Enabling Collaborative Anomaly Exploration in Smart Homes: Eliciting User Requirements and Security Scenarios

AZHAR A. ALSUFYANI, Cardiff University, UK
OMER RANA, Cardiff University, UK
CHARITH PERERA, Cardiff University, UK

Smart-home technologies are becoming increasingly pervasive, automating lighting, heating, security, and other vital household functions to enhance the comfort, efficiency, and convenience of residents. However, the growing complexity and interconnectivity of these systems expose them to advanced cyber threats, putting residents' privacy and safety at risk. In this study, we investigated the design of future smart home environments to support collaborative anomaly exploration, enabling occupants and devices to jointly identify and address emerging threats. Using a mixed-methods approach—an initial questionnaire (N=40) followed by interactive focus groups (N=36)—we gathered in-depth perspectives on smart home device configurations, user workflows, and potential security vulnerabilities. Our findings include: (i) a taxonomy of realistic security threats, (ii) illustrative layouts and scenarios that highlight how anomalies emerge in everyday household routines, and (iii) concrete examples of how these anomalies can be detected collaboratively. Building on these insights, we propose a comprehensive set of design criteria to guide the development of user-centered, resilient anomaly exploration capabilities in smart homes. Our results offer recommendations for researchers, system designers, and technology practitioners seeking to balance the benefits of automation with robust user-driven security in next-generation ubiquitous home environments.

CCS Concepts: • **Human-centered computing → Empirical studies in ubiquitous and mobile computing**; • **Security and privacy → Human and societal aspects of security and privacy**.

Additional Key Words and Phrases: Collaborative anomaly exploration, Smart homes, user-centered design, IoT security

1 INTRODUCTION

Internet of Things (IoT) systems are projected to experience both significant impacts and widespread adoption in the coming years, with forecasts indicating substantial market revenue growth between 2020 and 2030 [5]. Among the most prominent domains benefiting from this surge is the *smart home* sector, in which multiple automated devices and appliances—covering aspects such as lighting, temperature control, security, and voice assistance—are centrally connected and remotely accessible via the Internet [1]. These smart home environments promise residents greater comfort, efficiency, and convenience, while also exemplifying the broader shift toward pervasive and autonomous IoT-based solutions.

However, the interconnectivity that underpins these benefits substantially broadens the potential attack surface [39]. As homes integrate diverse, networked components into a single ecosystem, sophisticated vulnerabilities can emerge, ranging from malicious cyberattacks and operational failures to social engineering exploitation. Although smart-home architectures are intended to detect and mitigate risks to residents' safety [25], the *high degree of automation* poses new challenges: systems must not only recognize unusual events but also adapt their defenses in real time and clearly communicate with occupants. This underscores the importance of *collaborative anomaly exploration* in which human occupants, networked devices, and automated systems work together to jointly identify, interpret, and respond to anomalies in situ (see Section 3). Smart homes are increasingly targeted by a range of security breaches. For example, recent studies have shown that attackers can exploit firmware vulnerabilities to gain unauthorized control over smart devices, whereas others have demonstrated how physical security can be undermined through wireless attacks targeting Wi-Fi and Zigbee protocols [9, 12]. These real-world breaches underscore the urgency for robust and adaptive security frameworks.

Authors' addresses: Azhar A. Alsufyani, Cardiff University, School of Computer Science and Informatics, Cardiff, CF24 4AX, UK, alsufyaniaa@cardiff.ac.uk; Omer Rana, Cardiff University, School of Computer Science and Informatics, Cardiff, CF24 4AX, UK, ranaof@cardiff.ac.uk; Charith Perera, Cardiff University, School of Computer Science and Informatics, Cardiff, CF24 4AX, UK, pererac@cardiff.ac.uk.

Research Questions. In light of these challenges, our study investigates the design and deployment of **collaborative anomaly exploration** approaches that emphasize user-centric and device-integrated strategies for detecting and interpreting unusual events in smart homes. Specifically, we addressed the following research questions:

- **RQ1:** *How can we characterize the landscape of future smart homes (including devices, configurations, and occupant interactions) in ways that reveal potential points of anomalous or malicious behavior?*
- **RQ2:** *What categories of anomalies and security threats are likely to arise in these evolving smart-home ecosystems, and how might users and systems collaboratively identify and analyze them in situ?*
- **RQ3:** *Which design principles and use-case scenarios can guide the development of next-generation smart-home solutions, enabling occupants and devices to jointly explore and respond to anomalies for improved security, privacy, and trust?*

These research questions place a central focus on the *collaborative* dimension of smart-home anomaly handling, moving beyond traditional detection algorithms to examine how users, their devices, and the broader infrastructure can collectively contribute to proactive threat detection and resolution.

Contributions. Building on a mixed-method empirical study consisting of surveys and in-depth focus group sessions, this study makes the following key contributions.

(1) **Taxonomy of Future Smart-Home Anomalies:** We propose a refined classification of potential security threats, vulnerabilities, and anomaly types based on realistic device setups and user practices. This taxonomy is informed by the participants insights into the day-to-day operation of interconnected home environments.
(2) **Collaborative Anomaly Exploration Framework:** We introduce a novel framework that underscores how occupants and smart devices can jointly detect, interpret, and manage anomalous behaviors. This framework incorporates technical and user-facing considerations to foster adaptive and transparent security responses.
(3) **Scenario-Driven Design Guidelines:** Through synthesis of user feedback and simulated scenarios, we discuss actionable guidelines that inform the design of future smart home systems. These guidelines emphasize user engagement, system interoperability, and privacy-preserving strategies to enhance occupant trust and situational awareness.
(4) **Empirical Insights for Next-Generation Smart Homes:** We offer evidence-based recommendations for researchers, technologists, and practitioners of ubiquitous computing. Our findings demonstrate that smart-home architectures can balance automation with user-driven oversight, thereby advancing secure, resilient, and occupant-friendly IoT ecosystems.

Organization. The remainder of this paper is organized as follows. In Section 2, we provide a detailed overview of related literature, examining prior work on smart-home security, user-centered IoT research, and anomaly management. The definition of anomaly exploration is provided in Section 3. Section 4 presents the mixed-methods research design and data collection procedures. In Section 5, we describe the system architecture that emerged from our findings, define its role in collaborative anomaly exploration, and evaluate the proposed approach through scenario-based analyses and participant feedback. We then synthesize the broader implications of our results in 6, and offer concluding remarks in Section 7.

2 RELATED WORK

In this section, we focus on the broader research landscape by examining three key areas: (1) research on smart-home systems and their configurations; (2) existing efforts to identify and address anomalies within smart home environments; and (3) previous elicitation studies in computing and security contexts. Table 1 provides an overview of prior studies outlining their methods, data collection techniques, and analytical approaches.

2.1 Smart-Home Security and Privacy Systems

A significant area of research concentrates on the types of devices, configurations, and user practices that characterize smart homes. Alsufyani et al. [10] empirically documented common appliances and sensors already integrated into contemporary residences, whereas Krishna et al. [51] proposed simulations of centralized components, such as thermostats, security systems, and HVAC controls. Choi et al. [20] conducted user experiments with multiple product categories, ranging from desk lamps to window fixtures, and revealed how various device classes can introduce diverse avenues for threat exploitation. Xiao et al. [94] illustrated cross-manufacturer interoperability by assembling popular off-the-shelf products into a cohesive, testable environment, and Fu et al. [35] leveraged real-world test beds to evaluate anomaly detection algorithms.

These investigations confirm the complexity and heterogeneity of smart home ecosystems. Yet they often concentrate on specific device-level integrations or sensor fusion algorithms without deeply examining the *collaborative* dimension of anomaly handling. Our work bridges this gap by integrating user participation, security requirements, and context-aware device cooperation into a unified framework—one that actively involves occupants in the interpretation and resolution of anomalous events.

2.2 Anomaly Detection Techniques

A growing body of work addresses anomaly detection and analysis in smart-home environments. *HomeGuardian* [26] proposed a context-aware methodology to identify irregularities beyond simple rule-based triggers with the aim of enhancing overall security monitoring. Similarly, Fu et al. [35] developed an anomaly detection technique that synthesizes app-level events, sensor streams, and user behavioral patterns, thereby generating hypotheses on abnormal activities via the cross-correlation of multi-source data. Demetriou et al. [29] introduced a distributed control mechanism, wherein a phone-based monitor application sets access rights and a router-side controller enforces communication privileges for IoT devices in the home network. De Melo et al. [27] proposed a one-class classifier approach for classifying suspicious traffic flows in smart homes, illustrating how machine learning (ML)can detect potentially malicious activities in real time. In [19], AutoIoT leveraged large language models (LLMs) to automate the creation of IoT automation rules. By extracting device information and generating rules through LLMs, the platform can detect and resolve conflicts in automation, thereby preventing anomalous behaviors caused by conflicting commands. King et al. addressed potential anomalies in device behavior, ensuring that system responses aligned with user expectations and contributed to a secure smart-home environment.[50]. The authors of [77] examined the integration of LLMs with IoT devices, highlighting their role in enhancing functionalities such as predictive maintenance and anomaly detection.

Together, these studies underscore the necessity of *adaptive anomaly exploration* strategies that assimilate contexts from heterogeneous sources. However, most current methods focus on backend or automated systems rather than explicitly involving the end-user in understanding and responding to anomalies. Our work advances this perspective by emphasizing *collaborative* methods, in which occupants and devices jointly manage anomalies.

2.3 Elicitation Studies

Research on ubiquitous computing and human-centered security has frequently employed *elicitation* techniques to capture user experiences, privacy concerns, and interactions with emerging technologies. For instance, Naeini et al. [64] illustrated how varying contexts of IoT data collection can shape individuals' willingness to share personal information, whereas Emami et al. [33] highlighted the role of expert opinions in guiding users' privacy decision-making. Ahmed et al. [4] showed that people tend to disclose more information when robust access control mechanisms are in place, an insight similarly echoed by Wong et al. [92], who used design workbooks to prompt participants to reflect on their values, ethics, and privacy. Researchers have noted that user groups may differ in their privacy concerns, preferences, and expectations regarding audio recording [32].

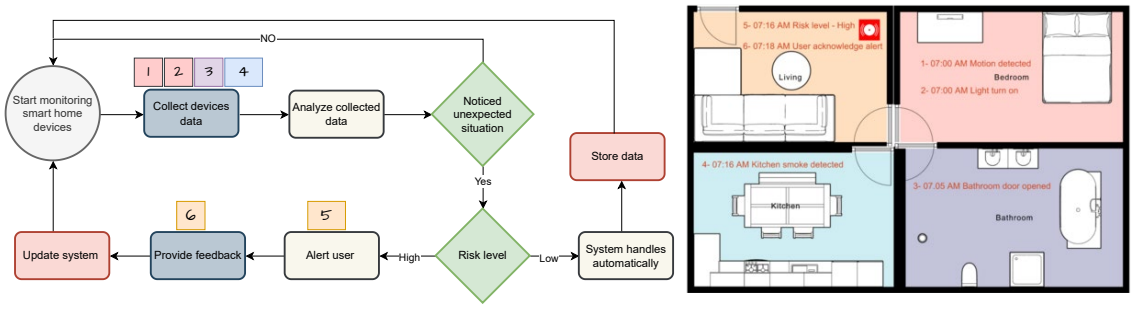
Table 1. Overview of representative related works.

	Participants	Recruitment	Duration	Data Collection	Analysis Method	Methodology	Materials
Haliburton et al. [38]	Online questionnaire (91), interviews (6)	Online questionnaire	45 min	Questionnaire responses, interviews	Quantitative analysis; qualitative coding (Atlas.ti)	Mixed-method: online questionnaire + interviews	Online questionnaire; design fictions + sketches
Rajaram et al. [73]	16	Email	1.5 hrs	Recorded sessions, notes, thematic analysis	Thematic analysis; consensus-distinct ratio; timeline visualization	Elicitation study with paired experts	Scenario prompts; design dimensions
Ng et al. [67]	24	Univ. participant pool + snowball sampling	45 min	Observations, video recordings, post-study interviews	Thematic analysis; subjective ratings	Gesture elicitation for co-located mobile gaming	Pre-/post-study questionnaires
Wong et al. [92]	10	Recruited for tech expertise/training	1 hr	Demographic questionnaire, interviews	Privacy analytic framework [63]	Workbooks to encourage values reflection	Design workbooks
Dunbar et al. [32]	Interviews (32), design session (19)	Social media, email lists, special-interest groups	85–90 min (design session)	Semi-structured interviews, focus groups, design workshops	Inductive-deductive coding [23]; thematic analysis [78]	Interviews, focus groups, design workshops	Scenario cards, parameter cards
Abtahi et al. [2]	24	Institution + adjacent companies	45 min	Post-task interviews, questionnaires, video recordings	Interaction analysis	Wizard-of-Oz elicitation for drone interaction	Deck of drone-condition cards; balanced Latin square tasks
Gallardo et al. [36]	21	Reddit forums, email listserv	60–90 min	Semi-structured interviews	Qualitative coding	Explored privacy/security for AR data collection	15 data types, 5 data use cases
Ahmed et al. [4]	Paratyping (62), interviews (9)	Two organizations	25–49 min (interviews)	Surveys, interviews	Avg. ratings, indifferent rate, thematic analysis	Examined impact + concerns of onlookers assisting visually impaired	Microsoft HoloLens, existing assistive tech
Lopez et al. [55]	23	Developers from multiple sites	–	Workshops, contextual + semi-structured interviews, observation	Descriptive + theoretical analysis	Software developers' security practices	Scenario cards, audio recordings, modeling materials, questionnaires

Recent elicitation approaches incorporate *scenario-based* methods for identifying security requirements, such as Rajaram and Chen's [73] user-driven design proposals for multi-user augmented reality. Gallardo et al. [36] documented how participants envision future privacy risks in augmented reality. Karre et al. [47] conducted a mapping study on requirements engineering methods for virtual reality application development. In [67], the authors explored user-defined gestures to enhance co-located mobile gaming by comparing interactions with a safe-to-touch drone prototype [2]. Studies [38] and [55] highlighted the factors in walking meetings and securing applications through standard practices. This body of work substantiates the idea that eliciting user perspectives can elucidate nuanced preferences, apprehensions, and threat models that purely system-centric analyses may overlook. Building on these findings, our study employs focus groups and scenario-based elicitation to better understand how stakeholders conceptualize anomalies in a smart-home context and how collaborative exploration might alleviate security gaps.

3 COLLABORATIVE ANOMALY EXPLORATION

In this section, we present a concise overview of the capabilities of the anomaly exploration process and highlight its key functionalities and objectives. We approach this process from two perspectives: the human aspect, which focuses on user interactions and interpretations, and the device aspect, which emphasizes the technological mechanisms and performance involved.



(a) Collaborative anomaly exploration framework, with numbered boxes indicating the room where each process step occurs, as referenced in Figure 1b.

(b) A smart home framework illustrating the process of collecting data and triggering alerts.

Fig. 1. Overall smart home and anomaly framework illustration.

3.1 Definition

Anomaly exploration is the process of identifying and reasoning about anomalies within collective information in a smart home environment to enable effective decision-making. This process involves analyzing data from various devices to uncover unusual patterns or behaviors that deviate from expected norms [28]. The requirements for anomaly exploration include the ability to analyze and interpret data collected from smart-home devices, such as *smart TVs*, which may not traditionally be used for security purposes but can provide valuable information through embedded sensors. Second, the reasoning capabilities integrate information from diverse devices to ensure comprehensive anomaly detection. Finally, support for user-driven queries to explore specific areas of concern will enable tailored exploration. Figure 1a illustrates the framework of the collaborative anomaly exploration system. The process begins with monitoring IoT devices and collecting their data. This data is then analyzed to detect any irregular behavior. If no anomaly is detected, monitoring continues. When unexpected activity is identified, the system assesses the risk level and either manages the situation autonomously or alerts the user. User feedback is subsequently incorporated to refine the system's responses, enabling continuous learning and adaptation through human–AI collaboration. The numbers shown above the boxes correspond to the rooms where each part of the process occurs, as illustrated in Figure 1b. To demonstrate its application, Figure 1b presents an example scenario. The motion sensor in the bedroom detects the user waking up. Shortly after, at 7:00 AM, the bedroom light is automatically switched on by the system, and by 7:05 AM, the user opens the bathroom door. These normal activities are collected as data and analyzed; since no unexpected situation is detected, the system stores the data as normal. However, at 7:15 AM, when the user moves into the kitchen, the motion sensor detects activity, followed immediately at 7:16 AM by smoke detection from the kitchen smoke detector. The system flags this as an unexpected situation and assesses the risk level as high due to the critical nature of smoke detection. As a result, the smart home system alerts the user through sirens and mobile notifications. After the user acknowledges the alert, the system collects feedback and updates its internal rules to enable faster detection of similar scenarios in the future.

3.2 Human Collaboration

Human collaboration in anomaly exploration refers to the integration of human interpretability into the explanation of detected anomalies, thereby enabling users to actively participate in decision-making processes. It provides clear, human-interpretable explanations of anomalies, ensuring that users understand the nature and potential impact of anomalies [21, 22]. It also facilitates user input during the exploration process, enabling the

refinement of anomaly detection and decision-making. The system generates explanations for anomalies, such as visualizations, summaries, and alerts, in a form that is easily understood by users. Users can interact with the system to provide feedback, ask questions, or prioritize areas for further exploration. The collaborative process ensures that exploration aligns with the user's goals and preferences, fostering trust and engagement.

3.3 Device to Device Collaboration

Device-to-device collaboration refers to the autonomous interaction and coordination of smart home devices for collectively exploring anomalies in shared areas. Devices can work together without human intervention to detect and analyze anomalies efficiently [11]. Ensuring that anomaly exploration process adapts to user needs and preferences while maintaining high performance and accuracy. These devices share relevant data and insights for building a comprehensive understanding of potential anomalies. Autonomous mechanisms, such as ML algorithms, are employed to detect patterns and correlations that might indicate anomalies. Collaboration is designed to comply with user-defined requirements, ensuring that the exploration process remains aligned with the overarching goals of the smart home system.

4 METHODOLOGY

We employ a two-phase empirical approach to investigate how diverse stakeholders perceive, understand, and collaborate on anomalies in future smart-home ecosystems. As illustrated in Figure 2, our study began with an *online questionnaire* to gather demographic information, classify participants according to technical and security/privacy orientations, and establish a broad context for smart-home adoption. We then conducted *focus group interviews* to capture in-depth, scenario-based insights into collaborative anomaly exploration.

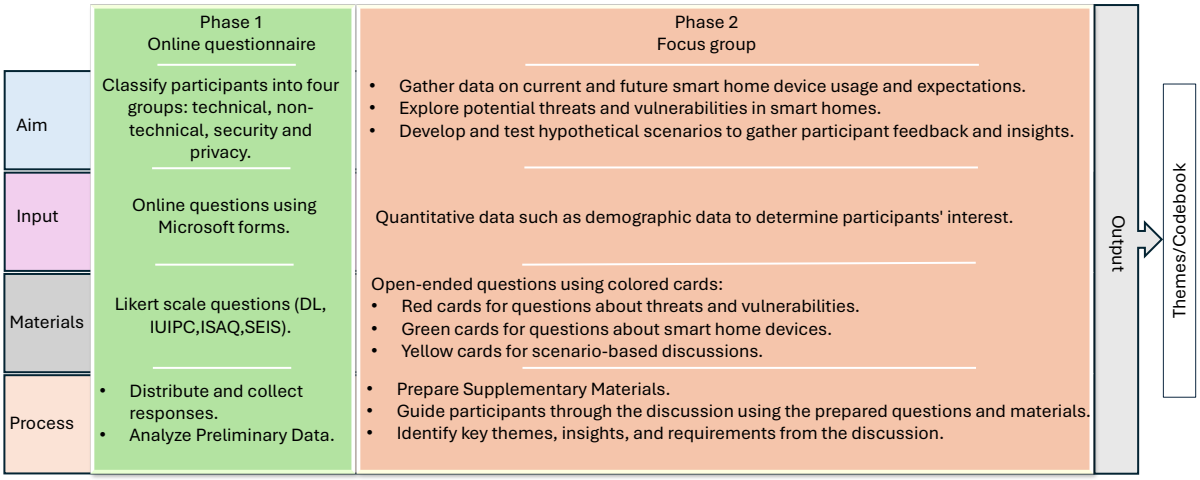


Fig. 2. Overview of our two-phase methodology: (1) Online questionnaire to screen and classify participants, and (2) focus groups to elicit deeper qualitative insights into user-driven anomaly handling in future smart homes.

4.1 Phase 1: Online Questionnaire

4.1.1 Rationale and Aims. The questionnaire has two primary objectives. First, it enabled us to collect demographic data (e.g., age, gender, and education) and measure participants' technological proficiency, security

awareness, and privacy concerns using validated scales. Second, it allowed us to classify respondents into distinct categories relevant to smart-home security, namely, *tech-savvy*, *non-tech-savvy*, *security-focused*, and *privacy-oriented*—ensuring a diverse pool of perspectives for subsequent focus groups.

4.1.2 Participants and Recruitment. We began our research with a quantitative approach [66], employing an online questionnaire [16, 93] as our primary data collection tool. Throughout the data collection process, we used theoretical sampling for recruitment [24] [37]. All participants were recruited through an email listserv and snowball sampling [40, 41], as well as post invitation on social media networking called Yammer. We used a university participant pool to gather a diverse sample of respondents with, we utilized a university participant pool, which provided access to a range of students. The questionnaire was administered using Microsoft Forms [69].

The demographic profiles of these 40 respondents their reflected wide-ranging backgrounds and expertise: 39% were male, 24% were female, and 5% identified otherwise. Their ages spanned primarily 20–40 years (M = 30.25, SD = 5.12), with educational levels including bachelor's (10%), master's (63%), doctoral (24%), and other degrees (2%). Approximately 15% specialized in information security (n = 6), 47.5% focused on privacy (n = 19), 17.5% were strongly tech-savvy (n = 7), and 20% considered themselves less technologically inclined (n = 8). This distribution establishes a solid baseline for capturing various views on smart-home technologies, security, and privacy.

4.1.3 Materials and Procedures. In addition to demographic questions, the survey incorporated four standardized scales:

(1) Digital Literacy (DL) [68] assesses an individual's ability to navigate, evaluate, and utilize digital technology effectively. It also evaluates the ease with which individuals can adopt and use unfamiliar technologies, emphasizing their adaptability and skill development in a digital environment.
(2) Internet users' information privacy concerns (IUIPC) [58] are utilized to gain deeper insights into individuals' perceptions of privacy risks associated with the IoT. It also explores the circumstances under which users prefer to be informed about data collection practices.
(3) Information Security Awareness (ISAQ) [52, 53] assesses the extent to which individuals understand and recognize information security risks. It evaluates their knowledge, attitudes, and behaviors related to protecting sensitive information and adhering to security best practices in both personal and professional contexts.
(4) Self-Efficacy in Information Security (SEIS) [74] evaluates individuals' confidence in and ability to engage in effective information security practices. It measures both technological usage behavior and conscientiousness when implementing security-aware actions.

These instruments gauged the participants' comfort with emerging technologies, their stance on privacy, and their awareness of and confidence in handling security incidents. We leveraged these survey responses with group respondents to ensure that each focus group session incorporated a mix of experiences and mindsets.

4.1.4 Analysis. We performed descriptive analyses of the data, summarized the key demographic distributions and confirmed that the participants were suitably diverse in terms of background and expertise. This ensured that subsequent focus groups represented multiple perspectives on smart-home adoption and anomaly handling. Thus, the final sample of 40 respondents served as the basis for selecting a subset of participants who agreed to continue with the qualitative phase.

4.2 Phase 2: Focus Groups

4.2.1 Rationale and Aims. Building on the questionnaire findings, we conducted focus group interviews to examine how the participants *collaboratively* detected and interpreted anomalous events in next-generation smart homes. This phase aligns with qualitative research methods [71] that highlight dynamic group exchanges,

enabling us to probe nuanced perspectives on socio-technical interactions and threat mitigation strategies. We validated this stage through a critical pilot testing phase [57, 86].

4.2.2 Participants. Of the 40 respondents, 36 proceeded to the focus group phase, which was organized into approximately 10 sessions with three to four participants each. We deliberately combined individuals with different technology skill levels, privacy attitudes, and security awareness to foster a robust dialogue. Each 90-minute session was conducted face-to-face, recorded (with participant consent), and transcribed. The participants received a £20 voucher to acknowledge their time and expertise.

4.2.3 Materials and Procedures. Our semi-structured focus groups were anchored in three thematic areas. First, the participants shared their *current smart-home device usage*, highlighting common practices, pain points, and opportunities for improvement. This set the stage for envisioning how future devices and configurations may enhance daily life. Second, we introduced the concept of *anomalies*, including suspicious device behaviors and data patterns, and asked the participants to reflect on both real and hypothetical examples. This discussion explored how humans and devices can *jointly* detect, analyze, and respond to anomalies (Appendices A, G.1, and G.2). Third, participants worked through *scenario-driven use cases* (Appendices D and G.3), collaboratively imagining occupant–device interactions in specific anomaly contexts to refine and expand the notion of "collaborative anomaly exploration." All participants provided informed consent and were informed aware of their right to withdraw from the study. This study was reviewed and approved by the Cardiff School of Computer Science and Informatics Ethics Committee.

4.2.4 Analysis. We conducted a reflexive thematic analysis [15, 17, 70] guided by Mile's methods [59] and Richards' techniques [75], followed by comparison and integration with related literature [30] using NVivo 14 tool [91]. This method was applied to analyze both the verbal comments made during the sessions and any written notes provided by the participants. Throughout this process, we continually revised our research questions [3] periodically to confirm that these themes aligned with the overarching aim of collaborative anomaly exploration in smart homes.

By combining quantitative breadth with qualitative depth, our approach captures a holistic view of how different stakeholders conceptualize and manage potential threats. The questionnaire phase established demographic and attitudinal baselines, whereas the focus groups uncovered scenario-based, user-driven insights into collaborative anomaly detection and resolution. This synergy allows our findings to inform both the design of technical frameworks and the development of human-centered strategies for future smart home ecosystems.

5 RESULTS

We present our findings in relation to the three research questions that guided this study. Section 5.1 addresses **RQ1** by exploring how participants characterize the landscape of future smart homes, including the devices they anticipate, potential configurations and the ways in which occupant interactions may reveal points of anomalous or malicious behavior. Section 5.2 focuses on **RQ2**, examining the categories of anomalies and security threats that are likely to arise in these evolving ecosystems, and how occupants and systems may collaboratively identify and analyze them. Finally, Section 5.3 addresses **RQ3** by outlining the design principles and use-case scenarios that enable next-generation smart homes to jointly respond to anomalies and foster improved security, privacy, and trust.

5.1 Characterizing Future Smart Homes for Potential Anomalous or Malicious Behavior

> **RQ1:** *How can we characterize the landscape of future smart homes (including devices, configurations, and occupant interactions) in ways that reveal potential points of anomalous or malicious behavior?*

Our first research question investigated how future smart home environments may be configured—spanning devices, occupant interactions, and overall ecosystem design—to reveal or enable anomalous or malicious activities. Table 2 summarizes the main themes that emerged from the participants' discussions, highlighting the current practices and anticipated evolutions in device functionality, integration, security, and privacy. In the following subsections, we outline a broad spectrum of interconnected systems, sensors, and robots that the participants believed could transform their daily routines while simultaneously introducing new vulnerabilities.

Table 2. Key Themes for RQ1: Characterizing Future Smart Homes and Potential Points of Anomaly.

RQ1 Focus	Theme	Definition/Illustrative Scope
How can we characterize the landscape of future smart homes (devices, configurations, and occupant interactions) in ways that reveal potential anomalous or malicious behavior?	**Smart Home Devices**	Examination of existing and emerging technologies (e.g., bulbs, switches, locks, sensors, robots) that shape everyday life and could introduce new threat vectors.
	Device Integration and Categorization	The integration of multiple devices enables seamless communication and enhanced functionalities but increases security risks. Categorizing devices by function, location, or connectivity helps manage these risks by offering a structured approach to understanding and securing data collection, processing, and sharing.
	Security and Privacy Concerns	Participants were concerned about hacking, unauthorized access, and manufacturer practices, along with large-scale data collection and surveillance, which heightened their anxiety over privacy and control.
	Human-Robot Interaction	Envisioned roles for domestic robots (e.g., chores, companionship) and their potential for intrusive data gathering or emotional implications.
	Implication for Anomalous or Malicious Behavior	The potential risks and vulnerabilities introduced by new functionalities and advanced automation in smart home systems, which may result in unexpected anomalies or security threats.

5.1.1 Emergent Classes of Devices: Systems, Sensors, and Robots. Participants consistently identified three primary classes of smart home technology that define current practices and shape their future vision.

- *Systems* (e.g., bulbs, switches, locks, security cameras)
- *Sensors* (e.g., door/window, motion, environmental, VibroSense)
- *Robots* (e.g., *Ballie, Amazon Astro*)

Figure 3 provides an overview of the selected devices, illustrating the gap between the current-day functionalities and future enhancements anticipated by the participants.

Systems (Bulbs, Switches, Locks, Security Cameras). Many participants explained that current **smart bulbs** allow for on/off control, dimming, and color changes. However, they envision future bulbs that could integrate context awareness, automatically adjusting brightness based on external lighting or user presence. Additionally, they anticipated remote control capabilities over vast distances and possibility of mind-gesture control. While **smart switches** remain physical in most households, the participants speculated that they might eventually be replaced entirely by speech, gestures, or neural interfaces, though this would necessitate heightened security measures to prevent unauthorized activation.

Smart locks have drawn particular attention owing to the dual risk/benefit of keyless entry. Many participants foresee sophisticated biometrics, such as facial recognition and fingerprint scanning, (e.g., face, fingerprint) being integrated with scheduling or collaborative sensing (e.g., locks and and cameras). However, they stressed the need of manual overrides in the event of power outages or biometric failures. In contrast, current **security cameras**

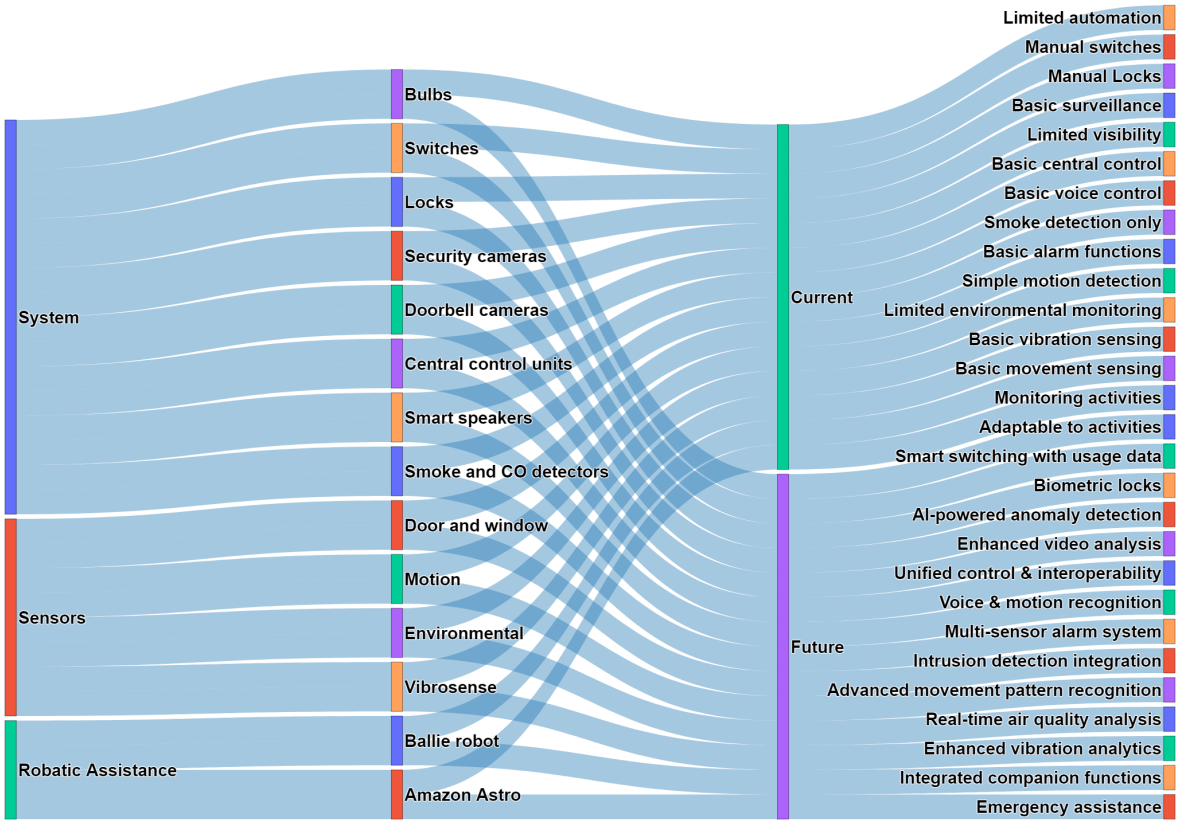


Fig. 3. Overview of each device's current functions and projected future enhancements.

typically offer basic monitoring and two-way communication. Participants anticipated these cameras evolving through AI-driven recognition and 360-degree coverage—advancements that would enhance surveillance but also raise critical privacy concerns.

Sensors (Door/Window, Motion, Environmental, VibroSense). The participants emphasized the expanding role of sensors, which now track everything from door/window states to indoor air quality. **Door/window** sensors are primarily used for security and energy-saving functions. **Motion** sensors currently trigger lights or alerts, but future models could distinguish between humans, pets, or objects, while factoring in occupant routines to better detect anomalies. **Environmental** sensors that monitor temperature, humidity, and air quality are anticipated to evolve with ML capabilities to prevent fires or automatically adjust ventilation systems. **VibroSense**, a niche technology that detects vibrations on stairs or floors was noted by participants for its potential fall detection (particularly for elderly care), child monitoring, and advanced anomaly detection (such as detecting earthquakes).

Robots (Ballie, Amazon Astro). Several participants viewed domestic **robots** as emblematic of future smart homes. While current prototypes like Ballie and Amazon Astro perform tasks such as remote patrols or sending notifications, many participants envisioned robots with physical manipulation capabilities, including arms and wheels, to assist with chores, caregiving, or advanced security checks. Offline functionality and embedded sensors were considered essential to safeguard privacy and minimize reliance on cloud services. However, some

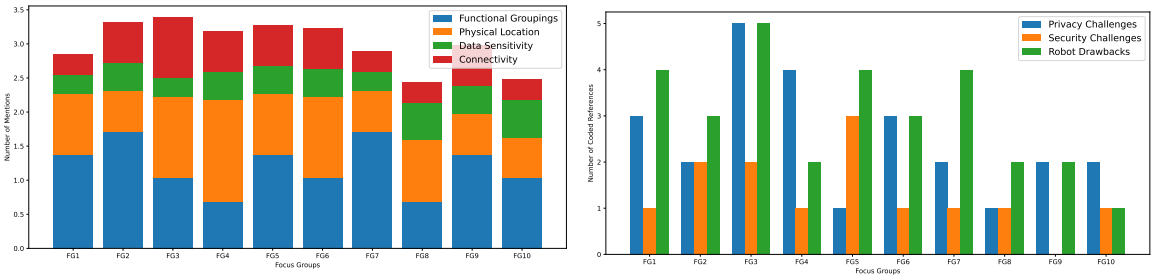
participants raised concerns about the implications of robots with constantly roving cameras, the risk of hacked robots roaming the home, and the emotional impact of robots potentially replacing genuine human interaction.

5.1.2 Integration and Categorization of Devices. Device Integration. Participants broadly agreed that an ecosystem of interconnected devices could boost convenience and security, but also expand the "attack surface." One participant noted, "*We can use switches with bulbs and locks ... also with the security camera*" (F1, P4), emphasizing how each element can collaborate to automate daily tasks. Another participant described a scenario in which a motion sensor triggers a robot to move and then notified the occupant via camera feed, illustrating the potential synergy among sensors, robots, and occupant oversight. Despite these benefits, participants stressed that centralizing control in a single hub (e.g., a smart speaker like Alexa) risks catastrophic failure if the hub is hacked or malfunctions. Figure 4 demonstrates the varying levels of emphasis that participants placed on each topic in the different group discussions. In Figure 4a, functional classification was the most frequently applied method, followed by location-based grouping; data sensitivity and connectivity appeared less frequently.

Approaches to Categorization. In classifying smart home devices, participants typically relied on:

- *Functional groupings* (security vs. convenience vs. environmental).
- *Physical location* (kitchen, bedroom, other).
- *Data sensitivity* (devices that collect personal information vs. those that do not).
- *Connectivity* (local vs. cloud-based).

Participants with privacy concerns favored segregating devices that gather personal data (e.g., cameras, locks) from relatively benign items (e.g., thermostats and lights), sometimes isolating them on separate networks. Others underlined how some devices (e.g., voice assistants) constantly listening, generating perpetual data streams that invite misuse if improperly secured or categorized.



(a) Device classification types by participant.

(b) Mentions of security, privacy, and robot challenge themes in focus groups.

Fig. 4. Visual summaries of participant responses across ten focus groups. (a) shows how participants classified smart home devices using four dimensions—functional grouping, physical location, data sensitivity, and connectivity—based on normalized NVivo reference counts. (b) presents the distribution of NVivo-coded references to security challenges, privacy concerns, and robot-related drawbacks, illustrating how these key themes varied across group discussions.

5.1.3 Security and Privacy Concerns. Security Vulnerabilities. A recurring fear was that connected devices could be hijacked to open doors, intercept camera feeds, or compromise occupant privacy. Several participants deliberately excluded certain high-risk devices from private spaces or employed separate Wi-Fi networks for the IoT. Many pressed manufacturers to implement stronger default protections, yet recognize user complacency (e.g., failing to change the default password) remains an obstacle. One participant remarked, "*If someone hacks your central system, they could basically see and control everything in your home*" (F4, P2).

Privacy Challenges. Beyond hacking fears, participants lamented constant data gathering and hyper-surveillance as aspects of modern IoT. Devices such as voice assistants, cameras, and roving robots foster convenience, but collect significant personal information. One participant observed, "*Smart speakers are always hearing, so you can not talk freely in your own house*" (F6, P1). These anxieties intensified with the realization that data might be fed back to manufacturers, third-party analytics, or, if breached, malicious actors. Participants balanced their appreciation for home automation with the moral and legal implications of unceasing data collection.

5.1.4 Human–Robot Interaction: Opportunities and Drawbacks. Evolving Roles for Robots. Many participants saw an inevitability in robots undertaking routine tasks (cleaning, carrying items, basic caregiving) and even providing emotional companionship. They envisioned robots as central to future homes—autonomously roaming rooms and interacting with other connected devices. Some highlighted the ability of robots to assist children, seniors, and individuals with disabilities. One participant imagined a scenario where "*Ballie could learn my habits offline, improving privacy and not needing to connect to the cloud*" (F2, P2).

Privacy, Security, and Social Implications. Notwithstanding these benefits, the participants remained skeptical about granting robots pervasive access to personal spaces. "*Privacy is a nightmare ... extremely risky,*" said one participant (F4, P3). These concerns included constant internal mapping, camera streams, or microphone usage. Others worried about job displacement (replacing caregivers or service animals) and diminishing real-world social connections if robots become too capable of fulfilling emotional roles. Hacking scenarios were especially alarming; one participant noted that a compromised robot could physically follow residents or provide an intruder with direct movement inside the home. In Figure 4b, robot-related drawbacks were the most frequently mentioned theme overall, followed by privacy concerns, which also featured prominently, and security challenges, which appeared less frequently.

5.1.5 Implications for Anomalous or Malicious Behavior. Discussions on RQ1 underscored that *every* new function—whether it AI-driven light adjustments or a roving caretaker robot—introduces potential anomalies and risks. The more integrated and automated homes become, the more "*single points of failure" or "chain reactions*" may appear. Participants saw an urgent need to balance convenience with robust security controls, including user education and transparent data practices. They emphasized that occupant routines (especially predictable schedules) could inadvertently expose vulnerabilities.

Summary for RQ1. By characterizing the future smart home landscape, the participants highlighted a continuum of evolving systems, sensors, and robots. They expect these devices to become increasingly integrated and context-aware, delivering unprecedented convenience while exposing deeper security and privacy challenges. In particular, **human–robot interaction** emerged as a critical domain, amplifying the potential for both beneficial services and intrusive data collection. Overall, these findings form the backdrop for subsequent analyses of *how* anomalies might manifest (RQ2) and which design principles could mitigate them (RQ3).

5.2 Categories of Anomalies and Collaborative In-Situ Analysis in Evolving Smart Homes

> **RQ2:** *What categories of anomalies and security threats are likely to arise in these evolving smart home ecosystems, and how might users and systems collaboratively identify and analyze them in situ?*

Addressing **RQ2** requires examining the types of anomalies and security threats that participants believe will emerge in *future smart homes*, alongside the *collaborative in situ* methods that occupants and systems might use to detect, interpret, and mitigate these events. Table 3 summarizes the key themes arising from the focus group discussions, ranging from mundane device glitches to active cyberattacks. Participants consistently emphasized that anomaly detection should blend automated processes with real-time user input and oversight.

Table 3. Key Themes for RQ2: Types of Anomalies, Security Threats, and Collaborative Detection Approaches.

RQ2 Focus	Theme	Definition
RQ2: What categories of anomalies and security threats are likely to arise in these evolving smart home ecosystems, and how might users and systems collaboratively identify and analyze them *in situ*?	**Suspected Anomalies and their causes**	A variety of unexpected device behaviors, sensor malfunctions, connectivity disruptions, and malicious intrusions that undermine normal operations.
	Reasons for Attack Opportunities	Underlying causes (e.g., improper configurations, predictable user routines, backdoors) that heighten the likelihood of breaches.
	Collaborative Countermeasures and Practices	Defensive strategies (firmware updates, robust authentication, layered alerts) aimed at preventing or detecting unusual system behaviors.
	Future Anomaly Detection Systems	Advanced frameworks (multi-sensor fusion, AI-based analysis) enabling both automated and user-guided threat identification.

Table 4. Overview of Common Security Concerns, Attack Motivations, and Recommended Countermeasures.

Category	Representative Insights
Anomalies	False device activation (e.g., Alexa responding to unintended voices), connectivity or update failures, over-sensitive sensors yielding false alarms, malfunctioning automation routines, active hacking exploits.
Reasons for Attacks	Use of default passwords, predictable occupant schedules, device placement near windows, technical backdoors, suboptimal physical layouts.
Countermeasures	Manual resets/backups, real-time monitoring, user education, strong authentication, network isolation, firmware checks, physical security improvements, and layered/redundant alerts.

5.2.1 Suspected Anomalies and Their Underlying Causes. False Activations and Update Glitches. Voice assistants occasionally misheard conversations, leading to random activations or unintended commands. One participant explained, "*Alexa can respond to every other voice... people can shout through the window*" (F1, P1). Others lamented that firmware updates or network downtime left devices unresponsive: "*Sometimes it cannot recognize my voice... if Wi-Fi is down, everything stops*" (F2, P2).

Overly Sensitive Sensors and False Alarms. Motion detectors triggered by sunlight, doorbells alerting nonexistent visitors, and cameras misidentifying harmless objects were common. "*I was alarmed someone was in the house, but it was just the sun's reflection*" (F7, P4). Such false positives risk "alarm fatigue," where users ignore legitimate alerts.

Device Malfunctions. Smart vacuums veering off course, thermostats freezing in the "on" position, and voice commands yielding opposite actions all highlighted how automation can fail. Participants noted that these glitches could mask genuine anomalies if users became accustomed to quirky behaviors.

Security Vulnerabilities. Hacking and data leaks remain the primary concerns. For example, compromised locks could grant intruders physical access, or cameras could be hijacked to spy on occupants. "*If you have a control system that opens doors, someone can hack it and open your home*" (F4, P2).

5.2.2 Reasons for Attack Opportunities. Improper Configuration and Defaults. Keeping default passwords and failing to apply firmware updates featured prominently. One participant admitted, "*I'm lazy... I often use a normal password for everything*" (F2, P2).

Predictable Routines and Device Placement. Attackers can exploit the occupant schedules and device locations. "*Putting devices near windows is dangerous if people can see them*" (F1, P1). Others noted that consistent daily routines "*let an attacker figure out when the home is empty or vulnerable*" (F5, P1).

Technical Backdoors and Environmental Limitations. Participants expressed skepticism about hardware-level backdoors: "*Lots of chip makers include major backdoors... no device is fully safe*" (F7, P4). Physical factors, such as humidity or suboptimal sensor placement, can also degrade performance, contributing to inaccurate anomaly detection or overlooked threats.

5.2.3 Collaborative Countermeasures and Good Practices. Participants proposed a combination of technical safeguards and user-driven tactics to handle anomalies more effectively (see Table 4).

Manual Reset and Backup Systems. Many participants pointed to simple resets as the first response, supplemented by backup power or alternative connections during updates. "*We've got a backup system... so you can use that first*" (F1, P1).

Real-Time Monitoring and Alerts. Early notification is important, especially for children or vulnerable occupants. "*If it's not what we usually do and it happens, that's an anomaly for me*" (F1, P2). This requires robust interfaces that let users quickly validate or dismiss alerts.

User Education and Strong Authentication. By setting unique passwords to enable multifactor authentication (MFA), participants recognized occupant awareness as critical. One participant stated, "*I change the password immediately... I use two-factor auth*" (F7, P4). These measures reduce the risk of casual hacking attempts.

Network Isolation and Firmware Updates. Separating IoT devices into distinct subnets can limit damage if one device is breached. Participants also stressed the need for timely patches: "*Scheduled inspections or monthly updates might prevent zero-day exploits*" (F8, P2).

Physical Security & Behavior Modification. Strategic device placement, unpredictable schedules, and locking down sensitive areas (e.g., routers) have been cited as effective ways to reduce risk. "*I change the time every now and then... so it's not obvious*" (F5, P2).

5.2.4 Future Anomaly Detection Systems: AI, Sensor Fusion, and Human Oversight. Looking forward, participants envisioned *collaborative anomaly detection* frameworks that combine AI with occupant judgment:

Multi-Sensor Corroboration. Cross-verifying temperature spikes with CO_2 or fire-alarm data can reduce false positives. "*You need a second opinion... if one sensor sees something but another doesn't, verify before alerting*" (F1, P1).

Self-Monitoring and Autonomous Updates. Systems capable of self-diagnosis or auto-patching vulnerabilities decrease the user's burden. "*If my home is so smart, it should fix anomalies itself... only alert me if it can not*" (F10, P2).

Severity-Based Alerts and Local Data Processing. To avoid user burnout, participants suggested categorizing alerts by severity (severe, moderate, low). Many also preferred local processing to reduce privacy risks: "*We can process data on cheap hardware at home... no need to send everything to the cloud*" (F7, P1).

Human–Device Collaboration. Ultimately, participants viewed occupant oversight as essential, even with sophisticated AI. "*Maybe just an initial notification for us to investigate*" (F9, P4). This collaboration ensures that anomalies are not solely filtered by algorithms but are also interpreted in the context of each household's unique routines.

Under **RQ2**, participants identified diverse anomalies—ranging from everyday glitches to critical cyber intrusions—and underscored that *collaborative, in situ detection* relies on combing smart automation with informed occupant supervision. They advocated for defensive practices (e.g., MFA, backups, and local networks) and next-generation anomaly detection systems that correlate sensor data, adapt notifications by severity, and give humans the final say. These insights directly inform how future smart homes may proactively recognize and manage threats before they escalate, paving the way for a discussion of design principles and use cases in **RQ3**.

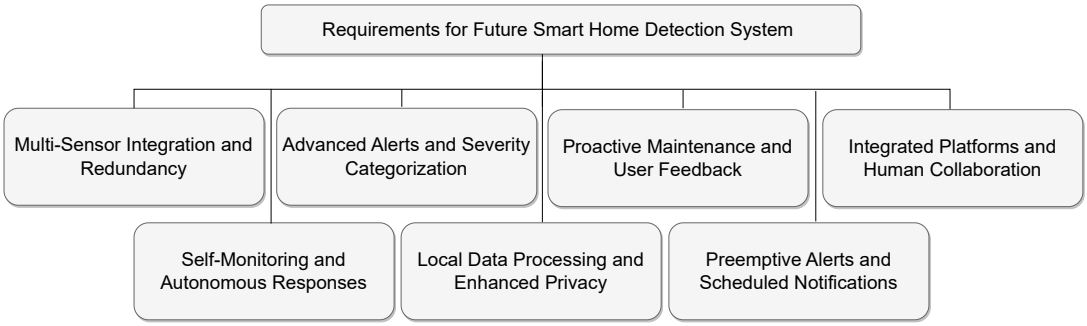


Fig. 5. Essential Components and Requirements of Future Smart Home Monitoring and Detection Infrastructure.

5.3 Design Principles and Use-Case Scenarios for Next-Generation Smart Homes

RQ3: *Which design principles and use-case scenarios can guide the development of next-generation smart home solutions, enabling occupants and devices to jointly explore and respond to anomalies for improved security, privacy, and trust?*

To address our third research question, we synthesized a set of user-driven *design principles* and *representative use cases* that illustrate how future smart home systems might detect, analyze, and mitigate anomalies. Table 5 provides an overview of key security measures and countermeasures related to common threat scenarios. Building on these examples, we highlight how participants envision user–device collaboration in practical contexts, emphasizing *multifaceted security*, *privacy safeguards*, and *human oversight* across both physical and cyber domains.

5.3.1 Design Principles for Collaborative Anomaly Exploration. In the future, smart home anomaly detection systems are envisioned to be more advanced, intelligent, and seamlessly integrated. Participants suggested several features and mechanisms for these systems, highlighting the importance of multi-sensor corroboration, real-time alerts, self-monitoring capabilities, and user control (See Figure 5). Below are some key insights with direct quotes from participants:

1) Multi-Sensor Integration and Redundancy. Many participants emphasized the importance of combining digital and physical measures—such as strong encryption and physically secured device placement—to prevent or limit malicious access. Use cases often mentioned backup power systems (e.g., battery/hub redundancy) and layered alerts (e.g., cross-validating sensor data) to ensure no single point of failure compromises the entire home. Additionally, participants noted that ML plays a critical role in smart home environments, enabling systems to learn from user activities and preferences. They pointed out that approaches such as deep learning can reduce the need for direct human intervention by allowing the system to autonomously recognize patterns and behaviors, ultimately improving control and personalization.

2) Self-Monitoring and Autonomous Responses. Several participants emphasized the need for smart systems that can self-diagnose issues and take action automatically. One participant noted, (F10, P2) "*If my home is so smart, I should not have to solve the anomalies; it should be able to solve itself,*" while another mentioned, (F10, P3) "*It can update itself or troubleshoot itself.*" This highlights the need for smart devices that could self-check for issues, update software, and alert the users only when human intervention is necessary.

3) Advanced Alerts and Severity Categorization. To avoid alert fatigue, participants suggested that systems should categorize anomalies by severity and communicate accordingly. One participant said, (F7, P4) "*I do not want to be notified for every incident.* Maybe categorize severe, moderate, and low anomalies." This allows users to prioritize responses based on the urgency of the issue.

Table 5. Representative Smart Home Threats and Proposed Countermeasures Based on Use Case Discussions.

Use Case	Threats	Solutions / Mitigations
Water Sprinkler	Spoofing attacks, malicious manipulation of watering schedules	Layered defense checks, regular device audits, real-time alerts
Smart Fan	Physical tampering (broken blades), unauthorized remote access	Backup power, routine self-diagnosis, system checks
Battery / Hub	Damaging or draining the battery to incapacitate devices	Backup battery systems, redundant power, scheduled inspections
Light System	Malware intrusion, remote hijacking of lights	Strong passwords, encryption, periodic resets, and updates
CO Detector	Alarm tampering, remote disabling	Encrypted Comms, Multifactor Auth, regular operational checks
Webcam	Physical sabotage (lens obstruction), feed hijacking	Secure passwords, MFA, antivirus/firewalls, strategic placement
Air Conditioner	Spoofing temperature data, hacker-induced overheating or shutdown	Robust cybersecurity measures, active monitoring, routine maintenance
Motion Sensor	Physical disabling, unauthorized remote control	Concealed placement, MFA, ML-based false alarm reduction
Garage Door	DoS attacks, forced entry	Encryption, multi-factor auth, and frequent security patches
Door/Window	Physical lock damage, remote unlocking	Manual key backups, real-time tamper alerts, advanced detection
Kettle	Continuous operation, remote manipulation	Physical inspections, strong passwords, auto-shutoff mechanisms
Smoke Detector	Sensor obstruction, spoofed no-smoke state	Independent defense layers, cross-checking with cameras/motion sensors

4) Proactive Maintenance and User Feedback. Participants favored solutions that could adapt to evolving user habits and environmental factors. For instance, sprinkler schedules adjusting to weather patterns or a motion sensor differentiating between human and pet movement. By embedding ML or rule-based logic, these systems would proactively detect unusual events (e.g., motion at atypical hours) and help occupants respond before major damage occurs.

5) Integrated Platforms and Human Collaboration. Although automation is prized for convenience, participants insisted on retaining occupant supervision. Suggested practices include *manual overrides* (e.g., a physical key for locks), user-friendly dashboards, and immediate notifications prompting occupant review. One participant explained, " *We can not let the system just do everything on its own—there needs to be an initial notification for us to investigate.*" (F9, P4).

6) Local Data Processing and Enhanced Privacy. Local data processing is preferred to protect privacy and reduce dependency on external servers. One participant stated, (F7, P1) "*Most of the data processing could probably be done locally on relatively cheap hardware,*" suggesting that future systems may rely more on in-home processing units, reducing the risk of data breaches and improving response times.

7) Preemptive Alerts and Scheduled Notifications. Several participants encouraged routine checks of device integrity—verification of firmware versions, scanning for malware, and physical inspection of mechanical parts. In the *smart fan* example, participants worried that broken blades or motor damage would go unnoticed until a catastrophic event occurred. Regular diagnostics would alert homeowners to incipient failures.

5.3.2 Representative Use Cases for Joint Anomaly Handling. Use Case 1: Water Sprinkler. Described by participants as "*an automated garden system that requires minimal oversight*" (F1), this scenario underscores layered defenses. Physical tampering (damaging pipes or nozzles) can be addressed via scheduled inspections, whereas cyber

attacks (spoofing weather data or watering schedules) required encryption and backup checks to ensure that there are no unauthorized adjustments.

Use Case 2: Smart Fan. Participants' vision of a *temperature-aware fan* exemplified both occupant convenience and vulnerability. Physical sabotage might cause mechanical issues, while hackers could remotely disable or manipulate the fan's speed logs. Recommended solutions include routine self-diagnosis (detecting motor strain), robust authentication, and occupant alerts for abnormal energy usage.

Use Case 3: Battery / Hub. A compromised battery in the home's central hub could render locks, alarms, and sensors inoperable. Participants stressed employing *redundant power sources*, real-time battery health monitoring, and layered device networks so that a failing hub does not disrupt the entire ecosystem.

Use Case 4: Light System. Although physically breaking bulbs is less common, cyber manipulation (e.g., flicking lights on and off to disorient occupants) can serve as a distraction for further intrusion. The proposed defenses include strong passwords and encryption, in addition to an auto-reset function to return the lights to their default states if tampering is detected.

Use Case 5: Carbon Monoxide Detector. Even a small chance of tampering poses lethal risks. Participants advocated for multifactor authentication to prevent remote disablement. They also recommended maintaining both local and cloud-based logs to detect false sensor readings and conduct frequent operational checks. Occupant collaboration is vital for prompt manual verification in the event of suspicious device behavior.

Use Case 6: Webcam. Intruders could physically obstruct lenses or hack feeds. To mitigate this, participants suggested strategic camera placement, frequent system checks, and robust authentication. ML-based analytics can also differentiate between normal and suspicious usage patterns (e.g., repeated toggling).

Use Case 7: Air Conditioner. Occupant comfort and device longevity hinge on stable temperature regulation; however, hackers may spoof or override these settings. Scheduled check-ups, local data validation, and occupant alerts for unusual usage spikes can minimize malicious control or hardware strain.

Use Case 8: Motion Sensor. A sensor providing real-time intruder detection could be physically disabled by blocking it. Participants favored concealing the sensor, using multi-factor authentication for remote access, and employing ML to reduce false alarms (e.g., wind, pets) which could otherwise compromise occupant trust.

Use Case 9: Garage Door. Physical prying or forcing the door is a known risk, but participants also noted the potential for Denial of Service (DoS) attacks or remote exploits on the door's networked system. Regular software patches, strong encryption, and occupant notifications were recommended to secure high-traffic entry points.

Use Case 10: Door/Window Locks. Cybercriminals could remotely unlock doors or windows, bypassing physical force. Users proposed manual keys as fallbacks, real-time tamper alerts, and occupant-defined access rules (time-based or multi-factor). A single compromise of the lock should not cascade to the entire home security system.

Use Case 11: Kettle. Though seemingly mundane, a networked kettle can be manipulated to boil water continuously or misreport temperatures. Participants advised physically securing it in visible locations, employing built-in auto-shutoff mechanisms, and applying encryption and MFA to app-based controls.

Use Case 12: Smoke Detector. Participants highlighted the paramount importance of detectors functioning reliably even if other subsystems fail. They suggested dividing critical devices onto separate sub-networks and cross-checking smoke alarms with motion/camera data to confirm actual hazards.

5.3.3 Toward Collaborative Anomaly Exploration in Next-Generation Homes. By integrating the above *design principles* (Section 5.3.1) with concrete use case scenarios (Section 5.3.2), participants envisioned a **collaborative anomaly exploration** model wherein occupants and devices jointly:

- Identify irregular behaviors through multi-sensor confirmation and adaptive AI.
- Communicate timely alerts to occupants, providing clarity on severity levels.
- Allow occupant input for ambiguous cases, ensuring human context is never overlooked.

- Automate routine or low-level anomalies, balancing trust with user oversight.
- Preserve privacy via local data processing and selective cloud interactions.

These insights highlight the growing need for occupant–device co-management to ensure *security*, *privacy*, and *trust* in IoT-driven homes. Participants stressed that this balance depends on both *robust technical safeguards* and *clear user engagement mechanisms*, especially as smart home adoption expands.

By examining a range of potential threat scenarios, we highlight not only the importance of layered defenses but also the need for occupant involvement in anomaly detection and resolution. The participants' proposed solutions—ranging from manual overrides to advanced ML-based filtering—suggest a future in which humans and smart devices can co-create a secure, privacy-respecting home environment.

6 DISCUSSION

This section consolidates the key insights drawn from our mixed-methods investigation. We first highlight the *requirements* for securing and enhancing the user experience in future smart homes, then turn to how participants expect these systems to *anticipate and address anomalies*, balancing robust security with daily convenience. Subsequently, we delve into a collaborative approach for identifying anomalies in home environments. Finally, we discuss the *limitations* of our study.

6.1 Requirements for Creating Future Smart Homes

Participants proposed a broad range of requirements for designing smart homes that are not only secure and adaptive but also protect user privacy and support inclusive usage. Figure 6 illustrates these criteria.

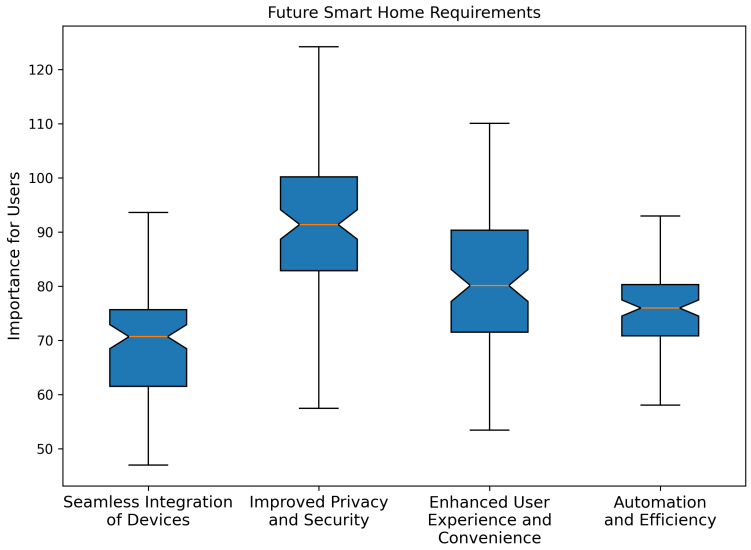


Fig. 6. Essential design criteria for next-generation smart homes, emphasizing security, adaptability, and user-centricity.

6.1.1 Seamless Integration of Devices. A major finding was the need for a cohesive ecosystem where diverse devices (e.g., thermostats, security systems, and lighting) function as a *unified whole*. Unlike application-level integration strategies that focus solely on code-level interactions [55], our study underscores the importance of secure and frictionless interactions among various smart home technologies. Participants stressed that device compatibility should encompass both functional interoperability and consistent security protocols to avoid

potential vulnerabilities. ML–driven sensor fusion techniques present promising avenues for enabling smarter, more adaptive systems [49]. Specifically, deep learning architectures—such as early, late, and hybrid fusion models [48]. Probabilistic reasoning frameworks, such as a Markov Chain model and context-aware systems [81], may provide more adaptive and interpretable decision-making.

6.1.2 Improved Privacy and Security. While some participants embraced the convenience of smart home automation, those with a stronger privacy or security focus raised concerns about the potential misuse of collected data. A consensus emerged regarding the use of *local data processing* to reduce reliance on cloud services, thereby mitigating risks of external breaches and unauthorized data usage. These perspectives align with privacy challenges cited in other IoT contexts [36], reinforcing the importance of *privacy-by-design* and respect for user consent [73, 92].

6.1.3 Enhanced User Experience and Convenience. Our findings also suggest a strong desire for personalization. Participants envisioned systems that could learn individual preferences for lighting, temperature, and routines, adapting intelligently over time. Although distinct from the mobile gaming context explored by Ng et al. [67], the underlying principle of *behavior-aware adaptation* remains relevant. Systems that dynamically adjust to user needs foster greater satisfaction and reduce the burden of manual control.

6.1.4 Automation and Efficiency. Participants recommended *proactive measures*, including predictive alerts for device malfunctions, to enable early intervention. They further emphasized the importance of energy conservation, suggesting that future systems should leverage user habit data to minimize resource wastage (e.g., turning off idle appliances). By marrying automation with occupant oversight, these homes could strike a balance between convenience and sustainability.

6.2 Preparing for the Future: Anticipating and Addressing System Anomalies

Participants underscored the need for robust, privacy-preserving solutions capable of *detecting and responding* to anomalies without overwhelming users with trivial alerts or unnecessarily intruding on their daily lives.

6.2.1 Intelligent Anomaly Detection. A dominant theme was the importance of accurate identification and classification of anomalies, ranging from environmental (e.g., flooding) to adversarial (e.g., hacking attempts). Some participants categorized anomalies into three types: *environmental, accidental, and adversarial*. They highlighted that clearly communicating these categories for end-users is critical, lest individuals become confused or disengaged by frequent or ambiguous notifications.

6.2.2 Self-Monitoring and Autonomous Problem-Solving. Many participants preferred *self-monitoring* systems that autonomously diagnose minor issues (e.g., sensor faults, outdated firmware) and initiate necessary updates or repairs with minimal user effort. They proposed periodic, scheduled checks—performed at off-peak hours to ensure that device maintenance does not disrupt normal usage.

6.2.3 Real-Time Alerts and Actionable Feedback. Another salient point was the tension between *immediacy and relevance* of alerts. Participants stressed that while rapid notifications are vital for urgent incidents, an overload of inconsequential alerts can desensitize residents to serious threats. To maintain a high level of trust and effectiveness, future designs must filter or categorize alerts to ensure occupants receive only *actionable* notifications for legitimate anomalies.

6.3 Collaborative Anomalies Exploration in Smart Home Systems: Insights from User Experiences

Analysis of user feedback and use cases highlights the alignment of design principles (Subsection 5.3.1) with real-world needs and challenges in smart homes. Below, we discuss the interplay between these principles and the observed practices, concerns, and preferences as observed throughout the study.

6.3.1 Device Maintenance and User Responsibilities. Participants frequently emphasized the importance of user awareness in maintaining device functionality, including regular updates, strong password practices, and monitoring physical damage. For example, they highlighted the need for users to routinely inspect devices for wear or anomalies, such as low battery levels or tampering. This underscores the critical interplay between autonomous smart systems and user intervention. Although automation reduces cognitive load, user engagement remains essential for resilience against system failures and cyber threats.

6.3.2 Cybersecurity and Privacy Concerns. Cybersecurity emerged as a primary concern, particularly regarding vulnerabilities in networked devices. Participants raised issues such as the hacking cameras or unauthorized control of lights, which not only compromise privacy but also introduce security risks. These concerns illustrate the importance of robust encryption protocols, secure authentication mechanisms, and user education about secure network configurations. Importantly, privacy and security are not merely technical challenges; they also reflect user expectations and trust in the technology.

6.3.3 Adapting to Environmental Contexts. Smart home systems need to consider the variety of contexts in which they function. Adaptive systems that can learn from and respond to unique environmental conditions are crucial for minimizing false alarms and enhancing reliability. Clear, user-friendly notifications and actionable alerts play a key role in this. Users appreciated systems that effectively conveyed information about issues such as device malfunctions, low battery levels, or connectivity problems.

6.3.4 Adaptive Learning Techniques. To address the integration of user feedback into the system, various ML approaches can be leveraged to support adaptive learning over time. For instance, as highlighted by Heartfield et al. [42], reinforcement learning can be employed to refine system accuracy based on user responses, enabling the dynamic adjustment of security thresholds and alert mechanisms. In addition, deep learning techniques, widely recognized for their ability to handle complex and high-dimensional data, can be applied to detect and classify a wide range of cyberattacks with high accuracy [87]. More recently, LLMs have emerged as a dominant paradigm in adaptive systems. LLMs offer the potential to capture user behavior patterns and generate automated, context-aware feedback [77], which can enhance personalization and reduce unnecessary alerts. Incorporating such learning frameworks could significantly improve a system's ability to adapt to individual user preferences and behaviors, thereby minimizing notification fatigue and enhancing its usability.

6.4 Limitations

Although our study featured a substantial participant pool, several limitations merit further consideration. First, the data collection took place within a specific geographic and institutional setting; Future work should replicate our methods across different regions and demographics to capture a wider range of smart home infrastructures. This includes recruiting participants through diverse channels—such as community organizations, public posts, and online platforms—and offering both remote and in-person participation options to reach individuals with varying levels of digital access and technical expertise. Second, although scenario-based focus groups yielded rich qualitative insights, real-world longitudinal deployments could confirm whether the proposed solutions and anomaly detection frameworks sustain user engagement over time. Third, while this study focused on the conceptual development and user-centered validation of the framework, future work involving the implementation and evaluation of collaborative anomaly exploration systems would serve as a valuable complement to the results

presented here. This includes benchmarking the framework against traditional anomaly detection models using standard metrics such as false positive rate, detection accuracy, and response latency, as well as assessing user satisfaction and system responsiveness in simulated deployment scenarios. Lastly, our research focused on a particular set of devices; investigating a broader spectrum of emerging IoT or wearable technologies may further deepen our understanding of collaborative anomaly exploration in diverse home environments.

7 CONCLUSION AND FUTURE WORK

Drawing on a mixed-method approach involving questionnaires and focus groups, this study offers a comprehensive perspective on designing next-generation smart homes that are user-friendly and secure. Our findings reveal how a device installation taxonomy can highlight functional requirements and privacy implications across diverse household contexts, whereas a scenario-based anomaly exploration framework addresses practical attack vectors (e.g., lock tampering, camera hijacking) through advanced technological safeguards and occupant oversight. Additionally, we emphasize collaborative design principles focused on context-awareness, multi-sensor detection, local data processing, actionable alerts, and explicit user control options—fostering deeper occupant–device collaboration. Taken together, these insights underscore the importance of integrating privacy-by-design, energy-conscious automation, and tailored anomaly detection to maintain a balanced and trustworthy smart home environment. Looking ahead, an important avenue for future work is the development of adaptive anomaly detection systems that fuse multi-sensor data while ensuring occupant privacy, potentially employing on-device machine learning to minimize cloud dependencies. Larger-scale and cross-cultural studies could validate the applicability of these design principles, extending the scenario-based approach to new device classes (e.g., wearables or health-focused sensors). Investigating long-term usability through real-world deployments would also shed light on how occupant behaviors evolve, how novel security threats emerge, and how these collaborative solutions can adapt under dynamic conditions.

ACKNOWLEDGEMENTS

The authors would like to acknowledge the scholarship and support provided by Taif University, Taif, Saudi Arabia. This work is partially supported by the GCHQ National Resilience Fellowship.

REFERENCES

[1] Abdulrahman Ihsan Abdulla, Ahmad Sinali Abdulraheem, Azar Abid Salih, MA Sadeeq, Abdulraheem Jamel Ahmed, Barwar M Ferzor, Omar Salih Sardar, and Sarkaft Ibrahim Mohammed. 2020. Internet of things and smart home security. *Technol. Rep. Kansai Univ* 62, 5 (2020), 2465–2476.

[2] Parastoo Abtahi, David Y Zhao, Jane L E, and James A Landay. 2017. Drone near me: Exploring touch-based human-drone interaction. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 1, 3 (2017), 1–8.

[3] Jane Agee. 2009. Developing qualitative research questions: A reflective process. *International journal of qualitative studies in education* 22, 4 (2009), 431–447.

[4] Tousif Ahmed, Apu Kapadia, Venkatesh Potluri, and Manohar Swaminathan. 2018. Up to a limit? privacy concerns of bystanders and their willingness to share additional information with visually impaired users of assistive technologies. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 2, 3 (2018), 1–27.

[5] Shadi Al-Sarawi, Mohammed Anbar, Rosni Abdullah, and Ahmad B Al Hawari. 2020. Internet of things market analysis forecasts, 2020–2030. In *2020 Fourth World Conference on smart trends in systems, security and sustainability (WorldS4)*. IEEE, 449–453.

[6] Bako Ali and Ali Ismail Awad. 2018. Cyber and physical security vulnerability assessment for IoT-based smart homes. *sensors* 18, 3 (2018), 817.

[7] Waqar Ali, Ghulam Dustgeer, Muhammad Awais, and Munam Ali Shah. 2017. IoT based smart home: Security challenges, security requirements and solutions. In *2017 23rd International Conference on Automation and Computing (ICAC)*. IEEE, 1–6.

[8] Mohammed Saeed Alkatheiri, Sajjad Hussain Chauhdary, and Mohammed A Alqarni. 2021. Seamless security apprise method for improving the reliability of sustainable energy-based smart home applications. *Sustainable Energy Technologies and Assessments* 45 (2021), 101219.

[9] Ashley Allen, Alexios Mylonas, Stilianos Vidalis, and Dimitris Gritzalis. 2024. Smart homes under siege: Assessing the robustness of physical security against wireless network attacks. *Computers & Security* 139 (2024), 103687.

[10] Azhar Alsufyani, Omar Rana, and Charith Perera. 2024. Knowledge-based cyber physical security at smart home: a review. *Comput. Surveys* 57 (2024), 1–36.

[11] Paolo Arcaini, Raffaela Mirandola, Elvinia Riccobene, Patrizia Scandurra, Alberto Arrigoni, Daniele Bosc, Federico Modica, and Rita Pedercini. 2020. Smart home platform supporting decentralized adaptive automation control. In *Proceedings of the 35th Annual ACM Symposium on Applied Computing*. 1893–1900.

[12] Radjaa Bensaid, Nabila Labraoui, Hafida Saidi, and Haythem Bany Salameh. 2025. Securing fog-assisted IoT smart homes: a federated learning-based intrusion detection approach. *Cluster Computing* 28, 1 (2025), 1–19.

[13] Akashdeep Bhardwaj, Manoj Kumar, Mohammed Alshehri, Ismail Keshta, Ahed Abugabah, and Sunil Kumar Sharma. 2024. Smart water management framework for irrigation in agriculture. *Environmental Technology* 45, 12 (2024), 2320–2334.

[14] Simon Birnbach, Simon Eberz, and Ivan Martinovic. 2022. Haunted house: physical smart home event verification in the presence of compromised sensors. *ACM Transactions on Internet of Things* 3, 3 (2022), 1–28.

[15] Richard E Boyatzis. 1998. *Transforming qualitative information: Thematic analysis and code development*. sage.

[16] Ian Brace. 2018. *Questionnaire design: How to plan, structure and write survey material for effective market research*. Kogan Page Publishers.

[17] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[18] Ziv Chang. 2019. IoT device security: locking out risks and threats to smart homes. *Trend Micro Research* 30 (2019).

[19] Ye Cheng, Minghui Xu, Yue Zhang, Kun Li, Ruoxi Wang, and Lian Yang. 2024. AutoIoT: Automated IoT Platform Using Large Language Models. *IEEE Internet of Things Journal* (2024).

[20] Eunjung Choi, Sunghyuk Kwon, Donghun Lee, Hogin Lee, and Min K Chung. 2014. Towards successful user interaction with systems: Focusing on user-derived gestures for smart home systems. *Applied ergonomics* 45, 4 (2014), 1196–1207.

[21] Jane Cleland-Huang, Ankit Agrawal, Michael Vierhauser, Michael Murphy, and Mike Prieto. 2022. Extending MAPE-K to support human-machine teaming. In *Proceedings of the 17th Symposium on Software Engineering for Adaptive and Self-Managing Systems*. 120–131.

[22] Jane Cleland-Huang, Theodore Chambers, Sebastian Zudaire, Muhammed Tawfiq Chowdhury, Ankit Agrawal, and Michael Vierhauser. 2024. Human–machine Teaming with Small Unmanned Aerial Systems in a MAPE-K Environment. *ACM Transactions on Autonomous and Adaptive Systems* 19, 1 (2024), 1–35.

[23] Juliet Corbin. 2007. Strategies for qualitative data analysis. *Journal of Qualitative Research* (2007), 67–85.

[24] Juliet Corbin and Anselm Strauss. 2014. *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage publications.

[25] Jessamyn Dahmen, Diane J Cook, Xiaobo Wang, and Wang Honglei. 2017. Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats. *Journal of reliable intelligent environments* 3 (2017), 83–98.

[26] Xuan Dai, Jian Mao, Jiawei Li, Qixiao Lin, and Jianwei Liu. 2022. Homeguardian: Detecting anomaly events in smart home systems. *Wireless Communications and Mobile Computing* 2022, 1 (2022), 8022033.

[27] Pedro HAD De Melo, Rodrigo Sanches Miani, and Pedro Frosi Rosa. 2022. FamilyGuard: a security architecture for anomaly detection in home networks. *Sensors* 22, 8 (2022), 2895.

[28] Marcos Paulo de Oliveira Camargo, Gabriel dos Santos Pereira, Daniel Almeida, Leandro Apolinario Bento, William Fernande Dorante, and Frank Jose Affonso. 2024. Ra4self-cps: a reference architecture for self-adaptive cyber-physical systems. *IEEE Latin America Transactions* 22, 2 (2024), 113–125.

[29] Soteris Demetriou, Nan Zhang, Yeonjoon Lee, XiaoFeng Wang, Carl A Gunter, Xiaoyong Zhou, and Michael Grace. 2017. HanGuard: SDN-driven protection of smart home WiFi devices from malicious mobile apps. In *Proceedings of the 10th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 122–133.

[30] Norman K Denzin and Yvonna S Lincoln. 2011. *The Sage handbook of qualitative research*. sage.

[31] Wenbo Ding and Hongxin Hu. 2018. On the safety of iot device physical interaction control. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. 832–846.

[32] Julia C Dunbar, Emily Bascom, Ashley Boone, and Alexis Hiniker. 2021. Is someone listening? audio-related privacy perceptions and design recommendations from guardians, pragmatists, and cynics. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 5, 3 (2021), 1–23.

[33] Pardis Emami Naeini, Martin Degeling, Lujo Bauer, Richard Chow, Lorrie Faith Cranor, Mohammad Reza Haghighat, and Heather Patterson. 2018. The influence of friends and experts on privacy decision making in IoT scenarios. *Proceedings of the ACM on Human-Computer Interaction* 2, CSCW (2018), 1–26.

[34] Earlence Fernandes, Jaeyeon Jung, and Atul Prakash. 2016. Security analysis of emerging smart home applications. In *2016 IEEE symposium on security and privacy (SP)*. IEEE, 636–654.

[35] Chenglong Fu, Qiang Zeng, and Xiaojiang Du. 2021. {HAWatcher}:{Semantics-Aware} anomaly detection for appified smart homes. In *30th USENIX Security Symposium (USENIX Security 21)*. 4223–4240.
[36] Andrea Gallardo, Chris Choy, Jaideep Juneja, Efe Bozkir, Camille Cobb, Lujo Bauer, and Lorrie Cranor. 2023. Speculative privacy concerns about AR glasses data collection. *Proceedings on Privacy Enhancing Technologies* (2023).
[37] Barney Glaser and Anselm Strauss. 2017. *Discovery of grounded theory: Strategies for qualitative research*. Routledge.
[38] Luke Haliburton, Pawel W Wozniak, Albrecht Schmidt, and Jasmin Niess. 2021. Charting the path: Requirements and constraints for technology-supported walking meetings. *Proceedings of the ACM on Human-Computer Interaction* 5, CSCW2 (2021), 1–31.
[39] Badis Hammi, Sherali Zeadally, Rida Khatoun, and Jamel Nebhen. 2022. Survey on smart homes: Vulnerabilities, risks, and countermeasures. *Computers & Security* 117 (2022), 102677.
[40] Julie M Haney and Wayne G Lutters. 2019. Motivating cybersecurity advocates: Implications for recruitment and retention. In *Proceedings of the 2019 on Computers and People Research Conference*. 109–117.
[41] Julie M Haney and Wayne G Lutters. 2021. Cybersecurity advocates: discovering the characteristics and skills of an emergent role. *Information & Computer Security* 29, 3 (2021), 485–499.
[42] Ryan Heartfield, George Loukas, Anatolij Bezemskij, and Emmanouil Panaousis. 2020. Self-configurable cyber-physical intrusion detection for smart homes using reinforcement learning. *IEEE Transactions on Information Forensics and Security* 16 (2020), 1720–1735.
[43] Ryan Heartfield, George Loukas, Sanja Budimir, Anatolij Bezemskij, Johnny RJ Fontaine, Avgoustinos Filippoupolitis, and Etienne Roesch. 2018. A taxonomy of cyber-physical threats and impact in the smart home. *Computers & Security* 78 (2018), 398–428.
[44] Grant Ho, Derek Leung, Pratyush Mishra, Ashkan Hosseini, Dawn Song, and David Wagner. 2016. Smart locks: Lessons for securing commodity internet of things devices. In *Proceedings of the 11th ACM on Asia conference on computer and communications security*. 461–472.
[45] Shama Naz Islam, Zubair Baig, and Sherali Zeadally. 2019. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. *IEEE Transactions on Industrial Informatics* 15, 12 (2019), 6522–6530.
[46] Abbas Javed, Amna Ehtsham, Muhammad Jawad, Muhammad Naeem Awais, Ayyaz-ul-Haq Qureshi, and Hadi Larijani. 2024. Implementation of Lightweight Machine Learning-Based Intrusion Detection System on IoT Devices of Smart Homes. *Future Internet* 16, 6 (2024), 200.
[47] Sai Anirudh Karre, Y Raghu Reddy, and Raghav Mittal. 2024. RE Methods for Virtual Reality Software Product Development: A Mapping Study. *ACM Transactions on Software Engineering and Methodology* 33, 4 (2024), 1–31.
[48] Ahmed Shany Khusheef, Mohammad Shahbazi, and Ramin Hashemi. 2024. Deep learning-based multi-sensor fusion for process monitoring: application to fused deposition modeling. *Arabian Journal for Science and Engineering* 49, 8 (2024), 10501–10522.
[49] Fasikaw Kibrete, Dereje Engida Woldemichael, and Hailu Shimels Gebremedhen. 2024. Multi-Sensor data fusion in intelligent fault diagnosis of rotating machines: A comprehensive review. *Measurement* (2024), 114658.
[50] Evan King, Haoxiang Yu, Sangsu Lee, and Christine Julien. 2024. Sasha: creative goal-oriented reasoning in smart homes with large language models. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 8, 1 (2024), 1–38.
[51] M Bala Krishna and Anudit Verma. 2016. A framework of smart homes connected devices using Internet of Things. In *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*. IEEE, 810–815.
[52] Hennie A Kruger and Wayne D Kearney. 2006. A prototype for assessing information security awareness. *Computers & security* 25, 4 (2006), 289–296.
[53] Benedikt Lebek, Jörg Uffen, Markus Neumann, Bernd Hohler, and Michael H. Breitner. 2014. Information security awareness and behavior: a theory-based literature review. *Management Research Review* 37, 12 (2014), 1049–1092.
[54] Chung-Yi Lin, Yi-Chen Ethan Yang, and Faegheh Moazeni. 2024. Flood Risks of Cyber-Physical Attacks in a Smart Storm Water System. *Water Resources Research* 60, 1 (2024), e2023WR034827.
[55] Tamara Lopez, Helen Sharp, Arosha Bandara, Thein Tun, Mark Levine, and Bashar Nuseibeh. 2023. Security responses in software development. *ACM Transactions on Software Engineering and Methodology* 32, 3 (2023), 1–29.
[56] George Loukas. 2015. *Cyber-physical attacks: A growing invisible threat*. Butterworth-Heinemann.
[57] Mohd Aliff Abdul Majid, Mohhidin Othman, Siti Fatimah Mohamad, Sarina Abdul Halim Lim, Aziz Yusof, et al. 2017. Piloting for interviews in qualitative research: Operationalization and lessons learnt. *International Journal of Academic Research in Business and Social Sciences* 7, 4 (2017), 1073–1080.
[58] Naresh K Malhotra, Sung S Kim, and James Agarwal. 2004. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information systems research* 15, 4 (2004), 336–355.
[59] Matthew B Miles and A Michael Huberman. 1994. *Qualitative data analysis: An expanded sourcebook*. sage.
[60] Yisroel Mirsky, Mordechai Guri, and Yuval Elovici. 2017. HVACKer: Bridging the air-gap by attacking the air conditioning system. *arXiv preprint arXiv:1703.10454* (2017).
[61] Richard Mitev, Anna Pazii, Markus Miettinen, William Enck, and Ahmad-Reza Sadeghi. 2020. Leakypick: Iot audio spy detector. In *Proceedings of the 36th Annual Computer Security Applications Conference*. 694–705.

[62] Arsalan Mosenia, Susmita Sur-Kolay, Anand Raghunathan, and Niraj K Jha. 2017. DISASTER: dedicated intelligent security attacks on sensor-triggered emergency responses. *IEEE Transactions on Multi-Scale Computing Systems* 3, 4 (2017), 255–268.
[63] Deirdre K Mulligan, Colin Koopman, and Nick Doty. 2016. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374, 2083 (2016), 20160118.
[64] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Faith Cranor, and Norman Sadeh. 2017. Privacy expectations and preferences in an {IoT} world. In *Thirteenth symposium on usable privacy and security (SOUPS 2017)*. 399–412.
[65] N Nanthini et al. 2024. Smart Home Security Enhancements with Cisco Packet Tracer. In *2024 International Conference on Computing and Data Science (ICCDS)*. IEEE, 1–6.
[66] Peter M Nardi. 2018. *Doing survey research: A guide to quantitative methods*. Routledge.
[67] Chloe Ng and Nicolai Marquardt. 2022. Eliciting User-Defined Touch and Mid-Air Gestures for Co-Located Mobile Gaming. *Proceedings of the ACM on Human-Computer Interaction* 6, ISS (2022), 303–327.
[68] Wan Ng. 2012. Can we teach digital natives digital literacy? *Computers & education* 59, 3 (2012), 1065–1078.
[69] Vanessa Peters. 2018. *Meeting Learners Where They Are: Using Microsoft Forms to Drive Improvement in Learning Outcomes*. Technical Report. Digital Promise.
[70] C Promwong. 1978. Introduction to social research: Quantitative and qualitative approaches. *Psychology* 18 (1978), 79–92.
[71] Keith F Punch. 2013. Introduction to social research: Quantitative and qualitative approaches. (2013).
[72] Ruobin Qi, Craig Rasband, Jun Zheng, and Raul Longoria. 2021. Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning. *Information* 12, 8 (2021), 328.
[73] Shwetha Rajaram, Chen Chen, Franziska Roesner, and Michael Nebeling. 2023. Eliciting security & privacy-informed sharing techniques for multi-user augmented reality. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–17.
[74] Hyeun-Suk Rhee, Cheongtag Kim, and Young U Ryu. 2009. Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & security* 28, 8 (2009), 816–826.
[75] Lyn Richards. 2020. Handling qualitative data: A practical guide. (2020).
[76] Abdiladif Said, Abdisalan Jama, Faysal Mahamud, Jayabalaji Mohan, and Prakash Ranganathan. 2018. Smart home vulnerabilities–a survey. In *Proceedings of the International Conference on Embedded Systems, Cyber-physical Systems, and Applications (ESCS)*. The Steering Committee of The World Congress in Computer Science, Computer ..., 83–87.
[77] Fatemeh Sarhaddi, Ngoc Thi Nguyen, Agustin Zuniga, Pan Hui, Sasu Tarkoma, Huber Flores, and Petteri Nurmi. 2025. LLMs and IoT: A Comprehensive Survey on Large Language Models and the Internet of Things. *Authorea Preprints* (2025).
[78] Eva-Maria Schomakers, Chantal Lidynia, Luisa Vervier, and Martina Ziefle. 2018. Of Guardians, Cynics, and Pragmatists-A Typology of Privacy Concerns and Behavior.. In *IoTBDS*. 153–163.
[79] P Shirisha, G Satish Kumarr, K Shivanjan, K Shiva Rama Krishna, and K Vineela. 2024. IoT based wifi fingerprint door lock system with raspberry pi & webcam. In *MATEC Web of Conferences*, Vol. 392. EDP Sciences, 01066.
[80] Zaied Shouran, Ahmad Ashari, and Tri Priyambodo. 2019. Internet of things (IoT) of smart home: privacy and security. *International Journal of Computer Applications* 182, 39 (2019), 3–8.
[81] Amit Kumar Sikder, Leonardo Babun, and A Selcuk Uluagac. 2021. Aegis+ a context-aware platform-independent security framework for smart home systems. *Digital Threats: Research and Practice* 2, 1 (2021), 1–33.
[82] Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A Selcuk Uluagac. 2021. A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials* 23, 2 (2021), 1125–1159.
[83] Shiva Sunar, Paria Shirani, Suryadipta Majumdar, and J David Brown. 2024. On Continuously Verifying Device-level Functional Integrity by Monitoring Correlated Smart Home Devices. In *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 219–230.
[84] Cisco Packet Tracer. 2013. Cisco Packet Tracer. *URL: http://www. cisco. com/web/learning/netacad/coursecatalog/PacketTracer. html* (2013).
[85] Sirisha Uppuluri and G Lakshmeeswari. 2024. Review of Security and Privacy-Based IoT Smart Home Access Control Devices. *Wireless Personal Communications* (2024), 1–40.
[86] Edwin Van Teijlingen and Vanora Hundley. 2001. The importance of pilot studies. *Social research update* 35 (2001), 1–4.
[87] Di Wang, Fangyu Li, Kaibo Liu, and Xi Zhang. 2024. Real-time cyber-physical security solution leveraging an integrated learning-based approach. *ACM Transactions on Sensor Networks* 20, 2 (2024), 1–22.
[88] Xuequn Wang, Tanya Jane McGill, and Jane E Klobas. 2020. I want it anyway: Consumer perceptions of smart home devices. *Journal of Computer Information Systems* (2020).
[89] Longfei Wei, Luis Puche Rondon, Amir Moghadasi, and Arif I Sarwat. 2018. Review of cyber-physical attacks and counter defense mechanisms for advanced metering infrastructure in smart grid. In *2018 IEEE/PES Transmission and Distribution Conference and Exposition (T&D)*. IEEE, 1–9.

[90] Evan D Wolff, KatE M GroWlEy, Maida O Lerner, Matthew B Welling, Michael G Gruden, and Jacob Canter. 2021. Navigating the solarwinds supply chain attack. *Procurement Law.* 56 (2021), 3.
[91] Li Ping Wong. 2008. Data analysis in qualitative research: A brief guide to using NVivo. *Malaysian family physician: the official journal of the Academy of Family Physicians of Malaysia* 3, 1 (2008), 14.
[92] Richmond Y Wong, Deirdre K Mulligan, Ellen Van Wyk, James Pierce, and John Chuang. 2017. Eliciting values reflections by engaging privacy futures using design workbooks. *Proceedings of the ACM on Human-Computer Interaction* 1, CSCW (2017), 1–26.
[93] Kevin B Wright. 2005. Researching Internet-based populations: Advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of computer-mediated communication* 10, 3 (2005), JCMC1034.
[94] Yinhao Xiao, Yizhen Jia, Chunchi Liu, Arwa Alrawais, Molka Rekik, and Zhiguang Shan. 2020. HomeShield: A credential-less authentication framework for smart home systems. *IEEE Internet of Things Journal* 7, 9 (2020), 7903–7918.
[95] Masaaki Yamauchi, Yuichi Ohsita, Masayuki Murata, Kensuke Ueda, and Yoshiaki Kato. 2019. Anomaly detection for smart home based on user behavior. In *2019 IEEE international conference on consumer electronics (ICCE)*. IEEE, 1–6.
[96] Tianfang Zhang, Huy Phan, Zijie Tang, Cong Shi, Yan Wang, Bo Yuan, and Yingying Chen. 2024. Inaudible Backdoor Attack via Stealthy Frequency Trigger Injection in Audio Spectrogram. In *Proceedings of the 30th Annual International Conference on Mobile Computing and Networking*. 31–45.

A FUTURE SMART HOME DEVICES BASED ON REAL DEVICES

A.1 Real Devices

In this section, different types of devices found in smart homes are categorized into two groups: devices and sensors. Table 6 presents the various smart home devices, their current status, and their potential future status.

A.1.1 Smart home technology. Smart home technology systems describe the arrangement of appliances, systems, and gadgets in a house that may be automatically or remotely controlled and monitored. Smart locks, smart lights, smart thermostats, smart security cameras, and smart home hubs or controllers are examples of the components that make up these systems. The main objectives of these systems are convenience, security, energy efficiency, and automation of home chores and operations.

A.1.2 Sensors. Sensors are electronic devices that recognize and react to specific physical or environmental cues. They serve as the "eyes and ears" of the smart home system, collecting information and communicating it to the hub or central control unit.

A.1.3 Robotic Assistance. Smart homes leverage robotic technology, offering substantial advantages for individuals seeking enhanced safety and comfort. The integration of automation and robotics into security systems and smart home solutions has transformed home security, home automation, and the completion of household chores.

A.2 Cisco Packet Tracer Device library

In this section, we list the devices used in the Cisco packet tracers. The Cisco Packet Tracer [84] is a robust network simulation tool that enables users to construct complex network setups and test various network scenarios. It can simulate and manage many smart home devices. Several commonly used smart home devices are supported.

- Air Conditioner: Lowers the temperature of a typical office space by -10°C per hour.
- Appliance: A smart home appliance can be turned on or off remotely.
- Battery: Displays the remaining charge as a percentage.
- Bluetooth speaker: Plays audio via Bluetooth connection from a portable music player.
- Carbon dioxide detector: Measures the concentration of carbon dioxide in the environment.
- Carbon monoxide detector: Measures the concentration of carbon monoxide in the environment.
- Ceiling fan: Automates the cooling process.
- Door: controls and monitors access to entry points
- Furnace: Raises the temperature of a typical office space by 10°C per hour.

Table 6. Current and future devices of smart homes.

Types of devices	Name	Current status	Future status
Systems	Outlets	Enable the remote control of any device.	Context-Aware access Control.
	Thermostat	Manages home heating and cooling systems.	Integrates other systems to enhance user comfort.
	Bulbs	Allow control of lighting, including turning on/off, dimming, and changing colors via a mobile app or voice commands.	Incorporate with sensors to adjust lighting (e.g., gesture sensor).
	Switches	Replace traditional light switches to provide remote control of lights.	Automatically adjust illumination based on user preferences.
	Locks	Provide keyless entry and remote locking/unlocking, enhancing home security and convenience.	Advanced biometric features including facial recognition, iris scanning, and multi-factor authentication.
	Security cameras	Provide video surveillance, allowing remote viewing and recording of video footage.	Receive live feeds showing individuals' identifies and recent behaviors.
	Doorbell cameras	Combine doorbells with cameras to remotely observe and communicate with visitors.	Obtain a real-time feed that shows the visitor's names and recent activities.
	Central control units	Serves as the central hub for managing and integrating various smart devices.	Predict user arrival times and adjust the environment accordingly.
	Smart speakers	Control smart home devices via voice, play music, and provide information.	Anticipate user demands and offer proactive suggestions throughout the day.
	Smoke and CO detectors	Monitor for smoke and carbon monoxide, sends alerts and integrate with other devices for safety automation.	Air quality monitoring involving detections of a wide range of pollutants and environmental.
Sensors	Door and window	Monitor opening/closing of doors and windows, often used for security.	Integrate with intelligent system to continuously learn and adapt, guaranteeing a safe, cozy, and energy-efficient home.
	Motion	Detect movement and can trigger actions such as turning on lights or sending alerts.	Create 3D maps of the surroundings to identify and distinguish between individuals and items.
	Enviromental	Monitor environmental data independently.	Utilize a combination of sensors for comprehensive environmental monitoring.
	VibroSense	Detects vibrations and monitor environmental changes.	Monitor vibrations and identify potential threats.
Robotic Assistant	Ballie robot		Provides autonomous assistance with tasks, monitoring, and interaction.
	Amazon Astro	Household robot for home monitoring.	Collaborates with other robots to ensure full home coverage.

- Garage door: Manages and restricts home access remotely.
- Home speaker: A loudspeaker with integrated voice command functionality.
- Humidifier: Increases the moisture content in the air.
- Humidity monitor: Detects and displays ambient humidity levels.
- Humiture monitor: Measures and reports both humidity and temperature.

- Lawn sprinkle: Controls water dispersion for lawn irrigation.
- Light: A lamp or lighting fixture that can be turned on or off remotely.
- Motion detector: Detects movement and triggers predefined responses.
- Portable music player: Plays audio via Bluetooth connectivity.
- Power meter: Displays real-time power consumption on a power line.
- Siren: Emits an alert when a dangerous event is detected.
- Smoke detector: Activates an alarm upon detecting smoke or unsafe environmental variables.
- Solar panel: Monitors and displays generated solar energy output.
- Sound frequency detector: Detects and analyzes environmental sound frequencies.
- Temperature monitor: Collects and translates temperature data into readable values.
- Thermostat: Enables remote control of central heating and hot water systems.
- Water drain: Drains water at a rate of 0.5 cm per hour in typical office setting.
- Water level monitor: Measures the water level in inches or centimeters.
- Webcam: Captures and transmits visual data in real-time.
- Wind detector: Detects the presence and intensity of wind in the environment.
- Window: A window that can be opened or closed remotely.

B HOME LAYOUT

In this section, we present three distinct home layout designs that could influence the security of smart home systems (Figure 7). Each layout was analyzed to highlight potential vulnerabilities and challenges in ensuring robust cyber-security and physical security. Additionally, we include one of these layouts (Figure 7d) reflect the participants anticipated cyber and physical attacks. These insights help identify variations in security requirements and strategies based on the different structural and functional arrangements of homes.

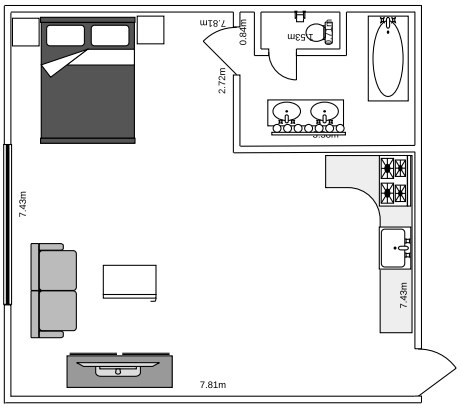
C ANOMALY EXPLORATION CAPABILITIES

To facilitate our research, we selected the attack types outlined in [10]. We presented these attack scenarios to the study participants as prompts. The goal was to stimulate critical thinking and spark creativity among participants. By exposing them to these potential threats, we encouraged them to envision and construct detailed scenarios. In addition, Table 7 presents the potential cyber-physical attacks on the devices provided in Appendix A.2.

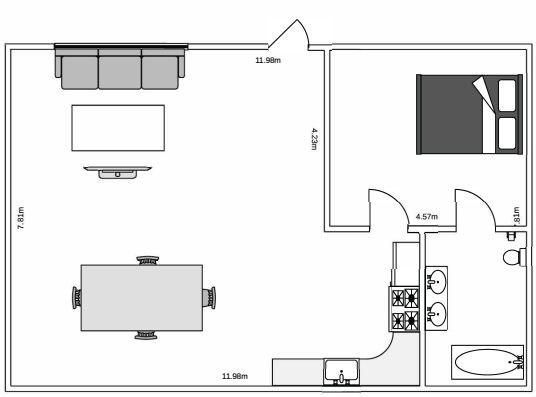
Table 7. Potential cyber-physical attacks on each device.

Device	Cyber Attack	Physical Attack
Air conditioner [60]	Unauthorized access.	Deliberately tampering with the device to cause malfunction or harm.
Battery [39]	Disabling the device by removing or destroying its battery.	Manipulating to give false reading or DoS attack to consume battery.
Carbon dioxide detector [62]	Hacking into the system to silence alarms.	Tampering with the sensor to produce erroneous results.
Appliance IoT [80][6]	Hacking the control system to turn appliances on and off at unsuitable times, resulting in inconvenience or danger.	Tampering involves preventing gadgets from functioning properly.
Bluetooth Speaker [56][43]	Disabling the speaker or its power supply.	Exploiting Bluetooth to broadcast unwanted audio.

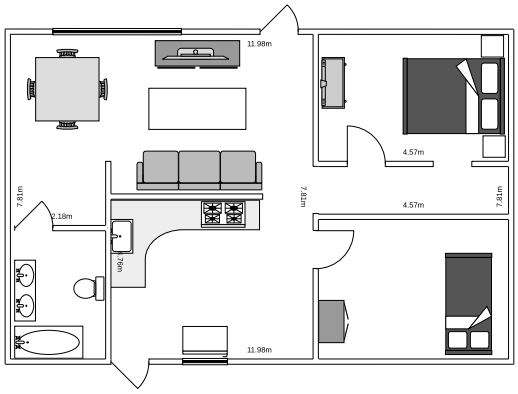
Carbon monoxide detector [34]	Manipulating the sensor to report false readings.	Breaching the system to deactivate alerts, risking health due to unnoticed CO2 increases.
Ceiling fan [60]	Unauthorized control to turn the fan on/off.	Damaging the motor or blades to induce failure.
Garage door and door [44]	Exploiting the smart lock system for illegal access.	Breaking the lock mechanism or forcibly entering.
Furnace [7]	Hacking the system to induce overheating or malfunction.	Sabotaging heating components or controls.
Home speaker [96]	Exploiting voice commands for unauthorized actions or spying on conversations.	Disabling speaker or power source.
Humidifier [95]	Gaining control over humidity levels.	Damage the water tank or misting mechanism.
Humidity monitor [83]	Altering data to display erroneous humidity levels.	Manipulating the sensor to yield erroneous measurements.
Lawn sprinkle [65]	Hacking to mismanage watering, risking plant damage from over or under-irrigation.	Wrecking sprinkler components or controls.
Light [18]	Hijacking by turning the light on or off at unpredictable times.	Breaking the bulb or damaging the fixture.
Motion detector [82][39]	Disable the sensor or cause false alarms.	Obstructing or destroying the sensor.
Portable music player [88]	Hijacking the Bluetooth connection to get access to music files.	Causing damage to the device.
Power meter [72][76][89]	Manipulating data to display erroneous power consumption.	Tampering with the meter to produce false readings.
Siren alert [34]	Disable the alarm system or cause false alarms.	Damage the siren to prevent it from emitting an alarm.
Solar panel [8][90]	Manipulating the system to provide inaccurate power generation readings.	Damaging the panel.
Sound frequency detector [61]	Manipulating data to display erroneous frequency values.	Damaging the sensor to hinder accurate detection.
Temperature monitor [85]	Hacking the system to provide erroneous temperature information.	Tampering with the sensor to provide misleading results.
Thermostat [46]	Changing the temperature without authorization, resulting in discomfort or energy waste.	Damaging the device to stop it from working.
Water drain [54]	Disabling the control system prevents drainage, perhaps resulting in flooding.	Blocking the drain to stop water flow.
Water level monitor [54][13]	Manipulating the data to show incorrect water levels.	Tampering with the sensor to give false readings.
Webcam [79]	Hacking the camera to acquire illegal access to video feeds.	Damaging to the camera and its connection.
Wind detector [45]	Manipulation of data to display erroneous wind speed/direction.	Damaging sensor by preventing accurate detection.
Window [31][14]	Using the control system to open and close windows without authorization.	Forcing entry or damaging.



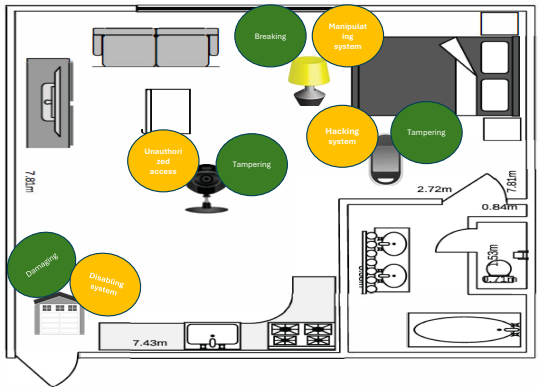
(a) Home layout 1.



(b) Home layout 2.



(c) Home Layout Number 3.



(d) Focus Group Use Cases.

Fig. 7. Home Layouts used by participants during focus groups and snapshot example for created use cases.

(1) Action-Interference Threats: These involve unauthorized actions that interfere with the normal functioning of a system, such as disabling alarms or manipulating thermostat settings.
(2) Trigger-Interference Threats: These occur when an attacker manipulates the triggers that cause certain actions in the system, such as altering motion sensors to prevent lights from turning on.
(3) Condition-Interference Threats: These threats involve altering the conditions under which certain actions are triggered, like changing temperature readings to prevent heating systems from activating.
(4) Impersonation: An attacker pretends to be a legitimate user to gain unauthorized access or perform unauthorized actions.
(5) False Data Injection: Injecting incorrect or manipulated data into a system to deceive the system or its users, such as feeding false temperature data to a thermostat.
(6) Side Channel Attack: Exploiting indirect information, such as power consumption patterns or electromagnetic emissions, to gain information about the system.

(7) DoS: Overloading the system with traffic or requests to make it unavailable to legitimate users.
(8) Triggering a Malicious App: Activating an application with harmful intent to perform malicious activities within the system.
(9) Internet Attack: Exploiting vulnerabilities in internet-connected devices or services to gain unauthorized access or disrupt services.
(10) Local Network Attack: Exploiting vulnerabilities within a local network, such as home Wi-Fi, to gain unauthorized access or disrupt services.
(11) Event Spoofing: Faking events, such as alarms or notifications, to deceive the system or its users.
(12) Over Privileged Control: Gaining access to control features or settings that should not be accessible to the attacker.
(13) Privilege Abuse: Misusing legitimate access privileges to perform unauthorized actions.
(14) Privilege Escalation: Exploiting vulnerabilities to gain higher-level access than initially authorized.
(15) Transitive Privilege: Gaining access to systems or data indirectly through compromised accounts or systems with legitimate access.
(16) Message Forgery: Creating fake messages that appear legitimate to deceive systems or users.
(17) Message Replay: Reusing intercepted messages to perform unauthorized actions.
(18) Masquerade Attack: An attacker pretends to be a legitimate user to gain unauthorized access or perform unauthorized actions.
(19) Device Compromise: Gaining control over a device to manipulate its functions or use it as a foothold for further attacks.
(20) Password Guessing: Attempting to gain access by systematically guessing passwords.
(21) Man in the Middle Attack (MIMA): Intercepting and potentially altering communication between two parties without their knowledge.
(22) DoS and Modification Attacks: Combining DoS attacks with unauthorized modifications to disrupt services and alter data.
(23) Malicious Enforcement Systems: Systems that enforce malicious policies or behaviors, often controlled by an attacker.

D USE CASES

Table 8. Use case scenarios.

Use case 1: Smoke system
In this scenario, when the smoke sensor in the kitchen detects gas, it suggests a possible gas leak from the cylinder, especially if the room temperature remains normal, indicating no fire. The high gas concentration, as confirmed by the proximity of the CO2 sensor to the kitchen and elevated gas meter readings, typically points to the cylinder as the source. If the meter's readings are unexpectedly high, this could either be due to a genuine leak or because the CO2 sensor's readings were altered either manually or remotely via the Internet. The motion sensor also becomes significant; by reviewing its data prior to the alert, we can determine whether there was any movement in the kitchen that might explain a gradual or sudden increase in CO2 levels. If no movement was recorded, it might be necessary to investigate the network traffic for potential remote interference with the sensor readings.
Use case 2: Plumbing system

If a pipe bursts, the water sensor attached to it will trigger an alert. To verify the accuracy of this alert, additional information is necessary. This includes measuring the water level around the affected pipe and examining the water meter readings to determine if there was a spike in water usage when the incident occurred. This data helps confirm whether the alert was valid. If the readings do not support a burst pipe scenario, it is possible that the sensor was falsely activated by an external interference or intrusion.
Use case 3: Doors/Windows accessing
On weekdays, the doors and windows are secured by 10 PM and by midnight on weekends. However, on a certain weekday, at 2 AM, a notification indicates that the external door is unexpectedly open. The system then accesses the camera to identify the person who has entered. If the individual is recognized as a member of the household, the system halts further action. If the individual is not recognized, the system activates to gather data from the motion sensors and lighting devices near the door and reviews CCTV footage from the time of the alert and the preceding 10 minutes. If no data is detected from these sensors, the alert is deemed false. Otherwise, it suggests the presence of an intruder.
Use case 4: Download applications without permission
The Google Nest Hub operates using house owner's unique credentials, which include biometric fingerprint, facial recognition, or a password, to authorize app downloads. It is expected to observe app installations when the owner is actively using the hub. However, if apps are downloaded at other times, it necessitates a review of the app store's history and settings is necessary to determine who installed them and when. If the installations are not attributed to the owner, it is essential to identify who else accessed the hub at the time of the downloads and monitor their activities. If no such user activity is detected, it suggests that hackers might have remotely executed the installations.
Use case 5: Light system
In the given scenario, when the living room light blinks unexpectedly, it suggests two potential causes: a technical glitch or unauthorized entry. To determine the cause, the initial step involves analyzing data from nearby devices. If the light, usually set to sleep mode, starts blinking erratically, this could indicate a security breach. In this case, data from motion sensors should be collected to track any unusual movement that might signal an attempt to disguise an intrusion. Additionally, checking footage from cameras positioned at doors and windows is crucial to identify any possible break-ins. If all these checks show normal results, the next step would be to inspect the network traffic to ascertain if the light is being manipulated remotely. Conversely, whether the light's blinking is part of its regular function and similar checks reveal no anomalies, then it is likely just a malfunction requiring human intervention.
Use case 6: Air conditioner system
Each room in the home is equipped with an individual thermostat system that can be adjusted manually or via connected devices such as smartphones. During the summer, adjustments are made to the bedroom's temperature setting if it exceeds both the preset value and the outdoor temperature. To determine whether these changes are legitimate or the result of a cyber-attack, the system checks the motion and sound sensors whenever the temperature setting is altered. If no presence is detected in the room or the adjacent corridor before and after the temperature change, a cyber-attack is suspected. Conversely, if the adjustment occurs while family members are at home during the day, it is likely normal. However, adjustments made when the house is unoccupied or during the night when the occupants are asleep could indicate a security breach. Therefore, further data must be gathered from the motion sensors and the control device near the thermostat to ascertain whether these changes are due to an intruder or a remote cyber-attack.
Use case 7: Unexpected events

Sarah arrives home at 6:00 PM, triggering the motion sensor. She then approach the door, enter the kitchen to grab some water, and finally settle down in front of the TV. This sequence of activities is established as a typical pattern. If an anomaly is detected, such as no network traffic indicating that the door was unlocked, or if the motion sensor is activated but the subsequent usual activities (like going to the fridge or sitting in front of the TV) do not occur within the next 30 minutes, it suggests that something unusual may be happening.
Use case 8: Heating system
At 1:00 AM in the Johnson family's smart home, everyone is asleep when a temperature sensor in the heating system detects a dangerously high temperature. The sensor sends this data to the home management system, which promptly shuts down the heating to prevent overheating or a potential fire, and sends an alert to Mr. Johnson's smartphone. Awakened by the alert, Mr. Johnson quickly checks his tablet, logs into the home management app, and views the real-time sensor data on the system dashboard. He reviews the temperature logs and system status to determine the urgency of the situation and whether it requires immediate attention or can be assessed by a professional in the morning.

E DEMOGRAPHICS

Our initial survey included questions about the participants' age, gender, and educational background (See Table 9). To further ensure a diverse and representative sample, we aimed to collect a comprehensive demographic profile. As a result, our screening survey comprises the following questions:
Q2: What is your email? (open-ended)
Q3: What is your gender? (Options: male, female, other, prefer not to say)
Q4: What is the highest degree that you have earned? (Options: bachelor's degree, master's degree, doctoral degree)

Table 9. Participant demographics.

Gender	Age	Education	Interest
Male 39%	20-25 20%	Bachelor 10%	Tech-savvy 17.5%
Female 59%	25-30 24%	Master's 63%	Not-tech 20%
Other 2%	30-35 34%	Doctoral 24%	Security 15%
	35-40 17%	Other 2%	Privacy 47.5%

F INSTRUMENT ITEMS

Table 10. Instrument items.

Construct	Item	Question
Digital literacy (DL) [68]	A1	I know about a lot of different technologies (such as: cloud computing, artificial intelligence, blockchain, cybersecurity, data sciences, software development, network administration, and others).
	A2	I keep up with important new technologies.
	A3	I can learn new technologies easily.
	A4	I know how to solve my own technical problems.
	A5	I use technologies to improve the convenience and efficiency of my daily routines.
	A6	I find technologies to be beneficial and worth the investment.
	A7	I feel comfortable recommending technologies to friends and family.
	A8	I am confident in my ability to search and evaluate information obtained from the Web.
	A9	I can install and uninstall software on my home devices.

Internet users' information privacy concerns (IUIPC) [58]	B1	I am aware of potential security threats.
	B2	I have sufficient knowledge about the cost of information security breaches.
	B3	I understand the risk of information security incidents.
	B4	I keep myself updated on information security awareness.
	B5	I regularly update the firmware of my smart home devices to ensure they are secure.
	B6	I use strong, unique passwords for my smart home devices and their associated accounts.
	B7	I understand how to configure my home network to enhance the security of my smart home devices (e.g., using WPA3 encryption, setting up a guest network).
	B8	I monitor my smart home network for unauthorized access or unusual activity.
	B9	I am confident in my ability to troubleshoot and resolve security issues with my smart home devices.
Information security awareness questionnaire (ISAQ) [52] [53] and self-efficacy in information security (SEIS) [74]	C1	In the context of smart home technology, privacy is a matter of users' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.
	C2	Control of personal information lies at the heart of user privacy when using smart home devices.
	C3	I believe that privacy is invaded when control is lost or unwillingly reduced as a result of using smart home technology.
	C4	Companies providing smart home devices should disclose how the data are collected, processed, and used.
	C5	A good privacy policy for smart home technology should have clear and conspicuous disclosure. It is very important to me that I am aware and knowledgeable about how my personal information will be used.
	C6	It usually bothers me when smart home device companies ask me for personal information.
	C7	When smart home device companies ask me for personal information, I sometimes think twice before providing it.
	C8	It bothers me to give personal information to so many smart home device companies.
	C9	I am concerned that smart home device companies are collecting too much personal information about me.

G INTERVIEW SCRIPT

Thank you all for taking the time to join our focus group today. My name is Azhar Alsufyani, and I will be facilitating our discussion. We have invited you here to explore your thoughts and experiences regarding the requirements for future smart homes, particularly focusing on collaborative anomaly detection capabilities. Our session is structured into three main parts, each lasting approximately 20 minutes. We will start by discussing various smart devices. For this part, you will find questions on red cards. Next, we will focus on smart home layouts. Questions related to this topic are on green cards. Finally, we will explore different use-case scenarios. The questions for this segment are on yellow cards. To assist with some of the questions, we have supplementary documents that you might find helpful: circle green cards provide information about cyber-attacks on smart devices. Separate cards within the circle green set also cover specific details on physical attacks.

G.1 Smart Home Devices

Q1. Please take a look at the table of devices provided. Based on their current status, what are the main functions of each device? How do you think these functions might change or evolve in the future?
Q2. Consider the devices listed in the table. Which of these devices could be integrated to work together for specific functions? Can you provide some examples of how they might collaborate? For instance, a motion sensor might work with a smart light.
Q3. What smart home devices do you currently use or are you familiar with? How do these devices interact or work together in your setup?
Q4. How would you categorize different types of smart home devices? What criteria would you use for grouping them?(e.g., by function or technology).
Q5. Let us think about smart home devices and how they can be grouped into different categories, such as sensors and tech systems. What do you think are some of the benefits and drawbacks of organizing them this way? Please share your thoughts on both the advantages and disadvantages.
Q6. Considering the smart home devices available today, how do you think they might change or improve in the future? What new features or capabilities would you expect to see?
Q7. Let us think about the future of robots in our homes. Currently, we have robots like vacuum cleaners that can clean our floors, and devices like Alexa that can control various aspects of our home. How do you envision the role of robots evolving in the future? How do you think they could assist with daily tasks beyond what they do today?
Q8. Let us discuss the potential roles of robots in our homes in the future. Currently, we have robots like the Hobbit robot, which helps the elderly with tasks. Thinking about this example, how do you envision robots assisting with various daily tasks in the future? Can you provide examples of tasks that future robots could help with, building on what current robots do today?
Q9. What do you think about robots like Ballie that can move around and help with tasks at home? How would you see them fitting into a smart home ecosystem?
Q10. Let us think about the future of smart home devices. How likely do you think it is that they will develop human-like senses such as sight

and hearing? What are some potential benefits and drawbacks of these capabilities?
Q11. Have you heard of VibroSense technology, which recognizes home activities through vibrations? If yes, how do you think this technology could be utilized in smart homes?

G.2 Smart Home Attacks

Q1. Do you think the layout and configuration of your smart home can affect the likelihood of attacks? Can you give examples of how layout might influence security?
Q2. What types of anomalies do you commonly encounter in your smart home? Can you describe some specific incidents?
Q3. What features do you think would be useful in detecting and exploring anomalies collaboratively in your smart home? Why would these features be beneficial?
Q4. What are some common issues or anomalies you encounter with your smart devices? How frequently do these issues occur e.g., malfunction?
Q5. How do you usually become aware of anomalies or unexpected behaviors in your smart home devices? Are there any specific signs or alerts you look for?
Q6. What actions do you take when you notice an anomaly in your smart home e.g., Updating password?
Q7. How would you prefer to explore and resolve anomalies in your smart home? What tools or methods do you think would be most effective e.g., real-time monitoring?
Q8. Can devices work together to resolve anomalies? What would this collaboration look like in practice?
Q9. What additional features or capabilities would you like to see in anomaly exploration tools for your smart home? How would these features help you?
Q10. Have you experienced any anomalies or unexpected behaviors with your smart home devices? Can you describe a specific incident and how you handled it?
Q11. How do you currently detect and handle anomalies in your smart home? Are there any tools or techniques you rely on?

G.3 Scenarios

Q1. Based on our discussion so far, please select specific smart devices and identify potential anomalies using the provided green cards for physical attacks and yellow cards for cyber-attacks. Which devices and anomalies do you think would be most relevant or interesting for creating your own use case? Please describe in detail the type of anomaly, the devices involved, and the potential impact of these anomalies.
Q2. Considering the different use cases we have discussed, what are the common characteristics of problems that occur? Are there any recurring themes or patterns in these problems? What characteristics do the solutions have?