smart home devices to protect your privacy.					

SUS-Google					
Questions (SUS)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that I would like to use this system frequently.					
I found the system unnecessarily complex					
I thought the system was easy to use.					
I think that I would need the support of a technical person to be able to use this system.					
I found the various functions in this system were well integrated.					
I thought there was too much inconsistency in this system.					
I would imagine that most people would learn to use this system very quickly.					
I found the system very cumbersome to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

AMAZON						
Task	Scenario	Task-Level Satisfaction Rating	Task Success Rate	Comments	Click Count/Number of Actions	Time on Task (Seconds)
Checking Software Updates	Ensure all your smart devices are running the latest software update to avoid any potential issues.					
Managing Smart Speaker Recordings	Review and delete some voice recordings from your smart speaker in the living room for privacy reasons.					
Ensuring Privacy During a Meeting	Ensure the smart speaker's microphone in the Office is turned off for privacy.					
Reviewing Security Camera Footage	Your neighbour mentions seeing a suspicious person near your house last night, and you want to check the camera video recording for any unusual activity.					
Turning of Location Services in all Devices	You want to disable location services for all smart home devices to protect your privacy.					

SUS-AMAZON					
Questions (SUS)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that I would like to use this system frequently.					
I found the system unnecessarily complex					
I thought the system was easy to use.					
I think that I would need the support of a technical person to be able to use this system.					
I found the various functions in this system were well integrated.					
I thought there was too much inconsistency in this system.					
I would imagine that most people would learn to use this system very quickly.					
I found the system very cumbersome to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

Apple						
Task	Scenario	Task-Level Satisfaction Rating	Task Success Rate	Comments	Click Count/Number of Actions	Time on Task (seconds)
Checking Software Updates	Ensure all your smart devices are running the latest software update to avoid any potential issues.					
Managing Smart Speaker Recordings	Review and delete some voice recordings from your smart speaker in the living room for privacy reasons.					
Ensuring Privacy During a Meeting	Ensure the smart speaker's microphone in the Office is turned off for privacy.					
Reviewing Security Camera Footage	Your neighbour mentions seeing a suspicious person near your house last night, and you want to check the camera video recording for any unusual activity.					
Turning of Location Services in all Devices	You want to disable location services for all smart home devices to protect your privacy.					

SUS-Apple					
Questions (SUS)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that I would like to use this system frequently.					
I found the system unnecessarily complex					
I thought the system was easy to use.					
I think that I would need the support of a technical person to be able to use this system.					
I found the various functions in this system were well integrated.					
I thought there was too much inconsistency in this system.					
I would imagine that most people would learn to use this system very quickly.					
I found the system very cumbersome to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

SH Dashboard						
Task	Scenario	Task-Level Satisfaction Rating	Task Success Rate	Comments	Click Count/Number of Actions	Time on Task (Seconds)
Checking Software Updates	Ensure all your smart devices are running the latest software update to avoid any potential issues.					
Managing Smart Speaker Recordings	Review and delete some voice recordings from your smart speaker in the living room for privacy reasons.					
Ensuring Privacy During a Meeting	Ensure the smart speaker's microphone in the Office is turned off for privacy.					
Reviewing Security Camera Footage	Your neighbour mentions seeing a suspicious person near your house last night, and you want to check the camera video recording for any unusual activity.					
Turning of Location Services in all Devices	You want to disable location services for all smart home devices to protect your privacy.					

SUS- Dashboard					
Questions (SUS)	Strongly Disagree	Disagree	Neutral	Agree	Strongly Agree
I think that I would like to use this system frequently.					
I found the system unnecessarily complex					
I thought the system was easy to use.					
I think that I would need the support of a technical person to be able to use this system.					
I found the various functions in this system were well integrated.					
I thought there was too much inconsistency in this system.					
I would imagine that most people would learn to use this system very quickly.					
I found the system very cumbersome to use.					
I felt very confident using the system.					
I needed to learn a lot of things before I could get going with this system.					

Interview

1.General Feedback

- How was your overall experience using the dashboard?
- Were there any tasks you found challenging or confusing? If yes, which ones?

2. Specific Usability Aspects

- How well did the dashboard align with your expectations for managing security and privacy?

3. Effectiveness

- Were there any features or functions you found missing or inadequate?

4. Scenario-Specific Questions

- Did you find the scenarios realistic and representative of your actual smart home management needs?
- Which scenario(s) did you find most relevant or helpful, and why?
-

5. Comparison to Other Platforms

- How does the dashboard compare to the individual apps/platforms (e.g., Amazon Alexa, Google Nest, Apple HomeKit) you've used?
- Would you prefer managing your devices with this dashboard or through individual platform apps? Why?
- Which system did you find the most intuitive and user-friendly, and why?

6. Satisfaction and Suggestions

- What features from the other systems would you like to see in this dashboard?
- What improvements or changes would you suggest making the dashboard more effective?
- Would you recommend this dashboard to others managing multiple smart home devices? Why or why not?

Appendix G: Ethics Material

This appendix presents the materials used for the ethical approval of the study. This includes the main application form, participant consent form, and Data Management Plan. These are presented in the sub-sections that follow.

G.1 Ethics Application Form

School of Computer Science Research Ethics Committee (CS REC)



Ethics application for research that obtains personal data through a users' trial and renders that data anonymous at the point of collection

This form should be used if the research obtains personal data through a users' trial *and* renders that data anonymous at the point of collection. If the data is not rendered anonymous at the point of collection you should use form CS_REC_1.

Personal data is information that relates to an identified or identifiable individual. Examples include name, address, and contact details; passport identification number; medical records; DNA; biometric data; location data and digital identifiers including IP addresses, cookie identifier, mac addresses, account handles, etc. Personal data also includes 'special category' data: health, genetic and biometric data and information about people's sexual orientation or sex life, racial or ethnic origin, trade union membership, political opinions, and religious or philosophical beliefs. Some special category information is routinely collected to understand participant biographies and EDI characteristics.

The ICO states that "personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable" is therefore "no longer personal data" and "the principles of data protection law no longer apply when you process it."¹

You may use this form **only if you anonymise personal data**, including special category data, **at the point of collection**. For example, if you elicit special category data but no identifiers (e.g., name, address, workplace, department, phone number, online account handle, etc.) that enable the respondent to be identified.²

If responses to topical questions could be correlated with responses to biographical or EDI questions and thus reveal a person's identity, you should use form CS_REC_1 instead. You also use form CS_REC_1 if you anonymise personal data, including special category data, *after* you have collected it, as this constitutes data processing as defined by the Data Protection 2018.

Sections A and B should be completed by the researcher. Complete all sections. Edit italicised text only. Do NOT modify this form prior to ethics review.

Section B should be provided to participants in the research. It may be modified (e.g., non-applicable sub-sections deleted or reformatted for use online) after the application has been approved.

The principal investigator or supervisor should sign-off this ethics application and submit the completed form to cs-ethicsadmin@cs.nott.ac.uk. The principal investigator or

¹ <https://ico.org.uk/media/about-the-ico/consultations/2619862/anonymisation-intro-and-first-chapter.pdf>

² <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data>

supervisor is responsible for ensuring the application has been completed correctly and providing feedback to the researcher if it is required. Principal investigators or supervisors must have completed ethics training.

A data management plan (DMP) should be put in place by the researcher and be reviewed and approved by the principal investigator, supervisor or CS REC (as appropriate) **before** submission of the ethics application.³

Section A. Information to be provided to the Research Ethics Committee, along with Section B

1. The applicant	
Applicant's name	Samiah Alghamdi
Applicant's role	PhD student
UoN email address	Samiah.Alghamdi@nottingham.ac.uk
Module / course details	n/a
Supervisor/PI's name	Prof. Steven Furnell Dr Steven Bagley
Supervisor/PI's email address	steven.furnell@nottingham.ac.uk steven.Bagley@nottingham.ac.uk
Clinical advisor's name	n/a
Clinical advisor's email address	n/a

2. The project	
Project title	Participants in a user trial for a Smart Home Dashboard
Proposed start date	25 November 2024
Date and version of application	14 October 2024
Type of application	Original
Application ID (if known) ⁴	

3. Change log

³ See CS REC Data Management Plan (DMP) Form and Guidance on the CS Ethics workspace.

⁴ An ethics application is usually allocated an ID by the CS REC *after* initial submission.

If this is a revision or re-submission, summarise how the application has been changed in response to the reviewers' comments, or delete if not applicable

4. Research ethics checklist (part one)	
Answer all questions:	Yes/No
a) Does the study involve participants who are unable to give informed consent (e.g., children, people with learning disabilities or dementia, prisoners, your own students)?	No
b) Will the study involve participants who are particularly vulnerable? ⁵	No
c) Will it be necessary for participants to take part in the study without their knowledge and consent at the time (e.g., covert observation of people in non-public places)?	No
d) Will it be necessary for participants to be kept in ignorance, misled or deceived at any point in the study (e.g., if revealing the full aims of the project during the consent process would undermine the research)?	No
e) Will the study involve the discussion of sensitive topics (including but not limited to racial or ethnic origin, political opinions, trade union membership, religious or philosophical beliefs, health or participant's sex life or sexual orientation)?	No
f) Will participants be asked to discuss anything or partake in any activity that they may find embarrassing or traumatic?	Yes (potentially, in case they are unable to complete tasks)
g) Is it likely that the study will cause offence to participants for reasons of ethnicity, religion, gender, sexual orientation or culture?	No
h) Are drugs, placebos or other substances (e.g., food substances, vitamins) to be administered to the study participants or will the study involve invasive, intrusive or potentially harmful procedures of any kind?	No
i) Is pain or more than mild discomfort likely to result from the study?	No
j) Could the study induce psychological stress or anxiety or cause harm or negative consequences beyond the risks encountered in normal life?	No
k) Will the study involve prolonged or repetitive testing for each participant?	No
l) Will financial inducement (other than reasonable expenses and compensation for time) be offered to participants?	No

⁵ A vulnerable person is defined as someone "who is or may be in need of community care services by reason of mental or other disability, age or illness; and who is or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation" (Department of Health *No Secrets: Guidance on Protecting Vulnerable Adults in Care*, 2000)

m) Will the study involve the recruitment of patients, staff, tissue sample, records or other data through the NHS or involve NHS sites and other property?	No
n) Does the research pose any risks to the researchers, participants, culture, the environment, and/or the reputation of those involved in the research or the reputation of university?	No
4. Research ethics checklist (part two)	
Answer all questions:	Yes/No/NA
a) For research conducted in public, non-governmental and private organisations and institutions (such as schools, charities, companies and offices), will approval be gained in advance from the appropriate authorities?	n/a
b) If the research uses human participants, personal data or the use of biological material, will explicit consent be gained?	Yes
c) Will participants be informed of their right to withdraw from the study at any time, without giving explanation?	Yes
d) If data is being collected, will this data be anonymised before publication or sharing?	Yes
e) Will participants be assured of the confidentiality of any data?	Yes
f) Will all data be stored in accordance with the Data Protection Act?	Yes
g) Will participants be informed about who will have access to the data?	Yes
h) If quotations from participants will be used, will participants be asked for consent?	Yes
i) If audio-visual media (voice recording, video, photographs etc) will be used, will participants be asked for consent?	Yes
j) If digital media (e.g., computer records, http traffic, location logs) will be used, will participants be asked for consent?	Yes
k) If the research involves contact with children, will appropriate safeguards be in place (e.g., supervision, DBS checks) if required?	n/a
l) If research data itself is to be published, shared or reused (e.g., alongside a publication or in an archive), will participants be asked for consent?	Yes

If you have answered "no" to all questions in part 1 and "yes" or "NA" to all applicable questions in part two of the research ethics checklist, your research is deemed to involve **minimal risk** and you may go to Section A6.

If you have answered “yes” to any of the questions in part 1 or “no” to any applicable questions in part 2 of the research ethics checklist, the research is deemed to involve **more than minimal risk**. Please explain overleaf (Section A5) why this is necessary and how you plan to deal with the ethical issues raised.

5. Research involving more than minimal risk

Explain here **why it is necessary** to conduct research involving more than minimal risk, what the risks are, and what steps will be taken / measures put in place to mitigate those risks.

This study evaluates a dashboard framework specifically created to harmonize the information gathered from multiple connected smart home devices. The goal is to enable users to easily manage and control their smart home devices from a centralized interface. The dashboard integrates various data streams into one unified view, including device status, security alerts, privacy settings, and data management functions. This study benchmarks the dashboard against established systems such as Amazon Alexa, Google Nest, and Apple HomeKit.

The study will use a scenario-based usability evaluation to gather quantitative metrics (such as task success rates, time spent on tasks, and error rates) and qualitative participant feedback. This evaluation will assess the dashboard's effectiveness in security, privacy, and data management.

The data for this study will be collected from a diverse group of participants, including students, staff, and affiliates of the University of Nottingham, as well as members of the public. Recruitment will take place through social media, Microsoft Teams, the UoN mailing list, and other public channels. Participants will have varying levels of experience with smart home devices, ranging from novice users to those with extensive expertise. This diversity will provide a broad array of perspectives for the usability evaluation.

By engaging users from various age groups and collecting detailed feedback, this study places the dashboard in the wider context of user-centred IoT privacy and security management, providing actionable insights for future enhancements in smart home interface design.

****Psychological Stress and Anxiety in Usability Trials****

Participants in the study may encounter psychological stress or anxiety, particularly concerning cybersecurity risks. This anxiety may be exacerbated if individuals experience difficulties in completing tasks related to privacy or security settings. To mitigate these concerns, participants will be reassured that their feedback is invaluable, irrespective of their success in task completion. A debriefing session will follow each trial to address any arising concerns and to remind participants of their autonomy in withdrawing from the study at any given time, thereby empowering them and respecting their control over their participation. Furthermore, participants will receive information regarding smart home security risks, along with strategies for safeguarding personal data, aimed at alleviating their apprehensions.

****Use of Identifiable Data****

The study involves the collection of identifiable data, specifically in the form of audio or video recordings during usability trials. To mitigate potential privacy concerns, all identifiable data will undergo anonymization or pseudonymization prior to analysis. Participants will provide informed consent before data collection commences and will be fully briefed on the procedures for handling and storing their data. Additionally, identifiable recordings will be securely destroyed following transcription and anonymization processes, ensuring participants' security and protection.

****Data Security****

A salient risk associated with this study is the potential for unauthorised access to data. To mitigate this risk, all collected data will be securely stored on the University's cloud storage service, OneDrive, which is protected by password access, ensuring exclusive access for the project team. Any identifiable data retained locally will be both encrypted and password-protected.

****Recruitment and Consent****

Recruitment for the study will be conducted openly through various digital platforms, with assurances that prior experience with smart home devices is not a prerequisite for participation. Informed consent will be obtained from each participant, ensuring they are adequately informed about the study's nature, their rights as participants, and their option to withdraw at any time without providing a reason. This process aims to uphold ethical standards and respect participants' autonomy throughout the study.

6. Data processing	
Data subjects	Participants in a user trial for a smart home dashboard evaluation, including users with varying levels of experience with smart home devices.
Data to be collected	Demographic information, task performance data, qualitative feedback, and recordings (e.g., audio, video, or screen recordings).
How data will be collected	Data will be collected during task performance via direct observation, and screen/audio recordings.
How data will be anonymised at point of collection	Data will be collected without requesting any details of participant names or contact details. As a result, other details that are collected would not be linkable back to an identifiable individual unless they provide such information elsewhere during the trial (if so, this would be anonymised during pre-processing). Regarding the recordings, they will be transcribed and anonymized immediately after the trial. Participants will be able to withdraw at any time during the trial and up until the point the recordings are transcribed. Once the transcription is completed, the recordings will be securely deleted. After this stage, withdrawal will no longer be possible, as the data will be fully anonymized.
Pre-processing of data	i. Pre-processing procedure(s) Redaction of identifying information, if participants provide any feedback or comments during the observation, interviews, it is essential to redact any personal details that could reveal their identity. ii. Anonymisation / pseudonymisation applied A unique ID will be assigned to each participant. Any information that identifies individuals will be redacted.
Data analysis	Statistical and thematic analysis of the responses.
Data sharing	Following any necessary anonymisation, the data asset might be shared in its entirety with the other participating universities, who are subject to the same data protection laws and regulations as the University of Nottingham.
Data storage	Data asset: Participants in a user trial for a smart home dashboard evaluation. Stored on: OneDrive at University of Nottingham. Owner: Samiah Alghamdi

7. Participant recruitment

a) How participants will be recruited

Participants will be recruited from both the University of Nottingham and the public through various channels to ensure diversity in the participant collection.

The study seeks to involve individuals with varying levels of experience with smart home technology, ranging from novice users (who may have limited or no experience) to experienced users (who actively use smart home systems). This range of participants will provide insights into how the smart home dashboard is used by different user groups, making the findings more generalizable.

Participants will engage in one-to-one user trials, where each individual will receive detailed instructions on how to interact with the dashboard during the study. These trials will involve step-by-step guidance through specific tasks designed to evaluate the usability, security, privacy controls, and data management features of the smart home dashboard. Each participant will receive instructions tailored to their experience level, ensuring that both novice and experienced users can engage with the interface effectively.

Participants will be encouraged to think aloud during the trial, providing real-time feedback on their experience, which will be recorded for analysis. A minimum of 15 participants will be recruited to ensure a sufficient range of insights are captured.

Before the trial begins, participants will receive clear information about the study's objectives, the data collection process, and their rights, including their right to withdraw from the study at any time without needing to provide a reason. Informed consent will be obtained from all participants prior to data collection to ensure they fully understand the study and how their data will be managed.

b) Incentives

N/A

c) Compensation

N/A

8. Further information

The study is based on a collaboration between the PhD student and her supervisors as follows:

- Samiah Alghamdi, PhD Researcher, University of Nottingham.
- Steven Furnell, Professor of Cyber Security, University of Nottingham.
- Steven Bagley, Assistant Professor, University of Nottingham.

Prof. Furnell is the main supervisor of the project while Dr Bagley is the second supervisor.

9. Applicant declaration

Please confirm each of the following statements:

Yes/No

The research is minimal risk	No
A data management plan has been put in place	Yes
Applicant	Samiah Alghamdi
Date	14 November 2024

10. Supervisor/PI declaration	
Please confirm each of the following statements:	Yes/No/NA
I have completed ethics training	Yes
The proposed research complies with the UoN Code of Research Conduct and Research Ethics	Yes
I have reviewed the data management plan, and it complies with CS REC guidance	Yes
Supervisor/PI	
Date	Enter date application submitted to cs-ethicsadmin@cs.nott.ac.uk

G.2 Consent to Participate

School of Computer Science University of Nottingham



Section B. Information to be provided to trial participants

PROJECT TITLE [Improving Security and Privacy insights for Smart Home Users]

1. Why we are asking you to take part in our Trial
a) Aims and objectives of our research
This research is part of a PhD project at the University of Nottingham, focused on evaluating a smart home dashboard designed to centralize and streamline the management of device information, privacy, security, and data across various smart home systems. The dashboard aims to provide users with an intuitive interface to manage their devices and personal data securely. This study specifically investigates how users with varying levels of experience interact with the dashboard, exploring their ability to navigate and manage their smart home systems effectively. Through a user-centered usability evaluation, we aim to understand how the dashboard enhances usability and security, identifying areas for improvement in providing an inclusive and user-friendly smart home security and privacy management experience. The study is being conducted by the following academic team: • Samiah Alghamdi, Researcher, University of Nottingham • Steven Furnell, Professor of Cyber Security, University of Nottingham • Steven Bagley, Assistant Professor, Faculty of Science, University of Nottingham
b) Funder information
N/A
c) Governance

2. Taking part in the Trial
The trial is divided into three stages as follows: 1- Introductory session (5-10 minutes) • Explain the purpose of the assessment to the participants. • Ensure users are comfortable and understand that their feedback will be used to improve accessible security. • Explaining the tasks and process. 2- Tasks session (60-75 minutes) • Prepare the environment to observe and document the users' interactions with some requirements needed such as recoding the screen (Screen Recording Software) and/or video recording and internet connection.

- Perform the tasks.
- Observe and document your interactions.

3- Feedback Collection Session (10-15 minutes)

- Conduct a short debriefing with participants to gather feedback on their experience with the dashboard.
- Ask participants for their opinions on the ease of use, clarity of security and privacy features, and any areas for improvement

3. Risks of participation *(delete if not applicable)*

a) Risks

This user trial has been designed to keep any personal data anonymous and to minimize the risk of collecting identifiable information during the usability evaluation itself. At the start of the experiment, each participant will be assigned a randomly generated identifier (e.g., a unique number between 1000 and 9999) instead of using names. We will collect limited demographic information—such as age, education, and the number of smart home devices owned—to help us categorize feedback based on age and familiarity with smart home technology. This information will be securely stored and kept separate from usability evaluation data.

During the usability tasks, no additional personal information will be intentionally collected. However, there is a small chance that participants may unintentionally identify themselves through comments or feedback. We encourage participants to avoid sharing identifiable information when describing their experiences with the dashboard, although we acknowledge that a minor risk remains.

b) Mitigation of risks

To protect your privacy, we will anonymize any comments that may identify you before the data is analysed. Since you'll be using our tablet with the smart home dashboard, there's no risk of exposing any personal information from your own device.

We will guide you on how to engage with the dashboard safely and ensure that no sensitive personal data is collected or displayed during the session. Additionally, we will provide an information sheet with general cybersecurity advice for smart home systems, helping you feel more informed about managing privacy and security settings. If you have any concerns during the session, feel free to speak with the researcher. A debriefing session will also follow each trial to address any questions or feedback.

4. What we use the trial data for

- The data collected during the usability evaluation, including task performance metrics and feedback shared during the feedback session, will be analysed to meet the aims and objectives of our research as described in Section 1.
- Observations and participant feedback may be reviewed and discussed in research meetings among the research team members.

- Anonymous quotations of comments made by participants may be used in scientific works, including presentations, reports, and publications stored in databases, posted online, or used in materials that promote the research and its findings.

5. Your ethical rights

a) Right to withdraw

You have the right to withdraw at any time during the trial without explanation. However, it will not be possible to delete any data you provide after the trial has been completed as the data is anonymous and we cannot track who provided it.

6. Consent to participate

a) I consent to participate in the trial and my signature or mark confirms the following: ⁶

- I understand the aims and objectives of the research
- I understand what taking part in the trial requires me to do
- I accept the risks of participation (*delete if not applicable*)
- I understand how the trial data may be used
- I understand that I can withdraw at any time without explanation during the trial
- I agree to participate, and my participation is voluntary

Signature or mark:

Name of participant(s)

Date

Witness

If participant(s) cannot sign

In signing I confirm the participant(s) named above have been fully informed about the research, have been able to ask questions, and consent freely.

⁶ This may be replaced by an online means of affirmation (e.g., ticking a box)

G.3 Data Management Plan

Data Management Plan (DMP) Asset Inventory <i>Answer all questions</i>	
1. Title of the data asset: User Trail for Smart Home dashboard <i>e.g., the project name</i>	
2. Data owner: Nominated replacement: Data steward(s): Data users	Samiah Alghamdi Director of Research Samiah Alghamdi, Steven Furnell. Samiah Alghamdi, Steven Furnell, Steven Bagley <i>Note: Details in this section may change and need to be updated over the lifetime of the project</i>
3. Who or where will the data be obtained from? <i>Include all persons, organisations or sources (e.g., websites) the data will be obtained from</i> The data for this study will be obtained from a broad range of participants, including students, staff, and affiliates from the University of Nottingham, as well as individuals from the public. Recruitment will be conducted through invitations shared on social media, Teams, the UoN mailing list, and other public channels. Participants will include individuals with varying levels of experience with smart home devices, from novice users to those with extensive experience, providing a diverse range of perspectives for the usability evaluation. Samiah Alghamdi, a UoN PhD researcher, will directly capture responses.	
4. 4.1 Where will the data (digital and / or physical) be stored? <i>UG, PGT and PGR students should store digital data on their University 0365 account</i> Data will be stored on the [University's cloud storage service, e.g., OneDrive] and a secured local device with encryption. 4.2 If the data is not stored on University services (e.g., 0365) or premises (if the data is not digital), how will the data be secured? It is secured on an encrypted and password-protected system. 4.3. How will you ensure only authorised users have access to the data? <i>You must notify the ethics committee immediately if a data breach occurs</i> Only authorized project team members with secure credentials will have access to the data.	

4.4 How will access be revoked?

e.g., if a user leaves the University

Removal of the affected user's access to the shared resources.

5. 5.1 Will the asset include data that identifies or could identify people involved in the research, either on its own (e.g., audio or video) or in combination with other data used in the research (e.g., location data)?

☒ Yes ☐ No

If yes specify the categories of identifiable or potentially identifiable data that will be collected and used in the research:

e.g., names, postcodes, audio data, video data, IP or MAC addresses, account handles, etc.

its own audio data and video data.

5.2 Will data that identifies or could identify people be de-identified (anonymised or pseudonymised) before it is used?

☒ Yes ☐ No ☐ N/A

5.3 Will data that identifies or could identify people be destroyed after it has been de-identified?

e.g., will audio recordings be destroyed after they have been transcribed or textual responses had identifying details removed

☒ Yes ☐ No ☐ N/A

If no please explain why not:

Note: It is best practice to de-identify data before use and destroy the original data that identifies or could identify people, if possible and practical to do so

6. 6.1 Will the data include special category data?

Special category data includes health, genetic and biometric data, and data about people's sexual orientation or sex life, racial or ethnic origin, trade union membership, political opinions, religious or philosophical beliefs.

☐ Yes ☒ No

If yes specify which special categories of data will be collected and used in the research:

6.2 Will large volumes of special category data that identifies or could identify people be collected and used?

If you are unsure as to what constitutes a 'large volume' please contact the ethics committee

☐ Yes ☒ No

If Yes has a data protection impact assessment (DPIA) been conducted?

Contact the University's Data Protection Officer for DPIA guidance

☐ Yes ☐ No ☒ N/A

If Yes please provide the DPIA reference and submit the DPIA with the ethics application:	
7.	7.1 Will data collected during the research be shared with third-party recipients (anyone outside the University, e.g., research partners)? <i>Please list them, if applicable</i> No 7.2 Will data that identifies or could identify people be shared with third-party recipients? ☐ Yes ☒ No 7.3 Will data that identifies or could identify people be shared with and / or processed by an online service that is not provided by the University (non-University software)? ☐ Yes ☒ No 7.4 If data that identifies or could identify people is to be shared with third-party recipients or online services not provided by the University, will the data first be anonymised or pseudonymised? ☐ Yes ☐ No ☒ N/A If No please explain why not: 7.5 If data that identifies or could identify people will be shared with third-party recipients or online services not provided by the University, do they comply with data protection regulation? <i>i.e., are they GDPR compliant</i> ☐ Yes ☐ No ☒ N/A
8.	8.1 Is it a requirement that the data is open and / or made available to others (e.g., following publication)? See SHERPA/JULIET http://www.sherpa.ac.uk/juliet/index.php ☐ Yes ☒ No 8.2 Will data that identifies or could identify people be de-identified before it is made available to others? <i>i.e., will the data be anonymised or pseudonymised</i> ☐ Yes ☐ No ☒ N/A If No the data should not be made available to others, unless it was clearly gathered for public purposes and consent has been obtained
9.	Is the data confidential? <i>e.g., does it involve trade secrets or is will it be protected by a non-disclosure agreement</i> ☐ Yes ☒ No

If Yes please provide the reference number of the confidentiality agreement signed by the University's Research Operations team:

10. Declaration

In signing this form, I confirm that the information provided above is correct.

I confirm that I will not make data that that identifies or could identify people available to others unless it is clearly gathered for public purposes as specified in the ethics forms, and consent has been obtained.

I confirm that I will notify the ethics committee immediately should a data breach occur.

Signed:

Print name: Samiah Alghamdi

Date: 14 November 2024

Appendix H: Analysis of Prior Dashboard Prototype

This appendix presents the initial dashboard design developed as part of a prior master's project. It is included to provide contextual grounding for the key limitations identified in that design, particularly in relation to interface fragmentation and complex user interaction. The critical evaluation of this early prototype establishes a baseline that justifies the need for the more unified and refined dashboard interface proposed in Chapter 5.

The development of the prototype presented in this study was influenced, but not solely determined, by prior supervisory experience with a master's dissertation (Karayiannis, 2023) that examined centralised user interfaces for smart home security. Serving as a co-supervisor in that project offered valuable insights into the design rationale and challenges encountered during its development and evaluation.

The prototype interface for the MSc prototype of a smart home security system was developed using Figma. Moreover, the prototype included several essential baseline features, such as multi-tier user roles, which include privileged, secondary, and guest, room-based device control, data and privacy panels, and a learning station aimed at educating household members about basic cybersecurity practices. Although these features addressed essential usability concerns, a thorough review of the design highlighted significant limitations that influenced the direction of our Dashboard for this research.



Figure H.1: Main menu Interface from MSc Prototype

A critical evaluation of the MSc prototype revealed several constraints that directly informed the need for a new design approach in this PhD research. The interface relied on a menu-driven navigation structure, which fragmented key security and privacy controls across separate interfaces. As shown in Figure H.1, for the MSc prototype's the main menu from illustrates a menu-driven navigation structure with a dark background. This design required multiple steps to access security and privacy features, contrasting with the harmonized Dashboard approach intended in the PhD prototype. As a result, users were required to navigate multiple layers to construct a mental model of their household's overall security posture. Additionally, the MSc prototype provided limited differentiation between types of data, such as tracking data and stored content. This lack of distinction hindered users' ability to make informed decisions about their privacy. As illustrated in Figure H.2, the data settings interface primarily centralises on controls for data consent, sharing, and backup. However, privacy policies and user rights were managed separately from these data settings, as shown in Figure H.3, where the controls were spread across different interfaces. In contrast, the PhD prototype consolidates these elements,

enabling users to view, assess and control the security and privacy information from a single view.

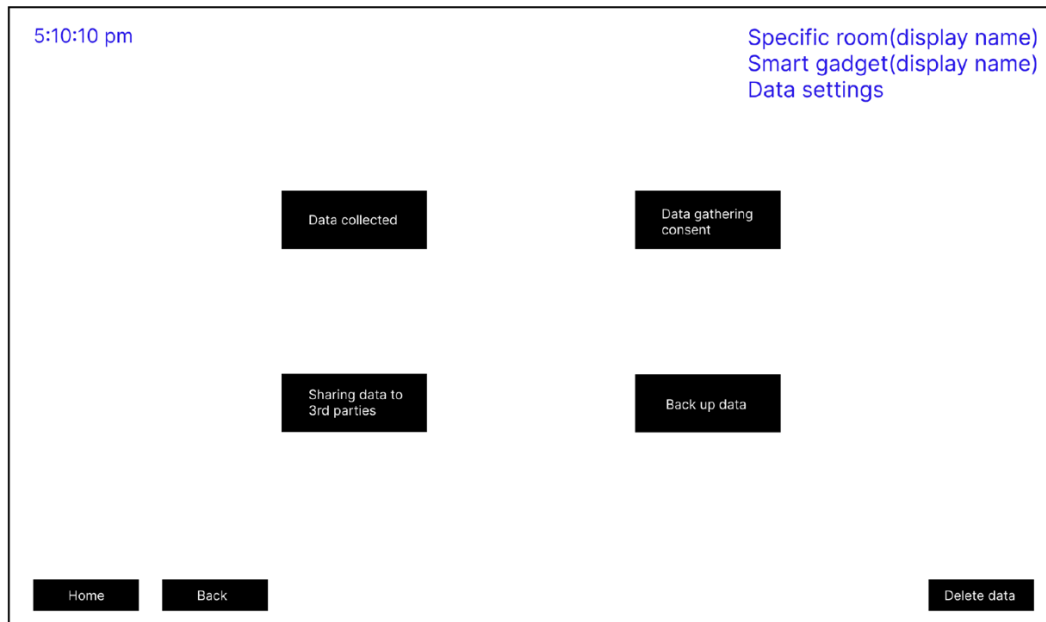


Figure H.2: Data settings Interface in the MSc Prototype

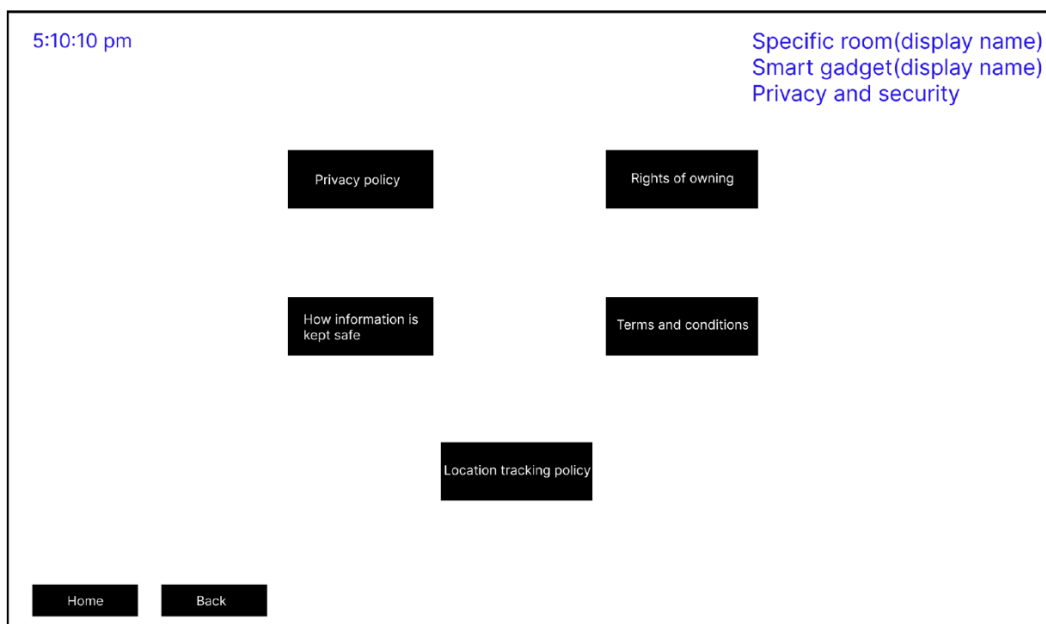


Figure H.3: Privacy and security Interface in the MSc Prototype

While the MSc project offered valuable initial insights into multi-user access control and device management, this PhD research required a more thorough and critically refined approach, given its broader scope, design priorities, and methodological ambitions.

In contrast, the PhD Dashboard was conceptualised with the explicit objective of harmonising security and privacy information across all smart home devices. By consolidating device status, data flows, and privacy controls into a single, comprehensible Dashboard, the design sought to minimise cognitive load and empower users to act confidently on security-related decisions. This shift from fragmented menus to an integrated Dashboard architecture represents a fundamental advancement in usability and supports the more ambitious research goals of this PhD study.