Journal of Reliable Intelligent Environments (2022) 8:67–74
https://doi.org/10.1007/s40860-021-00160-3

ORIGINAL ARTICLE

Securing the operation of Smart Home Systems: a literature review

Noureddine Amraoui[1] · **Belhassen Zouari**[1]

Received: 1 June 2021 / Accepted: 5 November 2021 / Published online: 1 December 2021
© The Author(s), under exclusive licence to Springer Nature Switzerland AG 2021

Abstract
Smart Home Systems (SHSs) represent one of the most prevailing Internet of Things (IoT) applications. While IoT-based SHSs can be user-driven or automatically operated, their unauthorized or unexpected operation brings new security and safety concerns that did not exist in legacy homes. This paper provides a review of the state-of-the-art approaches for securing the operation of SHSs. We first present security threats that may lead to unauthorized/unexpected operation of an SHS for both types of operation. Then, we review existing security approaches for each type of operation. Finally, we draw some conclusions and raise open research issues based on this review.

Keywords Internet of Things · Smart Home Systems · Cybersecurity · User authentication · Home automation

1 Introduction

Smart Home Systems (SHSs), also called Home Automation Systems, Connected Homes, or Domotics, represent a class of the most prevailing Internet of Things (IoT)-based systems [46]. The vision of the smart home is an old idea but no real-world implemented systems have existed before the emergence of IoT. Homes have been considered as one of the main environments for the widespread of IoT devices compared to other ones, such as factories and cities [14]. Indeed, consumers are transforming their homes into smart spaces with Internet-connected sensors, lights, and appliances. According to MediaPost [10], 69% of households in the U.S. have at least one smart device, while 12% of those (about 22 million homes) have several. Due to such growing interest in smart home environments, the number of systems designed to support them has risen considerably [15].

SHSs provide several intelligent services to consumers, such as energy-saving, physical security and safety, and elderly people assistance. To take advantage of different intelligent services, a consumer can operate an SHS in several ways. On one hand, SHSs may provide consumers with companion applications and web portals that can be run on end-user devices, such as tablets, smartphones, etc., so consumers can operate their devices on their own either from the inside when connected to the local network, or from any outside location via the Internet. On the other hand, many SHSs also allow consumers to install and delegate authorization to third-party applications (called SmartApps) to autonomously operate devices without user intervention. SmartApps use simple trigger-action rules, where the operation action of a given device is only performed when the triggering event has occurred [6]. For instance, a 'Welcome Home' SmartApp sets the mode to home when the light in the living room is turned on.

While bringing significant convenience to consumers, unauthorized and malicious operation of SHS devices brings new security and safety concerns. On one hand, malicious operation of SHS devices could be resulting from several attack vectors, such as:

- Direct remote operation: many IoT devices' web interfaces have a lack of authentication/authorization, a lack or weak encryption, and a lack of input and output filtering [24].
- End-user device compromise: end-user control devices can easily be compromised if they are not secured properly. For example, an attacker can lure a victim to install a malicious app that runs on his smartphone to take control over his/her SHS devices [12].

✉ Noureddine Amraoui
houcine1amraoui@gmail.com

Belhassen Zouari
belhassen.zouari@supcom.tn

[1] Mediatron Research Laboratory, Higher School of Communications of Tunis, University of Carthage, Technology City of Communications, El Ghazala, 2083 Ariana, Tunisia

– User account compromise: the account which an SHS owner uses to access control applications could be compromised in several ways, such as reverse engineering, password guessing, malware infection, etc. [12].
– User impersonation: to mount this attack an attacker first intercepts one or more login requests of a legitimate user. Then, he/she modifies/forges these requests in such a way to login on behalf of the legitimate user, pass the authentication test, and access the privileged resources not meant for him [20].

On the other hand, several threat vectors could lead to unexpected/malicious automated operation of SHS devices, such as:

– Permission misuse: once a user grants application permission to access a particular resource, the application can use that permission whenever it executes thereafter. This enables an application to access privacy-sensitive resources even when they are not needed for it to perform its expected functions [31].
– User poor configuration: poor configuration by novice SHS users (e.g., parents and kids) at the installing stage of SmartApps can transit the SHS to unsafe physical states due to the conflicting logic of common SmartApps [6].
– Embedded malicious logic: Trigger-Action model of SHS platforms provides flexibility for the attacker to embed their malicious logic into the SmartApps using available triggering events (e.g., home mode changing) [9]. The activation of malicious logic makes the SmartApp deviating from its past regular behavior, since it starts to perform unexpected automation actions.

As the adoption of any new computing technology is usually hindered by the security challenges it brings [4], the success of SHS is no doubt related to the confidence degree of SHS owners towards the operation of their devices. To this end, the existing research literature has been extensively contributing to the design of secure and safe SHSs.

The security of IoT-based systems is a very broad field of research, and it is possible to find a myriad of studies and surveys. Without going into much detail, we refer the readers to the study of Sikder et al. [38] for a survey of sensor-based threats, and the survey of Touqeer et al. [43] for a presentation of various security challenges and solutions at different IoT layers. In the particular context of Smart Home Systems, there have been several surveys that review the specific security threats as well as existing security approaches. Kuyucu et al. [21] surveys the SHS literature on security and privacy issues and the proposed solutions to mitigate them. Panwar et al. [29] presents security requirements and threats and focuses on a privacy-preserving model. Sarhan [35] surveys the existing proposed security solutions that leverage Arduino platform. Yoo et al. [50] provide recommendations and best security practices based on their conducted survey on the most important security approaches. Han et al. [17] described the security considerations for secure and trustworthy SHSs.

Although the aforementioned papers have been surveying different security threats and proposed solutions, there is a lack of reviews that study the literature related to the security threat and issues that may lead to an unauthorized or unexpected user-driven/automated SHS operation. Thus, none of the existing surveys have presented the existing approaches to mitigate such a type of security problem. To the best of our knowledge, the only work that could be found is the study of [41]. In particular, the authors discussed the main vulnerabilities of SHSs that are operated by Smartphones and the main proposals to mitigate them. However, the work does not go into detail and many security threats and existing approaches have not been discussed.

To provide a detailed literature review on the security of SHS operation, this paper presents the first classification of different proposed security approaches as shown in Fig. 1. In particular, our classification is based on whether an approach is dedicated to user-driven or automated operation as well as whether it integrates behavioral anomaly detection or not.

The remainder of this paper is structured as follows. In Sects. 2 and 3, we review existing security approaches to secure user-driven and automated operation of SHSs, respectively. Section 4 concludes this work and discusses open research directions.

2 Existing approaches for securing user-driven operation

The plethora of security threat vectors requires robust security schemes to prevent malicious user-driven SHS devices' operation. Existing approaches in this context have been leveraging both conventional security schemes as well as behavioral anomaly detection-based approaches.

2.1 Conventional security approaches

Current conventional security approaches have addressed particular attention to three types of viz., signature-based intrusion detection systems, user authentication, and access control models. In the following, we present some of the existing works for each type of mechanism.

2.1.1 Intrusion detection systems

Intrusion Detection Systems (IDSs) are a typical countermeasure against attacks targeting IoT devices [49]. An IDS detects attacks and malicious operation of SHS devices based

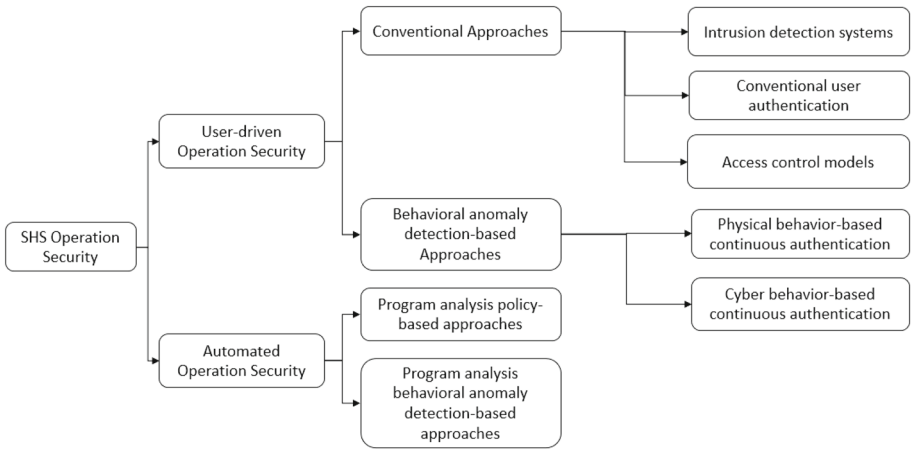

Fig. 1 Taxonomy of exiting approaches for securing SHS operation

on the analysis of outbound/inbound traffic between the IoT devices and the external world, i.e., Internet [28,40].

In this context, Martin et al. proposed a comprehensive home network defense method against attacks on home IoT devices. This method uses honeypot to find attacks by the signatures-based method and changes settings of firewalls to drop the attacking packets [23]. Besides, Zarpelão et al. presented an intrusion detection system to detect anomalous traffic over IoT devices by either comparing the packets to predefined rules to the observed traffic [51].

Recently, ur Rehman and Gruhn [44] proposed a firewall system between the central SHS hub and the connected devices and protects them from internet and external threats. Alghayadh and Debnath [1] proposed a hybrid IDS to analyze whether operation requests were benign or issued from malicious nodes by applying four sorts of machine learning algorithms. Ray and Bagwari [33] proposed a security analysis engine that monitors the device communication and transmission of data, traces logs, and generates alerts for any kind of misuse or suspected communication between nodes. For a comprehensive survey of existing works, we refer the reader to [37].

Although existing signature-based IDSs assume that legitimate and anomalous traffic signatures are notably different, both attackers and legitimate users send the same types of packets to operate SHS devices. For instance, if an attacker issued an operation command via a compromised end-user device (e.g., a malware-infected smartphone), a signature-based IDS cannot distinguish between packets sent by the legitimate user and those sent by the attacker based only on the available information (e.g., IP address) [49].

2.1.2 Conventional user authentication

Traditional and well-known authentication factors have been also leveraged to identify SHS users and prevent unauthorized operation. Factors include some secret that a user knows (e.g., passwords or PIN codes), some token that a user has (e.g., smart-cards), or something that a user is (e.g., fingerprint or face recognition) [25]. A comprehensive review of these schemes could be found in [22,36].

While the combination of these factors has led to a great improvement known as multi-factor authentication [36,45], these systems still suffer from several limitations. First of all, while users' credentials are not trivial to guess and are safely stored, they remain vulnerable to social engineering attacks. On top of that, there will always be the possibility that the user may forget his authentication secret, since the general attitude of users is to choose fairly guessable and, therefore, weak passwords [25]. Second, physical objects, such as smart cards can be forgotten or stolen. In addition, since the users are forced to carry around specific authentication token(s), the overall usability of the system decreases. Moreover, technologies measuring user's biometric characteristics are often intrusive and expensive as well as they are not always available on control device which SHS user uses.

2.1.3 Access control models

Access control models have also been proposed to govern who, under what circumstances, can actuate SHS devices [11, 39]. However, traditional access control models (i.e., Role-based Access Control (RBAC), Capability-based Access Control (CapBAC), etc.) have not been considered as an effective security mechanism for emerging technology, such as SHS [26].

In particular, RBAC authorization is not suitable for dynamic user role assignment requirements of IoT access control, such as sensor inputs, time of day, type and state of a device [13]. Moreover, CapBAC will fail to prevent the misuse of legitimate privileges by a malicious user. Finally, both models are not expressive enough to handle such complex access control needs [11].

2.2 Behavioral anomaly detection-based security approaches

Recently, the limitations of conventional security mechanisms have been warranting researchers to integrate the behavioral analysis of both SHS and its users to devise new schemes that are self-learning, personalized for each SHS configuration, and allow more intelligent authentication and authorization decisions. Tracing then assessing the behavioral patterns of users and entities to secure cyber systems is better known as Behavioral Anomaly Detection (BAD) [30]. A BAD-based security approach attempts to identify security threats and behaviors that are not known and do not match the predetermined patterns.

Continuous Authentication (CA) is one of the main emergent techniques from the BAD-based security approach. Also known as permanent authentication, CA is supposed to increase the level of security by keeping SHS users authenticated permanently and enhance the users' quality of experience by being non-intrusive and minimizing the usage of credentials during the authentication processes [34]. Existing CA approaches for securing SHS operation can be grouped into two categories viz., Physical Behavior-based and Cyber Behavior-based. We present them in the following.

2.2.1 Physical behavior-based continuous authentication

Physical behavior profiling-based CA aims to remedy the limitations related to intrusive authentication biometrics as keystroke dynamics, touchscreen dynamics, etc. [22]. The acquisition of data related to the physical behavior of SHS users could be done through several techniques:

- Wi-Fi signal-based: since different users will produce different Wi-Fi signal patterns albeit they perform identical gestures, recent works proposed the usage of Wi-Fi signals to capture unique human physiological and behavioral characteristics inherited from their daily activities, including both walking and stationary ones [18]. Wi-Fi-based user authentication attracts considerable attention because of the wide deployment of commercial Wi-Fi infrastructures in homes [19]. In addition, it is sensorless and does not require explicit user input. However, Wi-Fi signal-based authentication is only feasible on restricted setups. For instance, they require the user to walk through the same path, and the walk distance is also limited.
- Vision-based: vision-based solutions record an individual's gait patterns when walking via facility cameras. Then, background segmentation techniques are used to extract features from recorded images to verify user identities. However, the vision-based solutions are subject to environments including illumination and camera angle. Furthermore, the high computation consumption and privacy concerns make vision-based solutions infeasible for continuous authentication.
- Voice assistant-based: makes use of the sounds in the home to provide additional context information to decide whether to execute the command, prompt for confirmation or reject the command entirely. However, this feature can be circumvented as voice can be spoofed and users might not be comfortable with their voices being recognized due to privacy concerns [2].
- Smart floor-based: floor-sensor-based solutions use dense press sensors deployed underfloor to track the user's pressure dynamics or acoustic patterns when walking on the floor. Its advantages include the high resolution in terms of performance and unobtrusiveness for user interaction. However, floor-sensor-based solutions are not ideal for CA for two reasons. First, they often have sophisticated system design and high costs. Second, they only work in the enclosed environment with limited users and do not work in the open space with low scalability.

2.2.2 Cyber behavior-based continuous authentication

Given the limitations of physical user behavior-based techniques, researchers explore new opportunities for user authentication by leveraging the behavioral features extracted from user interactions with IoT devices [27]. User cyber behavior-based authentication provides a safer and more convenient way to identify users based on their behavioral interaction with the SHS.

Rath and Colin [32] proposed an access control framework to authenticate the operation of SHS devices in case of user account compromise using association rules as a means to learn user behavior. However, the framework does not use any behavioral features that may efficiently describe SHS user behavior.

Yamauchi et al. [49] proposed a method to detect the exceptional operation of SHS devices. The method first learns sequences of events performed by the user to construct a tree as a baseline. Then, anomalous event sequences are detected by checking whether the sequence is included in the constructed tree. However, the proposed method uses the operation sequence as the only user behavioral feature, thus it cannot accurately identify single commands for which related commands are not observed. Moreover, the proposal only considers the SHS devices separately and does have a global view of the SHS.

Ghosh et al. [13] proposed SoftAuthZ, a framework for estimating the confidence associated with a device access request. SoftAuthZ computes the belief on a requester based on his/her historical request patterns for a particular device type using a linear regression model. In particular, an access request with low variability is more likely to be legitimate in

Table 1 Summary of existing program analysis policy-based approaches

System	Approach	Policy definition	Enforcement technique	Purpose	Analysis type
SmartAuth [42]	Personalized	User-defined and extracted from SmartApps description	Not specified	Permission misuse prevention	Static
Soteria [7]	General purpose	Extracted from SmartApps and trigger-action rules	Model Checking	Abuse prevention	Dynamic
IoTGuard [8]			Reachability Analysis	Policy violation prevention	
Expat [48]		User-defined	Policy decision function		

contrast to an abnormal request that should have high variability. However, SoftAuthZ uses variability in device access requests as the only user behavioral feature besides other non-behavioral attributes such as environmental context, nature of the requested device, etc. Moreover, operation commands are not transformed into feature-based numerical data and are only treated with their original categorical nature. This obliged authors to use a variability calculation method specifically for categorical variables.

Recently, Amraoui et al. proposed a security framework that continuously authenticates smart home users [3]. The framework detects unauthorized operation commands by building a One-Class Support Vector Machine (OCSVM) over the regular operation logs of the legitimate user. However, the proposed framework assumed that user behavior does not change in the future.

3 Existing approaches for securing appified automated operation

To detect and respond to the plethora of threat vectors related to automated SHS operation and which may lead to severe safety consequences, research works have been focusing on well-known program analysis-based techniques which have been applied, either statically or dynamically. In static analysis, the source code of an SHS automation application (called SmartApp) is analyzed without running it. Whereas in dynamic analysis, the code is run, possibly under-instrumented conditions, to see if there are likely problems [6].

Existing program analysis-based approaches to secure SHS appified automated operation can be grouped into policy-based and behavioral profiling-based approaches. We present some of these works in the following.

3.1 Program analysis policy-based approaches

As summarized in Table 1, existing program analysis policy-based approaches have been focusing on the enforcement of policies that describe the security and safety preferences of the SHS.

Tian et al. proposed SmartAuth, an authorization policy-based system that learns about the SmartApp's actual functionality by analyzing their source code and the description provided by developers [42]. Then, the discrepancies between the SmartApps description and their programmed logic are pointed out and displayed to the user through an automatically generated interface. After that, SmartAuth retrieves the user's explanation and approval for the extracted discrepancies using natural-language-generation techniques. Once a user sets his/her policy settings through the user interface, SmartAuth enforces the policy by blocking unauthorized commands. Celik et al. proposed Soteria, a model checking based-system to verify whether installed SmartApps adhere to security and safety properties. The enforced properties are a set of systematically developed policies that represent the physical behavioral specifications of users' expectations about the safe and secure behavior of an SHS [7].

IoTGuard is another policy-based authorization system that retrieves SmartApps information (e.g., events and actions) at runtime and stores them in a dynamic model that consists of transitions and states [8]. The dynamic model represents the runtime execution behavior of the SmartApp. Using the reachability analysis technique, this model is then evaluated against the same policies used by Soteria [7]. Moreover, Expat allows a user to check the desired properties (e.g., consistency, entailment) of them; which due to their formal semantics can be easily discharged by an SMT solver [48].

Although the proposed systems consider additional design and security features beyond the existing authorization models in current SHS automation (e.g., SmartThings Permission Model), they suffer from a major problem related to the pre-definition of the security policy. Indeed, general-purpose policies as proposed by [48] and [8] are not personalized and may not suit all SHSs automation configurations. Moreover, as leveraged by SmartAuth [42], users may not be able to accurately explain their specific security preferences.

3.2 Program analysis behavioral anomaly detection-based approaches

Compared to user-driven operation, little effort has been made to secure the appified automated operation using the BAD-based security approach. The only work that one could find in this context is HoMonit [52]. This proposed system detects misbehaving SmartApps based on a Deterministic Finite Automaton (DFA) matching algorithm. In particular, HoMonit first extracts the expected DFA logic of the installed SmartApps from the source code or their text description. Then, it monitors the behavior of SmartApps from the wireless traffic between SmartThings hub and devices and then matching it with their current working logic using the DFA algorithm. However, the proposed approach does not use any behavioral features that may efficiently monitor the behavior of SmartApps.

4 Conclusion

In this paper, we have reviewed the state-of-the-art research works contributing to the design of secure and safe SHS operation. In light of the previous literature review, we may draw the following conclusions.

- Conventional signature-based IDSs cannot distinguish between operation commands' packets sent by legitimate SHS users and attackers.
- Conventional user authentication schemes suffer from many limitations and there is a growing need to integrate user behavior to make intelligent authentication decisions.
- Conventional access control models (e.g., CapBAC) fail to prevent the misuse of legitimate privileges by a malicious SHS user.
- Existing program analysis policy-based approaches are hindered by the pre-definition of the security policy and there is a growing need for a new scheme that is personalized for each SHS automation configuration and supports self-learning.

Moreover, Behavioral Anomaly Detection-based security has been recently considered as the alternative to respond to the limitations of conventional security approaches. Although some works have been leveraging such an approach to secure the operation of SHSs, they are still not sufficient. Thus, an important open research issue that would considered by future works is: *how to address the lack of relevant techniques that leverage the BAD-based approach to secure the operation of SHS?*

Furthermore, Blockchain technology has been extensively investigated in various contexts, such as smart cities [16] and cloud computing [47]. In the SHSs context, this technology has been also leveraged to create a platform that allows devices to communicate securely with one another [5]. Unfortunately, Blockchain has not been yet used to secure the user-driven/automated operation of SHSs. Consequently, future directions should consider such an approach to prevent malicious and unexpected operation of SHSs.

Finally, securing the operation of SHSs may be hindered by several challenges that should be considered by future works. First of all, recent studies have demonstrated that users are not comfortable with biometric data collection in IoT settings [27]; thus, an open research issue is: *how to design privacy-preserving SHS security techniques?* Besides, SHSs may both be user-driven and appified automated at the same time; thus, an open research issue is: *how to secure the operation of such type of SHSs?* Finally, user-driven SHSs may be operated by multiple inhabitants which are not considered by currently proposed approaches; thus, an open research issue is: *how to secure the operation of multi-user SHSs?*

Funding Not applicable.

Availability of data and materials Not applicable.

Code availability Not applicable.

Declarations

Conflict of interest Noureddine Amraoui declares that he has no conflict of interest. Belhassen Zouari declares that he has no conflict of interest.

Research involving human participants and/or animals This article does not contain any studies with human participants or animals performed by any of the authors.

Informed consent Not applicable.

References

1. Alghayadh F, Debnath D (2020) A hybrid intrusion detection system for smart home security. In: 2020 IEEE international conference on electro information technology (EIT). IEEE, pp 319–323
2. Alrumayh AS, Lehman SM, Tan CC (2020) Context aware access control for home voice assistant in multi-occupant homes. Pervasive Mob Comput 67:101196
3. Amraoui N, Besrour A, Ksantini R, Zouari B (2019) Implicit and continuous authentication of smart home users. In: International conference on advanced information networking and applications. Springer, Berlin, pp 1228–1239
4. Arias-Cabarcos P, Almenarez F, Trapero R, Diaz-Sanchez D, Marin A (2015) Blended identity: pervasive IdM for continuous authentication. IEEE Secur Priv 13(3):32–39

5. Arif S, Khan MA, Rehman SU, Kabir MA, Imran M (2020) Investigating smart home security: is blockchain the answer? IEEE Access 8:117802–117816
6. Celik ZB, Fernandes E, Pauley E, Tan G, McDaniel P (2019) Program analysis of commodity IoT applications for security and privacy: challenges and opportunities. ACM Comput Surv (CSUR) 52(4):1–30
7. Celik ZB, McDaniel P, Tan G (2018) Soteria: automated IoT safety and security analysis. In: 2018 {USENIX} annual technical conference ({USENIX}{ATC} 18), pp 147–158
8. Celik ZB, Tan G, McDaniel PD (2019) IoTGuard: dynamic enforcement of security and safety policy in commodity IoT. In: NDSS
9. Chi H, Zeng Q, Du X, Yu J (2020) Cross-app interference threats in smart homes: categorization, detection and handling. In: 2020 50th annual IEEE/IFIP international conference on dependable systems and networks (DSN). IEEE, pp 411–423
10. Chuck M (2019) Smart home technology hits 69 Technical report, MediaPost, 2019. [Online]. Accessed 06 Oct 2021
11. Dutta S, Chukkapalli SSL, Sulgekar M, Krithivasan S, Das PK, Joshi A et al (2020) Context sensitive access control in smart home environments. In: 6th IEEE international conference on big data security on cloud (BigDataSecurity 2020)
12. Gamundani AM, Phillips A, Muyingi HN (2018) An overview of potential authentication threats and attacks on internet of things (IoT): a focus on smart home applications. In: 2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (SmartData). IEEE, pp 50–57
13. Ghosh N, Chandra S, Sachidananda V, Elovici Y (2019) SoftAuthZ: a context-aware, behavior-based authorization framework for home IoT. IEEE Internet Things J 6(6):10773–10785
14. Gomez C, Chessa S, Fleury A, Roussos G, Preuveneers D (2019) Internet of things for enabling smart environments: a technology-centric perspective. J Ambient Intell Smart Environ 11(1):23–43
15. Guth J, Breitenbücher U, Falkenthal M, Fremantle P, Kopp O, Leymann F, Reinfurt L (2018) A detailed analysis of IoT platform architectures: concepts, similarities, and differences. In: Internet of everything. Springer, Berlin, pp 81–101
16. Hakak S, Khan WZ, Gilkar GA, Imran M, Guizani N (2020) Securing smart cities through blockchain technology: architecture, requirements, and challenges. IEEE Netw 34(1):8–14
17. Han J-H, Jeon YS, Kim JN (2015) Security considerations for secure and trustworthy smart home system in the IoT environment. In: 2015 International conference on information and communication technology convergence (ICTC). IEEE, pp 1116–1118
18. Jiang H, Cai C, Ma X, Yang Y, Liu J (2018) Smart home based on WiFi sensing: a survey. IEEE Access 6:13317–13325
19. Kong H, Lu L, Yu J, Chen Y, Tang F (2020) Continuous authentication through finger gesture interaction for smart homes using WiFi. IEEE Trans Mob Comput
20. Kumari S, Khan MK, Atiquzzaman M (2015) User authentication schemes for wireless sensor networks: a review. Ad Hoc Netw 27:159–194
21. Kuyucu MK, Bahtiyar Ş, İnce G (2019) Security and privacy in the smart home: a survey of issues and mitigation strategies. In: 2019 4th International conference on computer science and engineering (UBMK). IEEE, pp 113–118
22. Liang Y, Samtani S, Guo B, Yu Z (2020) Behavioral biometrics for continuous authentication in the internet-of-things era: an artificial intelligence perspective. IEEE Internet Things J 7(9):9128–9143
23. Martin V, Cao Q, Benson T (2017) Fending off IoT-hunting attacks at home networks. In: Proceedings of the 2nd workshop on cloud-assisted networking, pp 67–72
24. Miessler D (2015) Securing the internet of things: mapping attack surface areas using the OWASP IoT top 10. In: RSA conference
25. Nespoli P, Zago M, Celdrán AH, Pérez MG, Mármol FG, García Clemente FJ (2019) PALOT: profiling and authenticating users leveraging internet of things. Sensors 19(12):2832
26. Omolola O, More S, Fasllija E, Wagner G, Alber L (2019) Policy-based access control for the IoT and smart cities. Open Identity Summit 2019
27. Ongun T, Oprea A, Nita-Rotaru C, Christodorescu M, Salajegheh N (2018) The house that knows you: user authentication based on IoT data. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security, pp 2255–2257
28. Pan Z, Pacheco J, Hariri S, Chen Y, Liu B (2019) Context aware anomaly behavior analysis for smart home systems. Int J Inf Commun Eng 13(5):261–274
29. Panwar N, Sharma S, Mehrotra S, Krzywiecki Ł, Venkatasubramanian N (2019) Smart home survey on security and privacy. arXiv preprint arXiv:1904.05476
30. Powell MP, McCarthy JJ, Tang CY, Stouffer KA, Zimmerman TA, Barker WC, Ogunyale T, Wynne DM (2020) Securing manufacturing industrial control systems: behavioral anomaly detection
31. Rahmati A, Fernandes E, Eykholt K, Prakash A (2018) Tyche: a risk-based permission model for smart homes. In: 2018 IEEE cybersecurity development (SecDev). IEEE, pp 29–36
32. Rath AT, Colin J-N (2017) Strengthening access control in case of compromised accounts in smart home. In: 2017 IEEE 13th international conference on wireless and mobile computing, networking and communications (WiMob). IEEE, pp 1–8
33. Ray AK, Bagwari A (2020) IoT based smart home: security aspects and security architecture. In: 2020 IEEE 9th international conference on communication systems and network technologies (CSNT). IEEE, pp 218–222
34. Sánchez PMS, Valero JMJ, Celdrán AH, Bovet G, Pérez MG, Pérez GM (2020) A survey on device behavior fingerprinting: Data sources, techniques, application scenarios, and datasets. arXiv preprint. arXiv:2008.03343
35. Sarhan QI (2020) Systematic survey on smart home safety and security systems using the arduino platform. IEEE Access 8:128362–128384
36. Shah SW, Kanhere SS (2019) Recent trends in user authentication—a survey. IEEE Access 7:112505–112519
37. Sicato JCS, Singh SK, Rathore S, Park JH (2020) A comprehensive analyses of intrusion detection system for IoT environment. J Inf Process Syst 16(4):975–990
38. Sikder AK, Petracca G, Aksu H, Jaeger T, Uluagac AS (2021) A survey on sensor-based threats and attacks to smart devices and applications. IEEE Commun Surv Tutor 23(2):1125–1159
39. Singh MP, Sural S, Atluri V, Vaidya J (2019) Security analysis of unified access control policies. In: International conference on secure knowledge management in artificial intelligence era. Springer, Berlin, pp 126–146
40. Sivanathan A (2020) IoT behavioral monitoring via network traffic analysis. arXiv preprint. arXiv:2001.10632
41. Teixeira D, Assunção L, Paiva S (2020) Security of smart home-smartphones systems. In: 2020 15th Iberian conference on information systems and technologies (CISTI). IEEE, pp 1–5
42. Tian Y, Zhang N, Lin Y-H, Wang XF, Ur B, Guo X, Tague P (2017) Smartauth: user-centered authorization for the internet of things. In: 26th {USENIX} security symposium ({USENIX} security 17), pp 361–378
43. Touqeer H, Zaman S, Amin R, Hussain M, Al-Turjman F, Bilal M (2021) Smart home security: challenges, issues and solutions at different IoT layers. J Supercomput 1–37
44. ur Rehman S, Gruhn V (2018) An approach to secure smart homes in cyber-physical systems/internet-of-things. In: 2018 Fifth inter-

national conference on software defined systems (SDS). IEEE, pp 126–129
45. Wazid M, Das AK, Odelu V, Kumar N, Conti M, Jo M (2017) Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet Things J 5(1):269–282
46. Xiao Y, Jia Y, Liu C, Alrawais A, Rekik M, Shan Z (2020) HomeShield: a credential-less authentication framework for smart home systems. IEEE Internet Things J 7(9):7903–7918
47. Xie S, Zheng Z, Chen W, Wu J, Dai H-N, Imran M (2020) Blockchain for cloud exchange: a survey. Comput Electr Eng 81:106526
48. Yahyazadeh M, Podder P, Hoque E, Chowdhury O (2019) Expat: expectation-based policy analysis and enforcement for appified smart-home platforms. In: Proceedings of the 24th ACM symposium on access control models and technologies, pp 61–72
49. Yamauchi M, Ohsita Y, Murata M, Ueda K, Kato Y (2020) Anomaly detection in smart home operation from user behaviors and home conditions. IEEE Trans Consum Electron 66(2):183–192
50. Yoo SG et al (2018) Security over smart home automation systems: a survey. In: International conference of research applied to defense and security. Springer, Berlin, pp 87–96
51. Zarpelão BB, Miani RS, Kawakani CT, de Alvarenga SC (2017) A survey of intrusion detection in internet of things. J Netw Comput Appl 84:25–37
52. Zhang W, Meng Y, Liu Y, Zhang X, Zhang Y, Zhu H (2018) Homonit: monitoring smart home apps from encrypted traffic. In: Proceedings of the 2018 ACM SIGSAC conference on computer and communications security, pp 1074–108

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.