A blockchain-based access control scheme for smart home

Wentai Zhang, Huaizhi Yan
School of Computer Science and Technology, Beijing Institute of Technology, Beijing, 100081, China
Email: zhangwt@bit.edu.cn

Abstract. With the advancement of technology and economy, the scale of the smart home industry has exploded. While improving people’s lives, smart home systems are facing threats to privacy leaks, malicious attacks, and structural security. Effective security mechanisms are very important for protecting valuable data in smart home systems. Access control helps information systems prevent malicious access, thereby reducing the risk of privacy leakage. Blockchain can provide security support for the Internet of Things system due to its advantages of decentralization and immutability. Therefore, in this paper, a smart home access control scheme based on blockchain is proposed. The scheme uses Hyperledger Fabric and implements access control strategies through smart contracts. By designing a hybrid access control model based on dynamic attribute-based access control and static access control matrix, the remote access control initiated by the user through the Internet and the access control between local devices are well guaranteed at the same time. Through safety analysis and performance evaluation, the feasibility of the proposed scheme is demonstrated.

1. Introduction
Smart home (SH) refers to a home environment where smart devices can interact through the network and is an important application scenario of the Internet of Things (IoT) [1]. With the continuous development of technology and economy, IoT technology has made rapid progress, which makes the industrial scale and market of SH continue to expand. Data from Statista shows that global shipments of smart home devices will reach 1.77 billion in 2025 [2]. The progress of IoT technology has promoted the development of SH with diversified functions, intelligent products, and humanized services. However, at the same time, smart homes are facing challenges in terms of information security. First, smart homes contain a large amount of valuable data, which makes it easy to become the target for attackers [3]. In addition, the traditional IoT architecture faces threats to data confidentiality and integrity [4]. Also, the SH systems have the authority to control security devices such as door locks, which makes it easy to cause damage to property and even personal safety.

Access control and blockchain are two important technologies that can improve the security of smart home systems (SHS) from different perspectives. Access control is a classic technology to ensure the security of information systems, which stipulates the entity’s access rights to the resources in the system [5]. In the smart home environment, access control can effectively prevent malicious users from obtaining private data and controlling key devices. Attribute-based access control (ABAC) generalizes discretionary access control (DAC), mandatory access control (MAC) and role-based access control (RBAC). ABAC has improved dynamics, scalability and fine-grained [6]. It is widely used in the research of access control in the IoT scenario [6][14][16]. Blockchain, essentially a distributed ledger, was first proposed by Satoshi Nakamoto [7]. The typical data structure of the blockchain is shown in Figure 1. Blockchain has many advantages such as decentralization, immutability, non-repudiation,
transparency, anonymity, and traceability. Blockchain can enhance the security of IoT systems in data assurance, decentralization, trust and provenance [8][9]. A lot of work has verified the operability and rationality of the integration of blockchain and smart home [5] [10]-[14].

Previous research has tried to design an access control scheme for smart homes based on blockchain. However, they mainly realized the access of human users to the resources of the smart home, and did not design the access control between devices in the automation scenario.

In this paper, a smart home access control scheme based on Hyperledger Fabric is posed. The main contributions of this paper are as follows: according to the characteristics of the smart home environment, a hybrid access control scheme is proposed; the access between things is taken into account; auditing is achieved by recording access requests on the blockchain; we analysed the security, and designed experiments to evaluate the performance of the scheme.

The rest part of this article is organized as follows. Section 2 introduces the background knowledge and related work. Section 3 introduces the specific details of the model. Safety analysis and performance experiment are in Section 4. In Section 5, the work of this article is summarized and the future work is prospected.

2. Background Knowledge and Related Work
In this section, we will first introduce the background knowledge of Hyperledger Fabric and access control, then review the related work of smart home access control based on blockchain.

2.1. Hyperledger Fabric
The Linux Foundation launched the Hyperledger Fabric project in 2015 to build a platform for distributed ledger solutions [15]. Hyperledger Fabric is a consortium blockchain with higher efficiency and security [16]. The main concepts of Hyperledger Fabric are as follows.

Certificate Authorities (CA) distributes certificates to system participants as their digital identities. By verifying the signature of a certificate, participants who trust the CA can judge the legitimacy of others' identities and obtain their public information. Membership Service Provider (MSP) maintains a list of identities that are allowed to access the organization. Peer is the basic element that constitutes a blockchain network. Each peer can save a copy of the global ledger and smart contract. Orderer is used to achieving consistency. Ledger stores the data in the system. In Hyperledger Fabric, the ledger is composed of world states and blockchains. Smart Contract which can be understood as chaincode in Hyperledger Fabric defines the rules between different organizations in the executable code. It is developed using programming languages such as Golang and Java. After deploying to the network, all organizations in the same network can use it. Channel enables organizations to participate in multiple independent blockchain networks. And it can also guarantee data privacy.
2.2. Access Control

ABAC is an access control scheme, and access control matrix (ACM) is a specific access control implementation method. The formal definitions of the two are given below.

2.2.1. Attribute-based access control. In ABAC, attributes of subject, resource and environment are the three types of attributes we are concerned [17]. In addition, the attributes of the access should also be considered. Here we give the definition of the ABAC model on the basis of [17]:

1) S, R, E and A are subjects, resources, environments and access, respectively;
2) ATTR(s), ATTR(r), ATTR(e) and ATTR(a) are attribute assignment relations for subject s, resource r, environment e, and access a respectively:
   \[ATTR(s) \in RA_1 \times RA_2 \times \cdots \times RA_j,\]
   \[ATTR(r) \in RA_1 \times RA_2 \times \cdots \times RA_K,\]
   \[ATTR(e) \in EA_1 \times EA_2 \times \cdots \times EA_M,\]
   \[ATTR(a) \in AA_1 \times AA_2 \times \cdots \times AA_N,\]
   where \(SA_j (1 \leq j \leq J), RA_k (1 \leq k \leq K), EA_m (1 \leq m \leq M)\) and \(AA_n (1 \leq n \leq N)\) are the attributes for subjects, resources, environments and access, respectively;
3) A Policy that decides on whether subject s can get resource r in environment e by access a, is a Boolean function of ATTR(s), ATTR(r), ATTR(e) and ATTR(a):
   \[Policy: can\_access(s, r, e, a) \leftarrow f(ATTR(s), ATTR(r), ATTR(e), ATTR(a))\]

Access Control Matrix (ACM). ACM is a static access control method that expresses the access strategy between the subject and the object by using a matrix. An ACM can be defined as follows:

\[
ACM_{n \times n} = \begin{bmatrix}
    a_{11} & a_{21} & \cdots & a_{n1} \\
    a_{12} & a_{22} & \cdots & a_{n2} \\
    \vdots & \vdots & \ddots & \vdots \\
    a_{1n} & a_{2n} & \cdots & a_{nn}
\end{bmatrix},
\]

\(a_{ij}\) represents the access authority of entity i to entity j and its value is 0 to 3 (0: no right; 1: read only; 2: write only; 3: read and write).

2.3. Related Work

Blockchain-based access control (BCAC) schemes in smart home and IoT scenarios have been extensively studied. To improve the security and usability of the access system, the researchers also used edge computing and encryption algorithms when designing the access control scheme. The following is an introduction to the access control research of smart homes and IoT environments.

A BCAC scheme for smart homes with a reverse hash chain (RHC) consensus mechanism is proposed in [12]. It means that only authorized users who enjoy the hash seed can quickly pack the block. However, this scheme is limited to the local area network (LAN). Authors in [13] implemented a BCAC scheme in smart homes, and demonstrated the detailed process and interactions from verification requests. But the description of the architecture is not sufficient. Authors in [14] proposed an authentication scheme that combines ABAC with ERC-20 Token and edge computing to construct a security framework for IoT devices in SHS. Authors in [6] introduced a capability-based access control in blockchain-based IoT environments. Authors in [16] proposed Fabric-iot which is based on the Hyperledger Fabric and ABAC. They designed three smart contracts: device contract, strategy contract and access contract. However, this study did not take into account the user's request for the operation of the device, such as controlling a smart switch to remotely turn on the lights. FairAccess in [18] solved the high table query complexity problem and guaranteed the privacy of the access policy. But due to the need to design an access strategy for each device, the scalability of the solution is insufficient. A private BCAC scheme was proposed to provide unforgeable and auditable SHS in [19]. But private chain means weakening of scalability. Authors in [20] designed a verifiable collaboration mechanism to meet the
needs of controlled access authorization. Authors in [21] proposed a BCAC scheme for IoT and used symmetric encryption algorithm (SEA) to protect the privacy of the system.

Previous research work ignored the access from devices. However, this is widespread in automated SHS. If the disguised malicious node publishes the wrong data, it may cause serious losses. For example, a malicious node sending a cooking request to the rice cooker may cause a fire.

3. Proposed Scheme

This section describes the proposed scheme. First introduced the overall system architecture and main components. Then the access model and key smart contract algorithm are given. Finally, we introduced the workflow.

Figure 2. System Architecture.

3.1. System Architecture

The architecture of the scheme is shown in Figure 2. Hyperledger Fabric is used to build a blockchain system. The architecture is mainly composed of four parts, namely users, client, blockchain network and smart homes.

Users are divided into home owners (HO) and common users (CU). There is only one HO in each smart home. HO can access all the resources and also need to make the access control strategy.

Client refers to the program that interacts with the blockchain, which can be developed by using the SDK provided by Hyperledger Fabric to achieve the specified functions.

Blockchain network mainly includes CA, admin, channel, peer, orderer, ledger, and smart contract. Admin is the administrator of the blockchain and is mainly responsible for deploying smart contracts.

Smart home is composed of smart devices and smart gateways. Smart home devices include all kinds of IoT devices. The smart gateway realizes automatic control of home equipment. Also, a fabric client is installed in smart gateway to communicate with the blockchain.

3.2. Access Control Model

The attributes of entities in the proposed scheme are shown in Table 1. UserID can uniquely identify a user. HomeID identifies a smart home environment and corresponds to a unique HO. DeviceID identifies a smart home device and corresponds to a unique HomeID. Network refers to the environment to which the client belongs. Access_Type includes reading, writing, and execution. Based on these attributes, the access control strategy is defined as:
Policy: $can\_access(s, r, e, a) = f (ATTR(s), ATTR(r), ATTR(e), ATTR(a)) = \begin{cases} \text{true} \\ \text{false} \end{cases}$

Table 1. Attributes of Entities.

| Entity | Attributes                  |
|--------|-----------------------------|
| ATTR(s) | UserID, IP_Addr, Role       |
| ATTR(r) | DviceID, HomeID, IP_Addr, MAC |
| ATTR(e) | Time, Network               |
| ATTR(a) | Access_Type                 |

Table 2. Smart Contract Algorithm.

| Smart Contract | Main Function | Algorithm |
|----------------|---------------|-----------|
| AdminCC        | regSH         | First, determine whether the caller of the contract is admin; If not, return an identity error; If so, create a HomeID based on the UserID of HO, store the data using HomeID as the key, UserID as the value in the blockchain, and return the registration success message. |
| HOCC           | addPolicy     | Verify whether the caller is the HO user corresponding to HomeID according to the data stored in the blockchain; If the verification fails, the operation is rejected; If the verification is successful, parse the input value into specific attributes, and store the data with main attributes as the key, encrypted and signed strategy as the value in the blockchain, then return a success message. |
|                | updateHash    | Verify whether the caller is the HO user corresponding to HomeID according to the data stored in the blockchain; If the verification fails, the operation is rejected; If the verification is successful, store the data with the hash value of ACM as the key, the timestamp as the value in the blockchain, then return a success message. |
| VistorCC       | canAccess     | First, record the access request to the blockchain; Then parse out the attributes of the entity, resource, environment, and access; According to the input and environmental, calculate the value with the method of calculating the key in addPolicy, and use the value to query data from the blockchain, and according to the obtained result Follow-up operations: if there is no result, access is prohibited; if get a result, access is allowed. |

3.3. Smart Contract Design

According to the caller, three smart contracts are designed. AdminCC is used for smart home and HO registration, HOCC is used to manage access control strategies, and VistorCC is used to implement access request processing. The main functions and brief description of their algorithm is shown in Table 2.
3.4. Workflow
The system workflow includes two stages. The first stage shown as Figure 3 is initialization and policy setting. The second stage shown as Figure 4 is access request processing.

3.4.1. Initialization and Policy Setting. In the first step, the smart home service provider (SHSP) builds a blockchain network. The second step is to install the smart contract using the admin account. The third step is to call the smart contract to complete the registration of smart home and HO in turn. Lastly, HO deploy the access control policies of the smart home environment.

3.4.2. Access Request Processing. The access request is divided into two ways in our solution, including the user's access to the resources in the SHS through the client and the automatic access to the system resources by the smart gateway.

- The user access request is sent from the client to the blockchain to call the smart contract. First, the request will be recorded in the transaction log for audit. Then it will judge whether the access is legal according to the ABAC policy.
- The local access request mainly comes from the resource access process of the smart gateway. To determine the legitimacy of the request, first query the ACM hash value stored in the blockchain, and then compare it with the value calculated by the local ACM. If they are equal, the access legality can be judged according to the local ACM.

4. Security Analysis and Performance Evaluation

4.1. Security Analysis
Confidentiality, integrity, availability, non-tampering and non-repudiation are important attributes of information security. In addition, the ability to prevent access requests from malicious nodes is an element of verification of the access control scheme. The following is a security analysis of the proposed scheme from the above perspective.

Confidentiality, integrity and non-repudiation can be guaranteed by traditional techniques such as public key encryption algorithms, digests, and digital signatures. The traditional smart home architecture faces higher risks of service availability. It can be solved by the distributed solution based on blockchain. Non-tampering and non-repudiation are also the main advantages brought by the blockchain.

Malicious access may occur from external and local networks. For malicious access requests from the outside, due to the existence of the Hyperledger Fabric CA, users who need to obtain a certificate in the corresponding organization can access smoothly. In addition, even if a malicious user can send an access request to the blockchain, due to the existence of access control, its attributes cannot match the policy so that it cannot obtain the requested resources. For malicious requests from the local network,
the ACM will be consulted when processed by the smart gateway. The malicious node is not in the device list, so the access request cannot be satisfied either.

4.2. Performance Evaluation

In order to evaluate the performance of the solution, a Hyperledger Fabric network was deployed based on Ubuntu 16.04. The smart contracts are developed based on Golang, and the client is developed based on Node.js.

Smart contracts can be divided into query smart contracts (QSC) and modification smart contracts (MSC). The QSC only needs to perform the task of querying the ledger, but MSC requires changing the ledger data. We tested the response time of both QSC and MSC in concurrent scenarios. The number of requests is set from 10 to 500. The average response time is shown in Figure 5. The maximum response time of the two types of smart contracts is shown in Figure 6. It can be seen that the average response time of the MSC is below 0.6s, and the overall trend is decreasing as the number of requests increases. When the number of requests exceeds 100, the average response time stabilizes below 0.2s. The response time of QSC is within 0.1 seconds. It can be seen from the two figures that due to the consensus mechanism of the blockchain the running time of MSC is much longer than that of the QSC.

5. Conclusion

In this article, we propose a smart home access control scheme based on blockchain. Use attribute-based access control strategies for users' access requests through the Internet, which are implemented through smart contracts. For the access inside the home LAN, static access control based on the access control matrix is used. And we use Hyperledger Fabric as the blockchain solution. The security analysis and performance evaluation of the solution verifies that it can provide security support for smart homes. For future work, on the one hand, we can continue to study the access control scheme, and test the practicability of the scheme in actual scenarios. On the other hand, it may be necessary to combine technologies such as identity authentication to improve the security capabilities of the smart home environment.

Acknowledgment

This work is supported by China National Key R&D Program “The Human Reproductive Genetic Resources Service Management Cloud Platform Development and Safety Standard Specification System Construction” (2016YFC1000301).

References

[1] Almusaylim Z A and Zaman N. (2019) A review on smart home present state and challenges:
linked to context-awareness internet of things (IoT). *Wireless Networks* 25(6):3193-3204.

[2] Statista. (2021) Smart home device shipments worldwide 2020-2025. https://www.statista.com/statistics/1223274/smart-home-device-shipments-worldwide/.

[3] Moniruzzaman M, Khezr S, Yassine A, and Benlamri R. (2020) Blockchain for smart homes: review of current trends and research challenges. *Computers & Electrical Engineering* 83: 106585-.

[4] Md. Moniruzzaman, Khezr S, Yassine A, et al. (2020) Blockchain for smart homes: Review of current trends and research challenges. *Computers & Electrical Engineering* 83: 106585.

[5] Xiang Yu, Zhangxiang Shu, Qiang Li, et al. (2021) BC-BLPM: A Multi-Level Security Access Control Model Based on Blockchain Technology. *China Communications* 18(2): 110-135.

[6] Sun S, Du R, Chen S and Li W. (2021) Blockchain-based iot access control system: towards security, lightweight, and cross-domain. *IEEE Access* PP(99), 1-1.

[7] Nakamoto S. (2008) Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

[8] Cui P, Guin U, Skjellum A and Umphress D. (2019) Blockchain in IoT: current trends, challenges, and future roadmap. *Journal of Hardware and Systems Security* 3(4) p:338-364.

[9] Sreelakshmi K K, Bhatia A and Agrawal A. (2020) Securing IoT applications using blockchain: a survey.

[10] Ammi M, Alarabi S and Benkhelifa E. (2021) Customized blockchain-based architecture for secure smart home for lightweight IoT. *Information Processing & Management* 58(3): 102482.

[11] Zhou Y, H Meng, Liu L, et al. (2018) Improving IoT Services in Smart-Home Using Blockchain Smart Contract. *The 11th IEEE International Conference on Internet of Things. IEEE.*

[12] Kim D Y and J Lee. (2020) A reverse hash chain path-based access control scheme for a connected smart home system. *IEEE Consumer Electronics Magazine* PP(99), 1-1.

[13] Mbarek B, Ge M and Pitner T. (2020) Blockchain-Based Access Control for IoT in Smart Home Systems. *31st International Conference on Database and Expert Systems Applications.*

[14] Qashlan A, Nanda P and He X. (2020) Security and Privacy Implementation in Smart Home: Attributes Based Access Control and Smart Contracts.2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom).

[15] Hyperledger community. (2018) An Introduction to Hyperledger https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf, p:23.

[16] Han Liu, Han Dezhi and Li Dun. (2020) Fabric-iot: A Blockchain-Based Access Control System in IoT. *IEEE Access* 818207-18218.

[17] E. Yuan and J. Tong. (2005) Attributed based access control (ABAC) for Web services. *IEEE International Conference on Web Services (ICWS’05)* p:569.

[18] Aafaf O, Abou E A and Ouahman. (2016) A FairAccess: a new Blockchain-based access control framework for the Internet of Things. *SECURITY AND COMMUNICATION NETWORKS* 9(18) p: 5943-5964.

[19] Jingting Xue, Xu Chunxiang, Zhang Yuan. (2018) Private Blockchain-Based Secure Access Control for Smart Home Systems. *KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS* 12(12) p: 6057-6078.

[20] Yan Zhang, Li Bing, Liu Ben, et al. (2020) An Attribute-Based Collaborative Access Control Scheme Using Blockchain for IoT Devices. *ELECTRONICS* 9(2852).

[21] Guangsheng Yu, Zha Xuan, Wang Xu, et al. (2020) Enabling Attribute Revocation for Fine-Grained Access Control in Blockchain-IoT Systems. *IEEE TRANSACTIONS ON ENGINEERING MANAGEMENT* 67(4) p: 1213-1230.