A Harmonised Dashboard for Smart Home Device Security

Samiah Alghamdi, Steven Furnell and Steven Bagley
University of Nottingham, UK

Samiah.alghamdi@nottingham.ac.uk
Steven.Furnell@nottingham.ac.uk
Steven.Bagley@nottingham.ac.uk

Abstract: Smart homes increasingly rely on Internet-connected devices, offering convenient services yet raising significant concerns regarding the protection of personal information. As the number and variety of devices continue to grow, users face fragmented and inconsistent security, privacy, and data-management controls across different manufacturer ecosystems. Although commercial smart home applications provide centralised access, their interfaces often lack coherent structures for managing essential protection features, making it difficult for users to locate controls, understand device status, and maintain awareness of how personal data is collected, stored, and shared. This paper presents the design and evaluation of a harmonised approach to simplify and unify the user experience, via an integrated security and privacy dashboard. The dashboard provides a unified interface for managing heterogeneous smart home devices, with core functionalities structured around Security, Privacy, and Data Management to support consistent navigation and user control. A task-based study with 16 smart-home users evaluated the dashboard against Google Home, Amazon Alexa, and Apple HomeKit applications. Participants completed scenarios involving software updates, microphone controls, reviewing and deleting voice-assistant recordings, checking camera footage, and managing location services. Performance was assessed using task completion rates, task completion time, number of clicks per task, and the System Usability Scale (SUS), alongside qualitative feedback from participants. Results showed that participants were able to complete every task using the dashboard, whereas completion rates on commercial applications were substantially lower. Tasks were completed more quickly and in fewer steps, and the dashboard achieved an "excellent" rating on the System Usability Scale. Qualitative feedback highlighted its intuitive navigation, unified structure, and clear organisation of device-related information. Overall, the findings demonstrate that a harmonised dashboard can reduce complexity, improve user control, and support informed decision-making within smart home environments, ultimately enhancing trust and security for everyday users.

Keywords: Internet of Things, Smart home, Security, Privacy, Usability

1. Introduction

Smart devices have become an integral part of everyday life, with a growing number of households adopting smart home technologies to improve convenience, efficiency, and automation. These environments typically consist of multiple interconnected Internet of Things (IoT) devices that communicate through home networks and cloud services. While such technologies provide significant benefits, they also introduce serious security and privacy challenges that are often not apparent to non-technical users.

Recent studies indicate that managing security and privacy in smart homes has become increasingly challenging due to the rapid growth and heterogeneity of interconnected IoT devices from multiple manufacturers, which rely on diverse protocols, platforms, and continuous Internet connectivity. This complex architecture often results in fragmented ecosystems, inconsistent device interactions, and unclear information presentation, making effective management difficult for end users and leading to misconfigurations and security vulnerabilities (Ahmed and Ko, 2016; Zhu et al., 2023; Vardakis et al., 2024; Magara and Zhou, 2024).

Studies have highlighted the seriousness of these issues, demonstrating that a large proportion of consumer smart devices remain vulnerable to known security threats and that sensitive data transmissions can be exposed to interception (Zhu et al., 2023). These findings emphasise the widespread vulnerabilities in smart home environments and the urgent need for enhanced, user-oriented security solutions. Moreover, integrating smart home systems with cloud services, artificial intelligence, and mobile applications introduces additional security complexities. As digital ecosystems extend beyond local networks, it is more 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).

As responsibility for managing smart home systems increasingly shifts to end users, many individuals are required to configure, monitor, and maintain the security and privacy of their connected devices without sufficient technical knowledge. Previous studies highlight that users frequently struggle to understand device configurations, data flows, and privacy implications, resulting in misconfigurations and exposure to potential cyber threats (Ahmed and Ko, 2016; Geneiatakis et al., 2017).

Although many commercial smart home applications provide centralised access to devices, their interfaces primarily focus on convenience and automation rather than on user-centred security and privacy management. Security mechanisms frequently operate invisibly in the background, and privacy controls are often buried within complex menus or distributed across multiple applications. Consequently, users tend to rely on default configurations or implicit trust in manufacturers rather than actively managing their smart home security and privacy (Shuhaiber and Mashal, 2019).

This paper addresses these challenges by focusing the design and evaluation of a user-centred interactive dashboard, explicit designed to reduce complexity, improve user control, and support informed decision-making in smart home environments. By consolidating security and privacy information from multiple devices into a single interface, the approach aims to enhance user understanding, trust, and overall smart home security.

The remainder of this paper is structured as follows. Section 2 reviews security and privacy challenges in smart home environments and discusses related vulnerabilities and existing research in this area. Section 3 presents the design of the proposed harmonised security and privacy dashboard. Section 4 describes the user evaluation methodology and reports the experimental results. Finally, Section 5 concludes the paper.

2. Security and Privacy in Smart Homes

A smart home refers to a residential environment where household devices and systems are connected to the Internet, enabling automation, remote monitoring, and intelligent control through smartphones or voice-based interfaces (Satpathy, 2006). These environments integrate heterogeneous devices communicating via technologies such as Wi-Fi, Bluetooth, and ZigBee, and often rely on cloud-based services for data processing and coordination. While such connectivity enables convenience and automation, it also introduces security and privacy risks due to the continuous exchange of data and remote access.

2.1 Security and Privacy Vulnerabilities in Smart Home Devices

Recent systematic reviews have further confirmed that smart home IoT environments remain vulnerable to multiple security threats, including unauthorised access, insecure communication channels, and weak authentication mechanisms (Ben-Nakhi, 2025; Popoola et al., 2024). Numerous vulnerabilities have been identified in IoT devices. Eavesdropping, for instance, occurs when an attacker intercepts data transmitted between devices (Mohammad et al., 2019). Moreover, IoT devices are susceptible to various attacks, such as sleep deprivation, node capture, and replay attacks (Lu and Xu, 2018). Devices remain vulnerable due to continuous Internet connectivity and automated configuration mechanisms, which often retain manufacturers' default security settings.

Several studies have documented concrete security and privacy vulnerabilities in consumer smart home devices. Smart speakers have been reported to suffer from several security and privacy vulnerabilities, including continuous listening, unauthorised recording, and weak speech authentication mechanisms (Jackson and Orebaugh, 2018). Research on adversarial voice attacks has further demonstrated that attackers can inject inaudible commands without the user's knowledge, enabling covert device manipulation (Carlini et al., 2016; Zhang et al., 2017). Similar concerns have been identified in smart cameras and video doorbells. Prior work shows that weak authentication, insecure configuration management, and exposed network services can lead to the leakage of sensitive audio and video data (Bugeja et al., 2018).

Beyond vulnerabilities in individual devices, security and privacy risks also emerge at the ecosystem level. Studies have shown that many IoT applications are overprivileged, granting excessive permissions that unnecessarily expand the attack surface (Fernandes et al., 2017). Additionally, insecure over-the-air firmware update mechanisms and voice-based interfaces introduce further attack vectors, enabling hackers to manipulate device behaviour or inject malicious commands (Meng et al., 2018).

2.2 Privacy Concerns in Smart Homes

Privacy in smart home environments refers to users' ability to understand and control how personal data is collected, processed, and shared by connected devices and services (Kotz et al., 2009). Unlike traditional computing environments, smart homes operate through continuous data collection, capturing fine-grained information about users' behaviours, routines, and interactions within private living spaces.

Prior research has shown that privacy risks extend beyond direct data disclosure. Even encrypted or metadata-only network traffic can be analysed to infer sensitive information, including occupancy patterns, daily routines, and individual activities (Apthorpe et al., 2017). As a result, privacy threats in smart home environments often arise through indirect behavioural inference rather than explicit data breaches.

In addition to these technical risks, recent studies highlight that users remain concerned about how personal data collected by smart home devices is stored, processed, and shared with third parties (Magara and Zhou, 2024; Haney et al., 2025).

Although numerous technical solutions for privacy protection have been proposed, human–computer interaction studies consistently demonstrate that users struggle to understand data flows and privacy implications in smart home ecosystems. Users frequently prioritise convenience over privacy, rely on default configurations, and lack awareness of how their data is collected and used (Emami-Naeini et al., 2019). This gap highlights a mismatch between existing privacy mechanisms and users' practical ability to manage them effectively.

2.3 Related Work and Existing Solutions

Existing research on smart home security and privacy has examined both backend enforcement mechanisms and user-facing tools. Backend-oriented solutions, such as ProvThings (Wang et al., 2018) and SmartAuth (Tian et al., 2017), focus on detecting malicious behaviour and misconfigurations within IoT ecosystems. While these approaches are effective at a technical level, they are primarily designed for developers and system administrators, offering limited visibility or control for end users.

More recent work has shifted attention toward user-facing interfaces, introducing interactive dashboards to improve user awareness of device activity and data sharing. Systems such as SaferHome (Windl et al., 2022) and Peekaboo (Jin et al., 2022) visualise aspects of smart home behaviour, helping users understand where and how data is processed and transmitted. However, these solutions typically address specific dimensions of security or privacy and do not support unified management across heterogeneous devices.

Commercial platforms, including Google Home, Amazon Alexa, and Apple HomeKit, provide centralised device control but operate within closed ecosystems. As a result, they offer limited transparency into permissions, data flows, and security configurations. Users are often required to manage security and privacy settings across multiple fragmented interfaces, which increases cognitive load and raises the risk of misconfiguration (Geneiatakis et al., 2017).

In addition to commercial platforms, several open-source smart home frameworks have been developed, such as Home Assistant (Home Assistant, 2024) 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. However, their interfaces primarily focus on automation and device control rather than structured security and privacy management, which can make it difficult for non-technical users to understand and manage protection settings effectively.

Overall, prior work demonstrates significant progress in addressing smart home security and privacy challenges. Nevertheless, existing solutions remain fragmented, frequently separating security from privacy and prioritising backend protection over user-centred interaction. This gap highlights the need for unified and accessible interfaces that better support user awareness, understanding, and effective security and privacy management across diverse smart home devices.

3. Designing a Harmonised Security and Privacy Dashboard

The proposed dashboard is designed to address the fragmentation and complexity of security, privacy, and data management in current smart home environments. To achieve this, an effective all-in-one smart home solution should integrate key capabilities, including improved visibility of device status, integrated management of security and privacy settings, and greater transparency in data management.

The design requirements for the proposed dashboard were informed by prior analysis conducted by the authors (Alghamdi et al., 2024), alongside established usability and human–computer interaction principles. These insights were used to identify key usability challenges and user needs in smart home environments.

Based on these insights, the design of the proposed dashboard is guided by the following requirements:

- **Unified Interface**: Provide a dashboard to manage security, privacy, and data across all devices.
- **Consolidated Controls:** Combine related settings such as device status, permissions, and updates into a single clear view to reduce complexity.

- **Real-Time Status and Alerts:** Display live device status using clear indicators and timely notifications.
- **Unified Data Management:** Standardize data actions such as viewing, deleting, and scheduling deletion across devices.
- **Data Categorisation:** Clearly distinguish between different data types, including tracking data and stored content.
- **Role-Based Access Control:** Support multiple user roles, including admin, adult, child, and guest, with appropriate permissions.
- **Cross-Device Compatibility**: Enable seamless control of a wide range of smart home devices within a single platform.

The Dashboard is designed to provide users with an efficient means to determine 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 1. The design is tailored to enhance user experience, providing them with the necessary information in a clear, concise, and intuitive manner.

In a comprehensive analysis of various devices, key features were grouped into three main categories. These categories are derived from prior analysis conducted by the authors (Alghamdi et al., 2024), which examined security, privacy, and data management features across smart home devices, highlighting variations in how they are presented across different platforms. The Security category encompasses registration, authorisation, authentication, and security updates, which are essential for safeguarding user data. Privacy encompasses microphone access, location services, camera use, and usage habits, all of which are essential to protecting user privacy. Data Management comprises deleting specific or all recordings, scheduled deletions, and usage history, all of which are important for effectively managing user data.

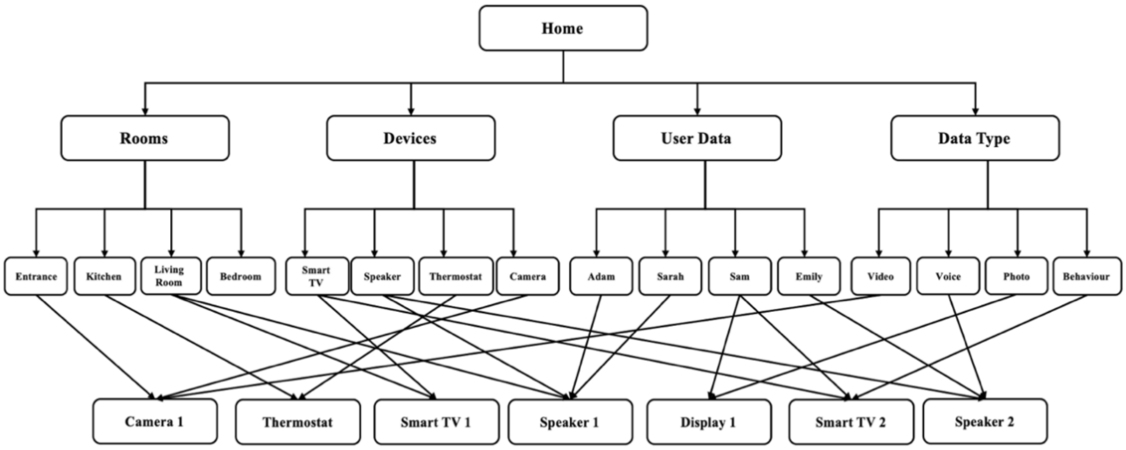


Figure 1: Dashboard Navigational Structure

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 well-established framework for assessing user interface quality and supporting both novice and expert users. Most principles, including visibility of system status, match between the system and the real world, consistency and standards, user control and freedom, recognition rather than recall, aesthetic and minimalist design, and error prevention, were fully implemented. Advanced flexibility and detailed error recovery mechanisms were partially addressed due to the scope and fidelity of the prototype.

In addition to general usability principles, Human Computer Interaction for Security (HCISec) guidelines were incorporated to address challenges specific to security-oriented systems. These principles emphasise clear visibility of security status, the use of minimal technical jargon, and support for informed user decision-making. Prior research highlights the importance of these factors in security dashboards, particularly in helping users understand risks and manage protective controls effectively (Ibrahim et al., 2010).

4. An Overview of the Dashboard Prototype

The initial dashboard interface, shown in Figure 2, provides a clear and structured overview that enables users to manage smart home devices from multiple perspectives. The interface is organised around four main categories: Rooms**,** Devices**,** User Data, and Data Types, which reflect users' primary concerns when managing a smart home. In addition, a set of core navigation icons on the left of the screen support system management, providing access to the home view, informational guidance, device health status, household members, software update, device management, and system settings. Together, they enable users to monitor device status, manage permissions, receive alerts, and configure preferences through a consistent and easily accessible structure.

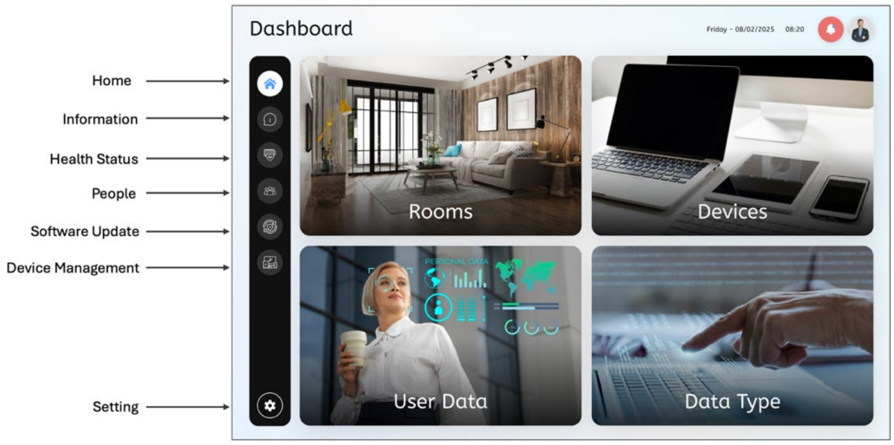
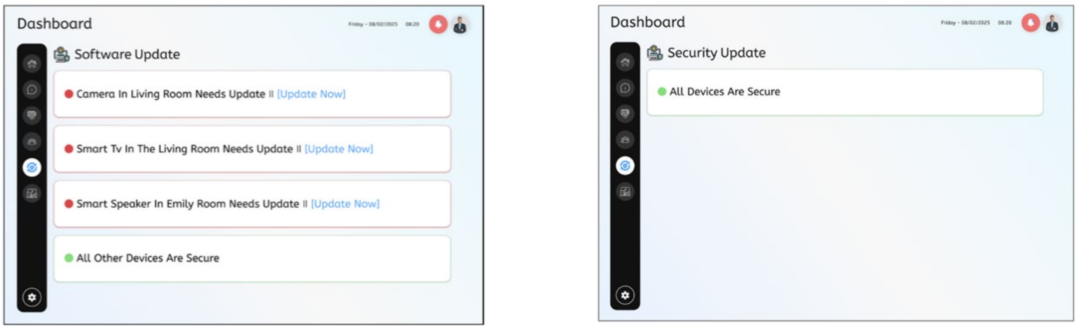


Figure 2: Home Interface

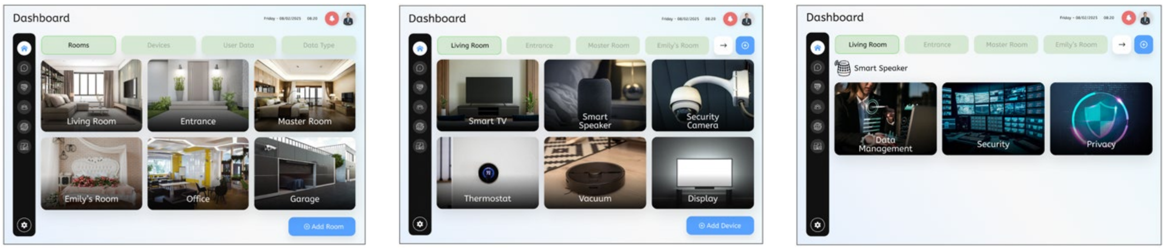
Figure 3 presents the software update interfaces, which provides an overview of update status across all connected smart home devices. Figure 3(a) highlights devices requiring immediate updates using red status indicators and provides an "Update Now" option to support prompt user action. In contrast, Figure 3(b) is displayed when all devices are fully updated, showing a single green status message. This conditional presentation ensures that users are shown only relevant information, reducing cognitive load and enabling efficient identification and resolution of security updates.



(a) (b)

Figure 3: Software Update Interfaces

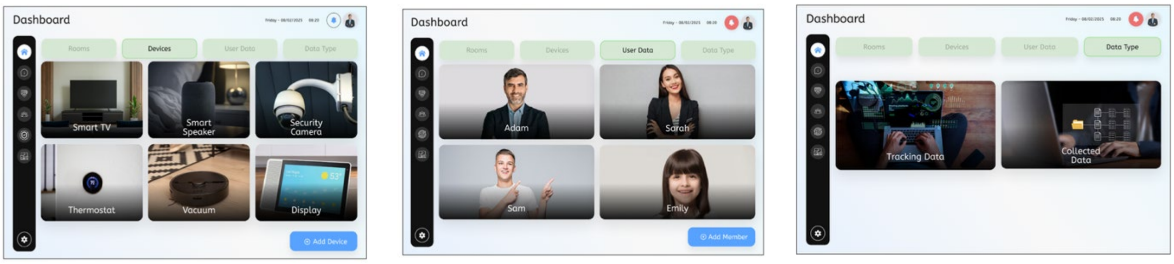
As illustrated in Figure 2, the Dashboard offers several routes by which users can explore their smart home configuration, namely via Rooms, Devices, Users, and Data Types. Each then offers a means to drill down to individual security and privacy settings. As an example, the Rooms view enables users to manage devices and privacy settings based on physical location within the home. As illustrated in Figure 4, users can navigate from a top-level overview of all rooms (4a), via devices in the room (4b), to a specific device within a selected room (4c), from which users can access device-specific Security, Privacy, and Data Management controls.



(a) (b) (c)

Figure 4: Rooms Interfaces route, showing: (a) rooms; (b) devices within a room; (c) settings on a device

Each of the other routes also expands in a similar manner. Space constraints prevent a full depiction of each route, but Figure 5 provides an illustration of the next level down within each one.

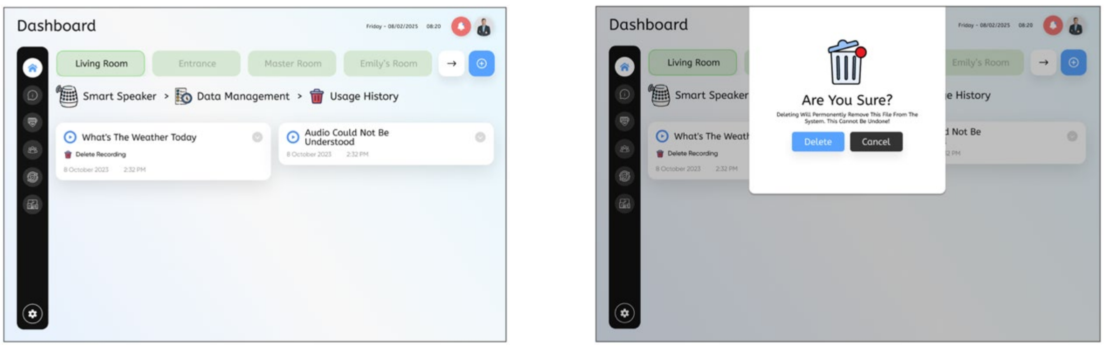


(a) (b) (c)

Figure 5: Alternative navigation routes, showing: (a) by device type; (b) by user type; (c) by data type

5. User Evaluation

A task-based user study was conducted to compare the user experience of the dashboard against three commercial platforms: Google Home, Amazon Alexa, and Apple HomeKit. These platforms were selected for comparison because they represent the three most widely adopted commercial smart home ecosystems. They support a broad range of consumer IoT devices and are commonly used to manage smart home environments through mobile applications. Evaluating the proposed dashboard against these platforms provides a realistic benchmark and enables comparison with interfaces that users are most likely to encounter in real-world smart home deployments. The evaluation aimed to assess how efficiently and effectively users could complete common security and privacy tasks, as well as their overall satisfaction with each platform, using a combination of quantitative performance metrics and qualitative feedback. Five scenarios were selected for the main evaluation, representing critical and common security and privacy interactions in smart home environments: Checking software updates; Managing smart speaker recordings; Muting microphones during meetings; Turning off location services across devices; and Reviewing security camera recordings. A set of task-specific interfaces were designed to reflect the interactions experienced by participants. The software update functionality was provided through the interface presented earlier in Figure 3. Figure 6 presents representative examples of the remaining interfaces used in the evaluation.



(a) (b)

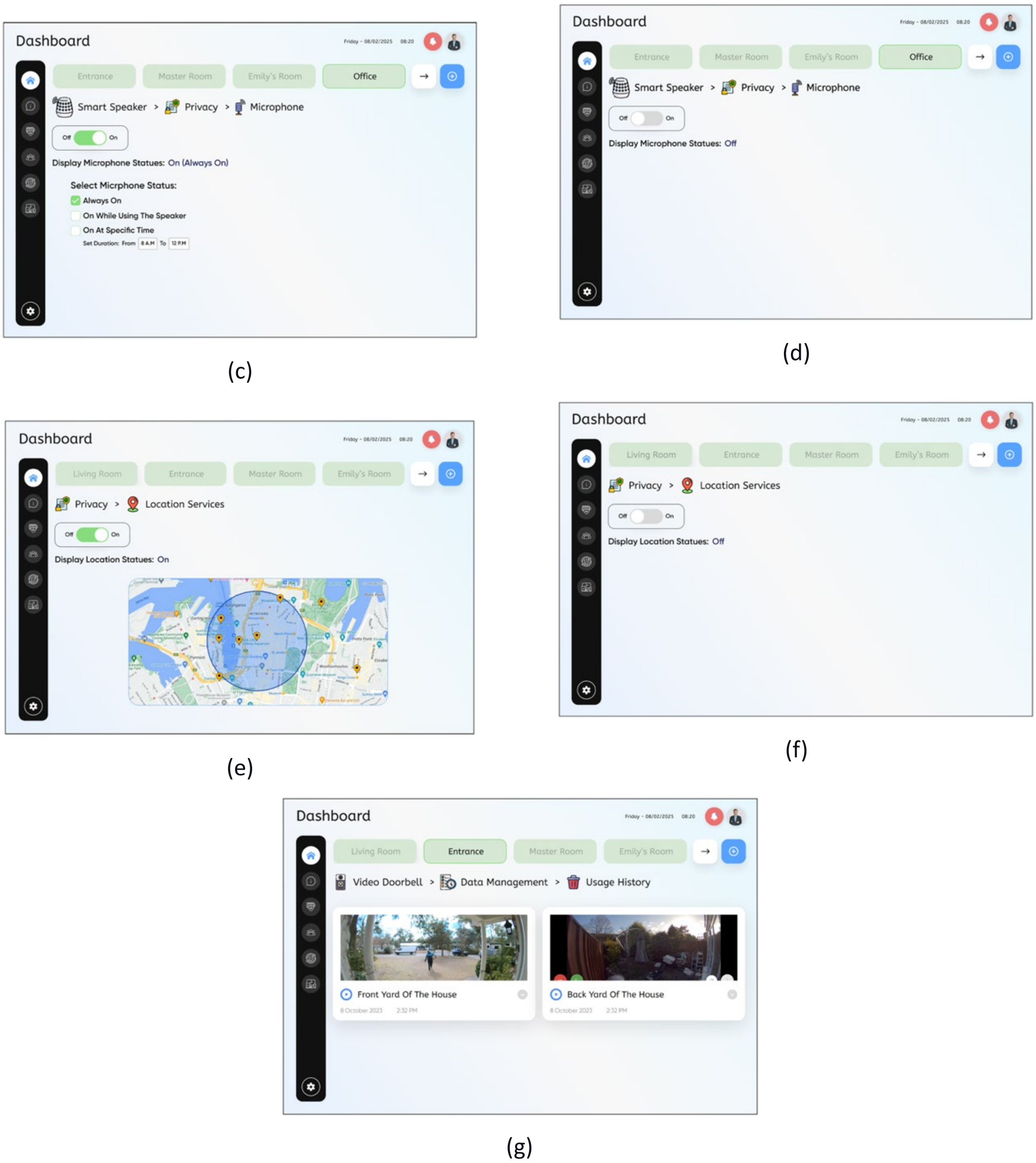


Figure 6: Task-based interfaces used during the evaluation: (a–b) managing smart speaker recordings; (c–d) muting microphones; (e–f) turning off location services; and (g) reviewing security camera recordings

A total of 16 participants took part in the study. This sample size aligns with established usability evaluation guidelines, which indicate that 12–20 participants are sufficient to identify most usability issues and derive meaningful insights (Nielsen, 1994; Virzi, 1992). All participants owned at least two smart home devices and had sufficient English proficiency to understand task instructions and complete post-task questionnaires. Participants represented a range of digital literacy levels and backgrounds, reflecting a realistic smart home user population.

To ensure realism, real smart home devices, including smart speakers and security cameras, were configured and connected to their respective platforms. Devices were preloaded with realistic data, such as voice recordings, video recordings, and privacy-related settings. All tasks were performed on the same tablet device to maintain consistent experimental conditions. Participants completed the same set of tasks on each platform. The order of platform exposure was counterbalanced to reduce learning and order effects. During task execution, task completion time, number of clicks, and task success were recorded. After completing the tasks on each platform, participants completed the System Usability Scale (SUS) questionnaire and provided qualitative feedback.

Efficiency is important for evaluating how easily and quickly users can complete tasks on different platforms and was assessed using task completion time and the number of clicks required per task.

- **Task completion time**: Figure 7(a) shows the dashboard achieving the fastest mean task completion time (33 seconds). Amazon consistently exhibited the slowest performance and the greatest variability, indicating less predictable task flows. Google and Apple had moderate performance but still required more time than the dashboard.
- **Clicks per task:** A similar pattern is observed in Figure 7(b), which presents the mean number of clicks per task. The dashboard required fewer interactions than other platforms, reflecting a more streamlined and direct interaction design. In contrast, Google and Amazon required the highest number of clicks, suggesting more fragmented navigation paths, while Apple occupied an intermediate position.

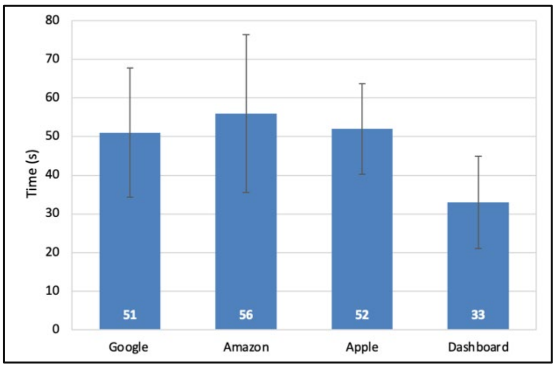
Overall, these results demonstrate that the dashboard supports more efficient task execution than Google, Amazon, and Apple by reducing both completion time and interaction effort.

Effectiveness was measured using task completion rates. Figure 7(c) shows that all participants successfully completed all tasks using the dashboard. In contrast, task failures were observed on all other platforms. Among these, Google achieved higher completion rates than Amazon and Apple, although with noticeable variability. Amazon exhibited the lowest and most inconsistent success rates, particularly for privacy-related tasks, while Apple showed more stable but generally lower completion rates. These findings indicate that, unlike the dashboard, existing platforms do not consistently support successful task completion across users.

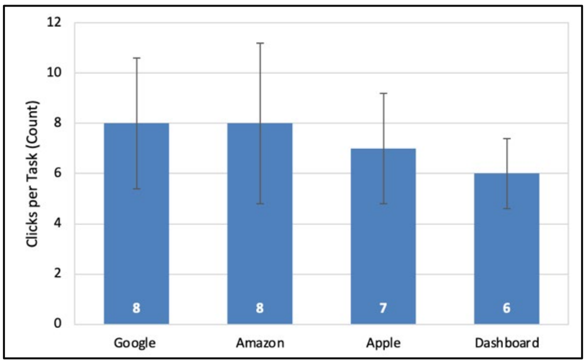
Finally, user satisfaction was evaluated using the System Usability Scale (SUS). As illustrated in Figure 7(d), the dashboard demonstrates the highest perceived usability, with a mean SUS score of 86, clearly outperforming Google, Amazon, and Apple. Amazon received the lowest usability ratings and the highest variability, indicating inconsistent user experiences. Google and Apple achieved moderate scores, with Apple showing more consistency but lower overall usability.

Qualitative feedback highlighted the dashboard’s intuitive navigation, unified structure, and clarity of security and privacy controls. Participants frequently described the dashboard as “easy,” “straightforward,” and “clear,” emphasising the benefit of managing all devices and data in a single interface. Many participants stated they would recommend the dashboard to others, including non-technical users. In contrast, Google, Amazon, and Apple were commonly described as confusing or overly complex, with privacy settings distributed across multiple menus. Several participants reported giving up on some tasks when using commercial platforms, particularly those involving recordings or privacy controls.

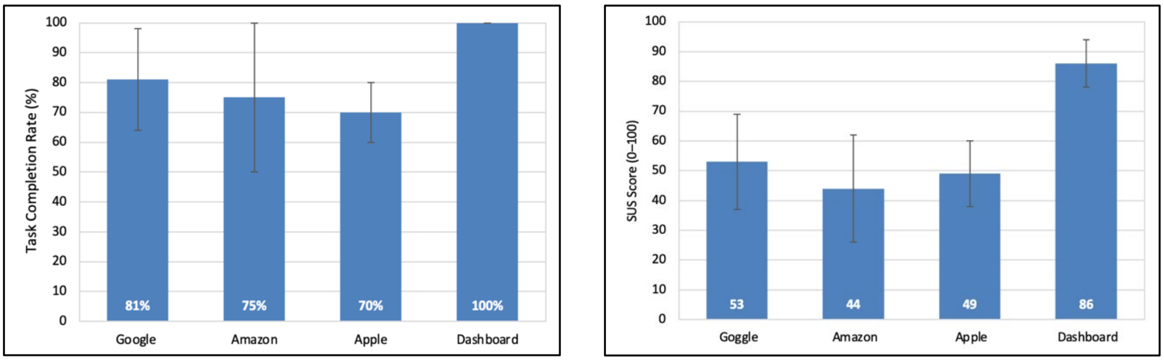
The task failures observed in these platforms appear to be largely associated with fragmented interface structures and the distribution of security and privacy settings across multiple layers of the interface. Participants frequently reported difficulty locating specific privacy controls, such as voice recording management or location permissions, which were often buried several levels within the interface hierarchy. By contrast, the proposed dashboard consolidates these functions within clearly labelled categories. This structure reduces navigation complexity and helps users more easily locate key security and privacy controls.



(a) mean task completion time



(b) mean number of clicks per task



(c) task completion rate

(d) System Usability Scale (SUS) scores

Figure 7: Efficiency, effectiveness, and satisfaction results by platform. Error bars represent standard deviation

6. Conclusion

This paper presented the design and evaluation of a harmonised dashboard for managing security and privacy in smart home environments. As smart homes increasingly consist of heterogeneous devices operating across multiple ecosystems, users are often required to manage complex security and privacy settings through fragmented and inconsistent interfaces. This work addressed these challenges by proposing a unified, user-centred dashboard that integrates security, privacy, and data management controls across devices.

A task-based user evaluation compared the proposed dashboard with three widely used commercial platforms, with the results demonstrating clear advantages of the dashboard across all evaluated dimensions. Participants completed tasks more efficiently, required fewer interactions, and achieved higher task success rates when using the dashboard. Notably, all participants successfully completed all tasks on the dashboard, while failures were observed on the commercial platforms, particularly for privacy-related scenarios. User satisfaction results further reinforced these findings. The dashboard achieved the highest SUS scores with low variability, indicating strong perceived usability and consistent user agreement. Qualitative feedback highlighted the dashboard's intuitive navigation, unified structure, and ability to support confident and informed decision-making. In contrast, other platforms were frequently described as complex, fragmented, and difficult to navigate.

Overall, the findings demonstrate that a harmonised, user-centred dashboard can substantially improve how users manage smart home security and privacy. By reducing complexity and providing consistent access to critical controls, the proposed approach supports more efficient, effective, and satisfying user interactions. This work highlights the importance of integrating usability considerations into the design of security-critical systems and provides a strong foundation for future research into scalable deployment and long-term use of unified smart home management interfaces.

Ethics Declaration: The study was approved by the School of Computer Science Research Ethics Committee [CS-2024-R21]. Data was collected anonymously and participants were informed that they could withdraw at any time.

AI Declaration: No AI tools were used in this paper.

References

Ahmed, F. and Ko, Y.B. (2016) "Mitigation of black hole attacks in routing protocol for low power and lossy networks", *Security and Communication Networks*, 9(18), pp. 5143–5154.

Alghamdi, S., Furnell, S. and Bagley, S. (2024) "Towards a harmonised approach for security and privacy management in smart home contexts", in *International Conference on Human–Computer Interaction*. Cham: Springer Nature Switzerland, pp. 170–187.

Apthorpe, N., Reisman, D. and Feamster, N. (2017) "A smart home is no castle: Privacy vulnerabilities of encrypted IoT traffic", *arXiv preprint*, arXiv:1705.06805.

Ben-Nakhi, A.A., Abd El-barr, M. and Qureshi, K.U. (2025) "Systematic literature review: Security challenges of IoT-based smart home systems", *Indonesian Journal of Electrical Engineering and Informatics*, 13(1), pp. 277–293.

Brooke, J. (1996) "SUS: A quick and dirty usability scale", in *Usability Evaluation in Industry*. London: Taylor & Francis, pp. 189–194.

Bugeja, J., Jönsson, D. and Jacobsson, A. (2018) "An investigation of vulnerabilities in smart connected cameras", in *European Intelligence and Security Informatics Conference*, pp. 172–175.

Carlini, N. et al. (2016) "Hidden voice commands", in *USENIX Security Symposium*.

Emami-Naeini, P. et al. (2019) "Exploring how privacy and security factor into IoT device purchase behavior", in *CHI Conference on Human Factors in Computing Systems*.

Fernandes, E., Rahmati, A. and Jung, J. (2017) "Security implications of permission models in smart-home application frameworks", *IEEE Security & Privacy*, 15(2), pp. 24–30.

Geneiatakis, D. et al. (2017) "Security and privacy issues for an IoT-based smart home", in *International Convention on Information and Communication Technology*, pp. 1292–1297.

Haney, J. et al. (2025) "Smart home users' security and privacy perceptions and actions differ by device category", *NIST Technical Report*.

Home Assistant (2024) "Home Assistant: Open-source home automation platform". Available at: https://www.home-assistant.io (Accessed: 15 October 2025).

Ibrahim, T. et al. (2010) "Assessing the usability of end-user security software", *Lecture Notes in Computer Science*, 6264, pp. 177–189.

Jackson, C. and 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).

Jin, H. et al. (2022) "Peekaboo: A hub-based approach to enable transparency in data processing within smart homes", *arXiv preprint*, arXiv:2204.04540.

Kalbo, N. et al. (2020) "The security of IP-based video surveillance systems", *Sensors*, 20(17).

Kotz, D., Avancha, S. and Baxi, A. (2009) "A privacy framework for mobile health and home-care systems", in *ACM Conference on Computer and Communications Security*, pp. 1–12.

Lu, Y. and Xu, L. (2018) "Internet of things cybersecurity research: A review", *IEEE Internet of Things Journal*.

Magara, T. and Zhou, Y. (2024) "Security and privacy concerns in the adoption of IoT smart homes: A user-centric analysis", *American Journal of Information Science and Technology*.

Meng, Y. et al. (2018) "Securing consumer IoT in the smart home", *IEEE Communications Magazine*, 25(6), pp. 53–59.

Mohammad, Z., Qattam, T. and Saleh, K. (2019) "Security weaknesses and attacks on IoT applications", in *IEEE Conference on Future Technologies*.

Nielsen, J. (1994) "10 usability heuristics for user interface design", in *Usability Engineering*. San Diego: Academic Press.

OpenHAB (2024) "OpenHAB: Empowering the smart home". Available at: https://www.openhab.org (Accessed: 15 October 2025).

Popoola, O. et al. (2024) "A critical literature review of security and privacy in smart home healthcare schemes adopting IoT and blockchain: Problems, challenges and solutions", *Blockchain: Research and Applications*, 5(2), 100178.

Satpathy, L. (2006) *Smart housing: Technology to aid aging in place*. Mississippi State University.

Shuhaiber, A. and Mashal, I. (2019) "Understanding users' acceptance of smart homes", *Technology in Society*, 58.

Tian, Y. et al. (2017) "SmartAuth: User-centered authorization for the internet of things", in *USENIX Security Symposium*, pp. 361–378.

Vardakis, G. et al. (2024) "Review of smart-home security using the internet of things", *Electronics*, 13(16), 3343.

Virzi, R.A. (1992) "Refining the test phase of usability evaluation", *Human Factors*, 34(4), pp. 457–468.

Wang, Q. et al. (2018) "Fear and logging in the internet of things", in *Network and Distributed System Security Symposium*.

Windl, M. et al. (2022) "SaferHome: Interactive smart home dashboards for communicating privacy assessments", *Proceedings of the ACM on Human-Computer Interaction*, 6.

Zhang, G. et al. (2017) "DolphinAttack: Inaudible voice commands", in *ACM Conference on Computer and Communications Security*.

Zhu, J. et al. (2023) "Smart home security challenges", *IEEE Access*.