KNOWLEDGE-BASED CYBER PHYSICAL SECURITY AT SMART HOME: A REVIEW

Azhar A. Alsufyani
School of Computer Science and Informatics
Cardiff University, UK
alsufyaniaa@cardiff.ac.uk

Omar Rana
School of Computer Science and Informatics
Cardiff University, UK
ranaof@cardiff.ac.uk

Charith Perera
School of Computer Science and Informatics
Cardiff University, UK
pererac@cardiff.ac.uk

October 31, 2023

ABSTRACT

Smart home systems represent the future of modern building infrastructure, integrating numerous devices and applications to elevate the overall quality of life. These systems establish connectivity among smart devices, leveraging network technologies and algorithmic control to monitor and manage the physical environment. However, ensuring robust security in smart homes, alongside securing the smart devices themselves, presents a formidable challenge. A substantial part of security solutions for smart homes rely on data-driven approaches (e.g., machine/deep learning) to identify and mitigate potential threats. These approaches involve training models on extensive datasets, distinguishing them from knowledge-driven methods. In this survey, we delve into the role of knowledge within smart homes, focusing on understanding and reasoning about various events and their utility towards securing smart homes. We propose a taxonomy to characterise the categorisation of decision-making approaches. By specifying the most common vulnerabilities, attacks, and threats, we are able to analyse and assess the countermeasures against them. We have also examined how smart homes have been evaluated in the reviewed papers. Furthermore, we explore the challenges inherent to smart homes and investigate existing solutions that aim to overcome these limitations. Finally, we take a look at key smart home security research gaps while defining future research directions of knowledge-driven schemes.

***K*eywords** Internet of Things, Reasoning, Cyber-Physical Security, Smart Home

1 Introduction

Cyber-physical systems (CPSs) combine hardware and software with doing a specific purpose. For example, actuators that function in the outside environment and receive information from sensors are controlled by embedded computers and communication networks to be capable of adaptation, autonomy, and efficiency in smart spaces [1]. The level of embeddedness of these devices where ranges between pervasive computing and ubiquitous computing [2].

In pervasive system [3], the main characteristics are effectiveness in smart homes, invisibility, localized scalability, and masking uneven conditioning. Thus, the biggest aim of pervasive computing is to make the connection between devices and applications seamless in our daily life. It assumes the environment is intelligent in a way that can detect any devices that enter and exit from the environment and also provide information that users need to it immediately.

While in ubiquitous system [2], which builds on the notion of free mobility by taking advantage of pervasive computing; as a result, it can create dynamic models of its multiple environments and apply its services accordingly. It is necessary to contribute to the artificial intelligence (AI) realm with high flexibility and effectiveness characteristics, providing the ubiquitous system the ability to take its planning autonomously and intelligently [4].

CPS enters various fields to perform some functions such as security, safety, reliability, monitoring environment, optimised services performance, and minimise costs. Typical applications of CPS include ambient assisted living, transportation, power grid, agriculture, industrial maintenance, healthcare, robotics, pollution control, and communication technologies.

A smart home is one of the applications in CPS that play a crucial role in human life from comfort, safety, management, security, and privacy perspectives. Moreover, the ultimate goal of a smart home is to improve the quality of life by developing all appliances of the house to become smart. Even though the concept of a smart home discuss more than two decades ago, it still does not achieve its main objectives and needs to investigate the obstacles to its progress [5].

It is argued that between 2025 and 2030, the number of devices connected to IoT will grow with economic values in various areas from $6.3 trillion to $12.6 trillion [6]. The responsibility for bolstering security also grows as a result of so much expansion. Meanwhile, smart home devices are prone to security threats and vulnerabilities. Thus, the developers are having difficulty maintaining the security of smart home systems.

1.1 Existing Surveys

Several recent surveys have focused on reviewing CPS or smart homes separately. To the best of our knowledge, there are no reviews about CPS at smart homes in terms of knowledge-based techniques. In this section, we study the novelty of our work and compare it against other surveys. Table 1 presents a summary of the surveyed papers.

The author of paper [7] discusses future technology for the smart house that is based on IoT. The paper also highlights the advantages of IoT-based smart home devices in terms of quality, reliability, and security. In [8], the authors performed an overview of demand response potential from smart buildings and discussed mechanisms to mitigate attacks at both the cyber and physical layers. Terence et al. [9] defined the seven major requirements for building smart homes depending on IoT technologies. Authors in [10] analysed the main technological and scientific trends development of smart homes for the next decades. This survey [11] focused on securing smart homes by detecting abnormal home and user behavior in the homes, then responding to threats. Gong et al. [12] discussed the architecture and framework for smart building in cyber-physical social systems (CPSS). Moreover, they proposed a CPSS-based smart building operation framework. A framework proposed by Stojkoska and Trivodaliev [13] aims to close the gap between today's smart home and future IoT-based smart homes.

The proliferation of communication between the cyber and physical world is a major challenge as a huge amount of data is produced [14]. Tavcar and Horvath [13] provide a review of data collection and analysis in real-time to support data-driven decision-making. As presented in [15], the existing solutions to protect physical, communication, processing, and storage components of cyber systems like cryptography, intrusion detection systems, and game theory are necessary to consider in some specific areas such as smart health, smart transportation, smart grid, smart home, public security. It is worth mentioning that the authors also stressed the importance of human error. Ahmad et al. [16] discussed the infrastructural transformation to smart cities taking into consideration that the CPS system is the pillar block for smart cities. For example, the smart city ecosystem in India is improved by building robust networking and enabling technological services. The analysis of security issues at the various CPS layers architecture as well as the risk assessment and methods of securing CPS was presented by [17]. Researchers in [18] analysed the main CPS security threats, vulnerabilities, and attacks, likewise cryptographic and non-cryptographic CPS security solutions. The threats categorise based on the three layers of CPS, and suggestion solutions to these threats are addressed in [19]. In terms of smart buildings, Ukachi [20] defined cyber-physical security threats, the negative consequences of these threats, and

some mitigation and defence mechanisms. In [21], we discussed security threats and security challenges on several applications of CPS systems.

Table 1: Related review papers.

Reference	Techniques		Domains		
	Data-driven system	Knowledge-based system	IoT	CPS	Smart home
Mussab et al. [7]			✓		✓
Jessamyn et al. [11]	✓				✓
Tavcar and Horvath [22]		✓		✓	
Ahmad et al. [16]				✓	
Terence et al. [9]			✓		✓
Junjian et al. [8]				✓	
Adam et al. [10]					✓
Kai et al. [12]	✓				✓
Hadi et al. [15]	✓			✓	
Yosef and Qusay [17]		✓			✓
Yaacoub et al. [18]				✓	
Nam and Shailendra [19]			✓	✓	
Ukachi [20]				✓	✓
Amit et al. [21]				✓	
Stojkoska et al. [13]			✓		✓
Conti et al. [14]				✓	
This article	✓	✓	✓	✓	✓

1.2 Contributions

This work presents a comprehensive systematic literature survey on cyber-physical security at smart homes. It presents a detailed analysis of the existing techniques that secure a smart home environment. This paper aims to benefit researchers in identifying future research directions and gaining insights for developing techniques by leveraging the context of smart homes to enhance home security. The key contribution of this paper can be summarized as follows:

- We provide a detailed overview of knowledge representation and context modeling methods in smart homes to identify sensing and actuating data.
- We survey the decision-making approaches, their inputs and outputs data, and real-time data required in some proposed approaches. We also present a taxonomy of the decision-making locations.
- We identify several threat models primarily in smart home systems. Moreover, we discuss the security countermeasures in order to mitigate the proposed attacks and threats in smart homes.
- We articulate smart home test beds and evaluation methods concerning the number of users and devices and the type of platforms and protocols used in each technique. We present figures to show the evaluation settings and its goals.
- Furthermore, we summarize most lessons from the reviewed studies. Finally, we highlight open challenges and discuss future research directions toward security in smart home systems.

1.3 Review Structure

The rest of the paper is structured into sections as follows: Section 2. presents the literature review method, including the research questions, search and selection process, inclusion and exclusion criteria, data extraction, and data analysis. The contextual information is presented in Section 3, along with modelling techniques. Section 4 reviews reasoning mechanisms for including inputs and output data in smart homes, whether inside or outside. Section 5 describes countermeasures against the different attacks. An in-depth analysis of current evaluation methods used in smart homes is provided in Section 6. Section 7 presents the lessons learned. We present the summary and future direction opportunities in Section 8. Finally, Section 9 presents the conclusions of the review.

2 Methodology

To create this review, we followed most of the steps proposed by Kitchenham [23] [24], which are illustrated in Figure 1. We concentrated our search on known scientific databases. These electronic databases include: Google Scholar, Scopus, Springer, IEEE eXplore, ACM Digital Library, Wiley Interscience, and Taylor & Francis Online.

2.1 Research Questions

The area of CPS for smart homes has considerably grown in the last decade. However, to the best of our knowledge, there is no review covering the knowledge-based mechanisms in the smart home. Hence, we aim to bridge this gap by reviewing this subject. In this paper, our analysis is guided by answering the following research questions (RQ):

- RQ1: How to represent and model the smart home knowledge?
- RQ2: What are the decision-making techniques, and how do these techniques capitalize on data produced in the smart home?
- RQ3: What is knowledge used for countermeasures against attacks and threats?
- RQ4: What evaluation strategies are practiced for evaluating smart home systems?
- RQ5: What are the open issues to be further investigated in regard to the security of smart homes?

These research questions are answered by fulfilling the contributions of this paper. To exemplify this, the definitions for knowledge representation and context modelling are covered in Section 3 (RQ1). For RQ2, we articulate smart home reasoning regarding contextual information in Section 4. Also, in Section 4 (RQ3), we discuss the smart home countermeasures. To address RQ4, we discuss the evaluation methods in terms of users, devices, protocols, and platforms. Finally, (RQ5) we investigate the further directions for security in smart home systems. Table 2 describes each research question with its rationale.

Table 2: The rationale behind the research questions.

Research question (RQ)	Rationale
RQ1: How to represent and model the smart home knowledge?	To define context types of smart home systems and find out the pieces of knowledge captured in these systems. With more focus on knowledge representation and modelling techniques.
RQ2: What are the decision-making techniques, and how do these techniques capitalize on data produced in the smart home?	This research question examines the decision-making approaches used in the smart home and explores its inputs, outputs, and location.
RQ3: What is knowledge used for countermeasures against attacks and threats?	This research question focuses on determining and discussing the countermeasures in the smart home against attacks and threats, which are mentioned in this paper.
RQ4: What evaluation strategies are practiced for evaluating smart home systems?	This research question aims to discover how the previous studies evaluate its proposed approaches.
RQ5: What are the open issues to be further investigated in regard to the security of smart homes?	To determine a possible research area in smart home security.

2.2 Search Process

Our search technique includes three methods: automatic, manual, and snowballing searches. The details of our search strategy are given below.

- Automatic search. It is performed using a search engine based on keywords that are shown in table 3. Google Scholar as a source because it has been recommended as a good way to minimise bias in favour of a specific

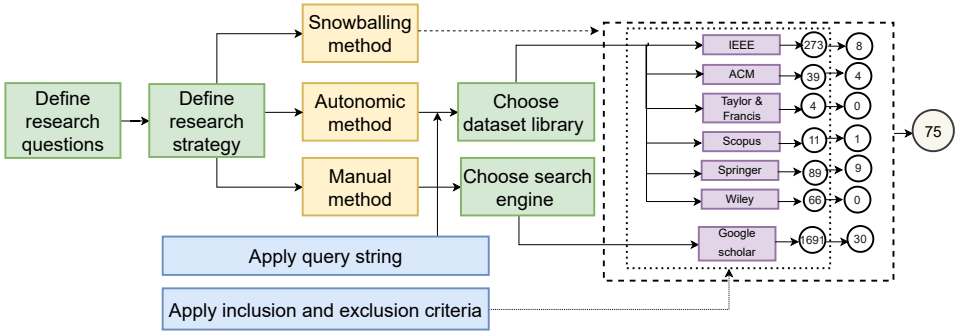


Figure 1: Search and selection process.

publication [25]. As a result, we were able to get a thorough overview of the entire range of publications available.

- Manual search. We conducted this stage by selecting sources from six databases: Scopus, Springer, IEEE, ACM, Wiley, and Taylor & Francis in different venues using terms in Table 3. For these sources, the studied time period is 2012-2022.
- Snowballing. We followed the guidelines of forward and backward phases of the snowballing method mentioned by Wohlin in [25]. The forward phase is based on known papers from the same relevant authors and time period that was acquired earlier through manual search. Then, using the references, backward snowballing is used to pick relevant papers based on title, abstract, and general structure review.

Table 3: Search Queries (SQ).

	Search query
SQ1	("self adaptation" OR "self-adaptive" OR "Self-adapting") AND ("Cyber Physical ")AND ("automation Home" OR "Smart Home" OR "connected Home").
SQ2	("cyber physical security" OR " cyber-physical security") AND ("Smart Home" OR "assisted living" OR "Automation Home").

2.3 Search Results

Our review goes through three phases: the first phase consists of a fast scan of the general ideas and notions. We are following the second phase, reading the abstract and conclusion for each paper to examine its relevance. Finally, applying the criteria phase. In the end, 41 papers have been selected for inclusion in our survey.

2.4 Inclusion and Exclusion Criteria

This review covers research published in English content between 2012 and 2022. Using the search terms in Table 3, to find papers in articles and conferences that focus on addressing CPS at smart homes with more focus on the knowledge base field. We excluded papers when we found that the main focus of the paper was on machine learning, and the sources could not be considered relevant for the purpose of our review.

2.5 Data Collection

Data extraction [25] is the process of collecting all relevant information from primary studies in order to answer the research questions defined in Section 2.1. The extracted information was used to build different taxonomies presented in the following sections in order to show the main streams of research focusing on smart home security systems.

2.6 Data Analysis

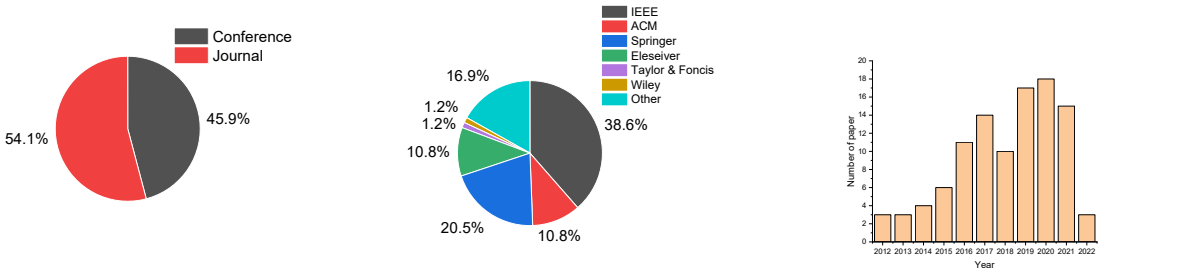
Figure 2a represents the percentage of the paper venue, which is nearly the same for both conference and journal, 46% and 54%, respectively. Looking at the specific details of Figure 2b, the first striking feature to report is that the IEEExplore dataset has the highest proportion. The most significant number of studies were published in the last three years Figure 2c.

3 knowledge representation and context modelling

In this section, we present the stages that data should go through before being processed which could be utilised to make decisions in Section 4. As tabulated in Table 6, various smart home contexts are considered in the literature. In subsection 3.3, a taxonomy of modelling methods is described.

3.1 Data Collection

This subsection aims at introducing the context types that used in smart home systems. Along with facts regarding the context-awareness concept, discuss the works that used it to improve the efficacy, efficiency, and relevance of systems, services, and interactions in smart homes. There is discussion of information that smart home devices have collected in the context of the smart home. Last but not least, how the data is entered, whether it is done manually or automatically.



(a) The percentage of Conference venue to Journal.

(b) The percentage of selected articles base on publication.

(c) Number of studies published per year.

Figure 2: An overview of the articles examined in various venues throughout a ten-year period.

3.1.1 Context Types

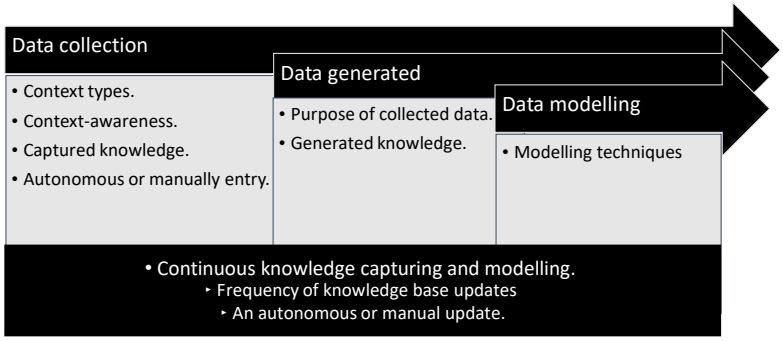


Figure 3: Dimensions of the three steps through which data in smart homes passes. It demonstrates the principles covered in each level, as well as the method of updating this data based on survey papers.

Context is information that can be used to describe the circumstances of an entity, such as a person, location, or object, that is deemed pertinent to the interaction between a user and an application which is referred to as contextual information [26]. Dynamism, stochasticity, and heterogeneity are inherent characteristics of the context [27]. As mentioned in [28] there are seven types of contextual information which are personal contexts, activity contexts, physical contexts, device contexts, systematic contexts, application contexts, and environmental contexts. Table 6 presents different types of context uses in a smart home. For example, PALS (Privacy via AnomaLy-detection System) [29] assumed the physical context, such as location, time, activity, roles. While in [30] considered the environmental context like temperature and dimmable light, as well as to [31], [32], [33], [34] [35] and [36] sense the context of a home environment, also [37] sense the smart home environment based on security functions. Authors in [38] take in their consideration the user activity context to understand the behavior of users correctly. Environment and applications context are mentioned in [27]. Situation information is the context of the initializing of communication network [39]. User context is captured in [40] to know the user expectation from the behavior of applications, in [41] covered the personal data that should protect. Moreover, in [42] discusses systematic context that collects the network traffic. Application context in [43] and [44] are concerned with analysing the smart applications in order to detect the over-privilege in the SmartThings framework or kinds of attacks. Besides, [45],[46] and [47] stated the application context. In [48], it contains contextual information from types of user context and physical context. Device context is mentioned in [49]. Amir et al. [34] concerned about the number of applications and users in a smart home.

3.1.2 Context-awareness

To describe the system that involved the ability to understand the intent of its users to improve its efficiency. Sikder et al. [38] proposed Aegies+ platform-independent context-aware security framework for smart homes that detects malicious activity. In [27], the authors presented a platform that enables the development of context-aware applications that can be autonomously adapted at runtime. ContextIoT [46] is a context-aware permission model to restrict unauthorised device access and detect malicious activities in a smart home. A context-aware authentication framework is being developed for smart home applications in order to access devices introduced by Ashibani et al. [28].

Table 4: Smart Home Contexts.

Reference		[30]	[50]	[38]	[29]	[31]	[51]	[45]	[52]	[46]	[56]	[47]	[39]	[40]	[42]	[32]	[58]	[28]	[44]	[34]	[48]
Personal context	Location	✓																✓			
	Service provider																				
	Metadata	✓																			
	Status	✓																			
	Priority		✓																		
	Role				✓																
	Time				✓																
	Endpoint communication	✓			✓																
	User expectation of app's behavior													✓							
	Name															✓		✓			
	Gender															✓					
	Height/Weight														✓						
	User's calendar																	✓			
	Historical information																	✓			
	Number of users																			✓	
	Age																			✓	
Activity context	User			✓																	
	Malicious			✓																	
	Location																				✓
	Posture																				✓
	Object																				✓
Physical context															✓						✓
Device context	Model	✓																			
	Description								✓		✓										
	Policies		✓																		
	States			✓		✓															
	Function								✓												
	Location								✓												
	Controller								✓												
	Control and flow attributes									✓											
	Trigger										✓										
	Action										✓										
Systematic context																✓					
Application context	Configuration information						✓														
	Semantic rules						✓														
	Meta data							✓					✓								
	Runtime information											✓									
	Situation information												✓								
	Abstract specification														✓						
	Behavior																		✓		
	Platform used																			✓	
	Number of application																			✓	
Environmental context	variable	✓																			
	Temperature																✓				

✓indicates this feature is present in the research.

3.1.3 Captured Knowledge

Determining the data type that should be used in a decision is the first step in the decision-making process. In [50], 219 diverse policies were gathered from actual smart home users, including 33 limitation policies and 146 demand conflicts. Likewise, data was collected from 50 malicious to assess the system against these threats. In [38], the authors gathered sensor features and smart home device states from day-to-day user activities, as well as malicious data from the adversary model. In [29], cloud service providers gathered information about a smart home from sensed data. In [31], the data collected from IoT devices is stored remotely in the cloud and locally in RES-Hub as a backup during a cloud outage, as well as to authenticate requests and issue commands that end devices can verify. Chi et al. [51] collect user configuration information from applications and send it to the cloud. In [52], features of home entities and set of concepts, devices capabilities, and security vocabulary are collected by cloud. ContexIoT [46] modifies the application code to add security-focused logic patches to the application to gather crucial running context. IOTGUARD [47] adds a new logic to an application's source code in order to collect data from it while it is running, including devices, events, actions, predicates that control device actions, and numerically valued properties of those actions. In [39], the application network connections are tracked. Authors in [40] derive user expectations from the behaviour of a set of installed automation applications. Authors in [53] claimed they collect raw data from smart home devices in real-time. In [44], it gathers wireless packets, including Z-Wave and ZigBee data. SERENIoT [35] are concerned with collecting packet signatures from network traffics. Mahadewa et al. collected the abstract definition of application-layer protocols and internal behaviours of entities in [54] [42]. In [55], proposed a monitoring system gathers bathroom activities. Device state information gathered from the cloud is utilized by RES-Hub [31]. Infrastructure is being gathered for smart homes in [45]. Ding et al. collect inter-app trigger-action interactions and physical channel information from the application description [56]. In [32], data packets transferred over a network are gathered in a knowledge base. User configurations are gathered [36]. The proposed approach takes static credentials, and contextual information [28]. Exchanged message semantic names are compiled [57]. HoMonit collects wireless packets [44].

3.1.4 Autonomous or Manually Entry

There are two sorts of data input methods used during the collecting process: manually and automatically. Lin et al. [30] suggested an automatic manager reduce the manual inputs from users, in some circumstances, the user still has to take action. In [50], users explicitly specify the priority and policies for smart home devices. Security analysts must provide input to HOMESCAN [42] [54]. In [29], a user provides feedback to an anomaly detection system. DepSys takes input from users to determine the application priority, and policy [45]. IOTGUARD requires inputs from the user for the application's configuration [47]. In applications for smart homes, users set their expectations [40]. In [36], the user identifies the configurations of smart home devices. However, the states of devices gather autonomously [38]. The suggested algorithm for automated categorization and decision-making [55]. To extract configuration information in [51], it used an automatic instrumentation script. A context collection logic is in charge of gathering application variables [46]. HanGuard sends situation information automatically over the control channel to the home router [39]. According to Ashibani et al., this method does not require human interaction [28]. HoMonit captures wireless traffic automatically [44].

3.2 Data Generated

Data generated in smart homes empowers homeowners and residents with information and control, leading to increased efficiency, convenience, security, and well-being. This subsection discusses the purpose of smart home data and data generated.

3.2.1 Purpose of These Knowledge

There are many reasons to collect smart home data. For example, [30] aims to collect data in order to assist the system in reasoning about attacks and to respond appropriately to them. In [50] use contextual information to identify user roles and consumer expectations for smart homes. Aegis built activity context to distinguish between benign and harmful uses of smart home devices and sensors for various user behaviors and use patterns [38]. HOMESCAN has the ability to discover security issues from the knowledge of smart home implementation [42] [54]. Discover abnormalities in data collecting from smart home device activity in [29]. In [55], it is a goal to recognise potentially life-threatening events. RES-Hub aims to provide resilience for smart homes when the cloud is unavailable [31]. Chi et al. collect application configurations to identify threats and minimise false alarms [51]. Depsys intends to provide comprehensive solutions for specifying, detecting and resolving conflicts in the home [45]. In [46], context information aids users in differentiating between benign and malicious behavior. The unanticipated physical interactions between applications are addressed by IoTMon [56]. Celik et al. aim to evaluate the collected data in light of a set of security and safety policies [47]. In [39], situation information is compared against policies to make sure that they originate from a legitimate home area network

(HAN) phone. To maintain user expectations from being violated, Expat captured this information from the installed application [40]. The knowledge base in [32] is used in order to protect smart home devices from network attacks. For devices to detect intrusions, user setups are required [36]. In [28], contextual information is used for the authentication process. It infers policies for which entity gains access control on devices based on entity names [57]. Wireless traffic is used to detect security threats in smart home applications [44]. The goal of SERENIoT is to examine network traffic to and from IoT devices in order to detect and prevent suspicious packets, and connections [35].

3.2.2 Generated Knowledge

The data collected in the smart home is leading to the conclusion of important knowledge that can be used to make decisions. In [30], uses the gathered contextual data to develop resource description frameworks (RDFs) triples as descriptions of the relationships between elements in smart homes. From the user credentials and device policies, user priorities and device policies are produced [50]. In [38], a context array of several user behaviors is constructed. A local labeled transition systems (LTS) representation of system integration is generated from the collected traces [42] [54]. Access control decisions are produced in the context of smart home [29]. Chi et al. built a risk ranking model for cross-app interference threats [51]. In [45], dependency information of the smart home application is inferred. In [56], inter-app interaction chains are built from an application analysis. Expat generated policies to be enforced on smart home platform [40]. In order to warn the user if there is a threat, device interaction rules are established [36]. User-defined rules are used to create home security policies, which are then applied to devices [57]. The operations of the SmartApps are derived from the encrypted traffic [44]. By separating packets and creating distinctive signatures, [35] retrieved the behaviour of the devices.

3.3 Data Modelling Techniques

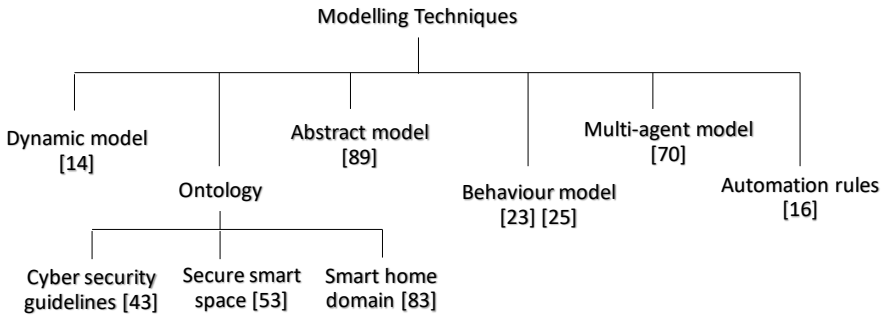


Figure 4: Types of modelling techniques.

Figure 4 shows a taxonomy of the modelling techniques. An ontology is used to model smart space as a knowledge base known as secure smart space ontology (SSSO) in [30]. Sofia et al. [29] represent the smart home context in a knowledge graph (KG) to aid in the definition of rules for controlling data access. In [51], each IoT application is represented by automation rules that adhere to the trigger-condition-action (TCA) paradigm in order to extract the application's rules for detecting threats. Tao et al. [52] proposed smart home domain ontology, ontology-based device description model, and ontology-based security management to fulfill the heterogeneity and security requirements. In [56], modelling the interaction behaviour of physical channels by assigning appropriate values to various physical channels in order to determine their distance from one another. To represent the runtime execution behaviour of applications in states and transitions, a unified dynamic model is proposed in [47]. In [40], an abstract model of an appified smart home platform is suggested to represent the user expectation invariants. Khan et al. [48] suggested an ontology called cyber security guidelines ontology (CSGO) as a way to express knowledge about security rules for interoperability and comprehension among smart home users. In [37], the smart home network uses a multi-agent approach to achieve shared security objectives.

3.4 Continuous Knowledge Capturing and Modelling

This subsection focuses on the pattern of knowledge-base updating, as well as whether it updates manually or automatically. These help to provide insights regarding the accuracy of the retrieved data and whether human intervention is required.

3.4.1 Frequency of Knowledge-base Updates

After each requested service is completed in the smart system, the RDF triples are updated in [30]. User priority and device policy lists are updated based on the user's expiration date in the system and each time another policy is issued, respectively [50]. Every time a new device or application is introduced to the system, the Aegis framework updates the training dataset [38]. HOMESCAN updated its collected information whenever new states were inferred [42] [54]. When PALS receives feedback from a user, it updates its knowledge graph [29]. Regular status updates from the cloud will be sent to RES-Hub [31]. DepSys updates the dependency information of the application when a conflicting dependency is found [45]. Applications' environment variables are changed when they are run [46]. Security policies of HanGuard are updated when the mobile phone is connected to the network [39]. Expat modifies the previous rules after creating the instrumented rules' file [40].

3.4.2 An Autonomous or Manual Update

The manager is responsible for updating the RDF triples automatically [30]. Kratos found any expiration dates and new additional policies automatically [50]. In [38], automatic updating of the training dataset whenever a new device is introduced. It seems that HOMESCAN updates its knowledge automatically [42] [54]. When an application is executed, its environment variables are updated automatically [46]. In [35], it updates its policies automatically.

4 Decision Making Approaches

Smart home context provided a huge amount of data collected from smart appliances and IoT smart devices. Hence, producing knowledge from these data is the role of the decision-making process. The responsibility of a smart home reasoning system is to determine the best course of action for meeting the efficiency and comfort objectives of the occupant, and their surroundings [59]. Furthermore, defined decision-making in self-adaptive systems as systems that make adaptive decisions dynamically in the face of unknown external situations to meet their functional and non-functional criteria [60]. The importance of decision-making approaches lies in their ability to improve the quality of decisions, increase efficiency, reduce risks, and enhance outcomes. This section discusses decision-making approaches that can assist in making informed and rational decisions. Furthermore, the inputs and outputs for various approaches, as well as whether it is performed locally or remotely. Bedsides, some key topics concerning decision-making are presented.

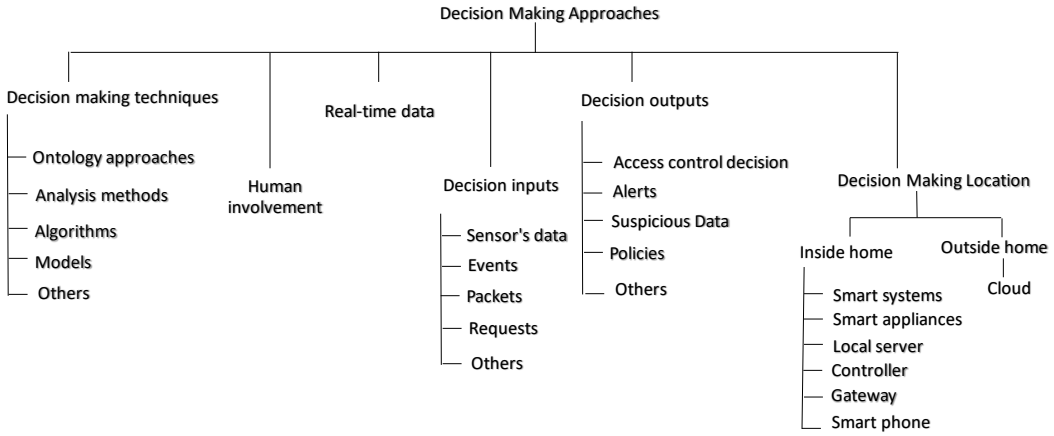


Figure 5: Decision making approaches taxonomy.

4.1 Decision Making Techniques

Better decisions that are in line with smart home concerns can be made by choosing the most appropriate method for a certain situation. Building a successful and functional context inside the house requires excellent decision-making. Table 5 summarises the decision-making techniques that are used by studies.

4.1.1 Ontology Approaches

Secure smart space ontology is suggested to help analysis and reasoning about the state of the smart space in a way that is intelligible by machines [30]. A context-based ontology [48] was developed to help security managers for making decisions about information security.

4.1.2 Analysis Methods

In [42] [54], authors proposed a hybrid analysis including dynamic testing, whitebox analysis, and trace analysis. Jia et al. [46] suggested using taint analysis to monitor runtime data, then identify the data source while displaying context information to the user. Ding and Hu [56] used a risk analysis mechanism to assess the dangers of the discovered chains of inter-app interactions. Side-channel analysis used by HOMONIT to monitor the encrypted wireless traffic [44]. To identify weaknesses in the framework architecture, [43] conduct an empirical investigation of the SmartThings platform and its applications.

4.1.3 Algorithms

Arun and Reza proposed a logic-based algorithm for detecting typical user behaviour at these access points and demanding user authentication [61]. IOTGUARD built a graph algorithm to extract events and actions of applications [47].

4.1.4 Models

Chi et al. presented a risk ranking model that may assess the severity of identified cross-app interference risks [51]. A user-specific score threshold for voiceprint verification is calculated using a Gaussian mixture model (GMM) [62]. The individual agents in the Beliefs, Desires, and Intentions (BDI) model function as autonomous agents making decisions [37]. In [63], STRIDE and DREAD models identify the threats in the network.

4.1.5 Others

Security management providers are presented in order to identify and address security/privacy risks for IoT [32]. The suggested system by Dutta et al. utilised semantic web technologies to carry out access control choices [29]. In [55], an effective reasoning module was proposed to identify user-critical scenarios and supply data for lifestyle pattern reasoning and daily function monitoring modules. ICN-iSapiens deployed intelligent monitoring and control applications in an effective and efficient manner by using information-centric networking [64]. Edge server can offer localised computation and storage [58]. A configuration tool that helps users in developing device interaction rules [36]. In [53], mutual authentication between smart devices smart home gateways is suggested. Self-signing technology [65] proposed to maintain the integrity of their security framework. The suggested method for mediating network communication across devices on the same network is made possible by software-defined networking [49]. In [35] proposed Blockchain as detecting anomalous in the network. A risk-based permission system in [34] reduces the malicious applications in the system.

4.2 Human Involvement

The automated manager drastically reduces human interaction while still requiring user entry [30]. Kratos [50] involved users in defining their policies and priorities, besides resolving the hard conflict in the system. In [54] [42], a security analyst needs in the specification extraction process of the proposed system. When conflicts are found, DepSys may need human input to adjust the policy [45]. User in [47] entered in application's configuration, and runtime prompts. A context-based ontology [48] involves the user in the modelling of security guidelines. SPIN (Security and Privacy for In-home Networks) keeps the user in control to stop an undesirable traffic flow [66]. Manju and Albert introduced an approach that entered users to configure smart home devices inside the internal network of smart homes [36]. In [28], authentication information needs to be input by users for security configuration. Alshaboti et al. proposed a user-defined network policy incorporating users in the security system [41].

4.3 Real-time Data

Real-time notifications are provided to users via Aegies+ [38]. The sensor knowledge graph maintains the real-time data that has been gathered from the smart home's sensors [29]. DepSys utilise real-time data in evaluating its approach [45]. The proposed platform implemented with real-time data [64]. In [58], processing of sensor data in real-time is facilitated by edge servers. SecFHome enabled smart gateway to analyse the collected data in the realtime [53].

Table 5: Decision Making Methods.

Techniques	Reference	Capabilities	Limitations
Ontology approaches	[30]	Dynamic access control	The suggested default policies are not appropriate for all possible cases. Manual labour is still required even if the manager strives to minimise human intervention.
	[48]	Support automation	Limited the sources of inputs.
Analysis methods	[54] [42]	Interacting with the system is necessary for the security analyst.	
	[46]	Decision made in context	Based on user decision.
	[56]	Discover unexpected behaviors	Based on user interaction.
	[44]	Detect the misbehave of smart applications.	
	[43]	Used combination of analysis mechanism	Conservative.
Algorithms	[61]	Local decision	Based on user behaviour only.
	[47]	Reduce the overhead	Need user interaction.
Models	[51]	Users do not need to set security objectives	False alarm.
	[62]	Used dynamic threshold method	The likelihood of a false rejection rate still exists.
	[37]	An autonomous entity	Cannot make decision on realtime data.
	[63]	Conscious of potential physical harm	
Others	[32]	Controls the user's firewall rules in a flexible manner	
	[34]	Static risk level	Human intervention.
	[55]	Adjustable to each user	As the number of possibilities is limited, a false alarm may occur.
	[64]	Fog services	
	[58]	Reduce latency	
	[36]	Increasing user awareness	Prone to human errors.
	[53]	Real-time decision and low latency	
	[65]	Done inside the smart home appliances	
	[49]	Convenient deployment	
	[35]	Distributed decision	Robustness.
	[29]	Dynamic reasoning	Coarse-grained policies.
Not mentioned	[50]	It has the ability to control a variety of individuals and devices.	If there are too many difficult conflicts, it could result in stalemate.
	[27]	Self-adapt and self-aware	Complex.
	[45]	Flexible	Non-critical safety system.
	[31]	Reliability	Complex.
	[39]	Static phone operating system	Flow decision cache limit.
	[40]	Support remote and local checking	High overhead.
	[66]		Human intervention.
	[28]	Real-time and continuous authentication	Human intervention.
	[57]	Both inputs and outputs are sent securely	Single point failure for controller.
	[41]	Support local and remote security	

Contextual data is gathered and evaluated in real time from secured sources [17]. HoMonit captures the wireless channel packets and detects the misbehaviors in real-time [44]. Also, SERENIoT monitors IoT devices data in realtime [35].

4.4 Inputs for Decision Making Process

Depending on the approach employed, different inputs are required, however the following components are present in many smart home decision-making methods.

4.4.1 Sensors Data

An effective reasoning module has been suggested based on the sensor data that appears in the proposed activities monitoring system [55]. In [31], data collected from smart home devices along with regular cloud status updates were employed as input to the suggested system.

4.4.2 Events

A succession of events that take place in the smart space is processed by the autonomic manager in order to assess their situations [30]. In [47], sensors collect application-specific events and their accompanying actions and predicates, then send them to a hub/cloud-based processing device for analysis.

4.4.3 Packets

Data packets transmitted across the home network are analysed in [57] as well as in [49] control packets of the local network. Side-channel data from the secured wireless traffic was utilised as the input in [44]. In addition, IoT device IP packets are tracked by [35]. In [41], used network traffic analysis to make a decision.

4.4.4 Requests

In [53], monitoring user access requests for smart home devices to maintain secure communication. Tyche uses application permission requests for device services as entry to the risk-based permission model [34].

4.4.5 Others

Priority assignment information and device rules are entered by the user [50]. System implementation, test cases, and prior knowledge serve as the foundation for HOMESCAN [54] [42]. In [29], decision-making is based on the user context and device type. The context reasoning of iCasa on its objectives, resources, and runtime architecture [27]. Configuration details are captured in [51]. DepSys analysis the metadata of applications to discover threats [45]. In [61], it is based on user actions and behaviors in making a decision. Amadeo et al. record stakeholder inputs, user preferences, and dynamic context-related aspects [64]. Interprocedure control and data flow information defined the context in the smart home in [46]. IoTMon is capable of recording physical interactions [56]. HanGuard gathers runtime data for the user's mobile device [39]. In [62], the log ratio score is used by analysis algorithm to make a decision. In [40], identifying user expectations. The design of the SmartThings programming framework is concerned by [43]. Threats that are related to the network are analyzed in [63]. User context and physical context are used to build its ontology [48]. In [32], it monitors network activity. Device security features are captured in [66]. Beliefs, Desires, and Intentions input into the proposed model [37]. It checked that the devices' connections were secure [36]. A module's codes are examined to ensure their integrity [65]. In [28], they gathered information on the user's location, profile, calendar, request time, and access activity patterns. Kumar et al. capture data for home devices [67].

4.5 Outputs for Decision Making Process

Decision-making procedures generate outputs that aid in decision-making and reaching conclusions; thus, the outputs of decision-making methods dependent on their input.

4.5.1 Access Control Decision

An in-context sensitive action is provided by ContexIoT [46]. HanGuard's router is responsible for making access decisions [39]. Tyche implemented risk-based access control decisions for the IoT system. In [65], authors support access control to identify user permissions. Services and data accessed by platform components [27].

4.5.2 Alerts

In [37], security alerts send to security agents when an attack in the smart home network is detected. The user is informed of an incursion using the authors' suggested approach [61]. In [36], unwanted contact triggers intrusion alarms to be generated.

4.5.3 Suspicious Data

Sivaramman et al. proposed a security solution to detect the network suspicious behavior in the network [32]. SPIN system distinguishes between normal and suspicious behavior at the network level [66]. SERENIoT [35] differentiate between malicious packets and connections using security policies.

4.5.4 Policies

Adaptive security policies are applied to threats that occur in the proposed system [30]. Kratos used a policy negotiation algorithm to resolve user disputes and optimise different conflict policies [50]. Moreover, Expat implemented contextual

access control policies for smart-home platforms on smart home applications [40]. PALS provides context dependent access control policies [29].

4.5.5 Others

In [42] [54], discovered security issues in smart home systems. The suggested system uses a reasoning algorithm to generate a daily activity report and send out notifications [55]. RES-Hub generates commands in accordance with the user specification [31]. HOMEGUARD can produce the analysis findings [51]. DepSys address conflicts that smart home technology detects [45]. Realtime services are provided in [64]. Ding et al. proposed an interaction chains algorithm to measures the risk level of interactions [56]. IOTGUARD recognises hazardous and insecure states in applications [47]. User authentication method results in differentiating the legal and illegal user in the system [62] [28]. In [43], discovered design flaws. Risk assessments that identify cyber-physical risks [63]. Security guidelines are produced in [48]. User commands are sent to carry out various activities [58] [57]. Flow decisions [49] and security decisions [41] are generated from smart home network services. Identifying inappropriate behaviour in applications [44].

4.6 Decision Making Location

We classified the studies that make a decision based on the site of the decision in their proposed approaches into inside and outside the home (Figure 5).

4.6.1 Inside Home

By securing devices and data inside home, the attack surface for potential cyberattacks is reduced. This makes it more challenging for attackers to infiltrate the smart home network. It is worth mentioning six locations in the home that can process data.

- Smart Phone. HOMEGUARD [51] collects configuration information by configuration collector to detect the cross-app interference threats without requiring users to identify security objectives. In [45], authors collect the application's metadata in order to resolve the conflict at installation time and run time. Although DepSys is flexible and allows for dynamic programme addition and removal at runtime, the safety criteria are not taken into account. HanGuard suggested a monitor on users' phones to create access control for applications [39]. In [62], the parameters of the GMM are compared to the dynamic threshold score to distinguish between legitimate and unauthorised users.
- Gateway. According to [49], there are controller devices and non-controller devices, and the controller devices only interact directly with controllers or the cloud to minimise privileges, leading to controllers issuing requests from smart home devices. SERENIoT [35] monitors network traffic to and from IoT devices in order to detect and block suspicious packets and connections. The reasoning module is proposed in [55], which uses raw data from (presence, humidity, and microphone) sensors to generate a daily activity report, trigger notifications, and alerts. The decision made in the gateway near the smart home may, in some cases, result in a false alarm. It is suggested that an autonomic manager [27] reason over three types of models, which include available services, goals, and architecture, before making a decision to grant an application, which is self-aware and self-adapt for the current situation, unless it is complex. In [31], when the cloud is unavailable, RES-Hub is responsible for collecting data from sensors and sending user specifications as commands to actuators. A setup tool to inform users if there is a network intrusion has been proposed by Pillai et al. In [53], the smart gateway makes the decision to securely collect and process data transmitted by smart devices in real time [36]. In [28], a secure gateway is proposed based on gathering the necessary contextual information and evaluating access to smart home devices.
- Controller. IoT controller devices in the home are used to control smart homes, as we found in Sovereign [57] suggested a local controller manages the authentication and access control system.
- Local Server. The work of Jose et al. [61] at multiple access points detected user activities and behaviours are compared with accepted user behaviour to spot intrusions or attempted intrusions. While this study analyses and stores the database at home, it is not much more secure due to the possibility of hackers gaining access to the IoT devices there. In [47], security services can approve or reject actions and use graph algorithms to lessen the burden of policy checking. To gather data from sensors and deliver commands to actuators, Qashlan et al. [58] developed smart home multi-edge servers in addition to cloud storage. Edge nodes conduct transactions, while the cloud is used for extensive analysis and long-term archiving.
- Smart Appliances. Lin et al. [30] an autonomic manager is responsible for analysing the system events such as user requests and threats, for producing adaptive security policies for IoT-based systems. The primary

strength of this manager is dynamic, which response to events in an adjustable manner, as opposed to being dependent on default policies, which are inappropriate in various cases. The suggested ontology in [48] assists the security manager in making decisions regarding the user and physical situation for the smart home devices. Kang et al. [65] offers security services for smart homes by assuring device authentication, availability, and data integrity. They employ access control and self-signing mechanisms to provide defence against threats.

- Smart Home Systems. HomeScan [54] [42] seeks to identify as many security flaws as possible in the partially implemented smart home integrations. Despite the fact that it provides dynamic analysis, the security analyst must interact with the system to perform the required functionalities. Authors [63] use threat analysis and risk assessment to identify threats and system-affected areas that should be the focus of investigators. Authors in [66] suggested a privacy manager that allows users to manually prohibit IoT devices on the network that exhibit potentially unfavourable behaviour.

4.6.2 Outside Home

Sending data from smart home devices to cloud servers for analysis, storage, and extra processing allows for the remote processing of smart home data on the cloud.

- Cloud. In [50], a policy manager evaluates device policies and user priorities that are collected by the backend server, starts user negotiations to settle conflict needs, and creates final policies. The policy manager is capable of manage different users and devices, but it may become impossible to resolve any hard conflict if there are too many of them, necessitating user engagement. Dutta et al. [29] proposed a cloud service provider, which is in charge of reasoning dynamically on user context, devices, and attributes. In [46], with the aid of the cloud-based permission service, a user can make an informed choice regarding control flow, data flow, and runtime value in order to carry out access control operations. By examining the SmartThings applications, IoTMon [56] directs developers and users to reduce the risk of inter-app interaction chains. Moosa et al. [40] proposed a satisfiability modulo theories (SMT) solver in the platform server to verify that policies satisfy the user expectation. In [43], they analyse the Samsung SmartThings programming framework to identify design weaknesses by using an empirical analysis including static analysis techniques, runtime testing, and manual analysis. It is the responsibility of the security management provider (SMP) to identify unusual activities in network activity [32]. A framework for multiple agents to engage in complicated reasoning is known as BDI modelling [37]. Within the cloud service layer, this BDI reasoning for agents takes place to detect network threats. In [67], the context of a smart home is in charge of the authentication procedure. In [44], presented a system for monitoring smart home applications of SmartThings based on encrypted wireless traffic called HoMonit. In [41], proposed security services monitor network traffic and issue security alerts. Tyche [34] proposed a permission-based model to categorise access requests into three risk levels to assist users in making decisions. Remote cloud and fog layers were suggested by Amadeo et al. [64] to enable real-time systems to monitor and manage smart home applications.

5 Countermeasures for threats and attacks

In the following subsections, we present common countermeasures and best practices to protect against different types of attacks. The countermeasure is aimed at protecting smart home against adversarial attacks. We first discuss the threats specific to that category and, then, follow it with the countermeasures approaches, and strategies both in literature and those used in existing systems. Finally, the knowledge employed in countermeasures has been mentioned (Subsection 5.3). A summary of the countermeasures related to the threat models described is shown in Figure 6.

5.1 Threats Model

It is interesting to note that there are a significant number of threats related to smart homes, and that number is rising as the number of gadgets in these homes increases. It is critical to create threat models for smart homes in order to identify potential security threats and vulnerabilities in these increasingly linked and automated environments. Here are a highlight of common threat models for smart homes.

5.1.1 Security Privileges

There are four types of these threats: firstly, over privileged control, like in [50] [44] smart devices are controlled by users in ways that go beyond what is necessary for their intended functioning, which could lead to unauthorised device access. Fernandes et al. [43] discussed the architectural fault in SmartApps that results in overprivilege. Second, privilege abuse unauthorised system changes by smart home users as potentially dangerous because they could lead

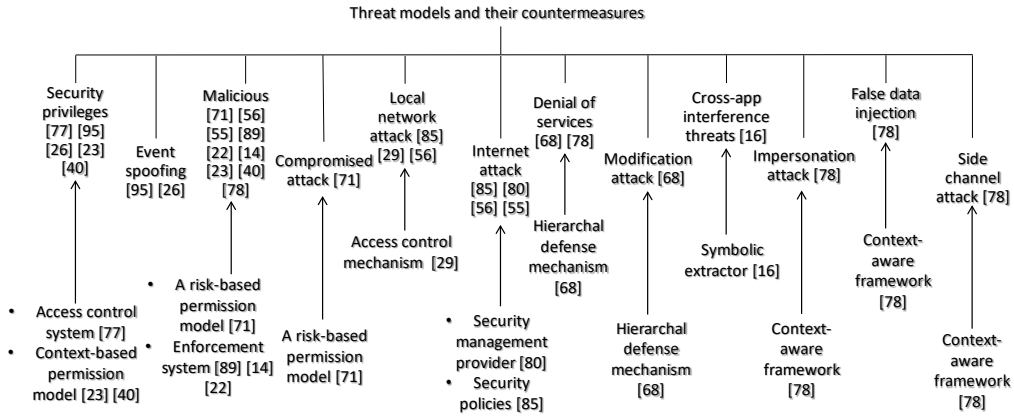


Figure 6: Existing related studies provide examples of threat models for smart homes, along with accompanying countermeasures.

to the installation of unknown applications [50]. Third, privilege escalation, by expelling system users who possess devices [50]. Authors highlighted how malicious programmes can access unapproved devices and sensitive event data due to the attackers escalate their privileges and cause security issues [56] [46]. Finally, transitive privilege, this occurs because of multiuser multi-device smart home access control that is insufficient, inaccurate, or uncaring [50].

5.1.2 Event Spoofing

To create a false event that legitimately activated certain devices [44]. Because SmartThings lacks proper security measures, Fernandes et al. developed this attack against it [43].

5.1.3 Malicious

In [34], discussed a malignant SmartApp. HomeScan [42] [54] conduct analysis against malicious control points, malicious hub, and malicious smart device attacks. Due to design and implementation issues in the applications, [40] was also investigated in harmful applications. Soteris et al. described IoT devices that trust the local network as being vulnerable to malicious software [39]. IOTGUARD [47] modeled harmful code which adds to an application or gives a user access to a programme that can lead to an unsafe situation. In [56] [46], demonstrated the attack happened because the malicious application resulted in unexpected behaviour. An application that modifies the status of connected devices in a specified way in order to launch a malicious application mentioned in [38].

5.1.4 Compromised Attack

A compromised SmartApp, as defined in [34], is the outcome of approving permission requests without understanding the danger an application presents, and an application might also seek more privileges than they require.

5.1.5 Local Network Attack

[35] taking into consideration malware in IoT devices from the local network. Compromised system in the local network via vulnerable devices studied in [49] [42].

5.1.6 Internet Attack

Corentin and David taking into account internet viruses on IoT devices [35]. Additionally, the attack at the network level was defined in [32]. Eavesdropping, intercepting and changing control activities, and intercepting and changing administration activities are the three forms of network attacks that were researched in [42] [54].

5.1.7 Denial of Service (DOS) Attack

In [58], defined DOS, in which the attacker sends the target a high number of transactions to prevent the target from being available. Skider et al. presented a malicious application that, at a certain value, terminates all active jobs on smart devices [38].

5.1.8 Modification Attack

An attacker might attempt to change or remove stored data for a specific person, or device mentioned by Qashlan et al. [58].

5.1.9 Cross-App Interference threats

Ten different cross-app interference threat types have been identified by Chi et al. [51]. It is divided into two action-interference threats, four trigger-interference threats, and four condition-interference threats.

5.1.10 Impersonation Attack

Skider et al. measured Aegis's performance against impersonation attacks in which an attacker uses the stolen code to open the smart lock by posing as a legitimate user after a battery monitoring software leaks the unlock code over SMS or an application that records voice commands and plays them back to pretend to be real users [38].

5.1.11 False Data Injection

The smart home may contain a malicious smart home application that uses falsified data to carry out harmful actions in a smart home device [38].

5.1.12 Side Channel Attack

An installed smart home application with design flaws can undertake lawful, but exposed side-channel actions that can be exploited by other applications in the system or the attacker himself [38].

5.2 Security Countermeasures

We classified the papers based on their purpose in regard to security. For example, some studies discussed how to mitigate the attacks or find a way to protect smart homes, while others gave ways to detect malicious or raised alerts. The classification of countermeasures reported in related research is shown in Table 6.

Table 6: The countermeasures purpose for proposed threat model.

Purpose	Studies	Threat model	Countermeasures
Detection	[51]	Action-interference threats, trigger-Interference threats, and condition-interference threats	
	[38]	Impersonation, false data injection, side channel attack, DoS, and triggering a malicious app	Context-aware framework [38]
	[54]	Internet attack, local network attack and event spoofing	
	[42]		
	[50]	Over privileged control, privilege abuse, privilege escalation, and transitive privilege	Access control system
Prevention	[67]	Message forgery, message replay, masquerade attack, device compromise, DoS threat, password guessing, and man in the middle attack (MIMA)	A secure session key-based unique addressing scheme (SSKUAI).
	[58]	Denial of Service and modification attacks	A hierarchical defence mechanism.
	[39]	Malicious	Enforcement systems.
	[56]	Privilege escalation and malicious	Context-based permission system.
Mitigation	[34]	Malicious and compromised attack	A risk-based permission model.
	[40]	Malicious	Enforcement systems.
	[49]	Local network attack	Access control mechanism.
Combination	[32]	Internet attack	Security management provider (SMP).
	[44]	Over privileged control and event spoofing	
	[43]		
	[46]	Privilege escalation and malicious	Context-based permission system.
	[47]	Malicious	Enforcement systems.
	[35]	Local network attack and internet attack	Security policies.

In [50], provided security by offering policy negotiation and conflict resolution. Aegis is a context-aware security system that monitors user behaviours in smart homes to identify malicious conduct [38]. Mahadewa et al. proposed

a system to discover security flaws in the implementation of smart home integrations [54] [42]. In [29], introduced an anomaly detection engine to produce warnings regarding suspicious actions in a home environment. A reasoning module was proposed in [55] to identify user-critical scenarios and offer data for the module that monitors daily function and lifestyle pattern reasoning. HOMEGUARD [51] aims to detect cross-app interference threats in smart home applications. Jose et al. [61] suggested a logic-based security method to detect intrusions in smart homes and provide alerts. IoT threats are recognised and countered by ContexIoT [46]. IOTGUARD [47], a dynamic, policy-based enforcement system for IoT, detects insecure device states and blocks them. Khan et al. [48] developed a context-based ontology that guideline the user to mitigate the vulnerability risks. In [37], presented a multi-agent collaboration model to detect threats in the smart home network. Pillai et al. [36] an intrusion detection system for detecting undesired actions in smart home devices and alerting users. In [68], reported authentication vulnerabilities caused by application developer mistakes. Zhang et al. observe the smart home application to find the inappropriate behaviour and then alert users via text message [44]. Doan et al. proposed RES-Hub use the OAuth 2.0 authentication and authorisation architecture to ensure safe access and management over home services and devices while the cloud is down [31].

In [39], presented HanGuard system to protect the smart home network from mobile application attacks. Sivaraman et al. recommended using software-defined technologies to protect IoT devices from unwanted network activity [32]. The authors of [58] used blockchain technology and edge computing to provide resistance against modification and DoS attacks. In [66], presented a platform that protects the home network by blocking traffic flow and devices that cause attacks. Guo et al. [53] proposed an authentication scheme to secure communication between the gateway and devices. In [65], introduced a security framework that offers an integrity mechanism for preventing security risks by utilising self-signing and access control approaches. A context-aware authentication framework is presented to secure communication to mitigate the attacks [28]. Moreover, Kumar et al. proposed a scheme to authenticate the communication between the user and smart home using a secure key session [67]. SERENIoT defends IoT devices from threats by blocking traffic different from the specification [35]. In [64], enhanced security since data is kept at the network edge and hostile attacks have less chance of success. To minimise risks, as seen in [30] suggested threat mitigation policies. Ren et al. [62] developed a mobile authentication system to reduce the false rejection rate. Expat [40] safeguards the appified smart-home system from hazards posed by rogue or malfunctioning automation apps. To mitigate the affected devices, Goutam et al. established least-privileges policies [49]. As a security measure to counteract address resolution protocol (ARP) spoofing attacks, authors suggested an IPv4 ARP server [41]. In [34], the proposed model for smart homes reduces the risk of overprivilege applications.

Table 6 provides an overview of the countermeasure methods against the proposed threats model in section 5.2. A secure session key-based unique addressing scheme (SSKUAI), [67] proposed to monitor smart home IoT networks by altering the conventional IPv6 protocol. To be resilient against modification and DoS attacks, a hierarchical defence strategy is provided in [58]. Sivaraman et al. [32] introduced a security management provider entity that offers security and privacy for the IoT devices in their home as a service. Kratos [50] is an access control system that resolves conflicts between user requests in order to preserve smart home security. A context-based permission system-ContexIoT [46] overcomes the threat model by including data dependence in the context definition. In [34], presented a risk-based permission model that reduces malicious application attacks. An enforcement system proposed in [40] to prevent installed malicious applications. IOTGUARD directly prevents dangerous and undesirable conditions in single-app, and multi-app contexts [47]. In [39], secure the smart home network by enforcing access control restrictions across user phones and IoT devices. Hesita deploys a least-privilege network strategy to lower the danger of compromise in smart homes [49]. Thomasset et al. developed security policies for IoT devices to detect and block aberrant behavior [35].

In order to improve the security of smart homes, security access control techniques should be included. According to the research, there are five different access control techniques:

1. Multi-user Access Control: Kratos [50] is a multi-user smart home access control system that addresses the diverse and conflicting demands of different users.
2. Context-aware Access Control: Using the attribute based access control (ABAC) model [69], determine the access control for the devices and data in the smart home environment [29]. ContexIoT [46] is a permission-based system that ensures the contextual integrity of IoT apps while they are running. In [40], proposed policies for fine-grained, contextual access control for smart-home platforms. The context-aware authentication framework introduced by Ashibani et al. in [28] is capable of protecting smart devices from unauthorised access from both anonymous and known users.
3. Situation-aware Access Control: Demetriou et al. [39] gather situation information via userspace applications, which detects whether an authorised application is establishing a network connection with a target IoT device.
4. Network Access Control: Distributed access control networks were recommended by [58] to guard against unauthorised data access in smart home systems utilising the ABAC system. Hestia [49] is a default access control mechanism for devices in the smart home network that is flexible to scale with the changing smart

home environment and simple enough to be deployed today. In [57], proposed access control policies for smart home local networks that authenticate entities through data encryption and decryption. Mohammed et al. introduced static and dynamic access control, both of which can be used to prevent or block malicious activities [41].

5. Risk-based Access Control: People may perceive varying levels of danger as acceptable because Tyche developed risk assessments of access control requests from applications by users [34].
6. Security Role: In [50], indicate the five various roles in smart home to understand the user priority: owners (father and mother), adult, guest, and child. By grouping applications into four categories—energy, health, security, and entertainment—semantic aware multilevel equivalence class based policy (SAMECP), which was first introduced in [45], reduces the cognitive strain on users. Each mobile device connected to the home network has a role assigned by HanGuard, such as HAN user for accessing a specific home domain, admin role for all domains, and guest for unregistered devices [39].

5.3 Knowledge Used for Countermeasures

Smart homes must be kept secure with the aid of defences against attacks that are based on specific knowledge that has been gathered previously. In [30], to apply its countermeasures, it bases them on the access policy, security/trust/threat levels and assessment policies, threat mitigation policy, and contextual security information. IOTGUARD gathers application-specific data from its source code to enforce the rules that stop undesirable behaviours [47]. The router receives the runtime scenario from the user's phone and acts accordingly to enforce the policy [39]. Users' voiceprints are used in a dynamic threshold technique to determine speaker ratings [62]. Expat [40] reviewed the user-entered policy to ensure that it was appropriate for user expectations. By using access control rules, Sivaraman et al. developed a security management provider entity to offer security for IoT devices at the network level [32]. In [58], it is based on the rules and regulations that are upheld by blockchain miners and smart contracts to safeguard smart home appliances. Devices in SPIN with security capabilities can prevent traffic from unreliable devices [66]. In [37], to achieve security, it represents the gathered data using the BDI model. Rules define how the detecting device interacts with the devices in the smart home network to identify intrusions and undesirable behavior [36]. SecFHome introduces an authentication mechanism to secure data after transferring the session keys [53]. The security dangers are lessened by defining the functions of each module in the suggested architecture [65]. Ashibani et al. proposed a context-aware authentication system for smart homes using the user's location, profile, calendar, and access behavior patterns to enable access to home devices [28]. Secret keys and device identities are used as knowledge in securing the communication over smart home network [67]. For resource identification, security implementation, and the definition of security rules, Sovereign leverages semantic names [57]. Hestia implemented least-privileges policies to protect smart home security [49]. In [41], by implementing various access control measures, network attacks are reduced. Physical device operations are used as knowledge to assess the potential threats from it [34].

6 Testbeds and Evaluation

Testbeds and evaluation offer a way to put the theories, models, and hypotheses put out in the research to the test and to validate them. They enable researchers to evaluate whether the suggested concepts perform as anticipated in practical settings. The following sections discussed evaluation procedures, followed by the factors used in these strategies.

6.1 Evaluation Approaches

This section focuses on the evaluation strategy that was applied in the studies. A summary of the evaluation methods is provided in Table 7.

To validate the performance of an autonomic security manager, Lin et al. [30] proposed a case study for a conference room with a large number of events. In [50], conducting a case study in order to evaluate the effectiveness and overhead of Kratos. The effectiveness and feasibility of Aegis+ were tested by building a smart home testbed [38]. Case studies were implemented in [54] to find security issues. To assess the applicability of the risk-based approach, three case studies were created [34]. In [63], a case study was built in order to evaluate the proposed model and provide a proof-of-concept for the compromised devices.

An experiment was carried out in the laboratory to highlight the vulnerability of smart home devices [33]. Lalanda et al. simulate the ICasa platform [27] to measure the complexity of services, timely execution, and the cost of adaptation. In [31], presented a demo as a proof-of-concept for SmartThings devices. Authors in [51] developed experiments to prove that HOMEGUARD can detect cross-app interference threats. Static and run time analysis was used in [45] to detect conflict in the smart home system. Also, the CASAS dataset [70] was used in the runtime analysis, which

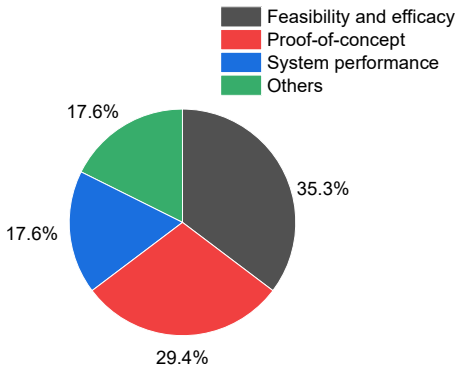


Figure 7: Evaluation goals.

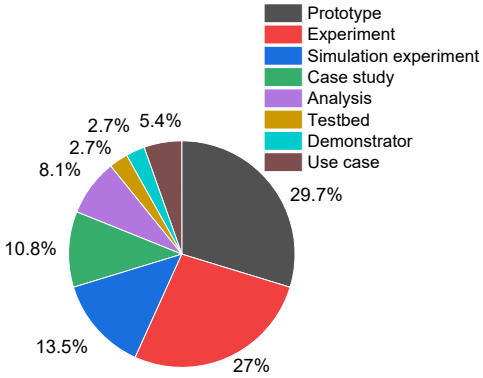


Figure 8: Evaluation settings overview.

lasted for 34 days. An experiment developed by Jose et al. [61] to observe user behaviour at different access points in a studio apartment over a 30-day period. In [52], evaluated the system performance by designing prototypes and proofs. Amadeo et al. deployed a testbed as proof-of-concept of the proposed framework [64]. Simulation experiment executed to measure the IOTGUARD's overhead performance [47]. Demetriou et al. [39] designed a prototype and experiment to evaluate HanGuard's performance. In [62], developed an experiment to test the performance of voice-print verification. Expat [40] evaluated its effectiveness using their own testbed and dataset. An experiment was presented in [42] to identify the vulnerabilities by extracting the execution log and Wi-Fi traffic from the implementation of smart home systems. As a proof-of-concept, Fernandes et al. [43] developed empirical analysis to exploit the flawed design by building the SmartApps dataset and conducting a survey on 22 participants. SERENIoT simulates network compatibility across numerous days on Amazon AWS as a proof-of-concept [35]. Attribute-smart contract based edge scheme [58] simulated to demonstrate its feasibility and efficiency in authenticating the smart home users and devices. For proof-of-concept, Rafferty et al. proposed a use case illustrating the coordination of threat response decisions between operational availability and security risk agents [37]. SceFHome was simulated in [53] to calculate communication and processing expenses. Security analysis proved the security of the proposed security scheme [67]. Hu et al. conducted proof-of-concept studies to assess the security of a smart home assistant application [68].

The authors created a prototype to test the privacy, security, and performance of Sovereign [57] and to evaluate the network performance of Hestia [49]. HoMonit's prototype was created by Zhang et al. to test the efficacy and efficiency of the suggested system [44]. In [41], SDN-based framework's feasibility was prototyped, countering malicious network monitoring and ARP spoofing. Contexlot prototyped [46] on a dataset consist of 25 SmartApps against 22 attacks. The suggested network-centric method was prototyped to demonstrate its efficacy in protecting multiple smart home devices that were deployed in the lab [32]. Ding et al. [56] implemented a prototype of over 185 official SmartThings applications. The authors created a prototype to evaluate the efficacy of a network intrusion detection system in a smart home network [36]. In [28], designed a prototype for a context-based authentication system to evaluate its flexibility. Lastdrager et al. implemented a prototype for the SPIN platform in their lab [66].

In Figure 7, it is obvious that Proof-of-Concept was the most stated goal (10 publications), followed by System Performance (8 publications). Then, feasibility and efficacy and others goals combined to constitute 12 papers. The terminology used to describe the various methods of evaluation varies greatly between publications. Figure 8 give an overview of the eight types of methods used in reviewed papers. The most stated evaluation type was "Prototype" with 11 publications. The second noticeable method used by authors is "Experiment". Then, followed by "Simulation experiment" and "Case study" with five and four papers, respectively. It is noted that the "Analysis" method used in three papers. However, the least-popular method used to evaluate studies papers are "Testbed", "Demonstrator", and "Use case".

6.2 Evaluation Factors

There are a variety of criteria that should be considered while evaluating the evaluation methods. The six variables that affect the evaluation are covered in this subsection.

6.2.1 Devices

Smart home environments are equipped with an assortment of smart devices in order to bring comfort to the home occupants. By the end of this decade, the number of smart devices in our daily lives will be in the billions [71].

Table 7: Evaluation strategy.

Reference	Evaluation method	Evaluation goal	Location	Duration	Data type
[30]	Case study	System performance for a large-scale smart space			
[50]	Case study	Effectiveness and performance overhead			User demands.
[38]	Testbed	The effectiveness and feasibility of system		15 days	Benign daily activities dataset (85,000 events)
[54]	Case studies	To find security issues			
[27]	Simulation experiment	To assess: • A fog-level platform's ability to manage the complexity of creating a context module. • The time that a context module will take to execute, especially if it deals with conflict resolution. • The price of the autonomous manager's dynamic context adaptability.	Orange Labs		
[31]	Demonstrator	Proof-of-concept			
[51]	Experiment	Proof of concept			Configuration information.
[45]	Static and run time analysis	To measure the likelihood of true conflict between applications, number of runtime conflict, conflict resolution capability, and a level of conflict for each app,		34 days (runtime analysis)	Dependency information.
[61]	Experiment	To track user activity at different access points	Studio apartment	A month	Logical sensing parameters.
[52]	Prototype	System performance			
[64]	Experimental testbed	Proof-of-concept			
[46]	Prototype	Proof-of-concept			Control and data flow attributes of the app, and runtime values.
[56]	Prototype experiment	Proof-of-concept			Inter-app trigger-action interactions and physical channel information
[47]	Simulation experiment	System overhead performance			Application's information.
[39]	Experiment	System performance			Situation information.
[62]	Experiment	System performance			Utterance from speaker.
[40]	Experiment	System performance			Rules and policies.
[42]	Experiment	To identify the vulnerabilities.			Execution log and Wi-Fi traffic.
[43]	Empirical analysis	Proof-of-concept			
[63]	Case study	Proof-of-concept			
[32]	Prototype	To demonstrate its effectiveness in safeguarding several smart home gadgets	Lab		
[58]	Simulation experiment	Feasibility and efficiency of the system			
[66]	Prototype		Lab		
[37]	Use case	Proof-of-concept			
[36]	Prototype	System performance			
[53]	Simulation	Communication costs and computation costs performance			
[28]	Prototype	To show the flexibility of the security framework			
[67]	Security analysis				
[68]	Experiment	Proof-of-concept			
[57]	Prototype	To assesses the privacy and security, and performance of system			
[49]	Prototype	Network performance			
[35]	Simulation	Proof-of-concept		From 1 hour to multiple days	
[44]	Prototype	To evaluate the effectiveness and efficiency of the proposed system			Wireless traffic.
[41]	Prototype	To show the feasibility of the proposed framework			
[33]	Experiment		Lab		
[34]	3 Case studies				

Accordingly, access control for multi-devices is deemed a daunting challenge in the smart home. To explain this, table 8 presents an overview of devices that are used in the smart home context. For example, seventeen different devices are considered in [50]. A real-world smart environment can be created using fourteen distinct kinds of commercially available sensors, devices, and controllers [38]. Author in [39] selected four devices (three actuators and one sensor) for real-world testing. Smart home in [40] equipped with eighteen devices. In [43], authors download one hundred thirty-two devices that are compatible with SmartThings, which are called device handlers. Authors used the Philips Hue light bulb and the Nest smoke alarm to show the value of having the security management provider provide IoT protection as a value-add service [32]. Five types of devices were used in the implementation of smart home environments [28]. This paper [44] collected data from (7) ZigBee devices and (4) Z-Wave devices. In [35], simulating their smart home context using fifty-three various devices. Twenty-nine devices were used in this paper to simulate the smart home [47].

Table 8: Smart home devices, users and applications.

Reference	Devices Number	Devices list	Users Number	Applications Number
[50]	17	Smart home hub, smart light, smart lock, smart camera, smart thermostat, motion sensor, door sensor, and temperature sensor.	43	10
[38]	6-24	Sensors, controllers (smartphone, tablet, and voice-controlled smart), and devices (smart light, smart lock, etc.).	20	
[39]	4	WeMo Switch and WeMo Motion, the WeMo in.sight.AC1, and My N3rd		55
[40]	18			15
[43]	132			499
[32]	2	Philips Hue light-bulb and the Nest smoke-alarm.		
[28]	5	Single-board computer, wireless router, smart switch, smart light hub, smart bulb		
[44]	11	ZigBee devices and Z-Wave devices		30
[35]	53			
[72]			7	
[47]	29			65

6.2.2 Platforms

There are different sorts of platforms that use in the smart home. For instance, Samsung SmartThings platform [73] is implemented in [50], [31], [46], [44], [34], [43], [56] and [51] which has the largest market share in consumer IoT and supports the greatest number of open-source apps and smart home devices, while in [38] used Google Home platform. Moreover, in [38], they selected the Samsung SmartThings platform for the purpose of developing a single-platform smart home environment in which all devices share the same access point, while in multi-platform smart home systems where the gadgets for smart homes are deployed as separate entities, and no common access point is taken into account during installation they selected Amazon Alexa, Philips Hue, LIFX smart bulbs, and Samsung SmartThings. ICasa platform [74] [27] offers a suitable model for development as well as a number of tools for interfacing with heterogeneous devices, gathering and displaying contextual data, and enabling the dynamic deployment of components and applications. The posited multi-layer cloud platform [52] for IoT-based smart homes consisted of a public cloud provided by Amazon EC2 and two private smart home cloud platforms supported by DGUT and Canbo. ICN-iSapiens platform [64] provides real-time services while obscuring the diversity of IoT devices. Celik et al. evaluated their system using the SmartThings platform and IFTTT [75] trigger-action platform [47]. In [40], authors integrated their prototype into OpenHAB smart-home platform [76], which is used to automate interactions between smart devices. An open source measurement platform called SPIN [77] builds a dynamic and user-friendly data model of the IoT devices in a home network used in [66].

6.2.3 Applications

Amit et el. [50] installed ten different official SmartThings applications that control other devices. In [39], they connected home area network IoT devices with WiFi/Internet only using 55 different Android applications. Fifteen automation applications are installed in the smart home platform [40]. In [43], 499 SmartApps were downloaded from the SmartThings app store, and a thorough examination was done. From the SmartThings public GitHub repository [78], thirty SmartApps were chosen where twenty SmartApps that work with ZigBee devices and ten SmartApps connecting Z-Wave devices [44]. In [47], authors used thirty-five SmartThings and thirty IFTTT market vetted applications (sixty-five applications) in order to evaluate their smart home. Table 8 summarizes the number of devices used in the smart home environment of the studied papers.

6.2.4 Protocols

In [54], communication protocols (ZigBee and Wi-Fi) that are used in Philips Hue, LIFX, and Chromecast are analysed to extract an end to end specification in order to detect security vulnerabilities. To link the devices to the hub, Tam et al. utilised MQTT (Message Queuing Telemetry Transport [79]) via TCP/IP, while they used Bluetooth, ZigBee, Z-Wave as communication protocol, and OAuth 2.0 authorisation protocol [80] [81] is used to authenticate SmartApps APIs to ensure that the Web-App has access to the devices it needs [31]. In [64], the CCN-Lite software [82] is a simple CCNx/NDNx protocol implementation. It has been chosen to facilitate ICN connections between different boards in smart homes and used IEEE 802.11g to communicate with devices wirelessly. In [43], studying the OAuth protocol used by the client-side Web IDE and the SmartThings backend to analyze its attack. Kumar et al. [67] proposed the modification of the IPv6 protocol, and they used Diffie-Hellman key exchange protocol in order to secure the communication in the smart home network. In [57], implementing a lightweight named data networking (NDN), [83] protocol that safeguards data by securing device-to-device communications. Wei et al. [44] detect misbehaving SmartApps by snooping the wireless (Z-Wave and ZigBee) traffic between the SmartThings hub and devices. In [33], it explained the issues of the universal plug-n-play (UPnP) protocol that devices use to communicate with the home gateway.

6.2.5 Events

An event is anything that occurs in the smart home system that alters its state. Aegis+ [38] notifies users of any malicious SHS activity in real time by comparing a dataset consisting of over 85,000 events collected from user's daily activities against 24 different datasets for a total of over 15,000 events. In [30], authors used a sequence of 160 events to validate their investigation. Yunhan et al. [46] evaluated the system on a dataset including 283 SmartApps by injecting device events to trigger 916 events handling logic. In [43], they found sensitive information is not adequately protected by the SmartThings event subsystem, which devices utilise to interact asynchronously with SmartApps via events. Celik et al. [47] for each IFTTT rule to be mapped to an IoT app, they extract the events (86, 30) and actions (78, 30) from SmartThings applications and IFTTT trigger-action applets, respectively. Authors in [44] prove the lack of event integrity protection in the SmartThings architecture leads to event spoofing attacks.

6.2.6 Users

Users of smart homes often share the installed smart home devices in a multi-user scenario, as a typical house consists of multiple people (See table 8). Author in [50] collected smart home data from forty-three real-life users. In [38], acquired information from twenty users where various users were simultaneously conducting daily tasks. Authors in [72] prototyped the smart home with seven households, including couples, roommates, and families with children of various ages. The needs and preferences of smart home users are defined in terms of as explained in these papers [72] [84] [85] [50] to include a fine-grained access control system to prevent the overprivileged challenges, role-based access control system to restrict access to the devices and applications in a home setting, location-based and time-based access control for transient users in a communal setting, automation rules aim to reconcile competing requests, and users accepted per-device roles for private rooms in a shared environment. Aegis+ [38] analyses user activity using a pattern of contexts in order to identify concurrent operations carried out by several people and devices in a smart home system. The proposed bathroom monitoring system [55] provides the user's daily activities, personal care routines, and lifestyle habits as knowledge for the reasoning module. In [63], explained the thorny issues stem from the disclosure of behavioural patterns such as the exchange of private information, insurance-related fraud, and burglary.

7 LESSONS LEARNED

As a vast amount of varied data is created [14], the growth of communication between the cyber and physical worlds is a serious problem. As a result, securing this data from assaults requires taking into account more than one level in the smart home architecture through which this data passes. Lack of user awareness, hacked devices, network risks, and malicious programmes are just a few examples. In this section, we show how the recommended strategies are inadequate. Based on peer-reviewed articles, we make the following observations:
Users. Cyber security guidelines ontology (CSGO) is suggested in order to help user to perform security guidelines automatically [48]. Furthermore, access control systems that define user roles and privileges depending on smart home conditions are being researched in the literature to avoid conflicting requests between users. Most current research is directed at making whole processes in smart home automation, despite the fact that adding the user into the loop of operations would make the user more aware of important faults in his system.
Devices. software defined networking (SDN) [86] is proposed in [39] in order to protect IoT devices. Qashlan et al. proposed a decentralization authentication scheme to secure IoT devices [58]. In [65], proposed a security framework

on smart devices to maintain the integrity of module codes. A risk-based permission model is proposed to classify the device operations in order to mitigate its risks [34]. However, these methods are just deafened against the specific type of attacks.
Networking. In [32], providing a range of services at the network-level like security, taking advantage of SDN technology. A distributed system for protecting the home network from hacked devices [66]. A multi-agent collaboration model to represent each entity in the smart home network as an agent in order to achieve security collaboratively [37]. The modification of IPv6 protocol for securing smart home IoT networks proposed in [67]. In [57], utilized the named data networking model to secure device-to-device communication. Access control policies enforce to reduce the communication with network [49]. Both [35] and [44] suggested detection systems to monitor the traffic of the smart home network. A network access control framework is enforced on the network-level of smart home [41]. Since the smart home network serves as the Internet's primary point of contact with the outside world, numerous security threats can be launched against it. In order to combat these attacks, which are becoming more frequent, studies must be increased.
Applications. Side-channel inference [44] monitor the activities of SmartApps in order to discover the misbehaviour. In [51], cross-app interference threats are recognised using SMT, which treats the problem as an automated theorem problem. As well as [40] uses SMT solver to check the satisfiability of policy. Dependency detection and resolution at installation and runtime to check conflicts across applications [45]. Patching is used in the context-based permission system [46] and the policy-based enforcement system [47], which increases the performance overhead. These methods may integrate to improve its defences accuracy further.

8 Research Challenges and Directions

This section summarizes the identified research challenges and directions derived from the evaluation and discussions of this review. Our findings show that there are four challenges in the smart home system where novel techniques and solutions may need to be employed. We present the researche areas that need to exploration the integration of self-adaptive in smart home (Section 8.1), processing data in edge (Section 8.2), lack of adequate testbeds and evaluation (Section 8.3), and beyond detection method techniques (Section 8.4).

8.1 Self-adaptive Security

Smart devices are heterogeneous, where each of them has a different set of capabilities in terms of sensing and actuation. Smart spaces may be hacked, exposing privacy and security, or rendering the entire area a hostile environment in which ordinary tasks are impossible to do. Therefore, securing smart spaces can be challenging due to device heterogeneity, continuous changes of context, and limited device resources. Self-adaptive security is crucial for smart home systems because it can offer real-time threat detection, flexibility to changing threats, resource optimisation, and a smooth user experience. By ensuring that smart homes are robust in the face of a constantly shifting threat landscape, it helps to safeguard users' security and privacy. Self-adaptive security measures are becoming more and more important to incorporate as smart home technology develops. To tackle this problem, smart devices should be configured dynamically to achieve the corresponding task. A Monitor-Analyze-Plan-Execute-Knowledge (MAPE-k) [87] method and multi-agent mechanism [88] show future directions to carry out the research work further in order to tackle this challenge. These techniques can monitor the smart home network and devices continually for any unusual activity or security breaches while automating security decisions and actions, reducing the reliance on human decision-makers who are frequently prone to error. In addition, an ontology (such as W3C SSN [89], W3C BOT [90], and W3C IoT-Lite [91]) are used to model the contextual information in the smart home environment.

8.2 On Edge Security

It is well-known traditionally that computation and storage of producing data in the smart home are saved in cloud backend servers. Due to the huge volume of traffic generated by the widespread use of mobile video and online social media applications led to the big data concept [92]. Thus, managing these big-data-driven networks in cloud environments is a critical issue [93]. As a result, edge computing or fog computing [94] is an emerging technology in which edge devices provide the capabilities of a cloud server to perform functions including communication, storage, and control. It seems that using edge computing is a possible direction for ensuring the security and safety of the cyber-physical system without needing cloud services. Edge security for smart home systems is of paramount importance and represents a critical area for future work to handle the increasing amount of data generated and processed at smart home. Likewise, it enables devices to continue operating autonomously in the case of network failures or disturbances. Smart home on edge systems are concerned with protecting the equipment and parts that are located at the network's edge, where data is produced and processed locally. As a result, because data processing takes place closer to the source, it

enables quicker response times. Edge systems are crucial to maintaining low latency for real-time applications like smart lighting or home automation while safeguarding the integrity and confidentiality of data. As the adoption of smart home technology continues to grow, further research and development in edge security are vital to address the unique challenges and opportunities presented by this rapidly evolving field.

8.3 Testbeds and Evaluations

Researchers can compare their suggested solutions or methodologies with ones that already exist thanks to testbeds and evaluations. The uniqueness and efficacy of the research are evaluated using this benchmarking. Moreover, insights into the generalizability of the research can be gained through testbed and evaluation results. Researchers can check to see if their findings hold true in various settings, populations, or circumstances. As seen in Section 6, most of the reviewed studies of smart home security utilize prototypes, experiments, case studies, analyses, and simulation experiments to evaluate their approaches. However, the testbed, demonstrator, and use cases are used in their evaluation, and it plays a minor role in the evaluation. To achieve the most realistic results, a real-world evaluation is required. This is one of the toughest challenges in the field. Therefore, implemented techniques for smart home security are needed to be done in the wild. For benchmarking purposes, a real world IoT test bed should be created using Arduino and Raspberry Pi sensor nodes. Each sensor node has several different sensors and different computation capabilities. In addition, to validate the system performance, we may conduct experiments on real-life datasets. There are different types of datasets based on their usage, for example, IoT smart home devices (YourThings dataset [95] and CASAS dataset [70]), smart home applications ([46] [44] [45] [43] [96]), and IoT network intrusion dataset ([97]). Therefore, it is important to collect datasets based on common security use cases. The number of data sets will be decided by the quality of each data set and the repeatability of the results.

8.4 Cyber-physical Anomaly Detection

Anomaly detection techniques aim to give users a sign that something happened wrong in the smart home. The security, privacy, and safety of smart home systems depend heavily on cyber-physical anomaly detection. In order to address changing threats and vulnerabilities, it will be crucial to create and implement efficient anomaly detection systems as smart home technology continues to expand and become more complicated. It is a viable area for further research to support the development and use of smart home systems. However, to the best of our knowledge, threat explanation has not yet been investigated in cyber-physical security for smart home systems. As a result, a unique challenge would arise in discovering and exploring incidents taking advantage of a whole gamut of smart home contexts. In order to accomplish this task, intelligence gathering functionality is a promising further research topic. This could explain where suspected cyber-physical threats occur in a particular spot by collecting more evidence and information to detect anomaly incidents. In such cases, the system needs to capture infrastructure knowledge and capabilities in order to improve the smart home's understanding of the potential given threats. Because of the relevance of detecting anomalous incidents in real-time based on contextual information, it is important that more effort should be devoted to it. The security, privacy, and safety of smart home systems depend heavily on cyber-physical anomaly detection. In order to address changing threats and vulnerabilities, it will be crucial to create and implement efficient anomaly detection systems as smart home technology continues to expand and become more complicated. It is a viable area for further research to support the development and use of smart home systems.

9 Conclusions

Cyber-physical security systems (CPSs) play a crucial role in smartness and digitization by integrating the cyber and physical worlds. This leads to the emergence of tremendous applications in various fields in our life. For example, the smart home is a primary domain of CPS that consists of many smart devices and applications in the interest of f providing services to maintain the comfort of households. Smart home environments are exposed to many challenges regarding functional and non-functional requirements. Numerous solutions are suggested using artificial intelligent mechanisms. These methods include drawbacks, including concentrating on a single issue rather than providing a comprehensive solution or the suggested remedies needing to be updated. Therefore, a complete solution that keeps up with the evolving vulnerabilities in smart homes is required.

In this review, we analyzed and evaluated the knowledge employed in smart homes to comprehend and analyze their happenings. We proposed a taxonomy that defines the classification of the place of decision-making. We presented the main countermeasures for attacks and threats in the smart home. We have also discussed the evaluation of smart homes from the past to hitherto. We reviewed the security of smart homes in different platforms and applications. Besides, we analyzed various aspects of the challenges and how the current solutions overcome these smart home limitations.

Finally, we look at four research gaps related to the smart home from a knowledge-based concept perspective that needs further research.

References

[1] Edward A Lee. Cyber physical systems: Design challenges. In *2008 11th IEEE international symposium on object and component-oriented real-time distributed computing (ISORC)*, pages 363–369. IEEE, 2008.

[2] Kalle Lyytinen and Youngjin Yoo. Ubiquitous computing. *Communications of the ACM*, 45(12):63–96, 2002.

[3] Mahadev Satyanarayanan. Pervasive computing: Vision and challenges. *IEEE Personal communications*, 8(4): 10–17, 2001.

[4] Ilche Georgievski and Marco Aiello. Automated planning for ubiquitous computing. *ACM Computing Surveys (CSUR)*, 49(4):1–46, 2016.

[5] Marie Chan, Daniel Estève, Christophe Escriba, and Eric Campo. A review of smart homes—present state and future challenges. *Computer methods and programs in biomedicine*, 91(1):55–81, 2008.

[6] Collins Patel Michael. Iot value set to accelerate through 2030: Where and how to capture it, 2022. URL `https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/iotvalue-set-to-accelerate-through-2030-where-and-how-to-capture-it`.

[7] Mussab Alaa, Aws Alaa Zaidan, Bilal Bahaa Zaidan, Mohammed Talal, and Miss Laiha Mat Kiah. A review of smart home applications based on internet of things. *Journal of Network and Computer Applications*, 97:48–65, 2017.

[8] Junjian Qi, Youngjin Kim, Chen Chen, Xiaonan Lu, and Jianhui Wang. Demand response and smart buildings: A survey of control, communication, and cyber-physical security. *ACM Transactions on Cyber-Physical Systems*, 1 (4):1–25, 2017.

[9] Terence KL Hui, R Simon Sherratt, and Daniel Díaz Sánchez. Major requirements for building smart homes in smart cities based on internet of things technologies. *Future Generation Computer Systems*, 76:358–369, 2017.

[10] Adam Zielonka, Marcin Woźniak, Sahil Garg, Georges Kaddoum, Md Jalil Piran, and Ghulam Muhammad. Smart homes: How much will they support us? a research on recent trends and advances. *IEEE Access*, 9:26388–26419, 2021.

[11] Jessamyn Dahmen, Diane J Cook, Xiaobo Wang, and Wang Honglei. Smart secure homes: a survey of smart home technologies that sense, assess, and respond to security threats. *Journal of reliable intelligent environments*, 3(2):83–98, 2017.

[12] Kai Gong, Jianlin Yang, Xu Wang, Chuanwen Jiang, Zhan Xiong, Ming Zhang, Mingxing Guo, Ran Lv, Su Wang, and Shenxi Zhang. Comprehensive review of modeling, structure, and integration techniques of smart buildings in the cyber-physical-social system. *Frontiers in Energy*, pages 1–21, 2022.

[13] Biljana L Risteska Stojkoska and Kire V Trivodaliev. A review of internet of things for smart home: Challenges and solutions. *Journal of cleaner production*, 140:1454–1464, 2017.

[14] Marco Conti, Sajal K Das, Chatschik Bisdikian, Mohan Kumar, Lionel M Ni, Andrea Passarella, George Roussos, Gerhard Tröster, Gene Tsudik, and Franco Zambonelli. Looking ahead in pervasive computing: Challenges and opportunities in the era of cyber–physical convergence. *Pervasive and mobile computing*, 8(1):2–21, 2012.

[15] Hadi Habibzadeh, Brian H Nussbaum, Fazel Anjomshoa, Burak Kantarci, and Tolga Soyata. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, 50:101660, 2019.

[16] Md Ahmad, Mohd Abdul Ahad, M Afshar Alam, Farheen Siddiqui, Gabriella Casalino, et al. Cyber-physical systems and smart cities in india: Opportunities, issues, and challenges. *Sensors*, 21(22):7714, 2021.

[17] Yosef Ashibani and Qusay H Mahmoud. Cyber physical systems security: Analysis, challenges and solutions. *Computers & Security*, 68:81–97, 2017.

[18] Jean-Paul A Yaacoub, Ola Salman, Hassan N Noura, Nesrine Kaaniche, Ali Chehab, and Mohamad Malli. Cyber-physical systems security: Limitations, issues and future trends. *Microprocessors and microsystems*, 77:103201, 2020.

[19] Nam Yong Kim, Shailendra Rathore, Jung Hyun Ryu, Jin Ho Park, and Jong Hyuk Park. A survey on cyber physical system security for iot: issues, challenges, threats, solutions. *Journal of Information Processing Systems*, 14(6):1361–1384, 2018.

[20] Ukachi Osisiogu. A review on cyber-physical security of smart buildings and infrastructure. In *2019 15th International Conference on Electronics, Computer and Computation (ICECCO)*, pages 1–4. IEEE, 2019.

[21] Amit Kumar Tyagi and N Sreenath. Cyber physical systems: Analyses, challenges and possible solutions. *Internet of Things and Cyber-Physical Systems*, 2021.

[22] Jože Tavčar and Imre Horvath. A review of the principles of designing smart cyber-physical systems for run-time adaptation: Learned lessons and open issues. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49 (1):145–158, 2018.

[23] Barbara Kitchenham, O Pearl Brereton, David Budgen, Mark Turner, John Bailey, and Stephen Linkman. Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, 51(1):7–15, 2009.

[24] Barbara Kitchenham, Rialette Pretorius, David Budgen, O Pearl Brereton, Mark Turner, Mahmood Niazi, and Stephen Linkman. Systematic literature reviews in software engineering–a tertiary study. *Information and software technology*, 52(8):792–805, 2010.

[25] Claes Wohlin. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, pages 1–10, 2014.

[26] Gregory D Abowd, Anind K Dey, Peter J Brown, Nigel Davies, Mark Smith, and Pete Steggles. Towards a better understanding of context and context-awareness. In *International symposium on handheld and ubiquitous computing*, pages 304–307. Springer, 1999.

[27] Philippe Lalanda and Catherine Hamon. A service-oriented edge platform for cyber-physical systems. *CCF Transactions on Pervasive Computing and Interaction*, 2(3):206–217, 2020.

[28] Yosef Ashibani, Dylan Kauling, and Qusay H Mahmoud. A context-aware authentication framework for smart homes. In *2017 IEEE 30th Canadian Conference on Electrical and Computer Engineering (CCECE)*, pages 1–5. IEEE, 2017.

[29] Sofia Dutta, Sai Sree Laya Chukkapalli, Madhura Sulgekar, Swathi Krithivasan, Prajit Kumar Das, and Anupam Joshi. Context sensitive access control in smart home environments. In *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing,(HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, pages 35–41. IEEE, 2020.

[30] Changyuan Lin, Hamzeh Khazaei, Andrew Walenstein, and Andrew Malton. Autonomic security management for iot smart spaces. *ACM Transactions on Internet of Things*, 2(4):1–20, 2021.

[31] Tam Thanh Doan, Reihaneh Safavi-Naini, Shuai Li, Sepideh Avizheh, and Philip WL Fong. Towards a resilient smart home. In *Proceedings of the 2018 workshop on IoT security and privacy*, pages 15–21, 2018.

[32] Vijay Sivaraman, Hassan Habibi Gharakheili, Arun Vishwanath, Roksana Boreli, and Olivier Mehani. Network-level security and privacy control for smart-home iot devices. In *2015 IEEE 11th International conference on wireless and mobile computing, networking and communications (WiMob)*, pages 163–167. IEEE, 2015.

[33] Vijay Sivaraman, Dominic Chan, Dylan Earl, and Roksana Boreli. Smart-phones attacking smart-homes. In *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 195–200, 2016.

[34] Amir Rahmati, Earlence Fernandes, Kevin Eykholt, and Atul Prakash. Tyche: A risk-based permission model for smart homes. In *2018 IEEE Cybersecurity Development (SecDev)*, pages 29–36. IEEE, 2018.

[35] Corentin Thomasset and David Barrera. Sereniot: Distributed network security policy management and enforcement for smart homes. In *Annual Computer Security Applications Conference*, pages 542–555, 2020.

[36] Manju Mohan Pillai and Albert Helberg. Improving security in smart home networks through user-defined device interaction rules. In *2021 IEEE AFRICON*, pages 1–6. IEEE, 2021.

[37] Laura Rafferty, Farkhund Iqbal, Saiqa Aleem, Zhihui Lu, Shih-Chia Huang, and Patrick CK Hung. Intelligent multi-agent collaboration model for smart home iot security. In *2018 IEEE international congress on internet of things (ICIOT)*, pages 65–71. IEEE, 2018.

[38] Amit Kumar Sikder, Leonardo Babun, and A Selcuk Uluagac. Aegis+ a context-aware platform-independent security framework for smart home systems. *Digital Threats: Research and Practice*, 2(1):1–33, 2021.

[39] Soteris Demetriou, Nan Zhang, Yeonjoon Lee, XiaoFeng Wang, Carl A Gunter, Xiaoyong Zhou, and Michael Grace. 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*, pages 122–133, 2017.

[40] Moosa Yahyazadeh, Proyash Podder, Endadul Hoque, and Omar Chowdhury. Expat: Expectation-based policy analysis and enforcement for appified smart-home platforms. In *Proceedings of the 24th ACM symposium on access control models and technologies*, pages 61–72, 2019.

[41] Mohammed Al-Shaboti, Ian Welch, Aaron Chen, and Muhammed Adeel Mahmood. Towards secure smart home iot: Manufacturer and user network access control framework. In *2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA)*, pages 892–899. IEEE, 2018.

[42] Kulani Tharaka Mahadewa, Kailong Wang, Guangdong Bai, Ling Shi, Jin Song Dong, and Zhenkai Liang. Homescan: scrutinizing implementations of smart home integrations. In *2018 23rd International Conference on Engineering of Complex Computer Systems (ICECCS)*, pages 21–30. IEEE, 2018.

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

[44] Wei Zhang, Yan Meng, Yugeng Liu, Xiaokuan Zhang, Yinqian Zhang, and Haojin Zhu. Homonit: Monitoring smart home apps from encrypted traffic. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 1074–1088, 2018.

[45] Sirajum Munir and John A Stankovic. Depsys: Dependency aware integration of cyber-physical systems for smart homes. In *2014 ACM/IEEE International Conference on Cyber-Physical Systems (ICCPS)*, pages 127–138. IEEE, 2014.

[46] Yunhan Jack Jia, Qi Alfred Chen, Shiqi Wang, Amir Rahmati, Earlence Fernandes, Zhuoqing Morley Mao, Atul Prakash, and SJ Unviersity. Contexlot: Towards providing contextual integrity to appified iot platforms. In *NDSS*, volume 2, pages 2–2. San Diego, 2017.

[47] Z Berkay Celik, Gang Tan, and Patrick D McDaniel. Iotguard: Dynamic enforcement of security and safety policy in commodity iot. In *NDSS*, 2019.

[48] Yasir Imtiaz Khan and Maryleen U Ndubuaku. Ontology-based automation of security guidelines for smart homes. In *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pages 35–40. IEEE, 2018.

[49] Sanket Goutam, William Enck, and Bradley Reaves. Hestia: simple least privilege network policies for smart homes. In *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, pages 215–220, 2019.

[50] Amit Kumar Sikder, Leonardo Babun, Z Berkay Celik, Abbas Acar, Hidayet Aksu, Patrick McDaniel, Engin Kirda, and A Selcuk Uluagac. Kratos: Multi-user multi-device-aware access control system for the smart home. In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 1–12, 2020.

[51] Haotian Chi, Qiang Zeng, Xiaojiang Du, and Jiaping Yu. Cross-app interference threats in smart homes: Categorization, detection and handling. In *2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, pages 411–423. IEEE, 2020.

[52] Ming Tao, Jinglong Zuo, Zhusong Liu, Aniello Castiglione, and Francesco Palmieri. Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes. *Future Generation Computer Systems*, 78:1040–1051, 2018.

[53] Yimin Guo, Zhenfeng Zhang, and Yajun Guo. Secfhome: Secure remote authentication in fog-enabled smart home environment. *Computer Networks*, 207:108818, 2022.

[54] Kulani Mahadewa, Kailong Wang, Guangdong Bai, Ling Shi, Yan Liu, Jin Song Dong, and Zhenkai Liang. Scrutinizing implementations of smart home integrations. *IEEE Transactions on Software Engineering*, 2019.

[55] Nikola Zaric, Milutin Radonjic, Milica Pejanovic-Djurisic, and Igor Radusinovic. An example of monitoring system with reasoning module for ambient assisted living applications. In *IEEE EUROCON 2015-International Conference on Computer as a Tool (EUROCON)*, pages 1–6. IEEE, 2015.

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

[57] Zhiyi Zhang, Tianyuan Yu, Xinyu Ma, Yu Guan, Philipp Moll, and Lixia Zhang. Sovereign: Self-contained smart home with data-centric network and security. *IEEE Internet of Things Journal*, 2022.

[58] Amjad Qashlan, Priyadarsi Nanda, and Xiangjian He. Security and privacy implementation in smart home: Attributes based access control and smart contracts. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pages 951–958. IEEE, 2020.

[59] Dagmawi Neway Mekuria, Paolo Sernani, Nicola Falcionelli, and Aldo Franco Dragoni. Smart home reasoning systems: a systematic literature review. *Journal of Ambient Intelligence and Humanized Computing*, 12(4): 4485–4502, 2021.

[60] Huma Samin, Nelly Bencomo, and Peter Sawyer. Decision-making under uncertainty: be aware of your priorities. *Software and Systems Modeling*, pages 1–30, 2022.

[61] Arun Cyril Jose and Reza Malekian. Improving smart home security: Integrating logical sensing into smart home. *IEEE Sensors Journal*, 17(13):4269–4286, 2017.

[62] Honglei Ren, You Song, Siyu Yang, and Fangling Situ. Secure smart home: A voiceprint and internet based authentication system for remote accessing. In *2016 11th International Conference on Computer Science & Education (ICCSE)*, pages 247–251. IEEE, 2016.

[63] Nikolay Akatyev and Joshua I James. Evidence identification in iot networks based on threat assessment. *Future Generation Computer Systems*, 93:814–821, 2019.

[64] Marica Amadeo, Antonella Molinaro, Stefano Yuri Paratore, Albino Altomare, Andrea Giordano, and Carlo Mastroianni. A cloud of things framework for smart home services based on information centric networking. In *2017 IEEE 14th International Conference on Networking, Sensing and Control (ICNSC)*, pages 245–250. IEEE, 2017.

[65] Won Min Kang, Seo Yeon Moon, and Jong Hyuk Park. An enhanced security framework for home appliances in smart home. *Human-centric Computing and Information Sciences*, 7(1):1–12, 2017.

[66] Elmer Lastdrager, Cristian Hesselman, Jelte Jansen, and Marco Davids. Protecting home networks from insecure iot devices. In *NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium*, pages 1–6. IEEE, 2020.

[67] Pankaj Kumar and Lokesh Chouhan. Design of secure session key using unique addressing and identification scheme for smart home internet of things network. *Transactions on Emerging Telecommunications Technologies*, 32(5):e3993, 2021.

[68] Hang Hu, Limin Yang, Shihan Lin, and Gang Wang. Security vetting process of smart-home assistant applications: A first look and case studies. *arXiv preprint arXiv:2001.04520*, 2020.

[69] D Richard Kuhn, Edward J Coyne, Timothy R Weil, et al. Adding attributes to role-based access control. *Computer*, 43(6):79–81, 2010.

[70] Diane J Cook and Maureen Schmitter-Edgecombe. Assessing the quality of activities in a smart environment. *Methods of information in medicine*, 48(05):480–485, 2009.

[71] Nicholas Shields. The us smarthomemarket report: Systems, apps, and devices leading to home automation, 2022. URL `https://www.businessinsider.com/the-us-smart-home-market-report-systems-apps-and-devices-leading-to-home-automation-2018-3-19?r=US&IR=T`.

[72] Eric Zeng and Franziska Roesner. Understanding and improving security and privacy in multi-user smart homes: A design exploration and in-home user study. In *28th USENIX Security Symposium (USENIX Security 19)*, pages 159–176, 2019.

[73] Rachel Gunter. Making sense of samsung's smartthings initiative, 2017. URL `https://marketrealist.com/2017/12/making-sense-samsungs-smartthingsinitiative`.

[74] Ada Diaconescu Philippe Lalanda, Julie McCann. Pervasive computing in practice, 2020. URL `https://self-star.imag.fr`.

[75] IFTTT. Every thing works better together, 2022. URL `https://ifttt.com/`.

[76] openHAB. openhab empowering the smart home, 2022. URL `https://www.openhab.org`.

[77] Cristian Hesselman. Spin: A user-centric security extension for in-home networks, 2017. URL `https://www.sidnlabs.nl/en/newsand-blogs/spin-a-user-centric-security-extension-for-in-home-networks`.

[78] SmartThings. Smartthings public github repo, 2018. URL `https://github.com/SmartThingsCommunity/SmartThingsPublic`.

[79] Andrew Banks and Rahul Gupta. Mqtt version 3.1. 1. *OASIS standard*, 29:89, 2014.

[80] Microsoft. The oauth 2.0 authorization protocol, 2018. URL `https://oauth.net/2/`.

[81] Dick Hardt. The oauth 2.0 authorization framework, 2012. URL `https://tools.ietf.org/html/rfc6749`.

[82] Eric Sesterhenn Michael Frey, Cenk Gündogan. Cnn lite, 2018. URL `https://github.com/cn-uofbasel/ccn-lite`.

[83] NDN Specification Contributors. Ndn packet format specification version 0.3, 2022. URL `https://named-data.net/doc/NDN-packet-spec/current/changelog.html#version-0-3`.

[84] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. Rethinking access control and authentication for the home internet of things (iot). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 255–272, 2018.

[85] Eric Zeng, Shrirang Mare, and Franziska Roesner. End user security and privacy concerns with smart homes. In *Thirteenth Symposium on Usable Privacy and Security (SOUPS 2017)*, pages 65–80, 2017.

[86] Diego Kreutz, Fernando MV Ramos, Paulo Esteves Verissimo, Christian Esteve Rothenberg, Siamak Azodolmolky, and Steve Uhlig. Software-defined networking: A comprehensive survey. *Proceedings of the IEEE*, 103(1):14–76, 2014.

[87] Yuriy Brun, Giovanna Di Marzo Serugendo, Cristina Gacek, Holger Giese, Holger Kienle, Marin Litoiu, Hausi Müller, Mauro Pezzè, and Mary Shaw. Engineering self-adaptive systems through feedback loops. In *Software engineering for self-adaptive systems*, pages 48–70. Springer, 2009.

[88] James McNaull, Juan Carlos Augusto, Maurice Mulvenna, and Paul McCullagh. Multi-agent system feedback and support for ambient assisted living. In *2012 Eighth International Conference on Intelligent Environments*, pages 319–322. IEEE, 2012.

[89] Michael Compton, Payam Barnaghi, Luis Bermudez, Raul Garcia-Castro, Oscar Corcho, Simon Cox, John Graybeal, Manfred Hauswirth, Cory Henson, Arthur Herzog, et al. The ssn ontology of the w3c semantic sensor network incubator group. *Journal of Web Semantics*, 17:25–32, 2012.

[90] Mads Holten Rasmussen, Maxime Lefrançois, Georg Ferdinand Schneider, and Pieter Pauwels. Bot: the building topology ontology of the w3c linked building data group. *Semantic Web*, 12(1):143–161, 2021.

[91] Maria Bermudez-Edo, Tarek Elsaleh, Payam Barnaghi, and Kerry Taylor. Iot-lite ontology. *W3C Member Submission, W3C, November*, 2015.

[92] Rachad Atat, Lingjia Liu, Jinsong Wu, Guangyu Li, Chunxuan Ye, and Yi Yang. Big data meet cyber-physical systems: A panoramic survey. *IEEE Access*, 6:73603–73636, 2018.

[93] Engin Zeydan, Ejder Bastug, Mehdi Bennis, Manhal Abdel Kader, Ilyas Alper Karatepe, Ahmet Salih Er, and Mérouane Debbah. Big data caching for networking: Moving from cloud to edge. *IEEE Communications Magazine*, 54(9):36–42, 2016.

[94] Babatunji Omoniwa, Riaz Hussain, Muhammad Awais Javed, Safdar Hussain Bouk, and Shahzad A Malik. Fog/edge computing-based iot (feciot): Architecture, applications, and research issues. *IEEE Internet of Things Journal*, 6(3):4118–4149, 2018.

[95] Omar Alrawi, Chaz Lever, Manos Antonakakis, and Fabian Monrose. Sok: Security evaluation of home-based iot deployments. In *2019 IEEE symposium on security and privacy (sp)*, pages 1362–1380. IEEE, 2019.

[96] Moosa Yahyazadeh, Proyash Podder, Endadul Hoque, and Omar Chowdhury. Expat github repository, 2019. URL `https://github.com/expat-paper/expat.git`.

[97] K Hyunjae, Dong Hyun Ahn, Gyung Min Lee, Jeong Do Yoo, Kyung Ho Park, and HK Kim. Iot network intrusion dataset. *IEEE Dataport*, 2019.