A Comprehensive Survey of Security Issues of Smart Home System: “Spear” and “Shields,” Theory and Practice

JIAN YANG AND LIU SUN

1School of Mathematics and Information Technology, Yuxi Normal University, Yuxi, Yunnan 653100, China
2Yunnan Key Laboratory of Smart City in Cyberspace Security, Yuxi, Yunnan 653100, China
Corresponding author: Jian Yang (yangjian@yxnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 62266048, and in part by the Yunnan Fundamental Research Project 202101AU070007.

ABSTRACT

The rapid development and wide application of the Internet of Things (IoT) and sensor technologies have produced good opportunities for the development of IoT-based smart home systems (SHSs). However, during the rapid market expansion of SHSs, security challenges associated with SHSs have become a primary concern of people because they are so closely related to people’s daily lives. These security problems may damage information assets and pose a serious threat to people’s health and life. This study investigates security issues in SHSs and provides a comprehensive overview of research to date. In this review, after analyzing the existing definition and concept of SHSs proposed by authoritative encyclopedias and academic literature, we propose a more accurate, elaborated definition of SHSs, analyze their architecture, extract six natural and contextual features, and summarize spears (cyber-attack means) vs. shields (countermeasures) in detail in the context of SHSs. Then, the security frameworks and evaluation technologies in SHSs are discussed. Different scenarios for technology integration and the practical research results in SHSs, such as blockchain, cloud computing, Internet of Vehicles, and AI are presented meticulously. After that, two special issues related to security are discussed. We believe that future research on SHS security should focus on four aspects: the unification of architecture, resource limitation, fragmentation, and code and firmware security. In addition, research on SHS security should be given priority over its commercialization process.

INDEX TERMS

Internet of Things, smart home system, security, privacy, IoT sensors.

I. INTRODUCTION

As early as 1992, Lutolf [1] proposed the concept of a smart home system (SHS). With the rapid development of the Internet of Things (IoT) and sensor technology, IoT-based SHSs have rapidly entered human life to provide more convenience, comfort and efficiency [2], [3]. In terms of household equipment management and paying for water and energy, an SHS also provides automatic options to intelligently and efficiently manage daily life. However, when using an SHS, people tend to worry about its safety and security. Smart home devices collect data from a family to perform their functions, and some data involve personal and family’s privacy. The cybersecurity and privacy problems of smart homes cause damage to the family’s virtual assets and may cause a loss of its physical assets and even directly threaten the resident’s life [4], [7].

In recent years, there have been many reviews and summaries of SHS and IoT security issues. Security attacks in SHSs have been investigated, and their impacts evaluated [8]; and the security requirements and possible future attacks in the coming years were also discussed. Almusaylim et al. [9] summarized existing interoperability, context-aware middleware, energy awareness and efficient consumption, security and privacy. Meneghello et al. [10] discussed the specific security mechanisms used by the most popular protocols in
the IoT. First, the authors summarized the possible cyberattacks and threats in different layers (i.e., perception, network, middleware and application layers) and identified the desired security nature of the network and communication with the optional cryptography mechanism. Then, the security issues and attack surfaces of four most popular protocols (ZigBee, Bluetooth low energy, 6LoWPAN and LoRaWAN) were analyzed in detail. The security practices of commercialized IoT devices were discussed from the perspective of specific hardware (i.e., microcontrollers and connection modules). The issues of integrity, usability, auditing, privacy, information protection, access control and anonymization of sensor data required more attention in the area of digital health [11]. From a statistical perspective, Talal et al. [12] analyzed the research results on the security of SHS devices for remote health monitoring from seven aspects (i.e., security analysis, system and architecture design, framework, mechanism, protocol, and experiment). However, security measures and practices were not discussed in detail. Jiang et al. [13] investigated the data security and privacy protection of medical wearable devices from the aspects of technology, management and law. The authentication and data protection requirements and future development of AI applications in edge computing, integrated with popular IoT scenes, such as smart grids, smart homes and smart transportation, were discussed and analyzed in [14]. Deep learning might also be used to strengthen SHS security, for example, when the intrusion detection rules must be extracted automatically [15].

However, in these summaries, either basic discussions about SHS security issues without detailed analysis were provided, or countermeasures [8], [9] or security schemes were proposed in terms of specific background [11], [13], specific methods or specific applications [14], [16], without a comprehensive summary from theoretical research to application practice at all layers of the SHS.

To describe the security challenges faced by SHSs, a comprehensive survey related to SHS security issues is performed in this review, particularly focusing on IoT-based scenarios. The differences between this review and other reviews are shown in TABLE 1. As can be seen from TABLE 1, this review describes the definition, features, architectures, attack and defense methods, evaluation strategies, scene fusion and practice technologies, and human factors in the security of SHS. In general, the following aspects are discussed in detail.

First, regarding applications, a new definition of SHS is given compared with the existing definitions with the development of its layered structures. The application features and security requirements are analyzed, and the contextual and environmental natures of smart homes are identified when facing security threats. These characteristics determine that the security solutions in SHS are different from other IoT-based scenarios.

Second, from the two perspectives of “spears” and “shields” (i.e., “attacks” and “defenses”), this paper discusses the overall security issues instead of a specific scenario or technology. Regarding attacks, the classification, technology and attack model are discussed. Regarding defenses, existing countermeasures and technologies in SHS are analyzed and summarized from seven aspects. In addition, some cute methods are also introduced.

Third, this review summarizes the practical research and integration with other information and communication technologies, and human and contextual factors that affect SHS security are also discussed in addition to community and human thought. In this regard, this review is a more comprehensive and thorough understanding that the security in SHSs can be divided into two aspects: hard security and soft security [17].

Finally, four important future directions of security research for SHSs are proposed. Among them, fragmentation is an important problem that needs special concerns from the industrial and business sectors.

It should be noted that we attempt to make an exhaustive and comprehensive review of the security issues in SHS from the perspective of theory and application technologies, instead of a meta-analysis of the literature on this subject from the perspective of statistics. We obtain the relevant literature on the security research of SHS and the Internet of Things from mainstream academic search engines, summarize the definition and characteristics of SHS, discuss the possible and important attack and defense strategies according to the

| Reference | Definition | Features and security requirement | Architecture and security framework | Spear (Attack) | Shield (Defense) | Evaluation | Scene fusion and practice | SDK platform | Human factor |
|-----------|------------|----------------------------------|----------------------------------|---------------|----------------|-----------|------------------------|-------------|--------------|
| [8]       | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [9]       | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [10]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [11]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [12]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [13]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [14]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [15]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |
| [16]      | ✓          | ✓                                | ✓                                | ✓             | ✓              | ✓         | ✓                      | ✓           | ✓            |

“✓” = contained, “.” = partially contained
natures of SHS, further extract and analyze the state-of-the-art research results at several sections and make the corresponding comparisons and comments. The goal of this review is to give researchers and developers a comprehensive perspective on the features and major research fields of security issues of SHS. The review makes the following contributions.

- The review proposes a new, definitude definition for SHS, and analyzes and presents its essential and unique attributes.
- The review presents a comprehensive survey of the state-of-the-art research results of security issues in SHS from the two perspectives of attack and defense.
- The review summarizes the latest research results on the security of SHSs in terms of technology integration, practical application, human factors, etc., and analyzes their contextual characteristics and countermeasures in detail.
- The review proposes four key future directions for the research and application development focused on SHS security.

The remainder of this review is organized as follows. In section II, the existing definition and hierarchy of the SHS are introduced; then, a new and more comprehensive definition is provided, and the unique natures and features of smart home security are identified and analyzed in detail. In section III, from the two opposing perspectives (“spear” vs. “shield”), the research progress on the security threats and risks faced by smart home scenarios and the feasible solutions are summarized. After that, in section IV, the progress on security-related architecture, evaluation and regulatory technology is reviewed. In Section V, the advances in technology integration and practical research used in security solutions are analyzed in detail from the perspective of real-world applications, particularly research on blockchain combined with SHSs. Then, the improvement of the application development platform and operating system is also summarized in the same section. In section VI, two special research issues are analyzed. Finally, in the last section, an overall conclusion is provided, followed by four key issues that should be given more attention in future research. The structure of this paper is described in FIGURE 1.

II. CONCEPT, ARCHITECTURE, AND FEATURES

A. CONCEPT AND LAYERED STRUCTURE

1) CONCEPT OF SHS

The early concept of SHS is building automation, which emphasizes the automatic control of building components using related technologies. A smart home system also refers to a convenient home setup [18], where facilities and devices can be automatically controlled remotely from anywhere with an internet connection using a mobile or other networked device, the key features of which are remote control, interconnection, convenience and cost savings. In Wikipedia, a smart home system is named a “home automation system”, in which home attributes such as lighting, climate, entertainment systems, and appliances are monitored and/or controlled to share data, personal security, energy saving, and convenient and comfortable life. It may also include home security such as access control and alarm systems. The controlled devices in the system typically are connected via a central gateway. When connected to the Internet, home devices are an important constituent of the Internet of Things and are controlled by the users with their computers or mobile terminals remotely. [19].

SHS was also defined as the symbiosis of different elements to build a dynamic heterogeneous architecture for efficiently managing home devices and provide to users with advanced services [20]. A smart home is a house equipped with smart objects used to interact with inhabitants or to observe them, in which a home network makes it possible to transport information between smart objects and a residential gateway to connect the smart home to the outside Internet world [21]. This definition emphasized the key functions and network connections of smart devices. Another definition of SHS from the view of energy consumption was given in [22].

However, the definitions and concepts in the above literature emphasized the automatic controls, functions, or interconnections (also as an important constituent of the Internet of Things) of smart devices in SHS. These definitions did not elaborate on the difference and relationship between SHS, traditional information systems, and the Internet of Things, and did not detail the key research and application areas involved in SHS from a systematic perspective. What is more important, they all did not mention the fountainhead of the “smart” nature in SHS. For these reasons, this review gives a new definition of SHS from the perspectives of technology integration, the convergence of different devices and services, control and interconnections, functions, and purposes.

Our definition of SHS is: an SHS is a hybrid physical and cyber platform in home buildings based on IT, IoT and the Internet that integrates multimedia processing, automatic control, AI and data analysis, cloud computing and edge computing, psychology and sociology, health care, and other topics. In SHSs, varieties of software, hardware and network
devices cooperate with each other to perform data collection, processing, storage, decision-making and feedback for a family, and provide interconnection with the Internet of vehicles, intelligent community, telemedicine, edge computing, remote control and other external access requirements. The primary purpose of an SHS is to provide authorized users with security, privacy-protected, convenient, comfortable, automated, controllable, energy-saving and environmentally friendly home facilities and application services.

2) HIERARCHICAL ARCHITECTURE

The IoT is one of the cornerstones of modern smart homes. To study the development of SHSs, we must understand the development of IoT architecture. Early IoT architecture includes a perception layer, network layer and application layer [23], in which a smart home is embodied in the last layer as a type of application service. However, this structure does not consider the nature of the SHS. With so many commercial applications, some common services, such as cloud computing and anti-virus services, are separated from the application layer to form a four-layer structure [24]. However, there are still some problems of security, storage and services that make the support layer disordered; thus, a processing layer and a business layer are added to make the support service clearer. The processing layer can be regarded as a middleware that assembles data from lower and preprocesses it, and the business layer can be regarded as an application organizer to play the role of function management, model configuration and procession control. Because the use and control of data are placed at high layers and isolated from the perception layer, the vulnerabilities from lower layers are introduced, such as internal traffic forgery. The evolution of hierarchy in SHS is shown in FIGURE 2.

In addition to this typical structure, a layered structure was also proposed in [25], in which the SHS is composed of three layers: field, automation and management. In this structure, sensors are connected through field buses and converge to the automation layer via a gateway, and the automation layer performs all application functions. System logs, user APIs and profiles are added to the management layer [25]. Many studies have investigated specific architectures. An SHS architecture based on wireless and IoT devices was designed using Cisco’s packet tracker [26]. In terms of the data life cycle, a simplified architecture composed of three parts can be established: data acquisition, network and transmission, and feedback and actuator [22]. From the perspective of functionality, devices in SHSs can also be divided into three types: those with only perceptual and monitoring ability, those with the ability of active control, and those with control and data processing. From the perspective of data utilization and the life cycle, an SHS can also be regarded as a feedback loop system with four phases, as shown in FIGURE 3.

B. BACKGROUND AND CONTEXTUAL FEATURES

Eight IoT features were summarized in [27]: interdependency, diversity, constrained, myriad, unattended, intimacy, mobile and ubiquitous. However, when IoT devices are used in SHSs, the security issues and countermeasures demonstrate their unique nature different from the above eight features. This review identifies six features as shown in the following.

1) LARGE SCALE

After its initial and evolutionary periods, the smart home industry is now experiencing rapid development, and its market scale is expanding rapidly. In the global market, it is estimated that more than 100 trillion IoT devices will be deployed by 2030, and the global market value is expected to reach $53 billion in 2022, with an average annual growth rate of 21% from 2018 to 2022 [28]. In real-world applications, an SHS is composed of many subsystems, such as security monitoring, environmental control, home facilities management, telemedicine and health monitoring, smart lock, intelligent software service for scenario management, data processing, or paying for household bills for water, electricity and gas. Different subsystems are composed of different sensors, software and hardware, and wired and wireless communication.
devices. Whether from the perspective of a single family or the entire internet, the number of SHS devices is massive. The large-scale feature represents the rapid development of the industry but brings new security challenges concurrently. For example, massive devices make it easier for attackers to launch distributed DoS attacks. The increase in the number of devices will increase the attack surface, and the data exchange between many devices will produce more security and privacy issues.

2) DIVERSITY
First, diversity is reflected in the multimodality of data traffic. The data transmission and service are driven by different patterns. After analyzing BACnet, a protocol widely used in building automation, Zheng et al. [29] found that the driving patterns of data traffic can be divided into three categories: time-, human-, and event-driven. Based on this observation, the authors construct flow-service models to detect abnormal network traffic, which is helpful to build an effective intrusion detection system (IDS).

Second, diversity is reflected in the multiscale perception and utilization of data due to the different granularity requirements of data in different scenarios. For example, a smart meter reads its value once a month to bill a customer but might also compute its energy consumption within a very short interval [30], [31] to detect whether there are suspicious events (e.g., energy-based attacks on the smart device).

Third, diversity also reflects the different types of smart devices, such as mobile or nonmobile devices, external or internal devices [8], and physical devices or software-defined devices [32]. From the perspective of system architecture, these devices can also be divided into sensors, transmission devices, computing and management devices and actuators.

Last, diversity is also reflected in the sophisticated social relationships among the users in SHS, which include family owners and members, intimate visitors (which can also be divided into different trust models – e.g., close friends, relatives), temporary visitors (e.g., repairmen, cleaners or nannies) and remote visitors [33], [34]. These complex social relationships result in many attack vectors, such as social engineering attacks, unauthorized access, and authority promotion.

3) HETEROGENEITY AND FRAGMENTATION
In SHSs, different functional devices often come from different vendors. Due to the lack of popular guidelines or standards universally used, the drivers and interfaces of these devices are highly heterogeneous. Generic interface standards should be built and widely used so that software and services can be independent of specific hardware. However, the diversity of devices hinders this effort. Many IT companies use their self-defined standards to produce smart devices used in SHSs, with the result that the interoperability and interconnection of different elements in SHSs cannot be easily achieved [35]. Domingues et al. [36] investigated the primary technical specifications in building automation (BA) and believed that no existing method could perfectly overcome the problem of heterogeneity. High fragmentation hinders the interoperability between devices and increases the complexity and the cost of service deployment. An implementation of W3C IoT standards supported by home automation ontologies was proposed in [37], such as SAREF and UniversAAL, to deploy the Living Lab Gateway (LLG), which provides security, authentication and authorization, dynamic configuration and device injection, as well as the ability to abstract and map devices into ontologies for securely using IoT devices in SHS.

It is a challenge to establish a secure session key between different devices using their secrets prefabricated by different vendors. Therefore, many studies have investigated key negotiation or anonymous authentication that does not require a trusted third party or preloaded secrets [38], [40]. The manufacturers defined their own product interfaces, which makes that particular functional assumptions are difficult to fit for all different SHS scenarios, and devices from different vendors are difficult to be compatible with each other. All these problems may lead to serious security vulnerabilities in SHSs during the processing of the integration. Mahadewa et al. [41] analyzed the security problems of SHSs from the perspective of integration and proposed a method called HOMESCAN to evaluate security solutions, which extracts and abstracts the specification of the protocols in the application layer and the internal behaviors of entities to conduct end-to-end security analysis for various attack models.

This review maintains that the root of fragmentation is the diversity of manufacturers, which can be partially alleviated by defining in detail and strictly obeying global norms and standards in SHSs. In addition, a software defined network (SDN) can mitigate fragmentation. Using well-defined design patterns, SDNs can mitigate the differences in network interfaces and functional interfaces of different devices under their concrete implementation to provide a general security framework for upper layers in an SHS.

4) ENERGY, STORAGE, AND COMPUTING POWER
The constraint of energy, storage and computing power of IoT devices is their inherent nature. This feature makes it difficult to use mature cyberspace security solutions and integrate novel security frameworks and technologies, such as block chains (BCs) [33]. More importantly, some new attack vectors, such as energy analysis and attack [42], [44] and energy lock vulnerability [45], may be directly introduced into SHS, resulting in information leakage, device failure, and even more serious consequences (e.g., DOS or strong magnetic field injection attack). Resource constraints should be considered from different perspectives to provide fine-grained support for different security solutions. In [22], the devices in an SHS are identified as the following three types according to their energy patterns: systems with energy monitoring, systems with active control ability, and systems with advanced data processing ability. When a security solution must be deployed in low-computing-power devices, secure
multiparty computing should be adapted to integrate into the system for multi-device collaboration. Low-level devices can borrow computing power via the central equipment of an edge NPU (neural network processing unit) [15].

5) COUPLED CYBER PHYSICAL SYSTEM

SHS is a typical Cyber Physical System (CPS), where damage from cyberspace can hinder devices in the physical world, while negligence and loopholes in the physical world can threaten cyberspace and even cause serious property loss and personal casualty [4], [7]; this problem requires more attention with wearable devices. However, this feature can also play a positive role in SHS security. The impact of coupled CPS on security is primarily reflected in the following aspects:

(1) Coupled CPSs increase the attack surface of social engineering [46], [47]. The increase in access to the physical world means that the possibility of attack using social engineering increases.

(2) Using voice, fingerprint, face and other bioinformation may produce vulnerabilities but may become an auxiliary countermeasure for security, such as biological factor authentication [48], [50]. This issue is also one of the important properties that SHS differs from other IoT-based scenarios (e.g., industry IoT).

(3) Cyber-physical coupling makes the system automatic and without human interaction, performing automatic data collection, processing and feedback. Automation means the integration of business rules and AI technologies [51], [53], which provides convenience to use and management whereas producing new security challenges [54].

(4) The use of humanoid robots in SHSs produces new security threats. The interaction between robots and their environment, as well as the vulnerabilities exposed by the devices in their context, may become a critical threat to SHS security [55].

6) COMPLEX TEMPORALITY

The complex temporality of SHSs is identified by the following aspects:

(1) Different devices enter a system at different times and cannot be initialized simultaneously. Families have always gradually increased the number of smart devices due to different life needs and wants, making it difficult to initialize devices with an identical timeline. In addition, when a device is aging or broken, it will be discarded, which might pose serious security problems [56]. For example, a preset key on the discarded device may be stolen.

(2) The online patterns of smart devices vary [29]. Some are always online, some are always dormant unless activated under certain conditions, and some devices are controlled by other devices, humans, or control requests from the Internet to be online, standby, or dormant. In addition, it cannot be guaranteed that a device would always be online. The durations of offline times of different devices are also inconsistent. This feature thus challenges the contextual configuration and management of SHS security.

(3) Different devices have different time precision demands for data perception, transmission and processing. It is a challenge to maintain the coordination of all devices. Some devices require frequent data acquisitions or timely and accurate online responses (e.g., healthcare monitoring [12]), and some devices can respond only once over a long period of time (e.g., reading water and energy consumption [30], and paying the bills monthly).

(4) When multiple devices cooperate to conduct services according to a command sequence [51], they may have different time granularities. For example, smart devices must work together for residents that wake up on time on working days but should also consider special settings on non-working days.

(5) Continuous certification is required. To facilitate users in SHS, some services require implicit continuous authentication [57], such as when wearable devices enter or leave the home. This process constitutes a security behavior sequence.

III. SPEAR VS. SHIELD

The relationship between the cyber-attack and the security protection can be described as a “spear” vs. a “shield”. The “spear” refers to the context, information and tools that attackers can exploit, while the “shield” refers to the usable conditions, security measures and methods that can be used in SHS. This review does not intend to analyze the vulnerability of network protocols used in SHSs in detail but summarizes possible security issues, countermeasures and mitigation at a high level, particularly from the perspective of devices and context.

A. SPEAR

Traditional attacks in CPS still exist in IoT-based SHSs and exhibit different features due to their particularity and the rapid explosion of household IoT-based devices. Due to resource-constrained, traditional security solutions used in PCs cannot be directly applied to IoT devices [10]. Hackers can easily steal sensitive information from devices, transmit malware to them, or commit other malicious acts. A detailed investigation on the security threats and privacy protection issues faced by the existing IoT devices was performed [58], in which some countermeasures that were specifically used to protect SHS sensors were proposed. Ali et al. [8] studied the cyber-attack and its impact on the entire smart home system, identified the security requirements and solutions, and proposed the objectives of security setting in SHS. To strengthen the security of IoT-based SHSs, we must first describe all possible attacks.

1) ATTACK TAXONOMY

A good taxonomy of cyberattacks is helpful to obtain better and targeted security countermeasures. Many studies classified attacks in light of SHS architecture. For example, security threats fall into three categories: physical (perception), network and application-layer attacks [59]. There is
also taxonomy from the perspective of hierarchy. For example, Andrea et al. [60] identified four types of attacks in the IoT: physical, network, software and crypt. This taxonomy provides a broad perspective for research on vulnerabilities in SHS [61].

According to how an adversary breaks the functionality of a device, attacks can be classified into four different types: ignoring, reducing, misusing and extending [4]. The starting point of the first three comes from a device’s real function, while the extending-functionality attack requires more attention because it expands a device’s capabilities and uses its cyber-physical coupling to cause additional damage (e.g., triggering epilepsy via a compromised smart light). According to features and technologies, attacks can also fall into four categories: DOS, Sybil attacks, spoofing/alternating/replay routing attacks, and node capture attacks (wormhole attacks) [62].

By classifying security threats from the perspective of coupled CPS [63], possible attack vectors and their potential impacts on the security of residents and their family members can be considered. Following this idea, Heartfield et al. [63] analyzed some legitimate but vulnerable SHS cases and identified 25 types of attacks, which may lead to various second-order attacks.

There are also taxonomy methods for specific devices. For example, Ho et al. [5] studied three attacks (i.e., unauthorized access, log integrity and user privacy) on smart door locks. Due to the diverse nature of SHSs, these methods may not be applicable to other devices or scenarios.

2) TYPICAL ATTACK TECHNOLOGIES

(1) A side-channel attack uses leaked information introduced from the additional physical quantities generated by the cryptographic algorithm to launch the attack. Schlegel et al. [64] introduced a Trojan called Soundcomber with a few harmless permissions that could be used to obtain user’s secrets, such as bank card number and pin number, by monitoring the interaction based on tone and voice. Another type of attack is to compromise the motion sensor in a smart watch as a side channel to infer keys typing on the touch panel. Different attacks were used to observe wrist motion in different scenarios to infer typed keys to obtain secrets [65]. However, there are few countermeasures for such attacks, in which data obfuscation is a low-cost and feasible solution.

(2) Physical/hardware attacks primarily refer to attacks involving physical means to compromise IoT-based devices. Many side-channel attacks also have this property. In addition, sensor eavesdropping and firmware analysis may also be considered hardware attacks [66], [67]. Considering multiple case studies, Jha et al. [68] indicated that micro-robots with micro-electro-mechanical systems (MEMS) can forge the data in NB-IoT. Meng et al. [48] conducted a comprehensive investigation of several new attacks on voice interfaces in an SHS and believed that the primary security threat in the physical layer should be a jamming attack, in which an adversary sends wireless signals with the same frequency as that in the target network using a high-power RF generator to interfere with or even paralyze all communications. The high-power RF generator can also be used to attack smart locks.

(3) Social engineering is a method of gaining someone’s trust by lying to them through psychological traps such as the victim’s psychological weakness, instinct response, curiosity, trust, and greed, and then abusing that trust for malicious purposes - primarily gaining access to systems. In SHSs, social engineering attacks are easier to execute due to the nature of diversity, heterogeneity, and CPS features. Attackers can entice home administrators to install malware into their mobile phones [69], and then obtain access and control of home devices remotely. Complex social and trust relationships bring more chances for social engineering attacks [17]. For example, attackers can exploit the compromised mobile devices of the home nanny to invade the SHS network. An example of a social engineering attack is phishing, which includes 32% of confirmed data leaks [70]. Devices in SHS have also become the victims of phishing [46], [47]. Using the STRIDE model, Abbas et al. [71] revealed that there are many potential threats that may lead to phishing attacks in two flowing IoT scenarios: self-driving and SHS.

(4) Energy attacks include energy analysis, consumption/theft, and energy device intrusion [30]. Devices in SHSs are vulnerable to energy theft, particularly passive devices. There are many solutions for energy attacks, such as optimizing energy consumption, confusing energy generation, energy regeneration, electromagnetic energy collection [72] and magnetic field energy collection based on indoor power lines [73]. Addressed to energy savings, Zungeru et al. [74] proposed a secure energy exchange system based on wireless communication and energy self-collection. To detect energy theft, special methods are required. An intelligent energy theft judgment and evaluation system based on ML (machine learning) and a statistical model was introduced [75]. First, a mixed ML scheme is used to predict the energy consumption, a simple moving average is then used to extract the anomalies, and finally, a model is built to determine whether energy was stolen or not. In addition, a block chain can be used to conduct energy trading, in which a novel Proof of Energy Generation (PoEG) and Proof of Energy Consumption (PoEC) are used as the consensus protocols. These two protocols can also be used as defense means for energy theft [34].

(5) In user-credentials and privacy attacks, the target is user access credentials and privacy information, which can be used to perform more harmful practices. The design bugs in security protocols may also help attackers easily obtain protocol parameters stored on users’ mobile devices to conduct offline dictionary attacks (i.e., offline password guessing) [39]. Credential-based access control will bring more chances to excessive privileged access [76], [77]. Xiao et al. [76] implemented an SHS controller to resist excessive privileged access by establishing a credential-free authentication framework based on the publicly available side channels in Android smartphones. There is also a
function-based fine-grained access control scheme using identity-based encryption to prevent applications from accessing unauthorized services [77]. In healthcare monitoring systems, anonymous failure means serious user privacy and access credentials disclosure. A good anonymous authentication protocol can help to alleviate this problem [78].

(6) Other internal attacks exist. When an adversary hacks into an SHS, they would have more ways to launch privileged insider attacks [79]. For example, a physical signal internal attack [48] can occur via compromised devices using light, electromagnetic, other energy or physical methods. Also, a spoofing attack [48] can forge communication data to obtain a wider range of permissions. Man-in-the-middle attacks can also be regarded as a type of internal attack.

(7) Traffic analysis [80], [81] in a complex Wi-Fi environment can allow an adversary to identify the target device’s status [82], [83], which is used to deduce the resident’s privacy. To prevent traffic analysis, air-padding was proposed in [81], which used a lightweight device to send data packets of specific structures to home gateways and other IoT devices to change the origin traffic features. To prevent traffic analysis of a target home, multiple smart homes adjacent in the same region use a differential privacy algorithm to select a proxy gateway. Multiple proxy gateways constitute a community via a wireless multihop network. In a smart community, the uplink/downlink transmission of data is performed by combining directed random walks with flooding hybrid routing algorithms, and the traffic feature of a specific home is hidden so that adversaries cannot accurately locate the home.

DoS is the most typical attack using traffic. In SHS, devices might be used to conduct DDoS. The behaviors of the compromised devices are important to security situation awareness. DDoS is also related to energy attacks, and protocols, attack rate, load size, and port status of victim devices are important factors that affect their energy consumption [84].

(8) In an Adverse Machine Learning (AML) attack, ML, a common technology in dynamic-learning-based IDSs, allows IDS becoming an attack portal. The disturbance of AML confuses the decision boundary of the IDS classifier and can misclassify malicious packets as benign. Anthi et al. [54] proposed a rule-based method to generate AML attack samples, which are used in a series of supervised machine learning classifiers for detecting DoS attacks in SHS. Then, an IDS with these classifiers is made, which is more robust against such attacks using adversarial learning such as GAN. There are other attacks based on AI algorithms or using statistical analysis.

This taxonomy is not a well-defined classification of all attacks in SHS. Some attacks cannot be clearly classified because they might contain several properties of different attacks concurrently. Some technologies must also cooperate with other technologies to cause harm. The types listed above are only based on their primary technical features, particularly focusing on the specific technologies in the SHS context.

3) ATTACK MODEL
The attack model plays an important role in network security because it clearly defines the boundary of problems and can help solve problems more effectively. Several studies have used the Dolev-Yao model [85], in which attackers can eavesdrop, intercept, inject, replay, and modify messages [86], [87] on an open channel. STRIDE [88] is also a commonly used attack model, which is a modeling method that can evaluate security from the perspective of attackers. The acronym STRIDE classifies threats as spoofing, tampering, repudiation, information disclosure, DOS or elevation of privilege, and covers most current security issues. Abbas et al. [71] used it to model the threat of phishing in two specific scenarios – smart homes and autonomous vehicles – to identify and mitigate the damage caused by the incorrect design of devices.

There are also some customized attack models for specific scenarios. Zhu et al. [81] defined an eavesdropper attack model in a Wi-Fi network encrypted with WPA2. Adversaries can passively eavesdrop through some monitoring devices without accessing the network, while these devices are difficult to perceive. Ho et al. [5] identified four additional threat models that smart locks might want to protect against.

4) A BRIEF SUMMARY OF THE “SPEAR”
An IoT-based SHS bears more security risks than a traditional system: various vulnerabilities are inherited from the IoT and legacy system, and new vulnerabilities are generated in the special context that can be exploited by hackers. Concurrently, the complex software and hardware architecture in SHSs challenges security and privacy protection, whereas some traditional effective solutions are difficult to directly apply. For example, in smart grids, the attack surface of social engineering is smaller, but in SHSs, due to human factors, many social engineering attacks can be conducted. For example, a home owner may inadvertently disclose the critical secret of the home gateway to a temporary repairer. This review summarizes the common attacks and optional security measures in SHSs. A comparison of the above listed attack technologies is shown in TABLE 2, where the attack type is described according to the three-layer architecture. The intensity of different technologies applied in traditional networks, common IoT and smart homes are compared, and typical attack vectors and the corresponding optional countermeasures are proposed.

B. “SHIELD”
The attacks that SHS tend to experience are not completely consistent with the traditional method of network attacks; thus, defense strategies and methods must be improved. In addition, compared with attackers, defenders have additional advantages: 1) at home, the owner has complete decision-making abilities over the device; 2) residents can have physical contact with smart devices; and 3) residents can use their biological characteristics to enhance security. The possible defense methods discussed in this paper are summarized by the mind map as the FIGURE 4.
TABLE 2. A comparison of different cyberattacks in SHS.

| Technology                  | Attack type | Traditional Network | IoT Application | Smart home application | Typical attacks                                                      | Optional countermeasure                                                                 |
|-----------------------------|-------------|---------------------|-----------------|-------------------------|----------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| Side-channel                | P           | -                   | ✓               | ✓                       | Exploit power, electromagnetic field, light, voice, sound, motion trajectory, etc. | Physical defense, data or signal obfuscation                                          |
| Physical/hardware           | P           | ✓                   | ✓               | ✓                       | Sensor monitoring, firmware analysis, signal jamming or spoofing      | Physical defense, IDS & IPS, cryptography                                             |
| Social engineering          | A           | ✓✓                  | ✓               | ✓                       | Fake email, phishing, whaling, etc.                                  | Confirm to the security rules, authentication, security audit, security consciousness |
| Energy attack               | P,N,A       | -                   | ✓✓              | ✓                       | Energy analysis, consumption, stealing & intrusion into energy management device | Energy anomaly detection, Energy consumption optimization, obfuscation of energy generation and collection |
| User credentials and privacy| P,N,A       | ✓✓                  | ✓               | ✓                       | offline dictionary attack(password guessing), excessive privileged access, anonymous failure, etc. | Cryptography, data hiding or obfuscation                                               |
| Other internal attack       | P,N,A       | ✓✓                  | ✓✓              | ✓                       | physical signal internal attack, spoofing, man-in-the-middle         | Physical defense, cryptography, data hiding or obfuscation                             |
| Network traffic             | P,N,A       | ✓✓                  | ✓               | ✓                       | Traffic analysis, jamming                                             | IDS & IPS, anomaly detection system, Air-paddling, differential privacy, traffic data obfuscation |
| Adverse machine learning    | A           | ✓✓                  | ✓               | ✓                       | Disturbing the decision of IDS/IPS classifier                       | Improved robust machine learning, Confrontational learning, GAN(Generative Adversarial Network) |

P = physical layer security, N = network layer security, A = application layer security.
- = rare, ✓ = normal happened, ✓✓ = frequently happened.

FIGURE 4. The mind map of the shield of SHS.
1) INTRUSION AND ABNORMALITY DETECTION
The intrusion detection system (IDS) is still an important tool in SHS, but it needs improvement to adapt to SHS. IDS can fall into rule-based schemes and dynamic learning-based ones. Compared with the latter, the former have a lower false-positive rate, but it is difficult to generate rules and have insufficient association with context features.

Research on rule-based IDSs primarily focuses on rule generation. Information system specification can be used to extract IDS rules [89]. Product documents or offline data can be analyzed to generate rules by data mining [90], [91]. It is also feasible to combine block chain and federated learning to build a hierarchical architecture to learn the global rules required by the IDS on a cloud server. Learning on the cloud is conducive to privacy protection and relieves the pressure on local devices, but also allows for the unified management of IDS rules using hierarchical block chain nodes [92].

Dynamic learning-based IDS and IPS typically require context to determine whether the system is abnormal; thus, ML is often required. State-aware machine learning technology was used in BACnet to identify legal command sequences that may lead to system failure, and an ANN classifier was used to detect such attacks [51]. Semantic awareness was used for anomaly detection [93], in which the communication model and generated alarm is user actionable, making it easier to manage. Zhang et al. [52] proposed an IDS based on a repeated games model, but the scheme had not been verified in a real-world environment. Its run-time, space and power consumption were not analyzed in detail; however, this problem remains a concern for IoT-based SHSs. Statistical signal processing and multiple regression models were used to analyze the behavior power profiling of heterogeneous wireless sensors to predict security threats [94]. The average prediction accuracy reached 80% and was as high as 89% with one single device.

2) AUTHENTICATION AND KEY AGREEMENT (AKA)
Due to resource constraints, the traditional AKA cannot be directly used in an SHS; thus, many studies have investigated lightweight schemes. Nandy et al. [16] summarized the security of authentication mechanisms in the IoT from the perspectives of attack classification, authentication methods, and verification and evaluation technologies. This paper focuses on anonymous authentication, multifactor and proxy remote authentication, and key agreement and generation schemes used in SHS.

a: ANONYMOUS AUTHENTICATION
The features of large-scale, diversity and complex temporality in an SHS indicate that anonymous authentication has many advantages. Ms et al. [38] proposed an anonymous authentication scheme using ECC that avoided retaining the authentication table for identification. A random number method was used against replay attacks and is useful for clock synchronization. However, the scheme is vulnerable to internal privilege attacks, offline password guessing, smart card theft, fake users, parallel sessions and password modification attacks. Considering these defects, Xu et al. [39] proposed suggestions to improve security, and Banerjee et al. [87] proposed a more secure and robust scheme. Using the more rigorous Dolev–Yao model, formal and informal security analysis with a real or random (ROR) model proved that the scheme can prevent the most common attacks in SHS. Similar to anonymous authentication, without the help of trusted third parties and preloaded secrets, Zhang et al. [40] designed an AKA scheme using the secret mismatch problem. Yuanbing et al. [78] proposed a protocol for a smart medical system based on ECC, which can resist internal privilege attacks and smart card theft without the problem of user anonymity loss.

With SDN architecture, a lightweight AKA scheme named ALAM and its upgrade version were proposed in [32] and [95]. When SHS communicates with the Internet of vehicles, sensitive information such as the user’s driving route, home location, and the connection profile between vehicle and home might be eavesdropped or abused. It is thus necessary to establish an effective AKA mechanism between vehicles and homes across vehicle networking and the internet. An anonymous authentication scheme was constructed for the WAVE protocol with the protocols in higher layers, in which a noninteractive zero-knowledge proof was used for the validity of the ownership of anonymous certificates [96].

The automatic verification of the user’s mobile phone number can improve the user’s experience with SHS. In a cellular network, a phone number can be extracted from signaling data but not directly from Wi-Fi-based SHS. To address this problem, an automatic extraction and signature scheme of mobile phone numbers for SHS was proposed based on deep packet detection of home broadband traffic [97].

b: MULTIFACTOR AUTHENTICATION
In addition to the authentication schemes based on ID and password [98], [100], multifactor mechanisms are widely used in SHSs. Biological hash information in smart homes was used to build a lightweight three-factor authentication scheme [49]. Chaotic mapping was combined with zero-knowledge proof and fuzzy extraction for remote multifactor AKA [50], in which fuzzy extraction was used to symbolize biometrics. To enhance the AKA protocols proposed in [101] and [102], Zhang et al. [52] proposed a new protocol based on smart cards and passwords. However, this protocol was shown to be insecure under several serious attacks, such as smart card theft, internal privilege attacks, legal user masquerading, password change and temporary secret disclosure attacks [103].

c: REMOTE AUTHENTICATION BASED ON A PROXY GATEWAY
It is dangerous for a user to directly communicate with his home devices due to side-channel sniffing, which places the user’s private data at risk of leakage, which would produce other threats. Using the home gateway to access the internet service of IFTTT (i.e., if this then that) type for
authentication is an option. Using cryptography primitives such as ECC, nonces, XOR and encryption hash function, Lyu et al. [104] designed an anti-tracking mutual authentication scheme with a key agreement mechanism, which provides perfect anonymity and forward security. However, in the IFTTT-type authentication, the user’s profile is stored on the cloud, the account of which might be hacked, resulting in the hosted devices being easily hijacked. To solve this problem, Luo et al. [105] established a gateway-specific secure framework for authentication based on the U2F protocol (a user authentication protocol in the FIDO online fast authentication standard) to provide secure management of IoT devices hosted on the cloud. In this protocol, authentication via an IFTTT gateway was achieved by a hardware token, and one authentication can be used to authorize multiple operations on the corresponding device.

d: KEY AGREEMENT
Jiang et al. [106] proposed a lightweight key agreement protocol based on ECDH, in which a one-way hash was used instead of mutual authentication to identify sensor nodes, and the Chinese Remainder Theorem (CRT) was used to improve security. The protocol was shown to verify the integrity of data and resist replay attacks, man-in-the-middle attacks, etc. In the context of the Telemedicine Information System (TMIS), a mutual AKA protocol based on bilinear pairing using biometrics was proposed in [107]. Its security is based on the strength of ECDLP and ECCDHP. There are other ECC-based mutual authentication protocols [108], [109] for TMIS systems.

With the assumption that SHSs have a certain risk assessment capability, Xiang et al. [86] proposed a device authentication scheme with situation awareness in the smart meter scenario. Under the Dolev–Yao model, the capabilities of message integrity, mutual authentication and session key generation under different risks were obtained in the scheme, which was claimed to prevent man-in-the-middle, replays and masquerading attacks with formal verification using the automatic verification tools of AVISPA. However, this scheme may suffer from device theft, counterfeiting and session key leakage, and cannot provide secure mutual authentication. To solve these defects, Oh et al. [110] proposed a lightweight authentication protocol for IoT-based smart homes. In addition, Kumar et al. [111] proposed LAKA, which stands for Lightweight AKA, with hybrid cryptography, to achieve trust, anonymity, integrity and sufficient security in smart energy networks.

e: KEY GENERATION VIA PHYSICAL SIGNALS
To solve the challenges of fragmentation, Zhang et al. [112] proposed a matrix-based cross-layer key establishment protocol without sharing preloaded secret. First, an IoT device extracts a master key in the wireless fading channel and then shares the key via a home gateway. Then, the home gateway distributes key seeds to other smart devices using the master key. Using the key seeds, any two devices can establish a session key at the application layer. There is also a method to generate a key using the channel features of the wireless link side, which has certain advantages in consistency, randomness and security [113]. To solve the problem of a low bit extraction rate while generating keys via physical signals, the Merkle puzzle was introduced to extend the low entropy seed to high entropy key so that an efficient key agreement scheme could be designed. However, this type of scheme requires more time and computing cost. To mitigate this problem, the scheme proposed in [114] extracted a short random key at the physical layer and then established a secret communication key at the higher layer (e.g., at the network layer using a home gateway).

3) DATA CONFIDENTIALITY AND EXCHANGE
Data confidentiality and secure data exchange are critical capabilities for comprehensive security in SHSs. Traditional encryption schemes cannot be directly used in SHSs due to their contextual features and is an option to improve the encryption algorithms or session key generation for access control using differential privacy or identity- or attribute-based encryption [28], [77]. Another option is to design lightweight steganography to hide secret information and secrets about its source, such as the generator’s profile [115], [117]. There are also some methods to use contextual features to conduct secure data exchange [118].

a: DATA EXCHANGE
To verify the integrity of the data uploaded to the cloud and prevent the external and internal unauthorized devices and malicious gateways from corrupting the data, Meng et al. [48] proposed a secure data upload scheme based on ECC, in which a session key generation algorithm was constructed between the device and the cloud SP with a guarantee on the uploaded data integrity verified using the Merkle hash tree. Adiño et al. [119] discussed the security of RSA and AES for data exchange between devices under real-world scenarios, wherein the RSA key is regenerated per day. The authors reported that it was difficult for external attackers to compromise the data exchange between devices in the proposed scheme. In addition to encryption, secure multiparty computing is a good option; thus, multiple devices participate in secure data exchange. Liu et al. [120] proposed a secure group data exchange protocol on a physical layer in a smart home, in which nested lattice physical layer network coding was performed in each sensor, and then, the coded data were summed on a home router. This scheme can resist attacks of untrusted home routers and external eavesdroppers, and has the advantages of being lightweight and free of secret sharing. However, not all devices have sufficient computing and storage capacities to use session keys for secure data exchange. Huang et al. [118] proposed a secure data exchange protocol using a home limited channel (HLC), free of session keys and resisting attacks conducted by malicious internal smart devices.
b: PRIVACY PROTECTION
According to the user’s profile, the real-time sensor data are identified as sensitive or common data through machine learning [117]. For sensitive data, the method of combining encryption and information hiding can be used for secure data transmission on open channels. To mitigate the economic loss caused by data theft in smart medical systems (SMSs), various data steganography methods with biological signals have been proposed. Sharma et al. [116] summarized the watermark-based data hiding for biological signals in SMS and proposed some research suggestions, such as reducing the computational complexity of watermark generation of 3D signals and applying encryption, compression and error correcting code. These issues are also worth discussing with regard to SHSs. For example, steganography or obfuscation can be used when uploading data from a home video monitoring device to a cloud or remote terminal. To mitigate the need for power consumption analysis, an efficient data aggregation scheme for privacy protection was proposed [115]. In the scheme, the users in a community are divided into different groups, and the users in the same group hide their real identities with pseudonyms. A user can create multiple pseudonyms and associate different data with different pseudonyms. Each group has a private block chain to store member data, and Bloom filters are used for fast authentication.

4) PROTOCOL ANALYSIS AND IMPROVEMENT
There are various communication protocols available in the SHS scenario. Four popular protocols were compared and analyzed in terms of security in [10]: ZigBee, Bluetooth Low Energy, 6LoWPAN and LoRaWAN. The security countermeasures and possible attack surfaces were discussed from a practical perspective, and the features of processing units, encryption hardware and software used by commercial devices for realizing the four protocols were analyzed [10]. In the context of SHSs, this review provides a simple survey of the research on several protocols popularly used as follows:

a: LoRaWAN
This protocol is a set of protocols and system architecture designed by Lora Alliance for long-distance communication. Lora Alliance is a cooperative organization composed of device manufacturers, solution providers, system integrators and network operators. A public, private or hybrid network provides the interoperability required to expand the IoT market around the world. After analyzing the secure solutions of LoRaWAN 1.1, the classification of threats faced by the protocol was provided, and the scale, impact and possibility of each threat were discussed and analyzed [121]. In particular, serious real-world threats are highlighted, such as the physical capture of terminals, malicious gateways and self-replay attacks.

b: BACnet
This protocol is designed for the control system of smart buildings, proposed by ISO, ANSI and ASHRAE. Many studies have focused on the security of BACnet. For example, IDS rules [90] could be generated using manufacturer’s product documents, and threats and network anomalies could be detected by combining situation awareness using machine learning or by offline data mining [51], [91]. BACnet network traffic data were analyzed [122], and anomaly detection could be performed on multsource data traffic [29].

c: NB-IoT
Various possible attacks in NB-IoT were analyzed based on the secrecy rate (SR) and the secrecy outage probability (SOP) [43], such as shared node attacks, synchronization attacks, node failure attacks, source code attacks and battery depletion attacks. NB-IoT-based bots with microwave electromagnetic systems (MEMS) might be compromised for malicious actions that can pose serious threats to national security. Different security cases from the perspective of hierarchical architecture were analyzed in [68], including attacks using NB-IoT-based bots in SHS. In that study, the authors reported that the MEMS bot could effectively cheat smart devices in the network, thus ruining the security of the SHS [68].

d: 6LoWPAN
The basic 6LoWPAN does not include the content of security and privacy protection. Tanveer et al. [123] proposed an AKE (authentication and key exchange) scheme for lightweight clients in 6LoWPAN, and the SHA-256, XOR and a simple encryption primitive were used for the authentication and the exchange of session keys between a remote user and a network entity.

e: MATTER
There are many mainstream communication protocols for smart homes, and it is difficult to establish an efficient connection between different devices with different protocols. To overcome this problem, in 2019, initiated by the CSA, a number of leading companies and organizations in the IoT industry jointly established a working group called Project CHIP, the goal of which is to develop a crossing platform, the underlying common protocol standard called Matter [124]. The advantages of the matter are important, but its security requires further research, analysis and evaluation.

5) BIOLOGICAL FACTORS
The cyber-physical coupling feature means that biological factors play an important role in SHS security. Today, traditional authentication has gradually been transformed into biological factor authentication, which is more convenient and secure [125] because the unique biological features are difficult to be forged, such as fingerprint, iris and face. Biological factors can be used to make remote AKA protocols more secure [50]. In [48], a novel voice activity detection system was proposed to perform authentication by analyzing wireless signals generated by IoT devices and voice samples received from users. The scheme can effectively mitigate...
the attacks on voice interfaces. In addition, millimeter wave radar was used to capture vocal cord vibration (VCV) and lip movement (LM) as multimodal biometrics for speaker recognition [126] in smart voice assistants. Physiological signals, such as the heart rate variability (HRV) provided by wrist wearable devices, were used for implicit persistence authentication after signal processing and cleaning with machine learning algorithms [57].

Activity recognition is a new aspect of biological factors. By recognizing human activities, many security and safety challenges from real-world applications might be overcome or mitigated, such as those produced by health-care monitoring. A region-based segmentation technology was proposed in [127], which can effectively slice the sensor data stream to accurately recognize human activities. Biological signals can also be used in data steganography to prevent data theft in smart medical systems [116].

6) PROGRAMMING FRAMEWORK AND SDK
Software development cannot be isolated from the programming environment, and a fragile programming framework will introduce additional attack vectors. A framework named ContexIoT [128] was proposed to provide a context-based permission system for appified IoT systems. ContexIoT supports fine-grained identification of sensitive behaviors of apps and helps users to perform effective access control at runtime. The authors developed and verified a prototype system of ContexIoT on Samsung SmartThings. In [129], the FlowFence framework was proposed and requires an app to explicitly declare its expected data flow pattern of sensitive data. In the data flow mode, the app will be forced to run in a low overhead state, while other undeclared data flows will be locked. This scheme improves the access control model used by Android, in which the original model is used after declaration.

7) DIGITAL FORENSICS
Effective digital forensics has a deterrent effect on imminent attacks, and forensics results can also be used to remedy or update the rules of IDS and other systems. Vulnerabilities of IoT devices make it easier to extract digital traces but may also be used by criminals to undermine the devices. To enhance the tracing capabilities to various IoT devices in smart homes, [130] showed how the tracing of IoT devices in SHS was helpful for investigation and evidence collection through some cases. There are also studies of the threats suffered by the current and future user-centric IoT (UCIoT). Based on the STRIDE and DREAD modeling methods [131], a network data flow model was built to evaluate, analyze and identify high-level threats and focus areas, which is helpful for digital forensics [7]. The authors also established a case study system using AllJoyn, an open source IoT framework.

8) OTHER TECHNOLOGIES
a: HONEYPOT
To prevent data leakage or other security problems caused by eavesdropping, honeypots and similar methods can be used.

Beyer et al. [45] proposed a life pattern analysis tool that could send fake wireless signals by imitating the devices in an SHS. This method can be considered to be a honeypot to prevent eavesdroppers from distinguishing devices, identifying events and tracking users. There is also the combination of the Kerberos authentication protocol and honey encryption to provide a strong multilevel security system [132].

b: USER ROLE
Users’ awareness and perception of security risks is important to enhance the security of SHSs [61]. The definition of network sentient analysis was proposed in [133], which can dynamically adjust the security level of the SHS network according to the risk assessment by the owner. The detected sentiment rank can be propagated to nearby homes (e.g., smart homes in the same building or community) to adjust their security levels, which forms a real-world collaborative security system. Combined with context, user behavior, belief and confidence in smart home security are useful for making authentication and authorization decisions [17].

c: DEVICE COLLABORATION
The security of smart meters for energy or water based on smart PI 2.0 was discussed [30]. The authors believed that cooperation between different smart meters could prevent external attacks and data undermining. This idea can be applied to other types of devices to establish a common, collaborative and secure SHS environment.

IV. ARCHITECTURE AND EVALUATION
A. ARCHITECTURE
It is necessary to introduce reference architecture in SHS to facilitate security analysis [35] due to their heterogeneous features. In the reference architecture, a high-level description of various functions and components required by IoT devices and smart home networks is essential. An appropriate architecture is helpful when identifying the attack surfaces of an SHS and deducing critical vulnerabilities.

1) ARCHITECTURE TAXONOMY
According to whether there is a home gateway (HG) and its role in smart homes, the current security architecture can fall into three categories:

a: CENTRALIZED
The typical centralized architecture takes an HG as the central node of a home, which aggregates data and control information, and then interacts with the Internet [38], [134], [135]. Research on this type of architecture primarily focused on enhancing the security of HG. Xu et al. [136] introduced intelligent programmable home routers, which provide efficient content distribution, content modeling for security monitoring, and a delegation model of security operations. Anthi et al. [137] proposed EclipseIoT, an adaptive hub that uses dynamically loadable add-on modules to communicate
with various devices, provide policy-based access control, and mitigate the exposure of local devices to remote attackers; this system can monitor attacks using warning functions. Different devices in an SHS should have different control rules corresponding to appropriate security levels. Barsocchi et al. [138] believed that off-the-shelf sensors and technologies could be used to ensure the regular exchange of critical message, and high-level configuration (i.e., sensors, usage control and access control rules) related to behavior could be decoupled from the events affecting the physical structure of sensors so that the infrastructure in SHS can obtain the features of low cost, easy installation, friendly UI, dynamic and flexible configuration.

b: HYBRID

In this type of architecture, homes and communities are distributed, and some gateways or compute nodes are selected by them through special algorithms to accumulate data, as shown in FIGURE 5. Then, aggregated data are sent to the cloud for centralized processing. Many SHSs combined with block chains use this architecture, as shown in the figure. One solution of the heterogeneity of an SHS is to introduce cloud service to store the configure rules of smart devices, which is also called IFTTT-type internet service. However, IFTTT is vulnerable to feature-distributed malware (FDM). By incorporating a one-time password (OTP) authentication scheme based on verification code and a physical unclonable function (PUF), a secure IFTTT-based SHS framework was proposed [139]. Before entering a system, selecting and setting up appropriate encryption algorithms for a new device is important [42] because it is the foundation and core of security in the usage phase. In hybrid architecture, the technologies of ECC, nonces, XOR, encryption hash function and other cryptographic primitives or hardware tokens were used in the remote authentication on proxy gateway [104], [105].

c: DISTRIBUTED

In this type of architecture, there is no special HG to hold security functions of SHS. Devices are all connected to cloud servers through wireless or wired networks for remote configurations and control. The mobile ad hoc network (MANET) allows wireless communication between various computers and devices, making it suitable for SHSs. Alam [140] studied the MANET framework based on cloud computing to provide security guarantees between smart devices. The author summarized the challenges and difficulties related to the security, reliability, privacy and availability of services from the perspective of cloud service in MANET. In addition, the combination of MANET with cloud computing can also be used for 5G heterogeneous networks.

2) SECURITY ARCHITECTURE

Currently, many architectures that improve security have been proposed. GHOST is a project funded by the EU Horizon 2020 Research and Innovation Foundation that aimed to develop reference architecture to ensure the security of the IoT-based SHS ecosystem. Under this project, a traffic capture and monitoring mechanism was proposed [141] to monitor smart home activities using an integrated system. A design and implementation of app consent forms were proposed under this project [148]. This system includes a distributed app that can interact with a group of smart contracts deployed on a private Ethereum network. To ensure the nonrepudiation, integrity and authentication of the obtained data, the consent forms were stored in a distributed ledger of a block chain in the form of digital signature transactions. Because these data may include users’ private data, it is necessary to inform the operating principles of the network to users and require them to sign consent forms to improve trust.

In addition to the overall security architecture, such as GHOST, there are also studies that focused on specific frameworks for specific scenarios. A lightweight Docker-based architecture called NETRA was introduced to virtualize network functions in [149]. This architecture could be deployed at the network edge and had advantages with regard to storage, memory usage, latency, throughput, average load and scalability compared with the standardized NFV (network functions virtualization), which is not suitable for IoT. Xiao et al. [88] proposed a novel, certificate-free authentication framework called HomeShield to protect an SHS by effectively preventing attacks caused by open-port and over-privilege problems. The authors built a prototype of HomeShield with open and available side channels in an Android smartphone, provided its workflow to prevent various attacks, and then tested it on a real SHS.

The insecure channels make low-cost sensors the entrances of cyberattacks because the sensors cannot take sufficient security countermeasures. Khan et al. [150] proposed a framework to enhance the security of resource-constrained devices based on secure crypto-policies and efficient AKA.

![FIGURE 5. Hybrid architecture. Families or communities are dispersed, and data are centralized on the cloud after being gathered at the home gateway.](image-url)
processes. The scheme regularly updates the token authentication process and enables nodes to resist serious attacks during communication. Based on the new security challenges produced by humanoid robots, a semantic trust model was proposed in the SHS scenario [47], in which each action of robots was evaluated according to its context and detected by the entire ecosystem of smart objects to mitigate the vulnerabilities and risks in the SHS.

3) SOFTWARE DEFINED NETWORK

SDN is an important technology that implements network virtualization. By separating the control facet from the data facet of network devices, SDN flexibly controls network traffic and makes the network more intelligent as a pipeline. SDN provides many features, such as programmability, agility, centralized management and supplier neutrality, which might overcome the traditional problems of network control, management and security. The security measures are implemented in the middle box of the SDN network rather than on low-end IoT devices, which can partly mitigate the problems of constrained resources, fragmentation and diversity in SHSs.

Iqbal et al. [59] proposed a framework based on SDN, in which security issues were investigated and software-defined security (SDSec) was discussed from the perspectives of DOS/DDoS Defense, data and communication security, privacy protection, anomaly detection and general security solutions. Considering the requirement of lightweight authentication in SHSs, a privacy-protected SDN-based framework called IoT-Guard was proposed, and an anonymous lightweight authentication scheme called ALAM was designed based on that framework [32]. However, this scheme has been shown to be vulnerable to injection session key disclosure, simulation attacks and man-in-the-middle attacks, and cannot provide user anonymity and mutual authentication [95]. To solve these problems, some basic secure rules were proposed as follows: (1) store masked secret credentials with a password and/or biometrics using a hash function and bitwise XOR operation to enhance the security; (2) use a physical unclonable function (PUF) to prevent physical attacks; (3) periodically update the shared secrets; and (4) encrypt and send messages using symmetric keys.

Iqbal et al. [145] proposed a privacy-protected communication scheme for SDN (PCSS), which can perform mutual authentication between users, controllers and smart devices, and conduct privacy-preserved user queries using lightweight symmetric-key-based authentication and searchable encryption. Relying on an SDN-supported home gateway and NFV on the cloud, the fine-grained connection control of IoT devices was achieved by defining isolated and use-oriented slice network functions [146]. There is also an SDN-based firewall to detect the behaviors of horizontal port scanning [147]. The FleXight information pipeline proposed by Shirali-Shahreza et al. [147] provided low overhead and necessary information for the controller in SHS that can be extracted using stream sampling with dynamic adjustment of the sampling rate.

B. EVALUATION AND AWARENESS

a: EVALUATION MODELS

The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method is often used to evaluate the security of smart homes [148]. Focusing on information assets, its core goal is to highlight different vulnerabilities in IoT-based SHS, show risks to residents, and propose countermeasures to mitigate identified threats. AVISPA (Automated Validation of internet Security Protocols and Applications) is also a popular tool used for risk assessment in SHS [149]. A framework to evaluate security risks in IoT devices was proposed for several typical scenarios of SHS [150]. Because the dynamic deployment of devices increases the attack surface, dynamic security evaluation is also required. In [151], a smart home network topology generator and a graph-based attack model based on the architecture proposed by Ghrardello et al. [35] were developed to analyze the relation between dynamic status and the infection and spread of malware. DREAD, a risk assessment model, was used to estimate the hazard degree of systematic risks from the five dimensions: damage, reproducibility, exploitability, affected users and discoverability [7], [131].

b: EVALUATION TECHNOLOGIES

Vitunkskaite et al. [152] evaluated smart cities based on their network security measures, particularly the technical standards and management frameworks; reviewed 93 security standards and implementation guidelines; analyzed three typical cities in terms of governance models, security measures, technical standards and third-party management; and then proposed a reference framework including technical standards, governance input, regulatory framework and compliance assurance to ensure that the safety and security could be observed at all levels of a smart city. Sicari et al. [153] proposed a common method for assessing end-to-end system risks. The authors objectively investigated the static and dynamic characteristics and components of the IoT system, and the reliability and robustness of IoT platform components against malicious attacks within the entire data life cycle were discussed. The security risk that emerged when the Android system connected to IoT devices was estimated from the perspective of cyber threat intelligence and situation awareness [69].

c: SITUATION AWARENESS

Based on the nature of the IoT, Chouhan et al. [154] provided a situation assessment method and highlighted the security enhancement for IoT applications in terms of local function, transmission and data storage. Combining edge devices with users, a pricing resource allocation model with utility maximization was constructed [155]. Although the model is not a solution to IoT security, it may be able to be adapted to
build a security situation awareness and assessment model in SHS. Xie et al. [156] proposed a security situation assessment model for the information system of smart mobile devices based on the modified interval matrix-entropy weight-based cloud (MIMEC).

V. TECHNOLOGICAL FUSION AND PRACTICE
A. TECHNOLOGICAL AND SCENE FUSION

The architecture and implementation of SHSs are closely combined with many technologies. When discussing security issues, we should thus focus on theory and perform practice-based research in real-world scenarios. Among the various fusion technologies, the most important ones are block chain and cloud computing.

1) BLOCK CHAIN (BC)

Due to the complex temporality and different demands of smart devices, a distributed, transparent and dynamic access pattern is required in SHSs. The anonymity, openness, non-repudiation and consensus mechanisms of BC can ensure security with this type of access pattern. Therefore, BC has become one of the hottest research directions on the security solutions of the IoT-based SHS. BC also provides interoperability, decentralization, security, auditability, privacy protection, consistency and continuity, which can provide more security guarantees for SHS. This paper summarizes the application of BC in SHSs from the following perspectives:

a: APPLICATION FRAMEWORK

There are three types of blockchain-based SHS. In family BC, each smart home has an independent private BC for security solutions. In community (hybrid) BC, private and federal block chains are combined at the community level. Each family has a super gateway, and multiple super gateways of different families in the same community constitute a BC network, where there is a private BC in every family. In public BC, service interfaces of multiple cloud service providers form a BC network [157]. Due to the resource-constrained property, traditional BC technologies must be adapted before being applied to the SHS scenario. The feasible methods include lightweight BC schemes or frameworks, novel consensus protocols, layered architectures (combined with public and private chains, such as the second type of framework proposed above) or sliding windows [158], [160]. Different structures are shown in FIGURE 6.

Consortium blockchain might be used to provide a secure data aggregation [31]. In the scheme, the home gateways in the same community elected an agent to aggregate the data generated by all home gateways, and then, the aggregated data were recorded on the consortium blockchain to preserve integrity. Permissioned blockchain is more suitable for SHSs due to its context features, but more security challenges must be solved to achieve that. Hyperledger fabric and Hyperledger composer were combined in the scheme [161], in which three basic concepts of Hyperledger composer (i.e., assets, participants and transactions) were mapped to the essentials in SHS (i.e., users, sensors and sessions) to build a blockchain-based framework with models, scripts and access control to enable customized security solutions according to different security requirements. When there is only one home in a region (e.g., in a remote district), the community-based blockchain cannot be used. Arif et al. [159] proposed a simple secure SHS framework based on an improved consortium blockchain, in which a smart device was identified as a blockchain node to perform transaction verification of the blockchain. However, only preselected nodes can participate in consensus verification and block generation, while each smart device acts as a node and participates in mining. For a new device, users can select at least two devices to mine. PoW was used with different mining difficulties that were set based on each device’s capabilities. To ensure security about external requests, the “firewall rejection rule” was used, and frequency detection was used because requests that are too frequent would be identified as aggressive behaviors.

b: REVIEW RESEARCH

Brotitis et al. [33] conducted a detailed and comprehensive review of the security of BC and distributed ledgers under the background of SHSs. Based on the analysis of system architecture and ecosystem requirements in SHSs, the advantages and disadvantages of typical consensus protocols were compared, and the possible attacks and secu-
rity issues of smart contracts were introduced. Different privacy protection policies that can be used in BC were also compared and analyzed. Considering the needs of IoT and SHS ecosystems, an evaluation scheme was used to score different consensus protocols and platforms according to their security, privacy-protection and performance. Platforms with higher scores (i.e., more suitable for IoT-based SHS) included Fabric with PBFT protocol, Hedera with Hashgraph, etc. Moniruzzaman et al. [34] analyzed the preconditions and frameworks of BC applied in SHS. By considering case studies, the primary challenges, such as interoperability, security, privacy, data collection and sharing, data analysis and delay of blockchain, were discussed. A four-layer (i.e., the IoT perception layer, BC layer, application layer and client layer) framework was used, and a home PC acted as a miner to conduct policy enforcement and verification. Considering the privacy and security issues of a three-layer (i.e., perception, network and application) IoT, BC was used to realize security assurance of the entire life cycle of different devices [56].

c: LIGHTWEIGHT BLOCKCHAIN AND CONSENSUS PROTOCOLS
To solve the storage problems faced by BC in the IoT, Qu et al. [162] proposed a hypergraph-based blockchain, in which the graph’s super edges were used to organize storage nodes, and each super edge stored a portion of a transaction, thus converting the entire data storage into partial network storage. The average storage load of each node increases based on its rank in the super edge instead of the degree. The entry and existence of devices were described using super edge splitting and aggregation. Balaji et al. [163] proposed a simple size extensible (SSE) BC. Two novel algorithms were introduced into the system to minimize the irregularity and delay of the system and maximize system throughput. The overlay BC manager (OBA) played the role of miner; thus, it is typical hybrid architecture. Mohanty et al. [164] proposed an efficient lightweight integrated blockchain (ELIB) model, of which the novelty has three characteristics: lightweight consensus algorithm, certificateless cryptograph and distributed throughput management (DTM). PoW is the most popular consensus protocol in blockchain. However, its mining process requires a lot of computing power. Addressing this problem, Kim et al. [165] proposed a reverse hash chain as a blockchain-based authentication scheme to replace PoW. Because this scheme only requires a few hash calculations for PoW, it is suitable for SHS.

d: BLOCKCHAIN-BASED AUTHENTICATION AND DATA SECURITY
Combining blockchain and distributed IPFS (InterPlanetary File System), a multiplatform model to mitigate the vulnerabilities of sensors was proposed with an authentication method based on color spectrum chain [166]. In [167], a novel block data structure based on homomorphic encryption (HEBDS) was proposed based on the Paillier cryptosystem, which provides privacy protection to the blockchain.

To provide secure cloud storage with multi-cloud service providers (CPSs) and to address the limited storage space and low addressing speed of blockchain transactions, an identity-based proxy aggregation signature (IBPAS) scheme was proposed [157]. This scheme improved the verification efficiency of signatures, reduced the required storage space, and reduced the required transmission bandwidth. To construct a security framework for IoT devices in SHSs, Qashlan et al. [28] proposed an authentication scheme that combined attribute-based access control with smart contracts and edge computing and used differential privacy to gather data securely into the cloud.

e: COMBINED WITH AI
DELM (deep extreme learning machine) can be used in BC to provide security [53]. In addition, a cloud IDS based on BC and federated learning was proposed in [92]. The alarms generated from smart devices were used for global prediction through hierarchical learning and aggregation on the cloud. Federated learning was used to train the model on local datasets and generate weight parameters, and then, the parameters were transferred to the global learning and prediction module on the cloud. The regional service provider (RSP) and the global training provider (GTP) are member nodes belonging to different layers in the BC. To reduce the storage pressure of BC, erase code was used so that each node did not have to store complete data of the blockchain while having the ability to recover all data. In an SHS framework combining BC with cloud computing, network traffic was analyzed utilizing multivariate correlation analysis to identify the correlation between different traffic for detecting DDoS [168]. This framework was also a community-overlay BC with a private cloud built on the SHS, in which each smart home maintained its own private BC. In terms of security, the features of new requests were extracted by a triangle area map (TAM) and judged to determine whether they are malicious by querying a signed rule database. Then, the abnormal patterns of malicious requests were analyzed by MCA to obtain the correlation between the traffic. Then, the home gateways were updated with the latest detection policies.

2) CLOUD COMPUTING
Due to the limited resources and computing power of IoT devices, it is impossible to load all resources into devices when conducting security countermeasures. Although the theories and techniques of edge computing can partly alleviate this problem, an increasing number of IoT-based smart home functions must still be performed on cloud or edge computing servers. Using cloud services in SHSs is a popular policy, including the solution described above when SHSs are integrated with blockchain. The introduction of cloud services will produce challenging problems, such as remote authentication, secure data exchange and collaborative control; however, cloud services can also enhance security. For example, cloud services are used to help prevent DDoS [169].
3) OTHER FUSION SCENARIOS

a: INTERNET OF VEHICLES (IoV)
A scheme for connecting the IoV with the SHS was introduced in [96] and can be deployed on the edge server of the IoV, allowing users to monitor and control household facilities when driving. For privacy protection, an anonymous authentication scheme based on efficient cryptographic building blocks was proposed, covered the entire WAVE protocol stack, and effectively fused multiple secure scenarios.

b: SMART GRID
Smart meters in an SHS can be considered to be the nerve endings of smart grids, and the data generated by them are used by social service companies to provide better services. However, if power consumption data are leaked, the user’s privacy will be at risk. For example, adversaries might use them to identify the usage patterns of home facilities. To solve this problem, a secure data aggregation scheme for smart meters without exposing the user’s identity [31] can be used. There are also communication architectures [170] for the hardware of smart meters, situation awareness schemes [86] and improvements [110] for efficient device authentication in the multiscenario fusion of smart grids and SHSs. SHS combined with blockchain can access the smart grid at the client layer of the system, in which energy transaction of the smart grid can be regarded as a special consensus protocol [34].

c: SMART CITY AND COMMUNITY SCENE INTEGRATION
Research progress on SHSs is critical to the success of smart city construction [161]. A home can be regarded as a cell within a city, while home facilities constitute its nerve endings. The data generated by massive home devices can provide fundamental data for urban governance, such as medical resource allocation, energy management, emergency awareness, network security situation awareness, etc. Massive homes in cities or communities can form a security infrastructure. For example, consortium blockchain can be used based on communities or cities for collaborative security purposes [144], [161], [171].

4) AI AND MACHINE LEARNING
AI and machine learning are widely used in security solutions of home devices, particularly IDS, IPS, multifactor authentication, etc. However, due to constrained resources, traditional schemes must be improved to fit in SHS scenarios. In [53], blockchain and DELM were integrated into a four-tier SHS, in which the former provides a data filtering function for the latter, such as repetition, loss of data value, errors and disruption. DELM randomly generates the parameters of hidden nodes; thus, this process has a fast training speed and can be used to realize lightweight data analysis, interpretation and prediction. The learned model can be deployed in the application layer or uploaded to the cloud for remote calls. Li et al. [15] summarized the potential of deep learning to enhance IoT security and discussed how to identify and prevent cyberattacks in the IoT and how to encrypt data for secure transmission. The authors proposed future research directions in this area, including sharing computing power with edge NPUs (embedded neural network processing units), testing the simulation model in the real world, malicious code detection, intrusion detection, production security, vulnerability detection, fault diagnosis and blockchain integrated technology. Nasir et al. [172] proposed a fully functional, cohesive SHS based on IoT and edge computing. The system used the edge device as a computing platform and has a self-defined, lightweight deep neural network to achieve automatic human fall detection. Although their work was oriented toward physical safety, the same idea can be used for cybersecurity. For example, automatic generation of the rules in IDS can use this architecture.

5) A BRIEF SUMMARY
SHS is a comprehensive and complex system, so its implementation includes various technologies. The technologies listed in this section are the most important and common syncretizing technologies in SHSs. The relation between the important research directions and results of these technologies and the layered architecture of SHS is shown in FIGURE 7. It should be noted that the four-layer structure described earlier is adopted in the figure.

B. PRACTICAL RESEARCH

1) SINGLE SCENARIO
The theoretical study and practical application of SHSs are currently growing rapidly, but their security and privacy issues have not been thoroughly studied. Many commercial devices have entered the market rapidly, and the diversified functions of smart home facilities distract people’s attention from the cyber security of SHSs. Geneiatakis et al. [20] identified the security threats of IoT-based SHSs, discussed device interactivity in the real world, analyzed the unauthorized access or DOS attack that adversaries might conduct, and described the possibilities of vulnerability utilization. Sun et al. [67] identified the vulnerability and attack vectors of common devices in some real systems, including smart light, smart switches, motion sensors, security cameras and smart home assistants. Under the influence of fragmentation, research on security issues in specific scenarios should be strengthened. Only when we have a full understanding of the security situation of the real world can we be fully prepared for building general, compatible and secure frameworks and protocols for SHSs.

To prevent DDOS attacks, smart home assistants (e.g., Amazon Echo Dot and Google Home) can partially mitigate the impediment to communication between users and smart devices [169] because their storage and computing can be performed on cloud services outside SHSs. Sowah et al. [173] proposed the design, development and implementation of a prototype on a secure wireless home.
2) LARGE-SCALE COMPARATIVE RESEARCH

Home devices can be detected quickly on the internet so that they may also be compromised and maliciously used quickly by attackers. Bodenheim et al. [174] studied Shodan, a search engine that searches any devices connected to the Internet, using a method that put four PLC devices openly on the Internet. Within 19 days, all four devices can be queried by Shodan. There is also research on large-scale cyber-physical system probes [175].

The vulnerabilities of firmware images in an embedded system can be used as entrance points for side-channel attacks, and the secrets contained in those images can also bring other risks. Therefore, security analysis of firmware images is an important method to identify the vulnerabilities of embedded systems. Costin et al. [79] unpacked 32000+ firmware images in 1.7 million individual files and found 38 unknown vulnerabilities in 693 images. Some of these vulnerabilities have caused security impacts on more than 140000 devices on the Internet. By analyzing the cases of misuse and abuse of devices of well-known and unknown vendors, and comparing the coverage of the vulnerabilities of devices produced by different vendors in the primary vulnerability databases, such as CVE (Common Vulnerabilities and Exposures) and NVE (National Vulnerability Database of U.S. A), Davis et al. [75] found that it is necessary to pay more attention to the devices of unknown suppliers.

Li et al. [177] analyzed the large-scale log provided by different vendors of home security cameras (HSC) and identified some defects, including massive useless uploads, asymmetric traffic between upload and download, incorrect user engagement, and limited monitoring positions. Through passive and active analysis, the authors reported that there are three types of privacy risks in the current HSC: traffic surge risk, traffic regulation risk, and rate change risk.

By analyzing the results of large-scale practice research, the firmware code of devices has been shown to produce many security problems. However, code-level security analysis of image files required skill, and manual decompilation analysis requires a lot of work; thus, the analysis of massive image files remains difficult.

C. SDK, OS, AND 5G

1) IOT DEVELOPMENT PLATFORM

To facilitate the development of application services of smart devices, major IoT manufacturers have released their own development platforms, such as Amazon’s AWS IoT, Microsoft’s azure IOT, Google’s Android things, Alibaba’s
cloud IoT, and Huawei’s cloud IOT. In addition, there are also some platforms aimed at smart home services, such as Samsung’s SmartThings, Apple’s HomeKit, Philips Hue Bridge and Google Home. Most of the above platforms support efficient energy utilization, interconnection, remote authentication and access control, auditing and third-party application development. However, the design problems inherent to platforms and a lack of secure coding have produce vulnerabilities in end-user products and service software. In addition, a lack of a global unified standard specification for different development platforms is an important cause of the fragmented nature of the IoT. An integrity oriented framework ContextIoT was proposed in [134], and a prototype was designed on SmartThings to provide dynamic context-based access control. Meng et al. [65] proposed a capability-based model to audit the permissions of remote apps in the SmartThings platform, but this model was so rough that it might lead to unauthorized access from malicious apps.

The service development on the device side can use multiple languages and platforms. Arduino is an open-source platform that can be used to develop hardware and software systems for IoT. This platform supports a variety of sensors and is widely used in SHSs. Sarhan [177] investigated 63 research papers that focused on using Arduino to build smart home security systems and summarized existing applications, architecture, practical technologies, component architecture and other research topics. A prototype of a secure wireless SHS was designed, developed and deployed [173] using the OpenHAB 2 framework with an Arduino Mega 2560 and Raspberry Pi Model B to run the OpenHAB software.

Considering platform problems, two topics must be addressed. First, we must formulate platform standards for SHS scenarios and provide different development options for devices with different capabilities. Manufacturers’ platforms will then need to comply with these standards to provide compatibility between different devices of different manufacturers. Second, we must establish a security specification to program the software and service development of SHSs, and determine the automatic method to detect malicious code and analyze firmware image files.

2) OS SECURITY
To ensure overall security, it is necessary to protect OSs (e.g., firmware) in sensing devices and OSs in user clients (e.g., smart mobile phones) for secure remote control. A typical attack vector on smart devices (e.g., mobile phones and smart TVS) is to install malware onto the client OS. Some studies in this area focus on the detection of malware. For example, Park et al. [69] combined machine learning to evaluate the potential threat of apps installed in Android. Meng et al. [178] performed a comprehensive analysis of 63 disclosed vulnerabilities in Android, discussed their features and taxonomy, and tested a group of selected vulnerabilities through practical cases. There are many OSs used in sensing devices, including Android-based Brillo, ARM Mbed OS, QNX, Windows 10 IoT core, and FreeRTOS. However, their security has not been widely analyzed or verified, and may result in serious security problems. In addition, the vulnerabilities of the firmware OS used in low-level devices must be identified and detected by firmware image analysis.

3) 5G
People typically use mobile devices to remotely access and control sensors and smart devices in their homes with the TCP/IP protocol via the Internet. The early IP mobility management mode was centralized, which was a brake on the edge network near IoT devices. IETF established the Distributed Mobility Management (DMM) working group in March 2021. DMM aims to solve the problem of centralized mobile IP addressing, and its flat architecture is suitable for the trend of 5G networks and IoT flats. However, without adequate security measures, DMM may also make the SHS vulnerable to various cyber threats. Therefore, it is necessary to support secure routing optimization to enable secure communication between associated devices and prevent information leakage during data transmission. Shin et al. [179] proposed a secure routing protocol for an SHS based on DMM that can provide mutual authentication, key exchange, perfect forward confidentiality and privacy protection. Wasiczek [180] believed that the future of the security of 5G-based SHSs will be based on microsegmentation, which integrates security strategies into virtual networks, virtual machines and OSs and other virtual instances to guarantee security.

VI. TWO SPECIAL ISSUES
A. COLLABORATIVE SECURITIES OF COMMUNITY AND INDUSTRY
Nurse et al. [181] reported a series of seminars and interviews with industry experts, including those in the enterprise, IoT industry and risk control area, to explore new methods for assessing secure risks and building system trust. When integrating IoT devices into an enterprise’s information systems, a deeper understanding of security risk and challenges is required. The authors investigated the key challenges faced by industry approaches to effectively and efficiently evaluate the network risks in the IoT [181].

The abnormality of a home local gateway can be exploited in a community environment via such attacks as DDoS attacks. Park et al. [171] reported that network service providers should participate in the security of home area networks. An anomaly detection strategy was proposed, in which users and service providers shared security responsibility, and machine learning was used to classify monitoring records and identify suspicious anomalies in the data center. The idea of the proposed scheme [171] was similar to the concept of cloud security: The high-performance analysis and process of cloud servers were used to improve the anomaly detection capability and resistance of cyberattacks on terminals.
B. SOFT SECURITY AND HARD SECURITY
To achieve overall security in SHSs, we require various technical methods to solve security problems and must also manage human factors, such as trust, risk, belief and confidence. The latter is referred to as soft security mechanisms [17]. Comprehensive security also requires dynamic analysis of access request patterns based on behavior-related criteria so that the security model is more flexible [17], [182]. This research topic is critical to identify the impact of user awareness on security risks. By considering optimal security configurations and usage habits, users can eliminate and avoid many risks, such as social engineering attacks. Based on the rational action approach in social psychology, Klobas et al. [183] established a new model on how perceived security risk affects people’s willingness to use smart home devices and showed that security risk perception has an indirect impact on users’ willingness. In addition, there is a national survey [184] to investigate the acceptance, experience, trust and satisfaction of people with smart homes.

VII. CONCLUSION, LIMITATION, AND FUTURE WORK
The state-of-the-art security research results of SHS are comprehensively summarized in the review. A definite, comprehensive definition for SHS is proposed, and the unique and essential features in the context of SHS are analyzed and presented. These features can help academic researchers and application developers clearly understand the connotation of SHSs and are crucial to security analysis and strategic research. In addition, the key content of this review includes: (1) existing research results of SHS security are discussed, analyzed, and compared in detail from the two opposing perspectives of attack and defense, including reviews of system evaluation strategies and layered architectures; and (2) practical research results, including integration with other technologies, such as blockchain, and the security of the development platform and tools, are discussed in detail. Human factors are also reviewed.

Although this paper makes a detailed and comprehensive review, analysis, and comparison of the security issues in the SHS scenario, there are still the following limitations; (1) a meta-analysis method is not used, and the detailed contextual sorting, causality analysis of all security researches involved in this field from the perspective of statistics are lacking; (2) Except for side-channel attacks, firmware analysis of smart devices, it does not detail other physical attacks. In the review, “security” refers to information and network security, not physical security. Of course, due to CPS features, cyber security also relates to physical security; (3) Except for the section on data security, there is no in-depth, specialized discussion on the cryptographic primitives used in SHSs. The resource-constrained nature of smart devices makes it difficult to apply traditional cryptography technologies, so lightweight encryption, identity-based encryption, and attribute-based encryption are widely used. It is also an interesting issue whether the latest research results of novel quantum-resistant cryptographic mechanisms can be applied in the SHS security field; (4) Blockchain and SDN are both interesting directions worthy of further exploration and analysis in SHS security. However, the review does not make a thorough summary and analysis of these two areas due to the review’s structure.

The above limitations will become important directions of improvement for our future work. Besides, we believe that the research on security issues in SHSs is far behind the speed of SHS development. Due to the fragmentation and diversity features of the IoT, the burst of the SHS industry will widen this disparity. According to the results of this review, in addition to the research on traditional cyber-security solutions (e.g., lightweight encryption algorithms, remote anonymous authentication), we believe that more research is required in the following aspects in the future:

- IoT-based SHS architecture has not yet taken shape. Various industrial alliances proposed different architectures according to their own needs, which impede compatibility between different products. In addition, the history of the Internet shows that a good hierarchical architecture (e.g., OSI architecture) can vigorously promote development. Therefore, based on comprehensive consideration of security issues, a general industrial architecture is the primary issue to be solved in SHS security research.
- Resource limitation is an inherent shortcoming of IoT devices that poses a challenge to conducting security countermeasures. Low-cost devices often do not have sufficient security protection policies due to their poor computing and storage. Therefore, future research should focus on the security role of low-performance and storage devices and secure functionalities in terms of their ability. In addition, it is also necessary to strengthen the research on the cooperative security theories and technologies of multiple devices.
- Fragmentation is also a serious obstacle in IoT development that makes it difficult for different devices of different vendors to be compatible with each other, which hinders mutual authentication, secure transmission, and the implementation of collaborative security. Currently, the feasible options are software defined network (SDN) and blockchain; thus, it is necessary to strengthen the research in these two aspects integrated with SHS.
- The runtime analysis of the security of codes resident on smart devices, particularly firmware security analysis, must also be addressed. In this area of research, automatic firmware code analysis and decompilation of firmware OS are challenging; the former is at the code level, and the latter is at the OS level and has more difficulties.

ACKNOWLEDGMENT
The authors would like to thank the anonymous reviewers for their insights, comments, and suggestions to improve the quality of the manuscripts.
REFERENCES

[1] R. Rutolf, “Smart home concept and the integration of energy meters into a home based system,” in Proc. 7th Int. Conf. Metering App. Tariffs Electr. Supply, Glasgow, U.K., vol. 367, Nov. 1992, pp. 277–278.

[2] M. B. Yassein, I. Hmeidi, F. Shatnawi, W. Mardini, and Y. Khamayseh, “Smart home is not smart enough to protect you—protocols, challenges and open issues,” Proc. Comput. Sci., vol. 160, pp. 134–141, Jan. 2019, doi: 10.1016/j把你删除了.1016.2019.09.853.

[3] S. Kumar, “Ubiquitous smart home system using Android application,” Int. J. Comput. Netw. Commun., vol. 6, no. 1, pp. 33–44, 2013, doi: 10.5210/ijcnc.v6i1.19103.

[4] E. Ronen and A. Shamir, “Extended functionality attacks on IoT devices: The case of smart lights,” in Proc. IEEE Ear. Symp. Secur. Privacy (EuroS&P), Saarbrucken, Germany, Mar. 2016, pp. 3–12, doi: 10.1109/1068SP.2016.13.

[5] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song, and D. Wagner, “Smart locks: Lessons for securing commodity Internet of Things devices,” in Proc. 11th ACM Asia Conf. Comput. Secur., Xi’an, China, May 2016, pp. 461–472, doi: 10.1145/2897845.2897886.

[6] D. Hodges, “Cyber-enabled burglary of smart Homes,” Comput. Secur., vol. 110, Nov. 2020, Art. no. 102418, doi: 10.1016/把你删除了.2021.102418.

[7] N. Akatyev and J. I. James, “Evidence identification in IoT networks based on threat assessment,” Future Gener. Comput. Syst., vol. 93, pp. 814–821, Apr. 2019, doi: 10.1016/把你删除了.2017.10.012.

[8] W. Ali, G. Dustgee, M. Awais, and M. A. Shah, “IoT based smart home: Security challenges, security requirements and solutions,” in Proc. 23rd Int. Conf. Autom. Comput. (ICAC), London, U.K., Sep. 2017, pp. 1–6, doi: 10.1109/把你删除了.2017.8082057.

[9] Z. A. Almusaylim and Z. Noor, “A review on smart home present state and challenges yet to be solved,” IEEE Internet Things J., vol. 6, no. 2, pp. 1606–1616, Apr. 2018, doi: 10.1109/把你删除了.2018.2847733.

[10] A. Qashlan, P. Nanda, X. He, and M. Mohanty, “Privacy-preserving mechanism in smart home using blockchain,” IEEE Access, vol. 9, pp. 103651–103669, 2021, doi: 10.1109/把你删除了.2021.3098795.

[11] Z. Zheng and A. L. N. Reddy, “Safeguarding building automation networks: THE-Driven anomaly detector based on traffic analysis,” in Proc. 26th Int. Conf. Comput. Commun. Netw. (ICCCN), Vancouver, BC, Canada, Jul./Aug. 2017, pp. 11–11, doi: 10.1109/把你删除了.2017.8038393.

[12] R. P. Díaz Redondo, A. Fernández-Vilas, and G. Fernández dos Reis, “Security aspects in smart meters: Analysis and prevention,” Sensors, vol. 20, no. 14, p. 3977, Jul. 2020, doi: 10.1109/把你删除了.2019.4349777.

[13] Z. Guan, G. Si, X. Zhang, L. Wu, N. Guizani, X. Du, and Y. Ma, “Privacy-preserving and efficient aggregation based on blockchain for big data communications in smart communities,” IEEE Commun. Mag., vol. 56, no. 7, pp. 82–88, Jul. 2018, doi: 10.1109/把你删除了.2017.8004041.

[14] W. Iqbal, H. Abbas, P. Deng, J. Wan, B. Rauf, Y. Abbas, and I. Rashid, “ALAM: Anonymous lightweight authentication mechanism for SDN-enabled smart Homes,” IEEE Internet Things J., vol. 8, no. 12, pp. 9622–9633, Jun. 2021, doi: 10.1109/把你删除了.2020.3024058.

[15] S. Trottis, K. Linnerud, N. B. Annuar Juma’at, I. Ahmedy, N. Abdul Ghani, and S. Bhateja, “On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance,” Comput. Netw., vol. 191, May 2021, Art. no. 108005, doi: 10.1016/把你删除了.2021.108005.

[16] M. Moniruzzaman, S. Khezz, A. Yassine, and R. Benlamri, “Blockchain for smart Homes: Review of current trends and research challenges,” Comput. Electr. Eng., vol. 83, May 2020, Art. no. 106585, doi: 10.1016/把你删除了.2019.106585.

[17] K. Ghirardello, C. Maple, D. Ng, and P. Kearney, “Cyber security of smart Homes: Development of a reference architecture for attack surface analysis,” in Proc. Living Internet Things: Cybersecurity IoT, London, U.K., 2018, pp. 1–10, doi: 10.1007/把你删除了.2018.00045.

[18] P. Domínguez, P. Carreira, R. Vieira, and W. Kastner, “Building automation systems: Concepts and technology review,” Comput. Standards Interfaces, vol. 45, pp. 1–12, Mar. 2016, doi: 10.1016/把你删除了.2015.11.005.

[19] F. Simeoni, E. Garza-Romero, R. D. Ruggeri, A. M. Medrano-Gil, D. F. Carvajal-Flores, G. Fico, M. F. Cabrera-Umpierrez, and T. M. Arredondo Waldemeyer, “A secure and scalable smart home gateway to bridge technology fragmentation,” Sensors, vol. 21, no. 1, pp. 3587–3587, May 2021, doi: 10.3390/把你删除了.21113587.

[20] Y. Shuai, N. Yu, H. Wang, and L. Xiong, “Anonymous authentication scheme for smart home environment with provable security,” Comput. Interact., vol. 86, doi: 132–132, Sep. 2019, doi: 10.1016/把你删除了.2019.06.002.

[21] M. Xu, Q. Dong, M. Zhou, C. Wang, and Y. Liu, “Security analysis on ‘anonymous authentication scheme for smart home environment with provable security,’” Wireless Commun. Mobile Comput., vol. 2020, no. 8, Nov. 2020, Art. no. 8838363, doi: 10.1159/把你删除了.2020/8838363.

[22] Y. Zhang, H. Zhao, X. Xiang, X. Huang, and X. Chen, “A key agreement scheme for smart Homes using the secret mismatch problem,” IEEE Internet Things J., vol. 6, no. 6, pp. 10251–10260, Dec. 2019, doi: 10.1109/把你删除了.2019.2956884.
D. Ekiz, Y. S. Can, Y. C. Dardagan, and C. Ersoy, “Can a smartband be secure and privacy-preserving? IoT enabled smart home: Architecture and experimental study,” Sensors, vol. 20, no. 21, p. 6131, Oct. 2020, doi: 10.3390/s20216131.

V. Kumar and S. Jain, “NB-IoT security: A survey,” Wireless Pers. Commun., vol. 113, no. 4, pp. 2661–2708, Aug. 2020, doi: 10.1007/s11277-020-07346-7.

M. Gajewski, J. Mongay Batalla, A. Levi, C. Togay, C. X. Mavromoustakis, and G. Mastorakis, “Two-tier anomaly detection based on traffic profiling of the home automation system,” Comput. Netw., vol. 158, pp. 46–60, Jul. 2019, doi: 10.1016/j.comnet.2019.04.013.

S. M. Beyer, B. E. Mullins, S. R. Graham, and J. M. Bindewald, “Pattern-of-life modeling in smart Homes,” IEEE Internet Things J., vol. 5, no. 6, pp. 5317–5325, Dec. 2018, doi: 10.1109/JIOT.2018.2840451.

B. B. Gupta, A. Tewari, I. Cvitić, D. Peraković, and X. Chang, “Artificial intelligence empowered mass media classifier for Internet of Things based systems in industry 4.0,” Wireless Netw., vol. 28, no. 1, pp. 493–503, Jan. 2022, doi: 10.1007/s11201-021-02619-w.

H. Sun, X. Wang, R. Buyya, and J. Su, “CloudEyes: Cloud-based malware detection with reversible sketch for resource-constrained Internet of Things (IoT) devices,” Softw., Pract. Exp., vol. 47, no. 3, pp. 421–441, Mar. 2017, doi: 10.1002/spe.2420.

Y. Meng, W. Zhang, H. Zhu, and X. S. Shen, “Securing consumer IoT in the smart home: Architecture, challenges, and countermeasures,” IEEE Wireless Commun., vol. 25, no. 6, pp. 53–59, Dec. 2018, doi: 10.1109/MWC.2017.1800100.

S. Shin and T. Kwon, “A lightweight three-factor authentication and key agreement scheme in wireless sensor networks for smart Homes,” Sensors, vol. 19, no. 9, p. 2012, Apr. 2019, doi: 10.3390/s190902012.

W. Liu, X. Wang, and W. Peng, “Secure remote multi-factor authenticaion scheme based on chaotic map zero-knowledge proof for crowdsourcing Internet of Things,” IEEE Access, vol. 8, pp. 8754–8767, 2020, doi: 10.1109/ACCESS.2019.2962912.

M. Peacock, M. Johnstone, and J. Hartog, “Timing attack detection on BACnet via a machine learning approach,” in Proc. 13th AUS Inform. Secur. MGT Conf., Perth, WA, Australia, Dec. 2015, pp. 35–44, doi: 10.1109/MGMT.2016.7485228.

R. Zhang, H. Xia, S.-S. Shao, H. Ren, S. Xu, and X.-G. Cheng, “An intrusion detection scheme based on repeated game in repeated game in smart Home,” Mobile Inf. Syst., vol. 2020, pp. 1–9, Sep. 2020, doi: 10.1155/2020/8844116.

M. A. Khan, S. Abbas, A. Rehman, Y. Saeed, A. Zeb, M. I. Uddin, N. Nasser, and A. Ali, “A machine learning approach for blockchain-based smart home networks security,” IEEE Netw., vol. 35, no. 3, pp. 223–229, May 2021, doi: 10.1109/MNET.2021.3005141.

E. Anthi, L. Williams, A. Javed, and P. Burnap, “Hardening machine measures via software-defined security,” IEEE Comput. Electr. Eng., vol. 72, pp. 266–273, Nov. 2018, doi: 10.1016/j.compeleceng.2018.08.021.

D. Ekitz, Y. S. Can, Y. C. Dardagan, and C. Ersoy, “Can a smartband be used for continuous implicit authentication in real life,” IEEE Access, vol. 8, pp. 59402–59411, 2020, doi: 10.1109/ACCESS.2020.2982852.

A. K. Sikder, G. Petracca, H. Aksu, T. Jaeger, and A. S. Uluagac, “A survey on sensor-based threats and attacks to smart devices and applications,” IEEE Commun. Surveys Tuts., vol. 23, no. 2, pp. 1125–1159, 2nd Quart., 2021, doi: 10.1109/MCOMST.2021.3064507.

W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf, and Y. A. Banagsh, “An in-depth analysis of IoT security requirements, challenges, and their countermeasures via software-defined security,” IEEE Internet Things J., vol. 7, no. 10, pp. 10250–10276, May 2020, doi: 10.1109/JIOT.2020.2997651.

I. Andrea, C. Chrysostomou, and G. Hadijichristofi, “Internet of Things: Security vulnerabilities and challenges,” in Proc. IEEE Symp. Comput. Commun. (ISCC), Larnaca, Cyprus, Jul. 2015, pp. 180–187, doi: 10.1109/ISCC.2015.7405513.

B. D. Davis, J. C. Mason, and M. Anwar, “Vulnerability studies and security postures of IoT devices: A smart home case study,” IEEE Internet Things J., vol. 7, no. 10, pp. 10102–10110, Oct. 2020, doi: 10.1109/JIOT.2020.2983983.

M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, “Internet of Things (IoT): Taxonomy of security attacks,” in Proc. 3rd Int. Conf. Electr. Design (ICED), Phuket, Thailand, Aug. 2016, pp. 321–326, doi: 10.1109/ICED.2016.7804466.

R. Hearfield, G. Loukas, S. Bodimir, A. Bezemski, J. R. J. Fontaine, A. Filipopoulou, and E. Eschen, “A taxonomy of cyber-physical threats and impact in the smart home,” Comput. Secur., vol. 78, pp. 398–428, Sep. 2018, doi: 10.1016/j.cose.2018.07.011.

S. Nasser, and A. Ali, “A machine learning approach for blockchain-based smart home networks security,” in Proc. IEEE Access, vol. 7, no. 9, pp. 1–14, Apr. 2019, doi: 10.1109/JIOT.2020.3003621.

A. Costin, J. Zuddlach, A. Francellon, and D. Balzarotti, “A large-scale analysis of the security of embedded firmware,” in Proc. 23rd USENIX Conf. Secur. Symp., San Diego, CA, USA, Aug. 2014, pp. 95–110.

A. Sun, W. Gong, R. Shea, and J. Liu, “A castle of glass: Leaky IoT appliances in modern smart homes,” IEEE Wireless Commun., vol. 25, no. 5, pp. 32–37, Dec. 2018, doi: 10.1109/MWC.2017.1800120.

R. K. Jha, H. Kour, M. Kumar, and S. Jain, “Layer based security in narrow band Internet of Things (NB-IoT),” Comput. Netw., vol. 185, Feb. 2021, Art. no. 107592, doi: 10.1016/j.comnet.2020.107592.

M. Park, J. Han, H. Oh, and K. Lee, “Threat assessment for Android environment with connectivity to IoT devices from the perspective of information assurance,” Wireless Commun. Mobile Comput., vol. 2019, Art. no. 6125539, doi: 10.1155/2019/6125539.

J. Yang, L. Sun: Comprehensive Survey of Security Issues of SHS
M. S. Farash, M. Turkanović, S. Kumari, and M. Hölbl, “An efficient user authentication and key agreement scheme for heterogeneous wireless sensor network tailored for the Internet of Things environment,” Ad Hoc Netw., vol. 36, pp. 152–176, Jan. 2016, doi: 10.1016/j.adhoc.2015.05.014.

J. Liu, C. Zhang, and Y. Fang, “EPIC: A differential privacy framework to defend smart Homes against Internet traffic analysis,” IEEE Internet Things J., vol. 5, no. 2, pp. 1206–1217, Apr. 2018, doi: 10.1109/JIOT.2018.2799820.

Q. Zhu, C. Yang, Y. Zheng, J. Ma, and H. Li, “Smart home: Keeping privacy on air-paddling,” IET Inf. Secur., vol. 15, no. 2, pp. 156–168, Mar. 2021, doi: 10.1049/iet-iss.20120151.

N. Athorpe, D. Y. Huang, D. Reisman, A. Narayanan, and Q. Zhu, C. Yang, Y. Zheng, J. Ma, and H. Li, “Smart home: Keeping privacy on air-paddling,” IET Inf. Secur., vol. 15, no. 2, pp. 156–168, Mar. 2021, doi: 10.1049/iet-iss.20120151.

W. Xiong and R. Lagerström, “Threat modeling—A systematic literature review,” Comput. Secur., vol. 64, pp. 115–145, Jan. 2017, doi: 10.1016/j.cose.2016.09.007.

S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, and Y. Park, “A trusted authentication and key agreement scheme for heterogeneous wireless sensor networks,” Sensors, vol. 20, no. 4, p. 1215, Feb. 2020, doi: 10.3390/s20041215.

W. Xiong and R. Lagerström, “Threat modeling—A systematic literature review,” Comput. Secur., vol. 64, pp. 115–145, Jan. 2017, doi: 10.1016/j.cose.2016.09.007.

S. Banerjee, V. Odelu, A. K. Das, S. Chattopadhyay, and Y. Park, “A trusted authentication and key agreement scheme for heterogeneous wireless sensor networks,” Sensors, vol. 20, no. 4, p. 1215, Feb. 2020, doi: 10.3390/s20041215.
S. Arif, M. A. Khan, S. U. Rehman, M. A. Kabir, and M. Imran, “Investigating smart home security: Is blockchain the answer?” IEEE Access, vol. 8, pp. 117802–117816, 2020, doi: 10.1109/ACCESS.2020.3004662.

P. Koshy, S. Babu, and B. S. Manoj, “Sliding window blockchain architecture for Internet of Things,” IEEE Internet Things J., vol. 7, no. 4, pp. 3338–3348, Apr. 2020, doi: 10.1109/JIOT.2020.2967119.

M. Ammi, S. Alarabi, and E. Benkhelifa, “Customized blockchain-based architecture for secure smart home for lightweight IoT,” Inf. Process. Manage., vol. 58, no. 3, May 2021, Art. no. 102482, doi: 10.1016/j.ipm.2020.102482.

C. Qu, M. Tao, and R. Yuan, “A hypergraph-based blockchain model and application in Internet of Things-enabled smart Homes,” Sensors, vol. 18, no. 9, p. 2784, 2018, doi: 10.3390/s18092784.

B. S. Balaji, P. V. Raja, A. Nayar, P. Sanjeevukumar, and S. Pandiyan, “Enhancement of security and handling the inconspicuousness in IoT using a simple size extensible blockchain,” Energies, vol. 13, no. 7, p. 1795, Apr. 2020, doi: 10.3390/en13071795.

S. N. Mohanty, K. C. Ramya, S. S. Rani, D. Gupta, K. Shankar, S. K. Lakshmananprabu, and A. Khanna, “An efficient lightweight integrated blockchain (ELIB) model for IoT security and privacy,” Future Gener. Comput. Syst., vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/j.future.2019.09.050.

D. Kim and J. Lee, “A reverse hash chain path-based access control scheme for a connected smart home system,” IEEE Consum. Electron. Mag., vol. 10, no. 1, pp. 93–100, Jan. 2021, doi: 10.1109/MCE.2020.3031064.

S.-K. Kim, U.-M. Kim, and J.-H. Huh, “A study on improvement of Blockchain application to overcome vulnerability of IoT multi-platform security,” Energies, vol. 12, no. 3, p. 402, Jan. 2019, doi: 10.3390/en12030402.

W. She, Z.-H. Gu, X.-K. Lyu, Q. Liu, Z. Tian, and W. Liu, “Homomorphic consortium blockchain for smart home system sensitive data privacy preserving,” IEEE Access, vol. 7, pp. 62058–62070, 2019, doi: 10.1109/ACCESS.2019.2916534.

S. Singh, I. H. Ra, W. Meng, M. Kaur, and G. H. Cho, “SH-BlockCC: A secure and efficient Internet of Things smart home architecture based on cloud computing and blockchain technology,” Int. J. Distrib. Sens. Netw., vol. 15, no. 4, pp. 1–18, 2019, doi: 10.1177/1551577918844159.

L. Huraj, M. Šimon, and T. Horák, “Resistance of IoT sensors against DDoS attack in smart home environment,” Sensors, vol. 20, no. 18, p. 5298, Sep. 2020, doi: 10.3390/s20185298.

R. de T. Caropreso, R. A. S. Fernandes, D. P. M. Osorio, and I. N. Silva, “An open-source framework for smart meters: Data communication and security traffic analysis,” IEEE Trans. Ind. Electron., vol. 66, no. 2, pp. 1638–1647, Feb. 2019, doi: 10.1109/TIE.2018.2808927.

L. W. Park, S. Lee, and H. Chang, “A sustainable home energy prosumer chain methodology with energy tags over the blockchain,” Sustainability, vol. 10, no. 3, p. 658, 2018, doi: 10.3390/su10030658.

M. Nasir, K. Muhammad, A. Ullah, J. Ahmad, S. Wook Baik, and M. Sajjad, “Enabling automation and data intelligence over resource constraint IoT devices for smart home,” Neurocomputing, vol. 491, pp. 494–506, Jun. 2022, doi: 10.1016/j.neucom.2021.04.138.

R. A. Sowah, D. E. Boahene, D. C. Owob, R. Addo, G. A. Mills, W. Owusu-Banahene, G. Buah, and B. Sarkodie-Mensah, “Design of a secure wireless home automation system with an open home automation bus (OpenHAB 2) framework,” J. Sensors, vol. 2020, pp. 1–22, Oct. 2020, doi: 10.1155/2020/8969602.

R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, “Evaluation of the ability of the shodan search engine to identify Internet-facing industrial control devices,” Int. J. Crit. Infrastructure Protection, vol. 7, no. 2, pp. 114–123, 2014, doi: 10.1016/j.ijcip.2014.03.001.

C. Fachhka, E. Bou-Harb, A. Keliris, N. Memon, and M. Ahamad, “Internet-scale probing of CPS. Inference, characterization and orchestration analysis,” presented at the Netw. Distributed Syst. Secur. Symp., San Francisco, CA, USA, Feb. 2017.

J. Li, Z. Li, G. Tyson, and G. Xie, “Characterising usage patterns and privacy risks in a smart-home security camera service,” IEEE Trans. Mobile Comput., vol. 21, no. 7, pp. 2344–2357, Jul. 2022, doi: 10.1109/TMC.2020.3039787.

Q. I. Sarhan, “Systematic survey on smart home safety and security systems using the Arduino platform,” IEEE Access, vol. 8, pp. 128362–128384, 2020, doi: 10.1109/ACCESS.2020.3008610.

H. Meng, W. L. L. Thing, Y. Cheng, Z. Dai, and L. Zhang, “A survey of Android exploits in the wild,” Comput. Secur., vol. 76, pp. 71–91, Jul. 2018, doi: 10.1016/j.cose.2018.02.019.

D. Shin, K. Yun, J. Kim, P. V. Astillio, J.-N. Kim, and I. You, “A security protocol for route optimization in DMM-based smart home IoT networks,” IEEE Access, vol. 7, pp. 142531–142550, 2019, doi: 10.1109/ACCESS.2019.2943929.

A. Wasiczek, “The future of 5G smart home network security is micro-segmentation,” Netw. Secur., vol. 2020, no. 11, pp. 11–13, Nov. 2020, doi: 10.1109/SI353-4858(20)30129-X.

J. R. C. Nurse, S. Creese, and D. De Roure, “Security risk assessment in Internet of Things systems,” IT Prof., vol. 19, no. 5, pp. 20–26, 2017, doi: 10.1109/MITP.2017.3680959.

J. B. Bernabe, J. L. H. Ramos, and A. F. S. Gomez, “TcIoT: Multidimensional trust-aware access control system for the Internet of Things,” Soft Comput., vol. 20, no. 5, pp. 1763–1779, 2016, doi: 10.1007/s00500-015-1705-6.

J. E. Klohas, T. McGill, and X. Wang, “How perceived security risk affects intention to use smart home devices: A reasoned action explanation,” Comput. Secur., vol. 87, Nov. 2019, Art. no. 101571, doi: 10.1016/j.cose.2019.101571.

S. Cannizzaro, R. Procter, S. Ma, and C. Maple, “Trust in the smart home: Findings from a nationally representative survey in the UK,” PLoS ONE, vol. 15, no. 5, May 2020, Art. no. e0231615, doi: 10.1371/journal.pone.0231615.