Private Blockchain-Based Secure Access Control for Smart Home Systems

Jingting Xue[1]*, Chunxiang Xu[1]* and Yuan Zhang[1,2].
[1] Center for Cyber Security, School of Computer Science and Engineering,
University of Electronic Science and Technology of China
Chengdu 611731, China
[2] Department of Electrical and Computer Engineering, University of Waterloo
Waterloo N2L 3G1, Canada
[e-mail: JTXXue@yeah.net; chxxu@uestc.edu.cn]
*Corresponding authors: Jingting Xue, Chunxiang Xu

*Received April 4, 2018; revised June 6, 2018; accepted July 4, 2018;
published December 31, 2018*

Abstract

Smart home systems provide a safe, comfortable, and convenient living environment for users, whereby users enjoy featured home services supported by the data collected and generated by smart devices in smart home systems. However, existing smart devices lack sufficient protection in terms of data security and privacy, and challenging security and privacy issues inevitably emerge when using these data. This article aims to address these challenging issues by proposing a private blockchain-based access control (PBAC) scheme. PBAC involves employing a private blockchain to provide an unforgeable and auditable foundation for smart home systems, that can thwart illegal data access, and ensure the accuracy, integrity, and timeliness of access records. A detailed security analysis shows that PBAC could preserve data security against various attacks. In addition, we conduct a comprehensive performance evaluation to demonstrate that PBAC is feasible and efficient.

Keywords: access control, private blockchain, smart home system, auditability, signcryption cryptography

http://doi.org/10.3837/tiis.2018.12.024 **ISSN : 1976-7277**

1. Introduction

Smart home systems provide residents with a safe, comfortable, and convenient living environment [1]. In such systems, many smart devices and sensors continually generate data, monitor the space and interact with one another. Data on home residents' daily behaviors are automatically collected for third-party service providers to deliver featured home services, as elaborated in [2, 3, 4, 5, 6]. For example, a home owner who wishes to leave his or her home for a period of time can request housekeeping services from a service provider. The service provider can use the data (such as monitoring data generated by a smoke sensor) generated by the smart devices and the sensors of a smart home system to monitor the home on behalf of the home owner.

Among the data generated by smart home systems, some information (such as meter data, which can be used to determine whether anyone is at home) is very personal and sensitive and must be protected to prevent the occurrence of abuses, such as illegal access and modification. However, recent reports have shown that existing smart devices do not sufficiently ensure data security or privacy [7, 8, 9], and critical security and privacy concerns related to data access issues have been raised [10, 11, 12, 13]. This issue is further exacerbated by smart devices always being resource-limited. Therefore, protecting the data privacy and security of such devices is more challenging than ever before. Another important question concerns whether service providers honestly deliver requested home services during the scheduled periods. An irresponsible service provider that is regularly absent during service periods can cause serious issues for a home owner. As such, a secure, efficient, and auditable access control method must be employed to ensure data privacy and protection from illegal access, leaks and service provider misconduct [14, 15].

The data access and acquisition processes of the service provider can be modeled as a sequence of access records that present details regarding the data generated and utilized for the service. However, access records are not useful when they cannot be trusted, and it is inadvisable to trust access records without receiving proper protection. For example, a malicious service provider can access sensitive but unnecessary data through a home service while denying engaging in such misbehavior later, or a misbehaving home owner might forge an access record to circumvent a service provider. Therefore, it is crucial to guarantee the integrity and unforgeability of access records.

To protect access records from forgery and illegal modification, a potential solution involves requiring that an access record be signed by both the smart device and the service provider. However, signature techniques cannot ensure the timeliness of access records, as a signature generated at one time can be regenerated at any later point in time. In reality, it is more important to know when an access record was generated than the type of record that it was. Therefore, protecting access record security via signature techniques could be insufficient.

In this article, we propose a secure and auditable access control scheme for smart home systems called PBAC. To protect the data generated by smart devices in smart home systems against illegal access, PBAC utilizes a secure authentication mechanism to verify the validity of service providers. Illegal service providers cannot pass the authentication test to violate data privacy and security. To audit the integrity, accuracy, and timeliness of access records, PBAC uses the blockchain technique, whereby each access record is recorded in a blockchain once it is generated and authenticated. Because a blockchain is inherently verifiable and is resistant to the modification of chained blocks and because each record is time-stamped once it is recorded in the chain, the integrity, accuracy, and timeliness of chained access records cannot be compromised by home owners or malicious service providers.

As part of our contribution, we propose a private blockchain structure as an underlying primitive that we believe might be of independent interest. A public blockchain mainly differs from a private blockchain with respect to who plays the role of the miner to verify the validity of the data to be chained and to maintain the blockchain. In a public blockchain such as Bitcoin, any participant in a network can become a miner. In a private blockchain, only authorized participants can become miners, indicating that the threat model of a private blockchain is different from that of a public blockchain.

Specifically, the *contributions* of this work are as follows.

- We design a private blockchain with a different architecture from that of existing public blockchains. Compared to existing public blockchains, the proposed private blockchain is more efficient in terms of its computational overhead and storage costs.
- We propose a secure and auditable access control scheme designed for smart home systems based on the proposed private blockchain referred to as PBAC. PBAC ensures protection from illegal data access and enables the integrity, accuracy, and timeliness of access records to be audited by the smart home administrator. We present a security analysis to demonstrate that PBAC can remain secure and protected against various attacks. We also conduct a comprehensive performance evaluation and show that PBAC is highly efficient.

The *remainder* of this article is organized as follows. We review the related research in Section 2, and we present preliminaries in Section 3. In Section 4, we describe the construction of a private blockchain. We then describe PBAC in Section 5. We analyze the security level of PBAC in Section 6, and we evaluate the system’s performance in Section 7. Finally, we draw conclusions and present avenues for future research in Section 8.

2. Related Work

To ease the data management burdens related to the use of local devices while enjoying the comfort and convenience of smart homes, smart home owners typically outsource such data to external service providers, as elaborated in [16]. In 2015, Li et al. [5] proposed a smart home monitoring system that analyzes sensor data to limit unnecessary energy consumption. Sendra et al. [6] used smart sensors to monitor children with chronic illnesses to reduce the costs of artificial entitlements. In 2017, Wu et al. [17] predicted future events based on historical data drawn from sensors and smart devices to reduce the likelihood of malicious events occurring.

However, large-scale personal data outsourcing introduces security risks to smart home environments. To protect the personal privacy of residents, many access control schemes for smart homes have been proposed. In 2012, Kim et al. [18] integrated a new access control model for specific smart home conditions that was designed to seamlessly integrate heterogeneous protocols and devices from different vendors. The proposed model largely addresses problems related to a lack of communication standards for smart homes. In 2013, Ur et al. [19] introduced an access control system for different devices used in smart homes and noted that none of these systems fully support user access to the home. They then discussed feasible means of managing access control in smart homes. Fysarakis et al. [20, 21] proposed web service access control systems for devices in 2015 and a cross-domain resource sharing and access control framework for smart environments in 2016 based on the application of extensible access control markup language and device profiles for web services. Their schemes facilitate heterogeneous intelligent device interactions and granular access control management. However, interactions among owners, administrators, visitors, and smart devices can be controversial in relation to smart home access. In 2017, Ouaddah et al. [22, 23] proposed an access control framework based on blockchain named Fairaccess, where smart contracts in the blockchain were used to distribute access tokens. Because Fairaccess only supports the authorization based on a token, the time involved in obtaining access licenses is high. Whereafter, Pinno et al. [24] pointed out that Fairaccess lacks the integration of access control and appropriate relational networks that are of great importance in the collaborative and integrated Internet of things. In addition, issues regarding data storage and immutable records access remain a challenge. In 2017, Dorri et al. [25] claimed that they had proposed an optimized blockchain instantiation for the IoT called a "lightweight scalable blockchain." However, the construction of this scalable blockchain and its related security certificates were not provided.

3. Preliminaries

In this section, we define the system model and threat model, briefly describe blockchains, and present our design goals.

3.1 System Model

The system model of our scheme is shown in Fig. 1, and it involves three entities: a smart home *administrator*, many *smart devices*, and a *visitor*. Note that, for the access control scheme, we define the aforementioned service provider as a visitor because, when the scenario in the Introduction is modeled as an access control model, the service provider in the scenario corresponds to the visitor in the access control model.

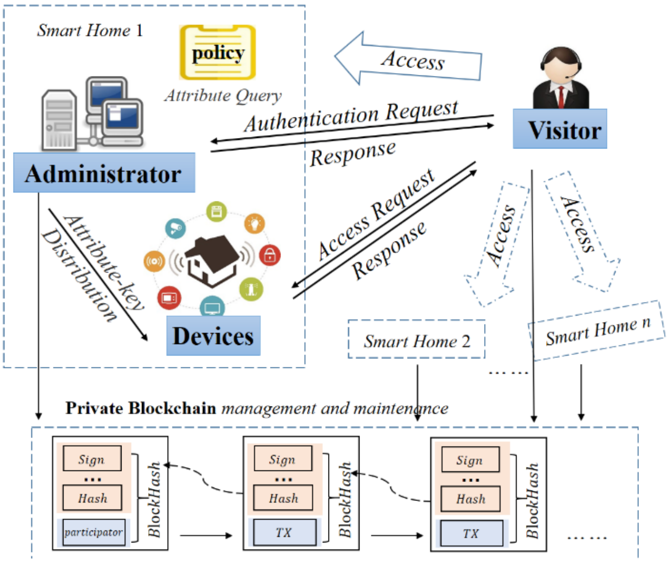


Fig. 1. System model

A smart home *administrator* is an online home server with access to numerous resources that manage access control for smart home systems, including maintaining access control policies, verifying visitor identities, and managing smart devices.

Smart devices, which are resource-constrained, collect data on residents living in a smart home environment. Any smart device provides a visitor with the requested data when a visitor possesses the access token distributed by an administrator.

A *visitor* requests data from smart devices, and these data are used to deliver services to the smart home owner. The visitor receives smart device data only when he or she has legitimate access rights. However, the visitor can attempt to access data that extend beyond access rights or can forge access records to deceive the smart home owner. In addition, the visitor maintains the private blockchain of storage requested data and access records. When a visitor serves multiple smart homes, the visitor maintains a private blockchain, and all of the administrators involved can access it.

Next, we briefly illustrate how a visitor accesses smart devices. In our scenario, the home owner who wishes to leave his or her home for a period of time can request housekeeping services from a service provider. The service provider, as a visitor, can use the data generated by the smart devices and the sensors of a smart home system to monitor the home on behalf of the home owner. Specifically, the visitor sends an authentication request to the administrator. After verifying the visitor's legitimacy, the administrator queries the access control policy. When the visitor's data request does not exceed his or her rights, the administrator assigns the visitor a token and a corresponding key to access smart devices. Then, upon receiving the visitor's data request, all of the smart devices involved send the requested data package to the visitor, and send the same data to the administrator backup. Finally, the visitor stores all of the access records in a block of the private blockchain after the administrator and the visitor reaches consensus on the requested data package and access record.

A formal definition of the proposed scheme is provided as follows.

Definition 1. PBAC involves five algorithms: *Initialization, Authentication, Access, Blockgen*, and *Revocation*.

Initialization. Based on the input security parameter, *Initialization* establishes the necessary parameters used in the following algorithms.

Authentication. Authentication completes the two-way authentication between the smart home administrator and the visitor.

Access. *Access* ensures that the visitor obtains data blocks from the involved smart devices.

Blockgen. *Blockgen* ensures that the visitor generates a block of the private blockchain for the visitor and administrator.

Revocation: *Revocation* completes the revocation of a visitor's access rights.

3.2 Threat Model

In relation to the threat model, we discuss two types of adversaries: internal and external. We assume that both internal and external adversaries can request access from a smart home owner, from an administrator, and from smart devices.

Internal adversaries.

- *Compromised administrator.* An adversary can control the administrator, extract keys saved by the administrator, and disrupt the private blockchain. Since the administrator is a highly resourceful server, we assume that the computational cost of damaging the administrator is greater than the value of the keys and data that it saves.

· *Controlled smart device*. Due to limited resources regarding smart devices, an adversary can manipulate smart devices to perform malicious actions. The adversary can intercept communications between smart devices and other entities, obtain keys saved by certain smart devices, or change the data stored on smart devices. However, we assume that the controlled smart device is discovered when the administrator shares the key again.

· *Semi-trusted visitor*. We assume that the visitor's identity is legal. However, the visitor can launch two attacks:

1. Attempt to access the device data extending beyond its own privileges. After receiving a token to access smart devices, the visitor sends an unreasonable access request to smart devices to attempt to view the owner's privacy rights or to obtain benefits. Here, we consider a special case in which a visitor still initiates an access request after his or her token or the assigned key expires. We view this behavior as an attack.

2. Forge access records. To save access overhead, the visitor forges access records to deceive the smart home owner and obtain service fees.

External adversaries.

· *Online adversary*. Such an adversary can control communications between entities of the system model. He or she can also pretend to be a visitor to request smart device data or even to destroy private blockchains.

3.3 Blockchain

Blockchains are well known for their outstanding manifestations in relation to a variety of cryptocurrency systems, such as Bitcoin [26], Ethereum [27], and Litecoin [28]. In the Bitcoin system, the public blockchain is an immutable ledger used to record transactions. Such transactions refer to the state of users in the system and users can conduct transactions without the help of a central authority. Structurally speaking, the public blockchain is composed of a one-way linear set of data units, in which each unit of data is called a block. Each block contains a pointer preblockhash that points to the previous block, a timestamp that records the time at which the current block was chained to the blockchain, and multiple transactions that record approved transactions.

Depending on the type of participants involved, blockchains are currently divided into two types: private (including consortium blockchains) and public. In the Bitcoin system, each participant can become a miner. Some miners verify the validity of each transaction and maintain the blockchain. A transaction can be recorded in the blockchain only when it has been approved and accepted by most (more than 50%) of the miners. Meanwhile, all the blocks are linked in chronological order, and are protected by cryptographic hash functions for integrity. Thus, the blockchain is inherently verifiable and resistant to tampering with recorded transactions. More information on public blockchains can be found in [29, 30, 31]. In a private blockchain, only authorized participants can become miners. Because of the limited resources of participants in a private chain, additional technological tools are often needed to ensure chain robustness.

3.4 Design Goals

In this article, we focus on access control in a smart home environment in relation to *the following challenges*.

1. Ensuring the safety of smart devices and of smart homes. A smart home system that allows for external server access is a semi-open environment; therefore, such a system can be attacked by insiders and outsiders. Moreover, smart device resources are limited and are thus insufficient to ensure data security. Therefore, the proposed scheme should be able to withstand all attacks on the threat model.

2. Verifying the credibility and integrity of access records. To enjoy personal services on demand, the smart home owner allows the service provider to access smart device data. However, the service provider can forge access records to cheat the home owner in an attempt to save access overhead. In addition, the home owner may not wish to pay service fees and may thus tamper with the service provider's access records to deny services. Therefore, the integral storage of visitor access records should be fully considered.

3. Improving the efficiency of a visitor's access to smart devices. After verifying a service provider's access rights, the administrator sends data requests to the smart devices and then aggregates all of the data to forward to the visitor. When we employ the typically used method to obtain data, a larger number of involved smart devices corresponds to a longer delay in the access process. Therefore, the efficiency of a device's access through a smart home system must be significantly improved.

To ensure secure and efficient access and control in a smart home environment via the above threat model, PBAC should achieve *the following goals*:

Functionality: The smart home administrator can engage in access control for the smart home. The visitor can store the device data and access records of the private blockchain, and all of the administrators involved can access the blockchain.

Security: Security should hold under the threat model described in Section 3.2. Specifically, PBAC should meet the following security requirements: (i) communications between visitors and smart home entities (administrator and devices) must satisfy confidentiality requirements, indicating that only the two parties with a key can read communication messages; (ii) visitors and the administrator can authenticate one another; (iii) visitors' access behaviors satisfy non-repudiation requirements; thus, undeniable access records are used to verify the authenticity of claims made by an entity; and (iv) devices are anonymous during communication with visitors. This rule suggests that external adversaries do not know which devices communicate with visitors.

Efficiency: Visitors can obtain requested device data of low latency. The smart home administrator can quickly determine the legitimacy of a visitor's identity, and can efficiently verify the validity of a visitor's signature on access data.

4. Private Blockchain Construction

4.1 Private Blockchain

Before introducing the private blockchain that we have constructed, we briefly review the (public) blockchain described in Section 3.3. A public blockchain, which is an immutable public record, is robust when all miners sacrifice large computational overhead and communication costs. However, in our scenario, neither the visitor nor the administrator has sufficient resources to apply the proof-of-work mechanism [26]. Moreover, we ask only the visitor and smart home administrator to authenticate access records, not all participants in the network. For the above reasons, we construct a new private blockchain to ensure the integrity of the device data and access records as shown in Fig. 2 Pilkington et al. [29] discussed the distinctions between public and private blockchains in greater detail, and these distinctions are not discussed here.

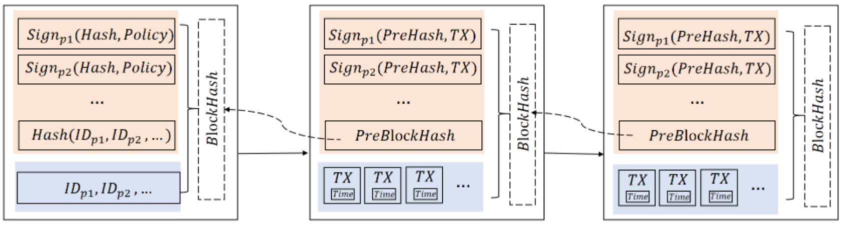
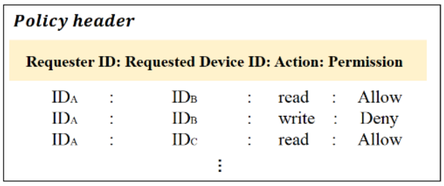


Fig. 2. Private blockchain structure

Our private blockchain is a private ledger managed and maintained by the administrator, and it is open to administrator(s). This blockchain employs a policy header with an access control list. Further information is shown in Fig. 3. The list saves the identities of legitimate visitors and the levels of access that the owner allows with in the home. In addition, our private blockchain stores the access records of transactions that involve different devices and/or different administrators (corresponding to different smart homes), which are discussed in Section 5.3.

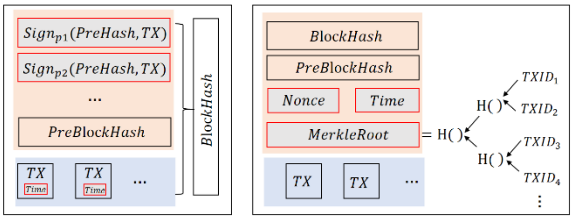


Policy header

Requester ID:	**Requested Device ID:**	**Action:**	**Permission**
ID_A :	ID_B :	read :	Allow
ID_A :	ID_B :	write :	Deny
ID_A :	ID_C :	read :	Allow
⋮			

Fig. 3. Policy header

To clearly illustrate the constructed private blockchain, we elaborate on the block structures of the private and public blockchains of the Bitcoin system in detail, as shown in Fig. 4, in which red-framed and dark items highlight *the differences*.



a. Block structure of private blockchain

b. Block structure of public blockchain

Fig. 4. Block structures of a private blockchain and of a public blockchain

1. We remove the nonce from the public blockchain. In a public blockchain, miners collect transactions in a block, vary a nonce until one solves the given hash puzzle and employ the proof-of-work mechanism to reach a consensus. However, in our scenario, an approach applying a low overhead can be used to convince the visitor and administrator of the credibility of stored data.

2. We remove the Merkle root from the public blockchain. As the number of Bitcoin transactions continues to increase, blocks maintain a uniform block size by Bitcoin supporting a simplified payment process [26] based on Merkle trees [32]. However, in a smart home system, smart home device data and visitor access records are uniformly generated over time and are not large. Thus, a private blockchain does not need to use the above method to limit block sizes.
3. We add signatures to the data of an entire block of the private blockchain. In the public blockchain, the proof-of-work tool is used as a consensus mechanism to guarantee the authenticity and non-repudiation of transactions. However, since visitor and smart home administrator resources are not unlimited in a smart home system, arbitrary additions and deletions by malicious adversaries cannot be prevented. Therefore, to achieve a consensus from all participants, we increase the signatures of the data of an entire block for participants in storage blocks.
4. The public blockchain of the Bitcoin system employs a distributed timestamp service similar to that of our private blockchain. However, in the access control of a smart home system, the home owner does not emphasize the amount of time needed to generate a block. The home owner instead determines the amount of time needed to request data and provide services. Thus, we determine the time required for each access record and not for an entire block.

Therefore, the private blockchain is also inherently verifiable and resistant to chained block modifications, and the timeliness of chained access records cannot be compromised by a home owner or by certain malicious service providers. In particular, the private blockchain ensures that there is undeniable evidence that it is necessary to audit all access behaviors. Even when the private blockchain is compromised, blockchain participants (visitors, administrators) can quickly detect stored data that have been lost, which is crucial for subsequent data recovery.

4.2 Private Blockchain Transactions

In the Bitcoin system, the status of users is represented by a series of messages referred to as “transactions”. A transaction involves the transfer of currency from one user to another (or to several) user(s). In our scheme, the data structure of a transaction (TX) includes two parts, Data and Record, as shown in **Fig. 5**. Data are a collection of device data that visitors access at a certain time. The *Record* is defined as a multi-signed access record for a visitor and administrator authorized by the smart home owner.

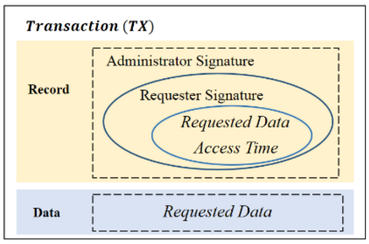


Fig. 5. Transaction

5. Proposed Scheme

5.1 Overview of PBAC

We present PBAC to achieve efficient authentication, secure access, and integrated storage. PBAC involves Initialization, Authentication, Access, Blockgen and Revocation. The initialization algorithm generates the necessary parameters for the following procedure. In the authentication algorithm, the administrator can quickly determine whether a visitor's identity is valid by comparing it with information included in a saved PK list and verifying the visitor's access rights. Specifically, the administrator checks the policy header to verify the visitor's access rights. When the request is valid, the administrator assigns the visitor a key and token for accessing smart devices. The smart devices send data to the visitor based on the token used in the access algorithm. In the Blockgen algorithm, the administrator and visitor mutually verify the validity of the other signatures on the stored data. After verifying the validity of the signatures, the visitor stores all of the data and signatures in the private blockchain. **Table 1** provides descriptions of the key notations used in PBAC.

Table 1. Notations and descriptions

Notation	Description
ID_ε	Unique global identity of an entity ε
$SC_k(m)$	Signcryption[1] on data m using key k
$(sk_\varepsilon, pk_\varepsilon)$	Signcryption and unsigncryption key of entity ε
$E_k(m)$	Message m is encrypted using key k
k	Content keys for encrypting data
H	Hash function $H:\{0,1\}^* \to Z_p$
TX	Transaction[2]
T	Token generated by the administrator to access devices
$\|\|$	Concatenation operation

[1] In the field of cryptography, signcryption is a public-key primitive that simultaneously performs digital signatures and encryption.

[2] In this article, transactions differ from Bitcoin transactions, which involve a signature message.

5.2 Basic PBAC Construction

A visitor V with identity ID_V, a smart home administrator with identity ID_A, and a set of smart devices $D_1, D_2, \ldots, D_n$ with identities $ID_1, ID_2, \ldots, ID_n$ are involved in PBAC, as shown in **Fig. 6**. In the Remarks section, we briefly describe the implementation of PBAC when a visitor serves multiple smart homes (corresponding to multiple administrators $A_1, A_2, \ldots$).

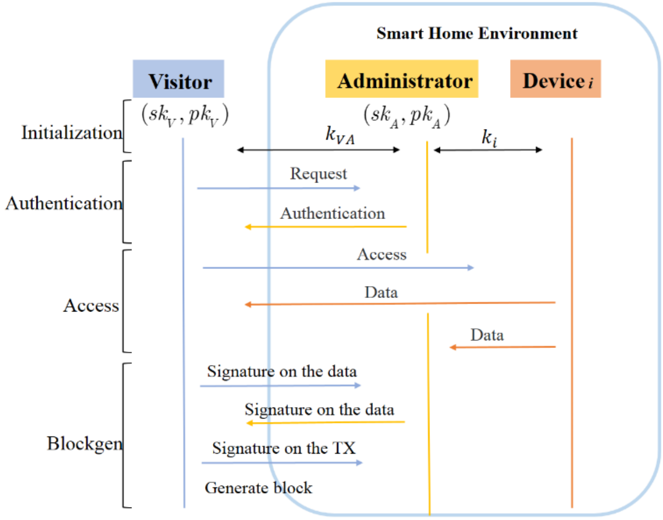


Fig. 6. Basic PBAC procedure

Initialization.

· For security parameter λ, the initialization algorithm selects groups G_1, G_2 of prime order p, symmetric encryption algorithm $E_k()$, signcryption algorithm $SC_k()$, and hash function $H:\{0,1\}^* \to Z_p$. In particular, $Para = \{G_1, G_2, p, E_k, SC_k, H\}$.

· A has an administrator-specific key pair (sk_A, pk_A), where $sk_A \in G_1, pk_A \in G_2$, and V has a visitor-specific key pair (sk_V, pk_V), where $sk_V \in G_1, pk_V \in G_2$.

· A shares k_{VA} with V and shares symmetric key k_i with device ID_i, where $ID_i \in \{ID_1, ID_2, \ldots, ID_n\}$; then it updates the local PK list and writes access control policies.

Authentication.

Step 1: V sends A request

$$req_1 = ID_V || SC_{skV}(ID_V, ID_A, r_1) \qquad (1)$$

to authenticate the identity and access rights, where r_1 is a random number.

Step 2: A inquires about the stored PK list. When V is included in the list, A uses sk_A and ID_V to decrypt the signcryption message and checks V's identity ID_V and r_1. After checking the freshness of the message, A sends

$$assign = SC_{sk_A}(k_{VDi}, ID_V, ID_A, ED, hash_0, t_1, r_1, r_2) \, || \, T \qquad (2)$$

to V to assign key k_{VDi} and token T, where $T = E_{ki}(k_{VDi}, ID_V, ID_A, t_1, ED, m_i)$ is a token generated by A that is used to access ID_i, t_1 is a timestamp, ED is the expiration date of k_{VDi}, m_i indicates the device data that the visitor is allowed to access, and $hash_0 = H(ID_V, ID_A)$.

Access.

Step 1: V sends the data request

$$req_2 = T \,||\, E_{k_{VDi}}(ID_V, t_2) \tag{3}$$

to device ID_i, where t_2 is a timestamp.

Step 2: D_i decrypts token T with k_i to obtain a shared secret key k_{VDi} and then recovers the identity of the visitor ID_V. Next, D_i sends V and A data package

$$\phi = E_{k_{VDi}}(ID_i, m_i, t_5), \tag{4}$$

where t_5 is a timestamp.

Blockgen.

Step 1: After auditing the integrity of m_i in ϕ, V generates signature

$$Sign_1 = Sign_{sk_V}(ID_V, m_i, t_2), \tag{5}$$

and sends it to A, where t_2 is the timestamp of requesting device data m_i.

Step 2: When V's signature on m_i is valid, A generates $M_{ji} = (ID_A, ID_V, m_i, t_2, t_4)$ and $S_{ji} = Sign_{sk_A}(ID_A, Sign_{sk_V}(ID_V, m_i, t_2),\ t_4)$, where S_{ji} represents the ordered multiple signatures of V and A found on an access record about m_i, and M_{ji} denotes the collection of all ϕ in one access, where j denotes that V visits D_i for the j-th time. Then A sends the entire j-block

$$block_j = TX_j \,||\, Sign_{sk_A}(TX_j, hash_{j-1}) \tag{6}$$

to V, where $TX_{ji} = (S_{ji}, M_{ji})$ and $TX_j = \{TX_{j1}, TX_{j2}, \ldots, TX_{ji}\}$.

Step 3: After verifying the validity of A's block signature and checking the authenticity and integrity of TX_j, V calculates the block signature

$$Sign_2 = Sign_{sk_V}(TX_j, hash_{j-1}), \tag{7}$$

and sends it to A. V then stores all of the data in the shared private blockchain, as shown in **Fig. 7**.

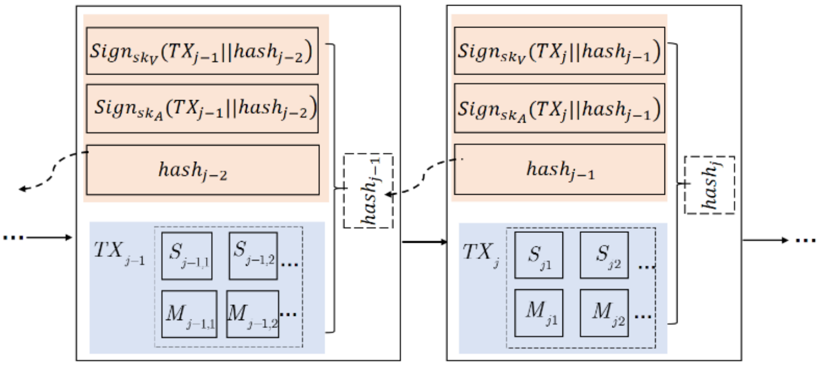


Fig. 7. Structure of the PBAC private blockchain

Revocation.

The revocation algorithm involves automatic and forcible revocation. After the expiration date of key k_{VDi} passes, a visitor's authentication request is automatically marked as illegal. Specifically, in step 1 of *Access*, after receiving the visitor's data request, the involved devices will simply check whether the ED in the token T has expired. If the ED has expired, the devices will not respond to the visitor's data request. When the visitor wants to continue accessing the device data, he or she must sign a new request to authenticate again. However, when a visitor's authentication information is forcibly revoked for some reason prior to the expiration date, the administrator updates the PK list, revises the access control policy and informs the involved smart devices.

5.3 Multi-home PBAC Construction

In this section, we briefly describe a multi-home PBAC scheme with a visitor serving multiple smart homes, in which the Authentication and Access algorithms are the same as those in the basic PBAC scheme. We discuss the construction of a multi-home private blockchain in detail.

A visitor maintains a private blockchain, which stores all of the relevant device data and access records involving different smart homes. Note that, in this case, the device data for different smart homes are stored in different blocks of the blockchain. The corresponding administrators $A_1, A_2, \ldots$ involved have the right to access this blockchain. To avoid a privacy issue, V uses key k_{VA_1} shared with administrator A_1 to encrypt data TX_j before storing the data in the blockchain, instead of directly storing the data itself. As shown in Fig. 8, although administrator A_1 can access the entire private blockchain, he or she can read only the data related to his or her smart home, such as TX_j stored in *Block* j.

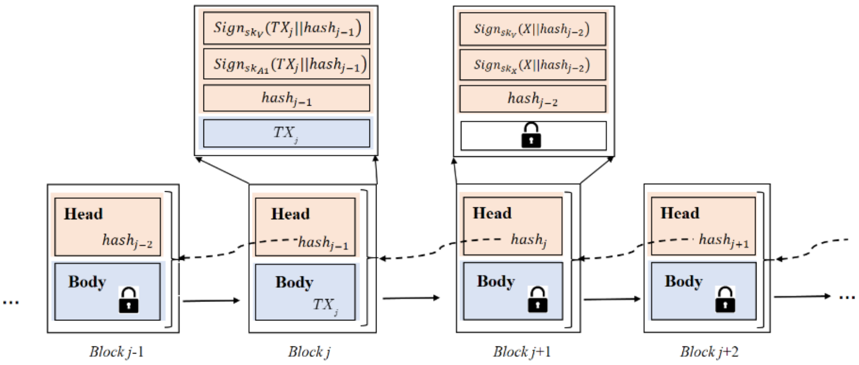


Fig. 8. Multi-home private blockchain structure

Typically, the administrators download the private blockchain locally, making it easy to query for specific data entries and to provide evidence of non-repudiation. To conserve local storage, multi-home PBAC advises administrators to download only the complete blocks associated with a respective smart home, as well as other blocks' headers.

5.4 Remarks

Using PBAC, we can combine the private blockchain and off-blockchain storage to construct a storage structure that accesses records and accesses data. That is, only the access records are stored on the private blockchain, and large-size access data are stored in off-blockchain storage, such as local storage or cloud storage. To a certain extent, the storage structure provides a better trade-off between the verification efficiency of the blockchain and the storage overhead. The details are not discussed here.

In the Blockgen algorithm, the verifier and administrator sign the access record and write it into the block after verifying its authenticity and integrity. That is, the accuracy and integrity of the access record are guaranteed by the cryptographic primitive “signcryption.” The blockchain's inherent non-tampering and timeliness ensure the timeliness of the access record written into the blockchain.

In addition, another efficient means of sending device data to the visitor is available. After verifying the legitimacy of a visitor’s data request, the administrator can request data from all of the involved smart devices and can then forward these data to the visitor. Note that the administrator does not wait for all of the data to be collected completely before forwarding them and instead receives the data from one device and then forwards them. This approach reduces the costs associated with smart device use, including the computational overhead for verifying the token and decrypting data requests, as well as the communication overhead for sending data to visitors. Because the administrator is an online high-resource server, we believe that sacrificing administrator resources to limit the resources consumed by resource-constrained smart devices is reasonable.

In the authentication algorithm, the smart home administrator and visitor decrypt and parse a signcryption message to verify each other’s identities. To simplify our description of PBAC, we do not discuss the detailed signcryption method used to complete this step. Li’s certificateless signcryption (CLSC) [33] and Barreto’s identity-based signcryption (IBSC) [34] algorithms of two different construction methods are both secure, efficient and compatible with PBAC. In Section 6.2, we apply CLSC and Barreto’s IBSC to demonstrate the feasibility of our administrator algorithm.

6. Security Analysis

We believe that smart device data should meet the three minimum security requirements required for any security design: confidentiality, integrity, and availability, i.e., CIA. Confidentiality indicates that only authorized users can read messages. Integrity ensures that a message is not tampered with during transmission. Availability denotes that services or data are available when users need them. In addition to CIA security attributes, we consider issues of authentication and anonymity. In this article, authentication indicates that the administrator and visitors can authenticate one another. Anonymity involves maintaining the secrecy of all of the accessed device identities except for those involving the visitor and administrator. In relation to several typical security threat models, we discuss the confidentiality and integrity of the data used, the availability of services and data, the authentication of visitors and administrators, and the anonymity of smart devices. We assume that an adversary cannot break an encryption or signature. We discuss in detail the following threat models, including threats to availability, threats to authentication and threats to anonymity, and we then analyze whether these include security threats to our scheme.

Theorem 1. If there exists an adversary A that can destroy the integrity of PBAC data, then the collision resistant of the hash function is broken.

Proof. Assume that there exists an adversary A that can forge a hash value without knowing the transaction details; then, we can construct another algorithm able to break the collision resistance of the hash function.

In the following game, we regard the hash function H as a random oracle, and each transaction $E_{VA}(TX)$ can only query H once.

Setup: On inputting a security parameter k, the challenger C generates the public parameter $Para$ and sends it to the adversary A.

Query: The adversary A can adaptively issue the following query to challenger C. The A can ask for block information about any block, such as j-block information including signatures $Sign_{sk_V}(TX_j \| hash_{j-1})$, $Sign_{sk_A}(TX_j \| hash_{j-1})$, encrypted smart device data $E_{VA}(TX_j)$, and the hash value of the previous block $hash_{j-1}$. C generates $hash_j$ and sends it to A.

End game: Receiving a sets of block information other than $E_{VA}(TX_k)$, the adversary A outputs a $hash_k$ under the k-block information. A wins if $hash_k$ sent by A is valid and differs from that of A while the challenger C does not reject it.

This outcome indicates that the adversary A can destroy the integrity of PBAC data. Obviously, this contradicts the collision resistance of the hash function. ■

Theorem 2. If there exists an adversary A that can access device data illegally, then the signcryption primitive is broken.

Proof. Assume that there exists an adversary A that can access device data without knowing the private key sk_V of the visitor; then, we can construct another algorithm able to break the security of the signcryption primitive.

In the following game, we regard the signcryption function SC as a random oracle, and each random number r can only query SC once.

Setup: On inputting a security parameter k, the challenger C generates public parameter $Para$ and sends it to the adversary A.

Query: The adversary A can adaptively issue the following query to challenger C. The A can ask for random number r_1. C generates the corresponding request $req_1 = ID_V \| SC_{sk_V}(ID_V, ID_A, r_1)$ and sends it to A.

End game: Receiving a set of authentication requests other than the target requests, the adversary A outputs a req_1' under a new r_1'. A wins if the req_1' send by A is valid and differs from that of A while the challenger C does not reject it.

This outcome indicates that the adversary A can access device data illegally. Obviously, this contradicts the security of the signcryption primitive. ■

Threats to availability. Many attacks against availability occur, such as denial of service (DoS) attacks, modification attacks, dropping attacks, and mining attacks. We focus on the impacts of representative DoS attacks and modification attacks with our scheme.

In a modification attack, an adversary may attempt to change or delete a specific user's storage data. To launch this attack, the opponent must compromise local storage security. However, visitors will be able to detect any changes in their stored data by comparing the local data to the stored hash values in the immutable ledger.

In a DoS attack, the adversary attempts to exhaust the resources of the attacked object through brute force methods, preventings legitimate users from accessing data or requesting services. For example, recent attacks [35] have occurred in which attackers have used a large number of zombie devices to launch large-scale DoS attacks, resulting in the paralysis of a service system. With PBAC, an adversary can initiate a DoS attack through two means: (i) an online adversary can send a large number of false authentication requests to the administrator or send a large number of data requests to smart devices; and (ii) a semi-trusted visitor can send malicious requests to devices that extend beyond his or her access rights. In the first form of attack, the administrator stores the identities and PKs of legal visitors in a PK list. The list helps the administrator quickly verify the identity of the visitor, greatly reducing the likelihood of a DoS attack. When the adversary directly sends a large number of data requests to a device with constrained resources, the device can become busy caching a large number of requests, resulting in downtime. In the Remarks section, we present a means for administrators to request and forward data to visitors that prevents external visitors from accessing smart devices directly. The second DoS attack approach does not work. Smart devices send data to the visitor based on the token distributed by the administrator and not based on the visitor's request.

Threats to authentication. To disrupt identity authentication, an online adversary can intercept and replay messages sent between legitimate entities. Specifically, the adversary intercepts authorized visitors' authentication requests and then forwards them, and he or she attempts to disguise himself or herself as a legitimate visitor to gain access to data. The above attack does not work because the messages are signed and encrypted by the administrator or visitors in our scheme. Adversaries cannot break encryptions to obtain the information required for authentication. In addition, random numbers are embedded into messages; thus, the receivers of messages can quickly detect replayed attacks. The timestamp also helps message receivers to recognize intercepted and replayed messages to be discarded.

Threats to anonymity. The third class of threats threatens anonymity, whereby an online adversary attempts to analyze various messages and other publicly available information to find the real world identities of devices. When the adversary knows the identities of the devices being accessed, he or she might be able to violate the owner's personal privacy. To avoid the above situation, the proposed scheme allows smart devices to send arbitrary requests to any entity in the smart home environment. The anonymity of devices is ensured by any accessed device's identity information being sent in ciphertext form through all interactions. This method, in turn, also increases the computational overhead for the administrator, since all of the stored shared keys must be traversed to decrypt a message and identify devices. Nevertheless, we believe that the added computational cost involved is acceptable and worthwhile.

Recent research [36] has shown that to break access control, attackers can control smart home devices or introduce fake devices into a home network. Our design uses graded defenses for these attacks. First, there is a central intelligent home administrator that controls all incoming and outgoing packets and prevents direct access to smart home devices from the Internet. If a smart home administrator detects a packet that does not conform to a policy defined by the smart home owner, the packet is discarded. The second defense is that all devices in the home must have original transactions in the immutable ledger, allowing them to initiate communication with the smart home manager and with other devices. A device that does not have a corresponding original transaction is isolated from the network, preventing attackers from bringing unauthorized devices into the network.

In general, PBAC guarantees data security in the smart home and protects the owner's privacy through the application of appropriate cryptography methods. Our framework is compatible with smart home environments because it constructs a block chain different from Bitcoin. To clearly show the security basis of the scheme, we summarize the main differences between Bitcoin's block chain and our private chain in Table 2.

Table 2. Comparison of the Bitcoin blockchain and the private blockchain of PBAC

Feature	**Blockchain in Bitcoin**	**Local private blockchain (ours)**
Blockchain visibility	Public	Private
Transaction chaining	Input, output	Previous data block of the same service
Mining requirement	POW	None
Transaction parameters	Input, output, coins	Block-number, hash of data, timestamp, output, PK list, policy
Transaction dissemination	Broadcast	Unicast
Block-headers	Puzzle	Access policy
Miner selection	Self-selection	Smart home owner chooses the administrator and the visitor
Miner rewards	Coins	Undefined

7. Performance Evaluation

We evaluate the performance of PBAC based on a smart home administrator, smart device computational overhead and communication costs. All of the experiments were conducted on a Linux system with a 3.2 GHz Intel Core i5 CPU and 8.00 GB of RAM installed on an HP desktop manufactured in China. The code was applied in the C language based on paired cryptographic library version 0.5.14 and using a symmetric elliptic α-curve with a base field size of 1024 bits and with an embedding degree of 2. All of the experimental results represent the average of 10 experiments.

To protect the privacy of smart home owners, we use the signcryption algorithm to achieve secure access control. Specifically, in the authentication algorithm, the administrator decrypts and parses a visitor's signcryption message to authenticate his or her identity. The administrator then generates a signcryption message to assign a key to the visitor. To prove the efficiency of the authentication algorithm (i.e., the process whereby the administrator authenticates the visitor's identity as involving low overhead), we use the authentication algorithms of Li's CLSC [33] and of Barreto's IBSC [34], cited in steps 3 and 4, respectively, where SHA256 is used to implement the hash function.

Fig. 9 shows the amount of time spent by the administrator in authenticating a visitor. This period involves deciphering a visitor's message and querying the PK list. In other words, less than 3 ms are typically needed for a smart home to complete a legitimate visitor authentication process. In addition, we find that the certificateless signcryption algorithm is more efficient than the identity-based signcryption algorithm when applied to our scheme setting. Fig. 10 shows the amount of time that an administrator spends assigning a key to a valid visitor. The figure shows that the home owner requires approximately 5 ms to assign a key and a token to the visitor.

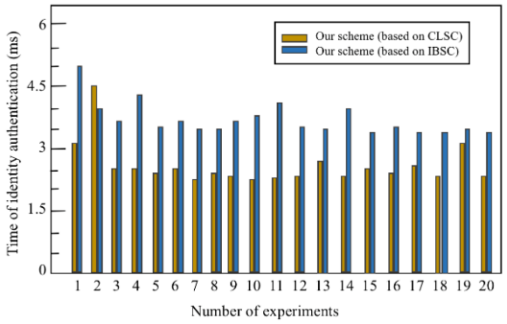


Fig. 9. Identity authentication period comparisons for our scheme based on the CLSC and IBSC.

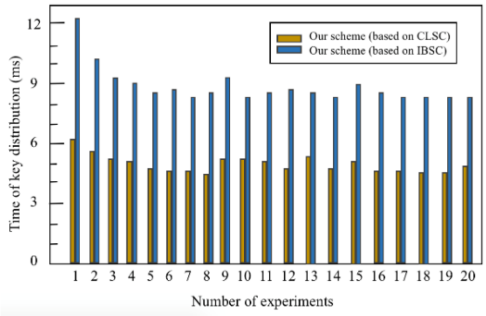


Fig. 10. Key distribution time period comparisons for our scheme based on the CLSC and IBSC.

To illustrate the feasibility of the authentication algorithm, we calculated the average of 100 trials. The average values show that, in the CLSC-based PBAC, the administrator requires only 2.541 ms to complete a visitor's authentication process and 4.916 ms to allocate a key to a legitimate visitor, whereas in the IBSC-based PBAC, the administrator requires only 3.608 ms to complete a visitor's authentication process and 8.404 ms to assign a key to a legitimate visitor, as shown in **Table 3**. Therefore, our scheme can achieve secure access control without adding much computational overhead to the administrator. In the above experiment, we ignore the overhead time for generating a token because token-generated symmetric encryption requires less time to execute than the signcryption algorithm.

Table 3. Computation time for the smart home owner

Item	Our scheme on CLSC	Our scheme on CLSC
Identity authentication time	2.541 ms	4.916 ms
Key distribution	3.608 ms	8.404 ms

*All experimental results reflect the mean of 100 trials.

Table 4 shows that the computation overhead of the visitor, the administrator and a smart home device in the three phases of PBAC. We apply RSA signature algorithm and AES encryption algorithm to implement the signature and encryption in our scheme respectively. From the table, it can be seen that the visitor requires only 11.009 ms to complete a data access; The administrator requires only 10.809 ms to complete access control once; And a smart device requires only 1.04 ms to complete data delivery once.

Table 4. Computation overhead of system participants

	Computational overhead		
	Visitor	Administrator	Device *i*
Authentication phase	6.149 ms	6.749 ms	/
Access phase	0.82 ms	/	1.04 ms
Blockgen phase	4.04 ms	4.06 ms	/

Table 5 shows the communication overhead of the administrator and for smart devices for one access control process. T, shown in the figure, denotes a token used to access smart devices. All of the timestamps are omitted from the communication overhead of both the administrator and smart devices. The data shown in the table illustrate that an

administrator must consume a $|Z_p|+2|G_1|+|T|$ communication overhead at most and that a smart home costs $|Z_p|+|ID|+|T|$ or $|ID|+|m|$. In addition, with the submission of a visitor's data request, the data encryption for a smart device requires only a symmetric encryption algorithm, and its computational overhead is negligible, even for resource-constrained smart devices. Therefore, our scheme is suitable not only for the access control of sensors and smart devices in smart home environments but also for that of various resource-constrained terminal devices.

Table 5. Smart home owner and device communication overhead

Entity-side	**Our scheme**
The smart home owner (Receive)	$\|Z_p\|+2\|G_1\|$
The smart home owner (Transmit)	$\|Z_p\|+2\|G_1\|+\|T\|$
A smart device (Receive)	$\|Z_p\|+\|ID\|+\|T\|$
A smart device (Transmit)	$\|ID\|+\|m\|$

* The timestamp is omitted in the communication overhead.
* T represents the token.

8. Conclusions and Future Work

In this article, we propose the first PBAC scheme developed for a smart home environment. PBAC can efficiently and securely control access, and it protects against a variety of internal and external attacks. For PBAC, we construct a new private blockchain that stores access records and that greatly reduces the computational and communication overhead while preserving the benefits of blockchain. We also perform a safety analysis and demonstration to illustrate the feasibility of PBAC. In addition, while our scheme is elaborated in relation to smart homes, it can be applied to several conditions that emphasize safe storage and resistance to data tampering.

In future work, we will continue to research useful combinations of traditional cryptographic algorithms and blockchain technologies to solve new challenges. Then, we will attempt to apply our approach to other areas requiring the protection of data security and the use of unalterable data. Data outsourcing has become a common paradigm in the rapidly evolving information age; thus, exploring data outsourcing paradigms and applications could have far-reaching implications for data outsourcing. However, ensuring the safety and traceability of outsourced data remains challenging.

9. Acknowledgements

This work was supported by the National Key R&D Program of China under Grant 2017YFB0802000 and the National Natural Science Foundation of China under Grant 61370203.

References

[1] V. Ricquebourg, D. Menga, D. Durand, B. Marhic, L. Delahoche, and C. Loge, "The smart home concept: our immediate future," in *Proc. of 1st International Conference on E-Learning in Industrial Electronics*, pp. 23-28, Dec, 2006. Article (CrossRef Link)

[2] I. Bisio, A. Delfino, F. Lavagetto, and A. Sciarrone, "Enabling IoT for in-home rehabilitation: Accelerometer signals classification methods for activity and movement recognition," *IEEE Internet of Things Journal*, vol. 4, no. 1, pp. 135-146, Feb, 2017. Article (CrossRef Link)

[3] D. J. Cook, M. S.-Edgecombe, and P. Dawadi, "Analyzing activity behavior and movement in a naturalistic environment using smart home techniques," *IEEE Journal of Biomedical and Health Informatics*, vol. 19, no. 6, pp. 1882-1892, Nov, 2015. Article (CrossRef Link)

[4] P. N. Dawadi, D. J. Cook, and M. S.-Edgecombe, "Automated cognitive health assessment from smart home-based behavior data," *IEEE Journal of Biomedical and Health Informatics*, vol. 20, no. 4, pp. 1188-1194, Jul, 2016. Article (CrossRef Link)

[5] M. F. Li and H. J. Lin, "Design and implementation of smart home control systems based on wireless sensor networks and power line communications," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 7, pp. 4430-4442, Jul, 2015. Article (CrossRef Link)

[6] S. Sendra, L. Parra, J. Lloret, and J. Tomas, "Smart system for children's chronic illness monitoring," *Information Fusion*, vol. 40, pp. 76-86, Mar, 2018. Article (CrossRef Link)

[7] R. Chowdhury, H. O.-Slimane, C. Talhi, and M. Cheriet, "Attribute-based encryption for preserving smart home data privacy," in *Proc. of 15th International Conference on Smart Homes and Health Telematics*, pp. 185-197, Aug, 2017. Article (CrossRef Link)

[8] "The smart home: Intelligent home automation," Article (CrossRef Link).

[9] B. C. Choi, S. H. Lee, J. C. Na, and J. H. Lee, "Secure firmware validation and update for consumer devices in home networking," *IEEE Transactions on Consumer Electronics*, vol. 62, no.1, pp. 39-44, Feb, 2016. Article (CrossRef Link)

[10] J. M. Batalla, A. Vasilakos, and M. Gajewski, "Secure smart homes: Opportunities and challenges," *ACM Computing Surveys*, vol. 50, no. 5, pp. 75:1-75:32, Oct, 2017. Article (CrossRef Link)

[11] E. Fernandes, J. Jung, and A. Prakash, "Security analysis of emerging smart home applications," in *Proc. of 37th IEEE Symposium on Security and Privacy*, pp. 636-654, May, 2016. Article (CrossRef Link)

[12] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," *IEEE Communications Surveys and Tutorials*, vol. 16, no. 4, pp. 1933-1954, Nov, 2014. Article (CrossRef Link)

[13] P. Kumar, A. Braeken, A. V. Gurtov, J. H. Iinatti, and P. H. Ha, "Anonymous secure framework in connected smart home environments," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 4, pp. 968-979, Apr, 2017. Article (CrossRef Link)

[14] X. Y. Huang, J. K. Liu, S. H. Tang, Y. Xiang, K. T. Liang, L. Xu, and J. Y. Zhou, "Cost-effective authentic and anonymous data sharing with forward security," *IEEE Transactions on Computers*, vol. 64, no.4, pp. 971-983, Apr, 2015. Article (CrossRef Link)

[15] X. Y. Huang, Y. Xiang, E. Bertino, J. Y. Zhou, and L. Xu, "Robust multi-factor authentication for fragile communications," *IEEE Transactions on Dependable and Secure Computing*, vol. 11, no. 6, pp. 568-581, Nov, 2014. Article (CrossRef Link)

[16] N. Feamster, "Outsourcing home network security," in *Proc. of ACM SIGCOMM workshop on Home networks*, pp. 37-42, Sep, 2010. Article (CrossRef Link)

[17] S. E. Wu, J. B. Rendall, M. J. Smith, S. Y. Zhu, J. H. Xu, H. G. Wang, Q. Yang, and P. Qin, "Survey on prediction algorithms in smart homes," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 636-644, Jun, 2017. Article (CrossRef Link)

[18] 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. of 8th International Conference on Intelligent Environments*, pp. 206-213, Jun, 2012. Article (CrossRef Link)

[19]B. Ur, J. Jung, and S. Schechter, "The current state of access control for smart devices in homes," in *Proc. of Workshop on Home Usable Privacy and Security*, Jul, 2014. Article (CrossRef Link)

[20] K. Fysarakis, C. Konstantourakis, K. Rantos, C. Manifavas, and I. Papaefstathiou, "Wsacd-a Usable Access Control Framework for Smart Home Devices," in *Proc. of International Conference on Information Security Theory and Practice*, pp. 120−133, Aug, 2015. Article (CrossRef Link)

[21] K. Fysarakis, C. Konstantourakis, K. Rantos, C. Manifavas, and I. Papaefstathiou, "XSACd cross domain resource sharing and access control for smart environments," *Future Generation Computer Systems*, vol. 80, pp. 572−582, Mar, 2018. Article (CrossRef Link)

[22] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "FairAccess: a new Blockchain-based access control framework for the Internet of Things," *Security and Communication Networks*, vol. 9, pp. 5943-5964, Dec, 2016. Article (CrossRef Link)

[23] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," *Europe and MENA Cooperation Advances in Information and Communication Technologies*, pp. 523-533, 2017. Article (CrossRef Link)

[24] O. J. A. Pinno, A. R. A. Gregio, and L. C. De Bona, "ControlChain: Blockchain as a central enabler for access control authorizations in the IoT," in 18th *Proc. of IEEE Global Communications Conference (GLOBECOM)*, pp. 1-6, Dec, 2017. Article (CrossRef Link)

[25] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in *Proc. of 15th International Conference on Pervasive Computing and Communications Workshops*, pp. 618-623, Mar, 2017. Article (CrossRef Link)

[26] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Article (CrossRef Link).

[27] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper. Article (CrossRef Link)

[28] "The cryptocurrency for payments based on blockchain technology," Article (CrossRef Link).

[29] M. Pilkington, "Blockchain technology: Principles and applications." Article (CrossRef Link)

[30] V. Buterin, "On public and private blockchains," Ethereum blog. Article (CrossRef Link)

[31] V. Buterin, "Visions, part 1: The value of blockchain technology," Article (CrossRef Link).

[32] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. of 4th International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT)*, pp. 369-378, Aug, 1987. Article (CrossRef Link)

[33] F. G. Li, Y.N. Han, and C. H. Jin, "Cost-effective and anonymous access control for wireless body area networks," *IEEE Systems Journal*, pp. (99):1-12, May, 2016. Article (CrossRef Link)

[34] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. of 11th International conference on the theory and application of cryptology and information security (ASIACRYPT)*, pp. 515-532, Dec, 2005. Article (CrossRef Link)

[35] "Hacker lexicon: what are dos and ddos attacks?" Article (CrossRef Link).

[36] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, et al, "Network-level security and privacy control for smart-home IoT devices," in *Proc. of 11th International Conference on Wireless and Mobile Computing, Networking and Communications*, pp. 163-167, Oct, 2015. Article (CrossRef Link)

Jingting Xue received the B.Sc. degree from the University of Electronic Science Technology of China, China, in 2014, and she is currently pursuing the Ph.D. with the School of Computer Science and Engineering. Her research interests are cryptography, cloud computing, and blockchain technology.

Chunxiang Xu received the B.Sc., M.Sc., and Ph.D. degrees from Xidian University, China, in 1985, 1988, and 2004, respectively. She is currently a Professor at the University of Electronic Science Technology of China, where she is involved in information security, cloud computing security, and cryptography.

Yuan Zhang received the B.Sc. degree from the University of Electronic Science Technology of China in 2013, and he is currently pursuing the Ph.D. with the School of Computer Science and Engineering. His research interests are cryptography, network security, and cloud computing security.