Tsinghua Science and Technology

Volume 26 | Issue 6 Article 12

2021

Access Control and Authorization in Smart Homes: A Survey

Ziarmal Nazar Mohammad
School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Fadi Farha
School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

Adnan O.M Abuassba
School of Computer Studies, Arab Open University, Ramallah 4375, Palestine

Shunkun Yang
School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China

Fang Zhou
School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

TSINGHUA SCIENCE AND TECHNOLOGY
ISSN 1007-0214 12/13 pp906–917
DOI: 10.26599/TST.2021.9010001
Volume 26, Number 6, December 2021

Access Control and Authorization in Smart Homes: A Survey

Ziarmal Nazar Mohammad, Fadi Farha, Adnan O.M Abuassba, Shunkun Yang, and Fang Zhou*

Abstract: With the rapid development of cyberspace and smart home technology, human life is changing to a new virtual dimension with several promises for improving its quality. Moreover, the heterogeneous, dynamic, and internet-connected nature of smart homes brings many privacy and security difficulties. Unauthorized access to the smart home system is one of the most harmful actions and can cause several trust problems and relationship conflicts between family members and invoke home privacy issues. Access control is one of the best solutions for handling this threat, and it has been used to protect smart homes and other Internet of Things domains for many years. This survey reviews existing access control schemes for smart homes, which concern the essential authorization requirements and challenges that need to be considered while designing an authorization framework for smart homes. Furthermore, we note the most critical challenges that other access control solutions neglect for smart homes.

Key words: access control; smart home; authorization frameworks

1 Introduction

Ever since Kevin Ashton conceived the Internet of Things (IoT)[1], and with the speedy development of networking technologies and the IoT, human lives have been constantly changing from a physical dimension to a virtual dimension in which people can talk, chat, work, and interact with the connected objects.

The smart home as an IoT application was introduced to facilitate human life and change the way we live, play, and do business. It is meant to make life more flexible, comfortable, and exciting. However, apart from the benefits of smart homes, several security and privacy issues need to be considered while building and designing a smart home. While introducing new technologies aiming to make our homes smarter and more automated, cyberspace is also growing fast[2–5], surrounding our lives with billions of smart devices that can invoke privacy and security issues[6–10].

Smart home technology, which is one of the most important and fastest-growing fields of the IoT, is being massively deployed by many manufacturers and companies. The smart home includes home automation, home monitoring, and home security for the local users.

Smart homes face many security and privacy threats. For instance, hacking the security cameras of the smart home can violate the user's privacy and access sensitive data, such as health data, pictures, and movies. These violations and unauthorized access to the smart home can lead to many critical and dangerous issues[11].

Smart home devices can be accessible by multiple users through a user-friendly interface, such as a web browser or mobile application[12]. Third-party vendor applications basically control smart home devices through mobile-based and web browser-based interfaces and interact with a back-end cloud system. This system

• Ziarmal Nazar Mohammad, Fadi Farha, and Fang Zhou are with the School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China. E-mail: nmziarmal43@gmail.com; fadi_farha@xs.ustb.edu.cn; zhoufang@ies.ustb.edu.cn.
• Shunkun Yang is with the School of Reliability and Systems Engineering, Beihang University, Beijing 100191, China. Email: ysk@buaa.edu.cn.
• Adnan O.M Abuassba is with the School of Computer Studies, Arab Open University, Ramallah 4375, Palestine. E-mail: adnanasba@yahoo.com.
* To whom correspondence should be addressed.
Manuscript received: 2021-01-02; accepted: 2021-01-20

can expose the services via web APIs that accept queries to control the devices and data from multiple vendors.

Companies and manufacturers need to enforce access control to solve smart home authorization problems and ensure that unauthorized users do not access sensitive resources. There are many commercial authorization frameworks, some of which enforce coarse-grained access controls, such as Nest Thermostat (store.google.com/us/category/connected_home?), which grants full access to the smart device or no access at all, and Apple Home Kit (www.apple.com/ios/home/), which provides a local and remote full control or view. Other authorization frameworks provide more robust access control policies that support environmental conditions, such as Samsung Smart Things (www.samsung.com/us/smartthings/), which tracks the user's smartphone GPS coordinates and determines whether the user is at home. However, because this framework is a real-time user tracking, it violates user privacy. Such shortcomings and challenges in implementing access control policies in smart homes can easily lead the devices and apps to access unauthorized users, which may cause privacy and data loss problems[13–15]. An example of these shortcomings is having full access or permission issues in baby monitors that are hacked and remotely controlled. Therefore, a fine-grained access control system should be enforced to prevent unauthorized access to smart devices and data and support multiple user management[16].

Fine-grained access control systems apply policies according to several aspects, such as smart device capabilities, the relationship between users, and context information, including location and time-based conditions[17]. Because of IoT integration with web services and APIs, suitable access control is needed, especially to open smart home platforms. The access control model needs to be flexible and not too strict. The strictness of the authorization framework will affect the dynamicity of the smart home system.

In recent years, several authorization frameworks have been proposed for the smart home with different assumptions and technologies. These variations and assumptions make the evaluation and effectiveness of the authorization framework complicated. Although many surveys discussed privacy and security challenges in the IoT[18–21], only a few research works addressed access control[22–26].

In this survey, we conduct a review and analysis of the most recently proposed access control solutions for smart homes. As shown in Table 1, existing surveys have the following limitations:

(1) They do not cover all aspects of access control. Most of these surveys only focus on the specification of policies, while the other two aspects, including management and evaluations of the policies, are partly or completely neglected.

(2) The existing surveys do not summarize the requirements of access control for smart homes, and no evaluation and analysis of existing authorizations frameworks are available.

This survey presents an overview and analysis of existing access control schemes in smart homes. We mainly note the unsolved challenges in existing access control frameworks for smart homes and turn research into more flexible and suitable authorization solutions. The main contributions of our survey are as follows:

(1) An overview of the current authorization solutions for the smart home and their evaluation based on specified requirements is presented.

(2) Guidelines and open challenges that should be considered while designing smart home authorization frameworks are provided.

The remainder of this paper is organized as follows: Section 2 explores the smart home architecture. Section 3 reviews access control and its different models. Section 4 concerns access control in smart homes. In Section 5, we analyze the existing access control solutions for the smart home, and Section 6 consummates our work and appoints a direction for future research.

Table 1 Comparison with existing surveys of access control.

Reference	Multi-user management	Policy specification	Policy management	Policy evaluation and enforcement	Smart home
[23]	– –	*–	– –	*–	– –
[22]	– –	**	*–	*–	*–
[24]	– –	*–	*–	– –	– –
[26]	– –	**	**	**	*–
[25]	– –	**	*–	– –	– –
Our survey	**	**	**	**	**

Note: **: Fully considered *–: Partially considered –– : Not considered.

2 Smart Home

The smart home is an important IoT application in daily life. Smart devices, such as doorbells, thermostats, door locks, smart ovens, smart lights, and smart refrigerators, are installed and configured in smart homes. They can be remotely controlled by home users via user-friendly interfaces, such as web browsers or mobile applications. The interactions inside the smart home can be machine-to-machine or human-to-machine. As an example of the machine-to-machine interactions, a smart fridge can automatically interact with a smartphone and send a notification to it when something is running low in the fridge, such as milk and fruit. An example of the human-to-machine interactions is a house owner controlling smart devices, such as light bulbs, or allowing other family members to control the smart devices using their smartphone application or a simple web browser.

The smart home application presents several challenges due to its multi-user and multiple device nature. Sharing smart devices between smart home users causes many conflicts in terms of user demands leading to many complicated scenarios[27]. Before explaining access control and how it works with the smart home, we briefly explain the smart home's elements and structure.

2.1 Smart home elements

The smart home elements, also named nodes, are divided into the following three categories[26]:

(1) Physical nodes: They include any entity or thing that can interact with the environment and provide resources, such as sensors, actuators, smart fridges, microwave ovens, light bulbs, cameras, and doorbells.

(2) Application nodes: They include the resources provided by physical nodes that feed the application nodes to deliver services to users.

(3) Intermediate nodes: They are located between physical nodes and application nodes. They connect two or more different networks and route traffic between them, such as a bridge and gateway.

2.2 Smart home architecture

The architecture of the smart home shows the actual functionality and connectivity of the smart home system, including architectural models and architectural styles.

2.2.1 Architectural models

Several architectural models have been proposed for the IoT[28–34]. Typically, the architecture models are divided into layers, and each layer has its own functionality. Because the smart home and other IoT systems are made of resource-constrained smart devices, the access control and authorizations solutions deployed in the architecture's middleware layer have been reviewed in this survey. For greater clarity, we separate middleware from the network layer. Thus, a four-layer architecture model is adopted.

As shown in Fig. 1, the application layer consists of application nodes that provide end-user services. The middleware layer consists of intermediate nodes to maintain connectivity and interoperability within the smart home system. The network layer provides communication and data transfer between nodes. Finally, the physical layer consists of smart devices.

2.2.2 Architectural styles

In recent years, several architectural styles have been proposed. The architectural style varies based on several factors, such as the domain and communication between application nodes, intermediate nodes, and physical nodes. As shown in Fig. 2, three main types of

Fig. 1 Architectural model and smart home elements.

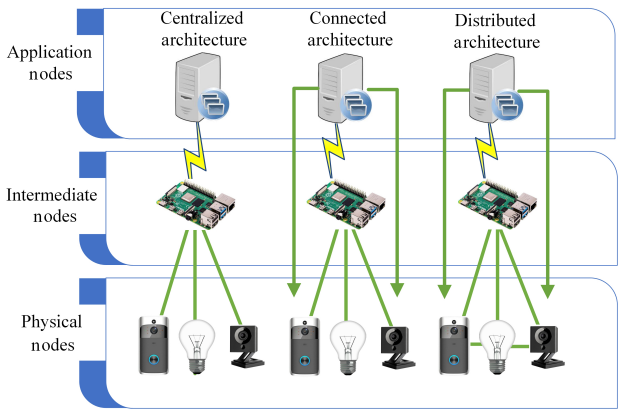

Fig. 2 Architecture styles of the smart home.

architectural style are used[23, 35]:

(1) Centralized architecture: In this architecture, all the physical nodes are connected through an intermediate node. Moreover, the requests from the application node must pass through an intermediate node. This type of architecture is usually used with resource-constrained smart devices.

(2) Connected architecture: Physical nodes can process and forward data to intermediate nodes, and application nodes can directly retrieve data from physical nodes.

(3) Distributed architecture: Intermediate nodes are unnecessary, and every node can process data and communicate with other nodes[26].

3 Access Control

Access control is an effective technique for addressing privacy, security, and access violation issues in smart homes. Its main goal is to ensure that the house resources can only be accessed by authorized users, data, and services. It protects the system by restricting legitimate users' access according to their privileges and preventing unauthorized users[36, 37].

3.1 Access control models

Several access control models are available and can be implemented in smart homes. They range from a very basic level, such as an access control list, to a slightly more advanced level, such as attribute-based access control.

3.1.1 Access Control List (ACL)

Traditionally, the access control matrix was one of the early techniques used for access control. Its columns and rows are composed of objects and subjects, and each record has a set of subject-related access rights[38]. Later, ACL was developed. It is a set of specific resources accessible only for specified users concerning their privileges[36].

3.1.2 Discretionary Access Control (DAC)

DAC is specially developed for systems and databases with multi-user platforms. It grants access depending on user identities. In DAC, the entire system is under the control of the owner, who grants access to the other users, which is why it is called discretionary access control. It allows users to substitute their privileges to other users[39]. The main disadvantage of DAC is that nonlegitimate users can gain access to resources.

3.1.3 Mandatory Access Control (MAC)

This model is static. Each object has an assigned label to indicate specific privileges of the object. Moreover, each subject has a label to indicate which object a requester can access[40]. In MAC, all users only have access to resources based on their task-related privileges, and because of its static nature, this model is not flexible and cannot be used for dynamic domains, such as smart homes.

3.1.4 Role-Based Access Control (RBAC)

It is commonly deployed for small and large organizations[41]. As the name of this access control model suggests, the users can have access to the resources based on their roles. RBAC mainly depends on the following elements: subject (users), object (resources), roles (collection of permissions), and operations (actions on the resources). In RBAC, access rights are granted to roles, and roles give users permissions based on their role rather than their identity. Every user can have multiple roles, and each role could be granted to multiple users. This model is also not recommended in the smart home system because of its limitations in context-awareness and dynamicity, so it cannot satisfy the smart home system requirements.

3.1.5 Capability-Based Access Control (CapBAC)

Unlike other models, CapBAC is a distributed approach-based model, where things can make the decision without any reliance on the central device. CapBAC can be implemented on highly capable devices. Hence, this model is not truly suitable for the smart home system because it typically consists of low-power and resource-constrained devices.

3.1.6 Usage Control (UCON)

Other models, such as Attribute-Based Access Control (ABAC) and RBAC, can only change the attributes after or before the access request. However, the attributes cannot be changed during the execution of the access rights. UCON provides more flexibility than other models while handling authorization by introducing decision factors (obligations and conditions) and mutable attributes. Mutable attributes are the actors, resources, or contextual information whose values can be changed based on an object's usage. With continuous policy evaluations, UCON can interfere with access to prevent misuse of the resources when the access right becomes invalid, even during ongoing access[42].

3.1.7 ABAC

ABAC is fine-grained, flexible, and dynamic access control. In this model, access rights depend on the subject, object, environmental conditions, and their related policies[43]. This model gives the best combination of various attributes for building a flexible and dynamic authorization framework. Its flexibility and context-aware nature make it a more suitable authorization model for smart homes and other IoT domains than other traditional role-based models.

4 Access Control in Smart Home

Access control is an essential technique for smart home systems, and it should adapt to the different requirements of smart homes. It is difficult and not optimal to only take the other systems' access control schemes and implement them in the smart home system. There should be a suitable access control that matches the requirements of the smart home.

Although there are many privacy and security issues in smart homes, in this survey, we only focus on the authorization and how to protect and ensure that smart home devices, applications, and data are safe from unauthorized access. To address this issue, access control of the smart home system needs to be enforced. This tactic guarantees that only the authorized users can have access to smart home resources.

As explained in Section 2, a smart home is different from other domains. It has its specific characteristics and requirements that need to be observed while designing and implementing the related access control scheme. Figure 3 shows the key functional characteristics of the smart home. The requirements of these characteristics differ as follows:

Scalability: The smart home is a dynamic environment in which new devices and resources can be added anytime. Therefore, the smart home system should provide sufficient scalability for users.

Heterogeneity: Because several vendors produce smart home devices, smart home components should be easily communicated with each other.

Reliability: As the smart home is becoming a part of daily life and multiple users may want to access its resources, the smart home system should be easy to use and designed to provide users with sufficient reliability and availability.

Lightweight: Because the smart home devices are resource-constrained with low-power and memory specifications, the access control system should be lightweight. The smart home system is also sensitive to latency, and it should be automated. Furthermore, the smart home is more suitable with a centralized structure, multiple user management, and a centralized access control system.

To summarize, as shown in Fig. 3, the smart home characteristics include low (scalability, reliability, and latency), medium (dynamicity and automation), and high (heterogeneity, lightweight property, and user involvement)[26].

In Table 2, we briefly discuss requirements that should be met while designing and developing an access control system for the smart home environment. It is strictly committed to Requirement1, Requirement2, Requirement3, and Requirement6, and partially committed to access control Requirement4 and Requirement5.

5 Smart Home: Use Cases and Challenges

To overcome the unauthorized access and unwanted

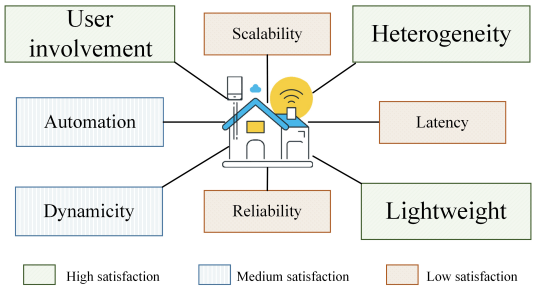

Fig. 3 Smart home characteristics.

Table 2 Access control requirements for a smart home.

Category	Requirement ID	Requirement details
Policy specification	Requirement1	There should be a fine-grained access control model for smart homes.
	Requirement2	There should be an access control model that can provide dynamicity for smart homes.
Policy management	Requirement3	The access control system should allow users to easily manage policies.
Policy evaluations and enforcement	Requirement4	The authorization decision of the access control model should be automated.
	Requirement5	The access control model should not bring inconvenience to the performance of the smart home devices.
	Requirement6	The access control system should always be operational.

application installations in smart home environments, some smart home platforms provide solutions, such as the apple home kit, which supports two types of access: remote view access and editing modes. In remote view access mode, a user can obtain access to the connected smart home devices but cannot edit anything. In contrast, in editing mode, a user can edit remote devices, data, and applications. Other smart devices, such as Kwikset Kevo Lock and August smart lock, also support temporary access rights for guest users[44, 45]. These solutions are device and vendor specific. Therefore, they are not suitable and applicable in a complex environment with multiple devices and users. As a result, existing access control frameworks fail to satisfy such complicated multi-user and multiple device demands. For example, parents do not want their children to have access to a smart TV; the house owner wants to give temporary access to the guest room TV and light bulbs to the guest; or the need for privacy among apartment roommates means that everyone only has access to one's own smart devices.

Suitable fine-grained access control can be designed and implemented to solve these problems[12], and several works have been completed to understand the needs and preferences of users to determine the needs and requirements of access control design in smart homes[17, 27, 46]. Recently, research[17] has been conducted among 425 users of smart homes to determine the effect of the relationship between users on access control requirements in smart homes. Other research[46] tried to understand the requirements and needs of access control in real-life smart homes. The authors[46] developed an access control prototype and measured its usability by performing a study of eight smart homeowners.

The authors in Ref. [47] mentioned use cases of access control in smart homes. For instance, all smart home members can have full access to smart devices, but that is not the case for guest users. Smart home systems have to compromise guest user access to stay within limited premises[48]. Guest users need to control light bulbs, the room temperature, the fridge, and other guest room devices. However, they should not have access to any other sensitive data or smart devices. Another common scenario concerns the external trusted people, such as a housekeeper and cleaning staff. While they have access to physical entry of the smart home and devices within the home premises (e.g., lamps, window blinds, heating, and the fridge), they obviously must also have access to the same devices in the digital world of smart homes[47].

Moreover, a police officer can sometimes request temporary access to the smart home outdoor security cameras or the door locks. Furthermore, members of the smart home temporarily leaving the city or country sometimes need remote access to the smart home.

6 Authorization Frameworks for Smart Homes

Several authorization frameworks have been developed in the last few years to fill the gaps in smart home resource authorization. This section reviews and analyzes recent existing solutions based on the smart home requirements and discusses which authorization framework is suitable for smart homes.

6.1 Existing authorization frameworks

Several authorization frameworks have been proposed for smart homes and can be categorized into two main types: policy evaluation strategy and architecture. Most of the policy evaluation strategy authorization frameworks[12, 42, 48–57] are inspired by the eXtensible Access Control Markup Language (XACML) standard[58]. Moreover, several policy evaluation strategies-based and architecture-based authorization frameworks[56, 59–61] are built on the top of OAuth[62] to enable token generation.

With the several architectural types of access control, several technologies and deployments are presented, such as Policy Decision Point (PDP), policy enforcement point, policy Administration Point (PAP), and policy information point, which can be deployed in the cloud or edge devices[49], in addition to authorization solutions built based on blockchain[42, 52, 57]. Some works, such as Refs. [12, 54–56, 60, 61, 63], are prototype implementations, and many others, such as Refs. [42, 52–55, 57, 59, 64], are conceptual level proposed solutions.

Another recent authorization framework specific to the smart home environment was proposed by Sikder et al.[12] and solves several problems, such as supporting multi-user management and context-awareness, but for the architecture of access control, it was based on RBAC, while the smart home needs a dynamic and flexible access control model, such as ABAC or UCON.

In the above mentioned authorization frameworks, if the user does not meet specific requirements, the policy server will reject its request. For instance, if a legitimate user temporarily left the country and wants to have access to smart home resources in an emergency,

then smart home access control should be flexible by providing more options to users, such as generating a verification code and sending it to the user's email or phone number or asking secret questions to provide temporary access. Tables 3 and 4 briefly explain the existing access control systems used for smart homes.

To implement the access control-based authorization frameworks on the real smart home domain, most of the existing authorization frameworks[42, 48, 52, 53, 57, 59, 64, 69] only mention that the access control architecture is built based on authorization framework, and the use cases only show the authorization flow. Few existing authorization frameworks have been conducted to implement and evaluate a real smart home[12, 56, 70]; hence, other research works only provide a prototype-based implementation[54, 55, 61, 66].

6.2 Discussing smart home authorization frameworks

According to the literature, we conclude that the smart

Table 3 Access control requirements for smart home.

Reference	Policy specification		Policy administration	Policy evaluation and enforcement		
	Requirement1	Requirement2	Requirement3	Requirement4	Requirement5	Requirement6
[42, 52]	−−	−−	−−	∗∗	∗∗	∗−
[61]	∗∗	∗∗	−−	∗∗	∗∗	−−
[49]	−−	∗−	∗∗	∗∗	∗−	−−
[47]	−−	∗−	∗∗	∗∗	∗∗	−−
[54]	∗−	−−	−−	∗∗	∗−	−−
[50]	∗−	∗∗	−−	∗−	−−	−−
[53]	∗∗	∗∗	−−	∗∗	∗∗	−−
[64]	∗−	−−	−−	∗∗	−−	−−
[55]	∗∗	∗∗	−−	∗∗	∗∗	−−
[56]	−−	−−	−−	∗∗	−−	−−
[65]	∗∗	∗−	∗∗	∗∗	∗∗	∗−
[66]	−−	∗∗	−−	∗∗	∗∗	∗∗
[12]	∗∗	∗∗	∗−	∗∗	∗∗	∗∗
[67]	∗−	∗∗	∗−	∗∗	∗−	∗−
[68]	∗∗	∗−	−−	−−	−−	−−
[57]	∗−	−−	−−	∗∗	∗∗	∗−

Note: ∗∗: Fully Considered ∗−: Partially Considered −−: Not Considered.

Table 4 Existing access control characteristics.

Reference	Architecture style	Maturity level	Access control model	Context aware	Multi-user management
[42, 52]	Distributed	Design	ACL	×	×
[61]	Connected	Prototype	ABAC	√	×
[49]	Connected	Product	ACL	√	×
[54]	Connected	Prototype	RBAC	×	×
[67]	–	Prototype	PBAC	×	√
[53]	Centralized	Design	UCON	√	×
[55]	Centralized	Prototype	ABAC	√	×
[64]	Connected	Design	ABAC	×	×
[57]	Distributed	Design	RBAC	×	×
[66]	Distributed	Prototype	–	√	×
[60]	Connected	Prototype	–	√	×
[59]	Connected	Design	–	×	×
[51]	Connected	Design	–	√	×
[12]	Connected	Prototype	RBAC	√	√
[48]	Connected	Design	ACL	√	×
[68]	–	Design	ABAC	√	×
[50]	–	Design	RBAC	√	×
[65]	–	Design	PBAC	×	×
[56]	Distributed	Prototype	Trust-based	×	×

home has several requirements, especially in policy management, totally different from other IoT applications, and these requirements need to be considered while designing and implementing access control for smart homes. As shown in Table 2, the smart home highly relies on Requirement1, Requirement2, Requirement3, and Requirement6, and partially relies on Requirement4 and Requirement5.

Concerning the policy specifications, an authorization framework that can support fine-grained (Requirement1) and context-aware (Requirement2) access control can be satisfied with the design and implementation of ABAC and UCON.

With respect to policy management and policy evaluation, there are other access control requirements. The smart home authorization framework should always be operational (Requirement6) and satisfied by the authorization framework's reliability and availability. Furthermore, homeowners may want to manage and specify policies themselves in a smart home with several devices. However, they might not have sufficient security knowledge, so the smart home authorization frameworks should be user-friendly, easy to specify, and access control policy managers. As a result, consideration of usability (Requirement3) is very important while designing and implementing an access control system for smart homes.

Two more essential requirements to be considered are the automation of access control (Requirement4) and the insensitivity of the resource-constrained device communication and computing capabilities to the smart home access control system (Requirement5).

Finally, the ideal access control framework for the smart home must be a centralized and policy-based framework in which the authorization decision should be automatic and dynamic based on the specified policies. It should also be location-aware and based on context. The policy authorization framework should be externalized, so any changes and updates in the policies will not affect the smart home application design and coding parts. This stipulation means that the PDP should be implemented in edge devices or the local cloud.

Moreover, the PAP should allow the homeowner to specify and modify the policies. Because of the small number of smart home devices, latency can be tolerated, and a run-time evaluation can be adapted.

Some authorization frameworks, such as Refs. [12, 48, 49, 55, 65, 68], are specially proposed for smart homes, but these frameworks do not cover all the requirements of smart homes. Works such as Refs. [48, 49] are coarse-grained authorization frameworks that are not suitable for all access control cases in smart homes, such as when the users change their location while accessing their smart home. Other works[12, 55, 68] propose a fine-grained and context-aware access control system for smart homes, but they do not consider the multi-users' role, robots' role, and usability of the access control-based authorization framework. Furthermore, none of the access control solutions for smart homes mentioned the robots' role, which nowadays can be considered users in smart homes. For instance, service robots may need to access the smart lock or smart coffee machine to brew coffee for home residents or perform other tasks.

6.3 Open challenges and future works

Because of the openness, heterogeneity, and nature of smart homes, many challenges need to be considered while designing and implementing an access control-based authorization framework for smart homes. Some of the unaddressed issues and future challenges that face the existing access control techniques in smart homes are as follows:

Multi-user management: Most of the existing authorization frameworks assumed that the smart home is a single-user domain, and the house owner is the only user responsible for having control over smart devices. As mentioned previously, there are many scenarios in which multiple users need to have access to smart home devices; therefore, while designing and implementing access control for smart homes, multi-user management needs to be considered.

Resource-constrained: Most smart home devices have a low-power and resource-constrained nature, so they cannot process high-computational encryption algorithms[71]. Such devices cannot decide which user should have privileged access. There should be a centralized authorization framework that helps these resource-constrained devices to make authorization decisions to address this challenge.

Dynamicity: The multi-user nature of smart homes brings a new challenge to the smart home system in which users may want to access the resources anytime and anywhere. Therefore, while designing and implementing access control for smart homes, the authorization decision should be made dynamically by the system, i.e., there is no need for a house owner or admin user to authorize the requests coming from other users manually.

Flexibility: The access control system should be tolerant with some changeable attributes and not too strict with the rules. For instance, a user may be out of the country and want to access smart home resources. In this case, if the access control is location-aware, the user will fail to satisfy the condition of the location attribute needed for the authorization decision. Consequently, the authorization framework will reject the user request. For example, the authorization framework should skip the location attributes if the user answers a secret question or enters the verification code correctly.

Machine-to-machine interaction: Robots in smart homes represent a new challenge to the existing access control solutions for the smart home. As we all know, robots are widely used in smart homes. By 2024, almost 79 million smart homes worldwide will use robots[72]. Almost all the existing access control solutions used in smart homes can only accept requests from a human. They cannot make authorization decisions for a machine, such as a robot, which can be considered a user in smart homes. For instance, the service robot helping people[73] needs to clean the house. To do that, it should have access to the smart lock to enter the room and perform its task. While designing access control for smart homes, this challenge needs to be considered. Access control solutions should identify the robot's identity and have an additional feature that could decide which robot has access to a specific device or resource.

7 Conclusion

This survey is conducted to provide an overview and analysis of existing access control-based authorization frameworks for smart homes and note the essential requirements and challenges in need of consideration while designing and implementing access control for smart homes. It also provides an idea concerning the ideal access control-based authorization framework for smart homes, which will cover all the existing requirements and challenges of authorization frameworks for smart homes. In the future, more focus will be on building more dynamic and flexible authorization frameworks for smart homes that can handle multiple users and different types of devices and tolerate emergency access rights cases. Moreover, the frameworks will be able to handle machine-to-machine (robots to other smart devices) access rights without any human interpretation.

References

[1] K. Ashton, That "Internet of Things" thing, *RFID Journal*, vol. 22, no. 7, pp. 97–114, 2009.

[2] H. Liu, H. S. Ning, Q. T. Mu, Y. M. Zheng, J. Zeng, L. T. Yang, R. H. Huang, and J. H. Ma, A review of the smart world, *Future Generation Computer Systems*, vol. 96, pp. 678–691, 2019.

[3] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, K. Akkaya, and M. Conti, IoT-enabled smart lighting systems for smart cities, in *Proc. IEEE 8th Annu. Computing and Communication Workshop and Conf.* (*CCWC*), Las Vegas, NV, USA, 2018, pp. 639–645.

[4] Y. D. Huang, Y. T. Chai, Y. Liu, and J. P. Shen, Architecture of next-generation e-commerce platform, *Tsinghua Science and Technology*, vol. 24, no. 1, pp. 18–29, 2019.

[5] H. S. Ning, H. Liu, J. H. Ma, L. T. Yang, Y. L. Wan, X. Z. Ye, and R. H. Huang, From internet to smart world, *IEEE Access*, vol. 3, pp. 1994–1999, 2015.

[6] J. H. Liu, Y. Yu, J. W. Jia, S. J. Wang, P. R. Fan, H. Z. Wang, and H. G. Zhang, Lattice-based double-authentication-preventing ring signature for security and privacy in vehicular Ad-Hoc networks, *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 575–584, 2019.

[7] A. K. Sikder, L. Babun, H. Aksu, and A. S. Uluagac, Aegis: A context-aware security framework for smart home systems, in *Proc. 35th Annu. Computer Security Applications Conf.*, San Juan, PR, USA, 2019, pp. 28–41.

[8] B. Zhao, P. Y. Zhao, and P. R. Fan, ePUF: A lightweight double identity verification in IoT, *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 625–635, 2020.

[9] F. Farha, H. S. Ning, S. K. Yang, J. B. Xu, W. S. Zhang, and K. K. R. Choo, Timestamp scheme to mitigate replay attacks in secure ZigBee networks, *IEEE Transactions on Mobile Computing*, doi: 10.1109/TMC.2020.3006905.

[10] M. C. Sánchez, J. M. C. de Gea, J. L. Fernández-Alemán, J. Garceran, and A. Toval, Software vulnerabilities overview: A descriptive study, *Tsinghua Science and Technology*, vol. 25, no. 2, pp. 270–280, 2020.

[11] R. Godha, S. Prateek, and N. Kataria, Home automation: Access control for IoT devices, *International Journal of Scientific and Research Publications*, vol. 4, no. 10, pp. 1–4, 2014.

[12] A. K. Sikder, L. Babun, Z. B. Celik, A. Acar, H. Aksu, P. McDaniel, E. Kirda, and A. S. Uluagac, KRATOS: Multi-user multi-device-aware access control system for the smart home, arXiv preprint arXiv:1911.10186, 2020.

[13] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, IoTDots: A digital forensics framework for smart environments, arXiv preprint arXiv:1809.00745, 2018.

[14] X. Tan, J. L. Zhang, Y. J. Zhang, Z. Qin, Y. Ding, and X. W. Wang, A PUF-based and cloud-assisted lightweight authentication for multi-hop body area network, *Tsinghua Science and Technology*, vol. 26, no. 1, pp. 36–47, 2021.

[15] E. Fernandes, J. Jung, and A. Prakash, Security analysis of emerging smart home applications, in *Proc. 2016 IEEE Symp. Security and Privacy* (*SP*), San Jose, CA, USA, 2016, pp. 636–654.

[16] M. Stanislav and T. Beardsley, Hacking IoT: A case study on baby monitor exposures and vulnerabilities, https://www.rapid7.com/globalassets/external/docs/Hacking-IoT-A-Case-Study-on-Baby-Monitor-Exposures-and-Vulnerabilities.pdf, 2015.

[17] W. J. He, M. Golla, R. Padhi, J. Ofek, M. Dürmuth, E. Fernandes, and B. Ur, Rethinking access control and authentication for the home Internet of Things (IoT), in *Proc. 27th USENIX Conf. Security Symp.*, Berkeley, CA, USA, 2018, pp. 255–272.

[18] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, Internet of Things (IoT) security: Current status, challenges and prospective measures, in *Proc. 10th Int. Conf. Internet Technology and Secured Transactions* (*ICITST*), London, UK, 2015, pp. 336–341.

[19] A. R. Sadeghi, C. Wachsmann, and M. Waidner, Security and privacy challenges in industrial Internet of Things, in *Proc. 52nd ACM/EDAC/IEEE Design Automation Conf.* (*DAC*), San Francisco, CA, USA, 2015, pp. 1–6.

[20] E. Vasilomanolakis, J. Daubert, M. Luthra, V. Gazis, A. Wiesmaier, and P. Kikiras, On the security and privacy of Internet of Things architectures and systems, in *Proc. 2015 Int. Workshop on Secure Internet of Things* (*SIoT*), Vienna, Austria, 2015, pp. 49–57.

[21] R. H. Weber, Internet of Things–New security and privacy challenges, *Computer Law & Security Review*, vol. 26, no. 1, pp. 23–30, 2010.

[22] A. Ouaddah, H. Mousannif, A. A. Elkalam, and A. A. Ouahman, Access control in the Internet of Things: Big challenges and new opportunities, *Computer Networks*, vol. 112, pp. 237–262, 2017.

[23] R. Roman, J. Y. Zhou, and J. Lopez, On the features and challenges of security and privacy in distributed Internet of Things, *Computer Networks*, vol. 57, no. 10, pp. 2266–2279, 2013.

[24] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, Security, privacy and trust in Internet of Things: The road ahead, *Computer Networks*, vol. 76, pp. 146–164, 2015.

[25] Y. P. Zhang and X. Q. Wu, Access control in Internet of Things: A survey, arXiv preprint arXiv:1610.01065, 2016.

[26] S. Ravidas, A. Lekidis, F. Paci, and N. Zannone, Access control in Internet-of-Things: A survey, *Journal of Network and Computer Applications*, vol. 144, pp. 79–101, 2019.

[27] E. Zeng, S. Mare, and F. Roesner, End user security and privacy concerns with smart homes, in *Proc. 13th USENIX Conf. Usable Privacy and Security*, Berkeley, CA, USA, 2017, pp. 65–80.

[28] M. Aazam, I. Khan, A. A. Alsaffar, and E. N. Huh, Cloud of things: Integrating Internet of Things and cloud computing and the issues involved, in *Proc. 2014 11th Int. Bhurban Conf. Applied Sciences & Technology* (*IBCAST*), Islamabad, Pakistan, 2014, pp. 414–419.

[29] M. R. Abdmeziem, D. Tandjaoui, and I. Romdhani, Architecting the Internet of Things: State of the art, in *Robots and Sensor Clouds, Studies in Systems, Decision and Control*. Cham, Germany: Springer, 2016, pp. 55–75.

[30] A. Alshehri and R. Sandhu, Access control models for cloud-enabled Internet of Things: A proposed architecture and research agenda, in *Proc. IEEE 2nd Int. Conf. C*ollaboration and Internet Computing (*CIC*), Pittsburgh, PA, USA, 2016, pp. 530–538.

[31] A. Alshehri and R. Sandhu, Access control models for virtual object communication in cloud-enabled IoT, in *Proc. IEEE Int. Conf. Information Reuse and Integration* (*IRI*), San Diego, CA, USA, 2017, pp. 16–25.

[32] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, Internet of Things (IoT): A vision, architectural elements, and future directions, *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[33] R. Khan, S. U. Khan, R. Zaheer, and S. Khan, Future internet: The Internet of Things architecture, possible applications and key challenges, in *Proc. 10th Int. Conf. Frontiers of Information Technology*, Islamabad, India, 2012, pp. 257–260.

[34] M. Wu, T. J. Lu, F. Y. Ling, J. Sun, and H. Y. Du, Research on the architecture of Internet of Things, in *Proc. 3rd Int. Conf. Advanced Computer Theory and Engineering* (*ICACTE*), Chengdu, China, 2010, pp. 484–487.

[35] I. Bouij-Pasquier, A. A. Ouahman, A. A. El Kalam, and M. O. de Montfort, SmartOrBAC security and privacy in the internet of things, in *Proc. IEEE/ACS 12th Int. Conf. Computer Systems and Applications* (*AICCSA*), Marrakech, Morocco, 2015, pp. 1–8.

[36] C. T. Hu, D. F. Ferraiolo, and D. R. Kuhn, Assessment of access control systems, https://www.nist.gov/publications/assessment-access-control-systems, 2006.

[37] Y. Cao, Z. Q. Huang, S. L. Kan, D. J. Fan, and Y. Yang, Specification and verification of a topology-aware access control model for cyber-physical space, *Tsinghua Science and Technology*, vol. 24, no. 5, pp. 497–519, 2019.

[38] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, Identity authentication and capability based access control (IACAC) for the Internet of Things, *Journal of Cyber Security and Mobility*, vol. 1, pp. 309–348, 2013.

[39] H. F. Atlam, A. Alenezi, R. J. Walters, and G. B. Wills, An overview of risk estimation techniques in risk-based access control for the internet of things, in *Proc. 2nd Int. Conf. Internet of Things, Big Data and Security*, Porto, Portugal, 2017, pp. 254–260.

[40] S. Bugiel, S. Heuser, and A. R. Sadeghi, Flexible and fine-grained mandatory access control on android for diverse security and privacy policies, in *Proc. 22nd USENIX Conf. Security*, Berkeley, CA, USA, 2013, pp. 131–146.

[41] K. Z. Bijon, R. Krishnan, and R. Sandhu, A framework for risk-aware role based access control, in *Proc. IEEE Conf. Communications and Network Security* (*CNS*), National Harbor, MD, USA, 2013, pp. 462–469.

[42] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, BlockChain: A distributed solution to automotive security and privacy, *IEEE Communications Magazine*, vol. 55, no. 12, pp. 119–125, 2017.

[43] D. Servos and S. L. Osborn, Current research and open problems in attribute-based access control, *ACM Computing Surveys*, vol. 49, no. 4, p. 65, 2017.

[44] A. Home, How august smart locks work, https://august.com/pages/how-it-works, 2020.

[45] RemoteLock, Smart locks by RemoteLock, https://www.remotelock.com/smart-locks, 2020.

[46] E. Zeng and F. Roesner, Understanding and improving

security and privacy in multi-user smart homes: A design exploration and in-home user study, in *Proc. 28th USENIX Security Symp.*, Santa Clara, CA, USA, 2019, pp. 159–176.

[47] S. Werner, F. Pallas, and D. Bermbach, Designing suitable access control for web-connected smart home platforms, in *International Conference on Service-Oriented Computing*. Cham, Germany: Springer, 2017, pp. 240–251.

[48] T. H. J. Kim, L. Bauer, J. Newsome, A. Perrig, and J. Walker, Access right assignment mechanisms for secure home networks, *Journal of Communications and Networks*, vol. 13, no. 2, pp. 175–186, 2011.

[49] Y. Tian, N. Zhang, Y. H. Lin, X. F. Wang, B. Ur, X. Z. Guo, and P. Tague, SmartAuth: User-centered authorization for the internet of things, in *Proc. 26th USENIX Security Symp.*, Vancouver, Canada, 2017, pp. 361–378.

[50] G. P. Zhang and J. Z. Tian, An extended role based access control model for the internet of things, in *Proc. Int. Conf. Information, Networking and Automation* (*ICINA*), Kunming, China, 2010, pp. 319–323.

[51] N. Ghosh, S. Chandra, V. Sachidananda, and Y. Elovici, SoftAuthZ: A context-aware, behavior-based authorization framework for home IoT, *IEEE Internet of Things Journal*, vol. 6, no. 6, pp. 10773–10785, 2019.

[52] A. Dorri, S. S. Kanhere, and R. Jurdak, Blockchain in internet of things: Challenges and solutions, arXiv preprint arXiv:1608.05187, 2016.

[53] G. P. Zhang and W. T. Gong, The research of access control based on UCON in the internet of things, *Journal of Software*, vol. 6, no. 4, pp. 724–731, 2011.

[54] J. D. Jia, X. F. Qiu, and C. Cheng, Access control method for web of things based on role and SNS, in *Proc. IEEE 12th Int. Conf. Computer and Information Technology*, Chengdu, China, 2012, pp. 316–321.

[55] J. E. Kim, G. Boulos, J. Yackovich, T. Barth, C. Beckel, and D. Mosse, Seamless integration of heterogeneous devices and access control in smart homes, in *Proc. 8th Int. Conf. Intelligent Environments*, Guanajuato, Mexico, 2012, pp. 206–213.

[56] P. N. Mahalle, P. A. Thakre, N. R. Prasad, and R. Prasad, A fuzzy approach to trust based access control in internet of things, presented at Wireless VITAE 2013, Atlantic City, NJ, USA, 2013, pp. 1–5.

[57] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, Towards a novel privacy-preserving access control model based on blockchain technology in IoT, in *Europe and MENA Cooperation Advances in Information and Communication Technologies, Advances in Intelligent Systems and Computing*. Cham, Germany: Springer, 2017, pp. 523–533.

[58] OASIS Standard, eXtensible access control markup language (XACML) version 3.0, http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-os-en.html, 2013.

[59] S. Gusmeroli, S. Piccione, and D. Rotondi, A capability-based security approach to manage access control in the internet of things, *Mathematical and Computer Modelling*, vol. 58, nos. 5&6, pp. 1189–1205, 2013.

[60] J. L. Hernández-Ramos, A. J. Jara, L. Marín, and A. F. Skarmeta, Distributed capability-based access control for the internet of things, *Journal of Internet Services a*nd Information Security (*JISIS*), vol. 3, nos. 3&4, pp. 1–16, 2013.

[61] D. Hussein, E. Bertin, and V. Frey, A community-driven access control approach in distributed IoT environments, *IEEE Communications Magazine*, vol. 55, no. 3, pp. 146–153, 2017.

[62] D. Hardt, The OAuth 2.0 authorization framework, https://www.hjp.at/doc/rfc/rfc6749.html, 2012.

[63] R. Z. Du, A. L. Tan, and J. F. Tian, An attribute-based encryption scheme based on unrecognizable trapdoors, *Tsinghua Science and Technology*, vol. 25, no. 5, pp. 579–588, 2020.

[64] S. Sciancalepore, G. Piro, P. Tedeschi, G. Boggia, and G. Bianchi, Multi-domain access rights composition in federated IoT platforms, in *Proc. 2018 Int. Conf. Embedded Wireless Systems and Networks*, Singapore, 2018, pp. 290–295.

[65] K. Fysarakis, C. Konstantourakis, K. Rantos, C. Manifavas, and I. Papaefstathiou, WSACd–A usable access control framework for smart home devices, presented at IFIP International Conference on Information Security Theory and Practice, Lecture Notes in Computer Science, Cham, Germany: Springer, 2015, pp. 120–133.

[66] R. Schuster, V. Shmatikov, and E. Tromer, Situational access control in the internet of things, in *Proc. 2018 ACM SIGSAC Conf. Computer and Communications Security*, Toronto, Canada, 2018, pp. 1056–1073.

[67] S. Bandara, T. Yashiro, N. Koshizuka, and K. Sakamura, Access control framework for API-enabled devices in smart buildings, in *Proc. 22nd Asia-Pacific Conf. Communications* (*APCC*), Yogyakarta, Indonesia, 2016, pp. 210–217.

[68] S. Dutta, S. S. L. Chukkapalli, M. Sulgekar, S. Krithivasan, P. K. Das, and A. Joshi, Context sensitive access control in smart home environments, in *Proc. IEEE 6th Int. Conf. Big Data Security on Cloud* (*BigDataSecurity*)*, IEEE Int. Conf. High Performance and Smart Computing* (*HPSC*) *and IEEE Int. Conf. Intelligent Data and Security* (*IDS*), Baltimore, MD, USA, 2020, pp. 35–41.

[69] D. Rivera, L. Cruz-Piris, G. Lopez-Civera, E. de la Hoz, and I. Marsa-Maestre, Applying an unified access control for IoT-based intelligent agent systems, in *Proc. IEEE 8th Int. Conf. Service-Oriented Computing and Applications* (*SOCA*), Rome, Italy, 2015, pp. 247–251.

[70] R. Neisse, G. Steri, and G. Baldini, Enforcement of security policy rules for the internet of things, in *Proc. IEEE 10th Int. Conf. Wireless and Mobile Computing, Networking and Communications* (*WiMob*), Larnaca, Cyprus, 2014, pp. 165–172.

[71] J. Bugeja, A. Jacobsson, and P. Davidsson, On privacy and security challenges in smart connected homes, in *Proc. European Intelligence and Security Informatics Conf.* (*EISIC*), Uppsala, Sweden, 2016, pp. 172–175.

[72] J. Collins, The robot and the smart home, https://www.abiresearch.com/blogs/2019/08/28/robot-and-the-smart-home/, 2020.

[73] B. Fang, X. Wei, F. C. Sun, H. M. Huang, Y. L. Yu, and H. P. Liu, Skill learning for human-robot interaction using wearable device, *Tsinghua Science and Technology*, vol. 24, no. 6, pp. 654–662, 2019.

Ziarmal Nazar Mohammad received the bachelor degree at the School of Computer Science, Sayed Jamalludin Afghan University, Afghanistan. Currently working toward the master degree at the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interest includes cybersecurity, and Internet of Things & Intelligence.

Fadi Farha received the BS degree at the Faculty of Informatics Engineering, Aleppo University, Syria in 2009. He received the MS degree from University of Science and Technology Beijing in 2017 and is currently pursuing the PhD degree at the School of Computer and Communication Engineering, University of Science and Technology Beijing, China. His current research interests include physical unclonable function, ZigBee, computer architecture, and hardware security.

Adnan O.M Abuassba is an assistant professor at Arab Open University-Palestine. He obtained the PhD degree in computer science and technology from the University of Science and Technology Beijing. He obtained the master degree in computer science from Al-Quds University, Palestine. For 14 years, he has taught all ages and levels. He participated in international conferences as the 2015 Smart World Congress, Beijing and IEEE Workshop, 2015. He taught at Arab American University, Palestine during 2013 and Alquds Open University, Palestine between 2008 and 2011. His current research interests include neural networks, machine learning, extreme learning machine, ensemble learning, and computational intelligence.

Shunkun Yang received the BS, MS, and PhD degrees from the School of Reliability and Systems Engineering at Beihang University in 2000, 2003, and 2011, respectively. He is an associate research professor at Beihang University since 2016. He was an associate research scientist at Columbia University between September 2014 and September 2015. His main research interests are reliability, testing and diagnosis for embedded software, CPS, IoT, intelligent manufacturing, etc.

Fang Zhou received the BS, MS, and PhD degrees in computer science from the University of Science and Technology Beijing, China in 1995, 2002, and 2012. From 2015 to 2016, she was a visiting researcher at the Department of Computer and Information Sciences, Temple University, USA. She is currently an associate professor at the School of Computer Science and Technology, University of Science and Technology Beijing. Her research interests include machine learning, information retrieval, and computer vision.