Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 4393314, 12 pages
https://doi.org/10.1155/2022/4393314

Research Article

Design of the Secure Smart Home System Based on the Blockchain and Cloud Service

Kun Liao

Art College, Chongqing Technology and Business University, Chongqing 400067, China

Correspondence should be addressed to Kun Liao; 2012a42@ctbu.edu.cn

Received 19 August 2021; Revised 2 September 2021; Accepted 30 December 2021; Published 17 January 2022

Academic Editor: Deepak Gupta

In this paper, a variety of cloud service combinations is used to form the control core of a smart home, realize data forwarding, storage, and analysis in the cloud, and complete the remote management of smart home devices. This paper studies the secure access control of smart home data combined with the blockchain technology and password technology to realize the secure and efficient access control of smart home data. The system can achieve the goal of independent research and development. Aiming at the problem that the access control of a smart home is generally managed by third-party authorized institutions and there is an unauthorized access, a blockchain-based smart home (BSH) access control scheme is proposed. The scheme extends the attribute-based access control model (ABAC) and applies the blockchain technology to the smart home ABAC model to realize fine-grained access control. In the scheme, the resource provider first publishes the access control policy of the resource to the blockchain. If the resource visitor wants to access the resource, he needs to submit an access request to the blockchain and use an SM2 threshold signature to process the transaction proposal. The endorsement peer node in the blockchain runs the access control policy smart contract to decide whether to grant access rights. This scheme can ensure that resource providers can participate in all the processes of access control and avoid the risk of unauthorized access caused by the centralized management of the third party. Finally, the simulation experiment is carried out on the Hyperledger Fabric alliance chain development platform. The results show that the BSH access control scheme has good applicability in the smart home scenario.

1. Introduction

In modern society, the smart home has become the trend of intelligent life. In order to build a good smart home interconnection system and provide users with more valuable services, it is usually necessary to share smart home data with the outside world. However, these shared data often contain a large number of user sensitive privacy data and there is still a lack of an effective smart home data access control scheme to ensure the security of user data, which will become the bottleneck of the development of the smart home field. At present, more than 90% of smart home network access is carried out through mobile smart terminals. These terminal devices generally have the characteristics of scattered network topology and limited resources and are vulnerable to external attacks resulting in key leakage. In addition, the traditional smart home access control system is a centralized management, which does not include all participants in the access control decision-making process, and the data owner lacks the right to speak in the access control policy formulation and decision-making process. This enables the data requester to access the data of smart home devices without the authorization of the data provider, and there is a risk of ultra vires access.

Smart home is becoming more and more popular in recent years, because it brings us comfort and convenience of life; it has been recognized and widely used by people [1]. Its main core is to embed intelligence into sensors and actuators to integrate devices. When people apply, there may be multiple users visiting home devices at the same time or at different times, which requires no one to participate in data processing and exchange. On the one hand, the rise of a smart home improves our quality of life; on the other hand, because its information system mainly shares information through smart devices (IoT) and embedded sensors [2], there are some potential safety hazards. Mainly in the process of data transmission, privacy or user's privacy information will be exposed. A new secure smart home system solution based on blockchain is proposed, which aims at dealing with the security constraints in the blockchain method and uses the combination of Hyperledger Fabric and Hyperledger Composer. The popularity of a smart home in the Internet of things will increase the cost of security requirements [3]. How to use a relatively low-end design to strengthen the research on network security in families is very meaningful. This paper puts forward the method of localization by using the private blockchain technology and trilateral measurement. After our investigation, it is found that using private blockchain has great advantages. Blockchain plays a great role in the field of Internet of things [4], and it can also solve security problems. We apply it to a smart home, which can effectively optimize security, attacks, user privacy, and so on. It is found that blockchain plays three roles in smart home applications [5]. The superiority of a smart home is self-evident, and it can fundamentally improve our quality of life. However, we also find that its data storage security cannot meet our needs for privacy security.

2. Blockchain Technology

2.1. Key Features. Blockchain uses distributed ledgers to maintain stored data [6], so blockchain has the following key characteristics [7]:

(1) Decentralization. Blockchain abandons the traditional and centralized network architecture and uses distributed computing methods and decentralized storage mode to ensure that any node in blockchain is equal to each other and every data block in the chain needs the participation and maintenance of each node

(2) Transparency. The data stored on the blockchain is open and transparent, and the nonprivate information can query the data stored on the blockchain in an open interface and develop related applications

(3) Autonomy. In order to avoid human intervention and exclude the trust of "people," blockchain uses consensus-based norms and protocols and any human intervention will not work

(4) As long as the information is added to the blockchain through verification, it cannot be tampered with and will be stored permanently. Under special circumstances, more than 51% nodes in the control system can be modified at the same time

(5) Anonymity. The exchange of data between nodes follows a fixed algorithm. Blockchain data exchange and even transactions can be conducted anonymously

2.2. Blockchain Structure. Blockchain is a distributed ledger, and internal blocks are connected by hash values in chronological order. As the basic technology of digital cryptocurrency, blockchain stores information blocks with digital signatures in distributed networks [8].

Blocks in the blockchain are linked to each other through parent blocks. Each block header consists of metadata, including a version number, parent block hash, Merkle tree root hash, nBits, and random number, as shown in Table 1.

The block body of blockchain consists of two parts, namely, trading counter and trading. As shown in Figure 1.

Because of its unique open attribute, the public blockchain can attract many users and is particularly active. Alliance blockchain is used in commercial applications, and Hyperledger is developing the blockchain framework of business alliance [9]. Ethereum also provides tools for building alliance blockchain.

2.3. Consensus Process. In blockchain, how to reach an agreement among untrusted nodes is a transformation of the Byzantine General (BG) problem. How to reach consensus in an environment lacking trust is a challenge. Because the blockchain network is distributed [10], it is also a challenge for blockchain. We need protocols to ensure that the distributed books of different nodes are consistent. Then, the common ways to reach consensus in blockchain are as follows:

2.3.1. Proof of Workload (PoW). The consensus technology is to identify nodes in the existing chain that add new block rights by providing sufficient evidence to prove their workload. In fact, each node tries to broadcast the block of authentication transaction and chaos will occur. PoW can try to solve the difficulty adjustment problem by attaching a new block to the current chain. This process is called miner digging, where miners are responsible for selecting verified transactions and then forming a block. And add some additional information to the block, such as the hash value and timestamp in the parent block. Then, all the information in the block header is converted into a hash value by the SHA-256 hash function.

Such a scene can be considered. Several miners found random numbers that met the requirements almost simultaneously. When the miner node M_1 digs out the block $Block_{21}$ based on the block $Block_1$, it broadcasts to the whole network. However, since the miner node M_2 is far away from the miner M_1, it does not receive the block $Block_{21}$ for a period of time and digs out the block $Block_{22}$ at the same height as the block $Block_{21}$ and broadcasts to the whole network. According to the blockchain protocol, when different miners generate different blocks of the same height at the end of the blockchain, each node separately selects which block to receive. In the absence of other factors, nodes typically receive the first block they see. This creates an obvious problem, as different nodes receive the same height blocks $Block_{21}$ and $Block_{22}$ separately, resulting in the main chain of the blockchain being bifurcated. There will also be a rare continuous fork in the blockchain. As shown in Figure 2, at the fifth height of the block chain, when the branch blocks Block51 and $Block_{52}$ have not been solved, the branch blocks $Block_{61}$ and $Block_{62}$ at the sixth height appear. The block interval depends on various parameter settings, such as

Table 1: Block header attributes.

Block header attribute	Definition
Version number	Used to indicate which set of block validation rules to follow
Parent block hash	256-bit hash value pointing to the previous block
Merkle root hash	Hash value of all transactions in the block
Time stamp	The current timestamp is from 1970-01-01T00: 00UTC seconds
nBits	Target value corresponding to mining difficulty
Random number	A 4-byte field, usually starting from 0, is incremented by each hash calculation

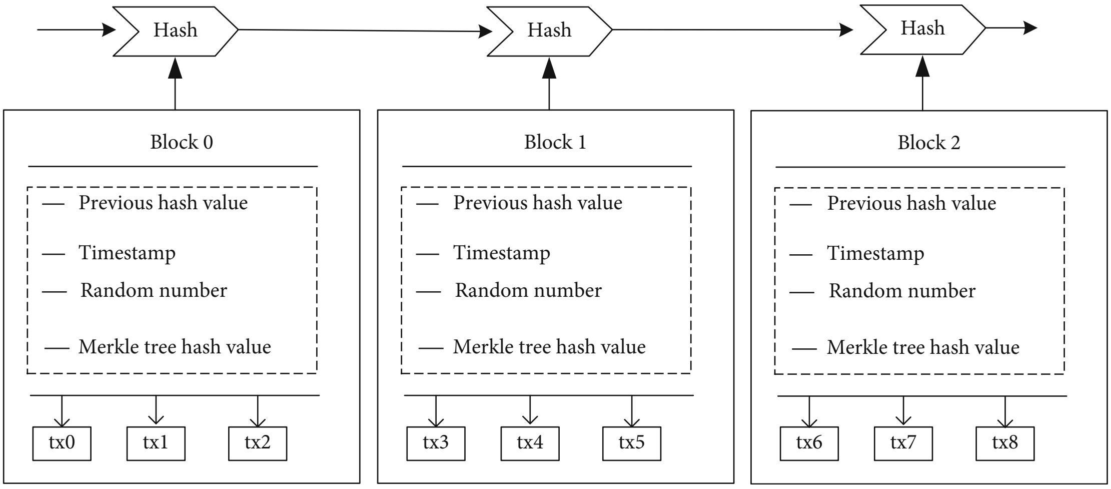

Figure 1: Blockchain structure.

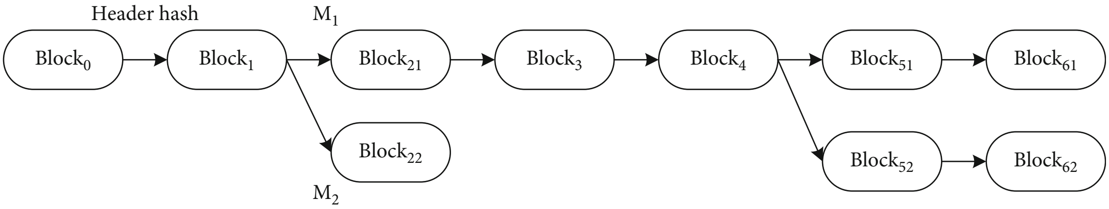

Figure 2: Blockchain bifurcation process.

generating Bitcoin blocks every 10 minutes and Ethernet blocks every 17 seconds [11].

The main problem with the PoW algorithm is that miners need to spend a lot of computing resources to solve this problem. In addition, only one miner succeeded in the end and the process was unsustainable.

2.3.2. Certificate of Equity (PoS). In this consensus algorithm, miners do not need to waste a lot of computing resources to solve mathematical problems. Since the selection of verifiers is based on equity relationships, the richest nodes may be given more opportunities to verify a block, thus becoming more advantageous in the network, which may lead to unfairness or concentration of rights. Because the mining cost and workload are much lower than PoW, PoS is more vulnerable to malicious attacks.

2.3.3. Certificate of Entrusted Equity (DpoS). It is a selective consensus process. In order to ensure efficiency, network parameters, such as the block size, can also be adjusted. However, it has the tendency of centralization, which is also its limitation. Equity ownership can not only vote for itself but also manipulate others. However, dishonest witnesses will be voted down by shareholders because they will do anything malicious.

2.4. Intelligent Contract. Smart contracts are usually executed by system nodes, so it is impossible for a single entity to bypass the rules defined in this code, because this requires the consent of most consensus nodes. The main advantage of intelligent contract is that it can automate the business logic of the organization. The shift to automation eliminates the impact of possible legal disputes due to human error and misunderstanding. Legal contracts may have personal explanations, but blockchain intelligent contracts realized by software algorithms are decisive, and there is no possibility of subjective explanations. In the scheme proposed in this paper, the intelligent contract stores the data owner list, and when the data user searches, the data owner list will be provided to the data user. The specific functions of smart home access control and data sharing scheme need to be realized by executing smart contract functions.

2.5. Hyperledger Fabric. Hyperledger Fabric is implemented by an open-source blockchain platform [12]. It provides a modular architecture to implement various functional modules by utilizing well-known and proven technologies. The core artifacts in Hyperledger Fabric [13] are described in Figure 3.

(1) Organize peer node channel: in Hyperledger Fabric, peer node is the node that hosts blockchain and runs intelligent contract. Peer stores critical data and executes specific programs. The stored data mainly include books and smart contracts, and the executed procedures mainly include endorsement and smart contract execution. The functions of the following node can be divided into the submission node and endorsement node. All nodes in the blockchain network are submission nodes, which are responsible for recording complete blockchain data information and verifying the correctness of each transaction. They are nodes that package transactions into blocks and add them to the blockchain. Nodes with smart contracts are called endorsement nodes, which are mainly responsible for accepting transaction requests, executing smart contracts and sending signed data back to clients after verifying that transactions are valid. There can be one or more peer nodes in an organization. As shown in Figure 3, organization 1 manages two peer nodes, P1 and P2, and one peer node can be added to one or more channels, such as P1, P3, and P7 in the same channel

(2) Membership service provider (MSP): MSP provides certificates to each peer node, so that the nodes connect to the blockchain network and trade. Organizations can have separate MSPs and get services

(3) Sorting service: subscription service refers to the transactions that are approved first, which are sorted by the consensus protocol, and finally, the designated peer nodes get the results

(4) Chain code: chain code is similar to smart contract. These are programs written in traditional programming languages such as Go, Java, and node.js, which can operate blockchain

(5) Blockchain data structure: blockchain contains two different data structures in Hyperledger Fabric: state database and distributed ledger. The blockchain is modeled as key value storage (KVS) to store its latest state. It is maintained and managed by the peer node and can be operated by the chain code triggered by the transaction. On the other hand, distributed books store verifiable historical data of all failed attempts and successful changes as a completely ordered hash chain of transaction blocks

3. SM2 Elliptic Curve Cryptography Algorithm

SM2 elliptic curve cryptography [14] is composed of the digital signature algorithm, public key encryption algorithm, and public key exchange protocol. The digital signature algorithm and public key encryption algorithm are used in this paper. Before the algorithm is executed, all parties need to set the public security parameters, including the scale q of finite field F_q, the parameters of elliptic curve equation, and the basic point $G = (x_G, y_G)$ on the elliptic curve, and select cryptographic hash algorithm H_{256} and hash algorithm H_v.

3.1. SM2 Digital Signature Algorithm. The key generation is as follows:

(1) The signer randomly selects d as the private key, $d \in [1, q-1]$. After that, the public key is calculated

$$P = dG. \tag{1}$$

The public key P is made public and the private key D is kept secretly.

(2) The signer selects the random number $k \in [1, q-1]$ and calculates

$$kG = (x1, y1). \tag{2}$$

(3) The subscriber's placement is as follows:

$$\bar{M} = Z_{\mathrm{A}}||M. \tag{3}$$

Among them,

$$Z_{\mathrm{A}} = H_{256}(\mathrm{ENTL_A}||ID||a||b||x_G||y_G||x_1||y_1). \tag{4}$$

$\mathrm{ENTL_A}$ is two bytes converted from the integer entlenA, a and b are the parameters of the elliptic curve, and (x_G, y_G) is the coordinates of the G point.

Calculate later

$$e = Hv(M). \tag{5}$$

The data type of E is converted to an integer according to the method given in the SM2 elliptic curve public key cryptography algorithm.

(4) The signer calculates through the message M to be signed

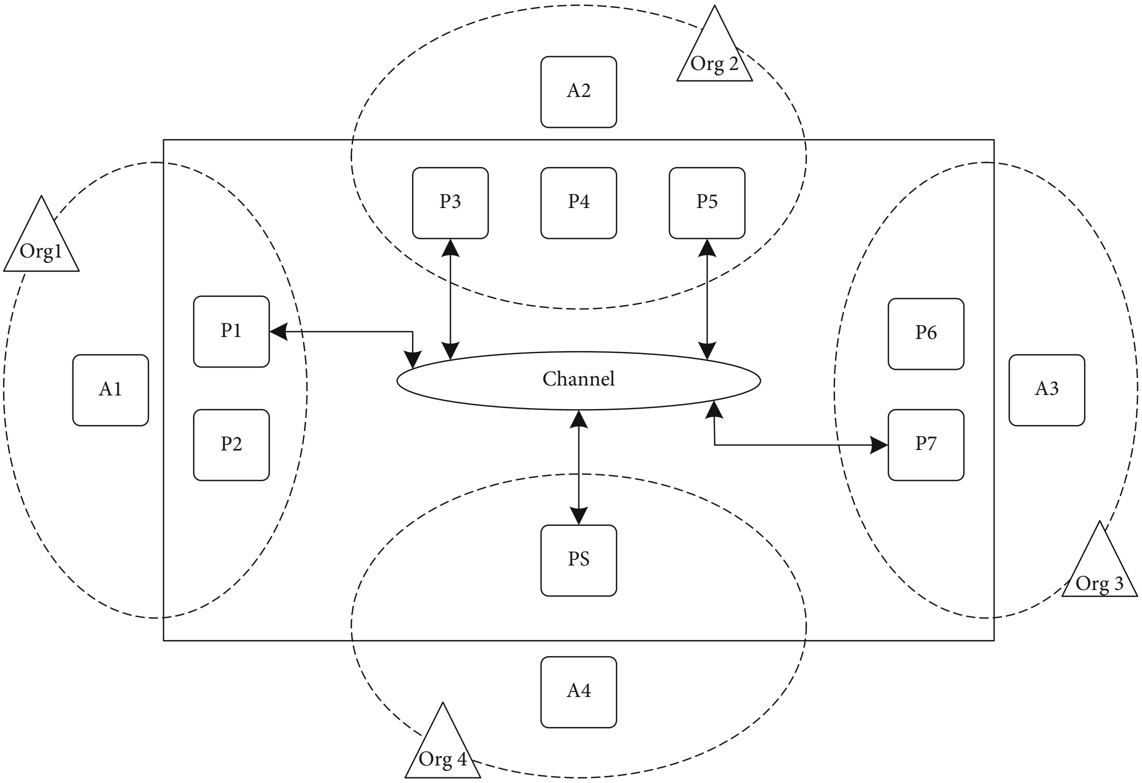

Figure 3: Peer node organization channel diagram.

$$r = (e + x_1) \bmod q. \tag{6}$$

If $r = 0$ or $r + k = q$, the signer needs to reselect the random number k.

(5) The calculation is

$$s = (1 + d)^{-1}(k - rd) \bmod q. \tag{7}$$

If $s = 0$, choose a new random number k. If $s = (1 + d)^{-1}(k - rd) \bmod q$, the signer outputs (r, s) as the signature result.

(6) When the signature verifier receives the message M and the signature (r, s), the signature verifier first checks whether r, $s \in [1, q-1]$ and $r + s \neq q$ is true. Then, calculate $e' = Hv\,(m)$, and then, calculate

$$\left(x_1', y_1'\right) = sG + (r + s)P. \tag{8}$$

(7) Calculate $r' = (e + x1')\bmod q$, and judge whether r $' = r$ is true. If the equation is true, the verification passes; otherwise, the verification fails

3.2. SM2 Public Key Cryptography Algorithm. The bit length of the plaintext M is mlen and KDF is the key derivation function.

The encryption algorithm is

(1) Choose the random number $l \in [1, q-1]$, and then, calculate

$$\begin{gathered} C1 = lG = (x2, y2), \\ lp = (x3, y3). \end{gathered} \tag{9}$$

(2) Calculate later

$$e = \text{KDF}(x_3 \| y_3, \text{mlen}). \tag{10}$$

Recalculate

$$C_3 = \text{hash}(x_3 \| M \| y_3). \tag{11}$$

(3) Finally, output ciphertext

$$C = C_1 \| C_3 \| C_2. \tag{12}$$

The decryption algorithm is as follows:

(1) First, the decrypter needs to verify whether C_1 is on the elliptic curve and calculate

$$dC1 = (x3, y3). \tag{13}$$

(2) After that, the decrypter needs to calculate $e = \text{KDF}\,(x_3 \| y_3, \text{mlen})$ and calculate

$$M = C2 \oplus e. \tag{14}$$

(3) The decrypter calculates $C_3' = \text{hash}(x_3 \| M \| y_3)$ and passes the verification formula

$$C_3' = C_3. \tag{15}$$

Determine whether the decryption is correct. If not, exit the decryption process. If true, output message plaintext m.

3.3. Signature Scheme. When nonmembers of the group want to join the group and become members of the group, they need to perform an interactive registration process with the home gateway HG. The specific process is as follows:

(1) Group member U_i sends a registration request to HG_i

$$\text{Req}_{\text{enroll}} = \text{Enc}_{\text{SM2}}\left(\text{ID}_i, pk_{\text{HG}_i}\right). \tag{16}$$

EncSM2 is the SM2 public key encryption algorithm, and ID_i is the identity information of group member U_i. After receiving the registration request, HG_i uses its own private key $sk_{\text{HG}i}$ to decrypt the registration request message $\text{Req}_{\text{enroll}}$, thus obtaining the true identity information of U_i. After that, HG_i needs to check whether the member has been registered in the local identity list, and if the member has been registered, it will refuse its registration request. Otherwise, it will randomly select $u \in Z^*p$ for the group member U_i applying for registration and obtain the first anonymous identity ID_{i1} of U_i by the following calculation:

$$\begin{aligned} U &= uG = (x_u, y_u), \\ \text{ID}_{i1} &= (x_u + sk_{\text{HG}_i})h(\text{ID}_i) + u \bmod p. \end{aligned} \tag{17}$$

Thereafter, the HG_i sends response information $M_H^1 : \{U, \text{ID}_{i1}, T_H^1\}$ to the group member U_i, where T_H^1 is the current timestamp

(2) After receiving the response information from HG_i, U_i, a group member, first checks the freshness of T_H^1. After that, verify whether the equation $\text{ID}_{i1} G = (x_u G + pk_{\text{HG}_i})h(\text{ID}_i) + U$ holds. If not, U_i needs to repeat step (1). Otherwise, U_i will generate part of the private key $sk_{u_i}^{x_i} \in Z_p^*$ and calculate the corresponding pub $pk_{u_i}^{x_i} = pk_{u_i}^{x_i} G$ lic key. After that, the U_i selects the random number $v \in Z_p^*$ and obtains the second anonymous identity ID_{i2} of the U_i by the following calculation:

$$\begin{aligned} V &= vG = (x_v, y_v), \\ \text{ID}_{i2} &= \left(x_v + sk_{u_i}^{x_i}\right)h(\text{ID}_{i1}) + v \bmod p. \end{aligned} \tag{18}$$

After that, a response message $M_U^1 : \{sk_{u_i}^{x_i}, V, \text{ID}_{i2}, T_U^1\}$ is sent to the HG_i.

3.4. Cloud Server Technology. At present, the standard definition of the cloud server refers to "virtual servers" running on the same physical hardware which are independent of traditional servers. Compared with the characteristics, cloud services are a cluster and their functions need to be coordinated with each other. Because there is no need to install hardware equipment, the cost performance of the cloud server will be higher and the host configuration and business scale of the cloud server can be configured according to the needs of users, so users are more flexible in cost control. Cloud servers can enable clients such as smart phones, PCs, or tablets to access the server through public networks. Common servers include Alibaba Cloud, Tencent Cloud, Jinshan Cloud, and Baidu Cloud, which support Internet applications such as e-commerce, enterprise or personal websites, social networking services (SNS), cloud storage, and office automation (OA), such as office software collaboration tools and forums.

4. Smart Home

4.1. Smart Home System Model. In Figure 4, the main actors in the system and the system components are introduced in turn.

4.1.1. Participating Roles. The data collected from participants equipped with smart home devices varies according to different devices and comes from the sensing data in the home, including the temperature, humidity, and luminosity, even from medical data generated by wearable devices, images generated by monitoring systems, and audio and video data.

Any party accessing the data of smart home devices is the requester. Usually, the party that relies on smart home data to provide different services is regarded as the data requester.

4.1.2. System Components. The role of the router is as the network coordinator and connection gateway. The gateway is a channel to connect with external networks. It can not

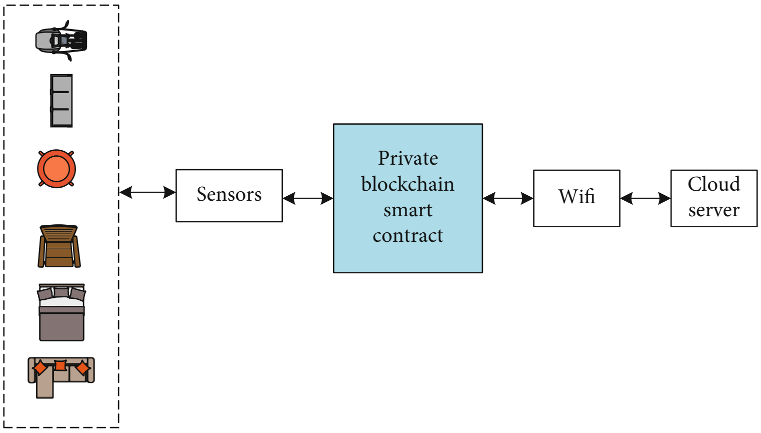

Figure 4: Smart home system model diagram.

only have its own IP but also connect to the cloud of the public interface. As the manager of all available information in intelligent home networks, multiple local smart home networks can exist at the same time and each network represents a home, office, school, etc. equipped with smart home devices.

All verified attributes and access control policies are stored in the blockchain. It can also be used as the execution point of the access request policy for specific smart home resources. Blockchain provides a unified access control platform for the whole smart home network.

4.2. Attribute-Based Access Control (ABAC) Model. Attribute-based access control (ABAC) is a logical approach to access control [15]. Attributes are the core concept of this model. In the attribute-based access control model, attributes are usually represented in quadruple (S, O, P, and E):

(1) S (subject attribute): the attribute of the entity in the system that initiated the access request, such as the organization, identity, and rank

(2) O (object attribute): attributes of entities that provide resources and can be accessed in the system, such as the name, type, and format of resources

(3) P (permission attribute): various operations on object resources, such as querying, writing, creating, and deleting

(4) E (environment attribute): the environment information in which the access control process is going on, such as the time, place, network location, and concurrent access restrictions when the access requester initiates the access. This attribute is independent of the access request subject and the accessed resource object

The basic framework of the attribute-based access control (ABAC) model [16] is shown in Figure 5. The basic steps of the authorization process of the access control policy are as follows:

(1) The subject sends the access request to the object through the system: the access request subject sends the access request information to the policy enforcement point PEP, and then, the PEP forwards the access request information from the requesting subject to the policy decision point PDP

(2) PDP carries out policy decision evaluation: the policy decision point receives the access request information from the main body of the access request from the policy execution point, then, obtains all the attributes in the attribute library and the environment attribute library, then, matches the access control policies satisfying the conditions in the policy library, evaluates according to the access control policies, and finally sends the evaluation results to the policy execution point PEP

(3) Policy enforcement point execution decision result: after the policy enforcement node PEP receives the evaluation result, if the return value of the result is true, then, the subject returns the evaluation result to the object and grants the permission to access the object resources. If the evaluation result is false, this access of the principal will be denied and the result will be sent to the principal

It can be seen from the above access control process that the ABAC model authorizes access control decisions based on the attributes of access objects and has nothing to do with the identity information of subjects. Therefore, it can ensure the anonymity of smart home users and ensure that their privacy is not leaked. In the ABAC model, access control policies can be changed according to users' needs. Based on the attributes of access entities, the model can enter fine-grained access control and dynamic authorization, which enhances the scalability of the model and makes it have high application value in smart home scenarios.

4.3. Simulation Experiment

4.3.1. Smart Home Network. A smart home network test platform is realized by FIWARE [17]. FIWARE is an open-source experimental platform of the Internet of things created in Europe, which provides a general API for intelligent

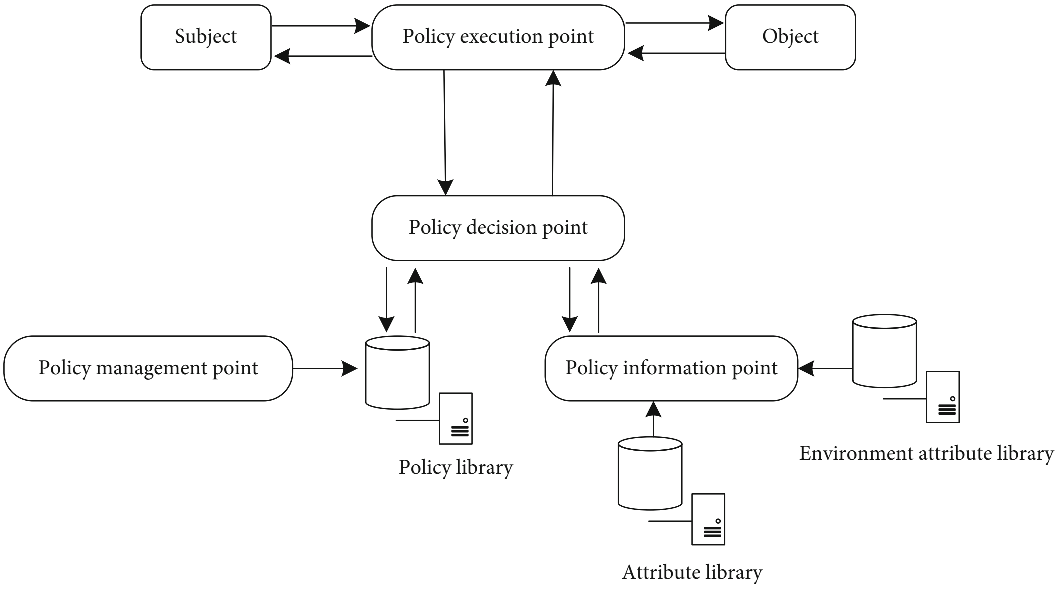

FIGURE 5: ABAC model frame diagram.

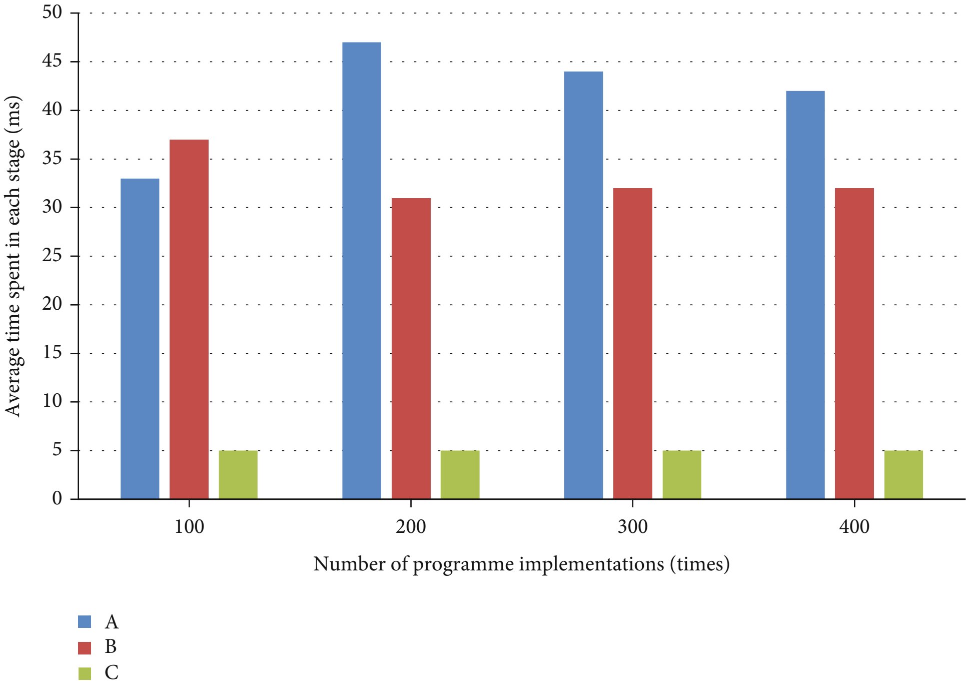

FIGURE 6: Average result of the signature scheme test performed by the mobile terminal device.

application development. The platform integrates many basic components in the smart home network, for example, the integrated temperature, illumination and humidity sensors, and IEEE 802.15.4 radio-integrated antennas. On the smart home network test bench, the sensors are divided into three groups: each group has four FIWARE devices, among which three are smart home terminal devices and one is a router. Using Java to write an independent gateway program, using the MySQL database to store the routing table, resource directory, and data table, each group constitutes an independent smart home network. Device discovery and resource discovery in smart home networks are based on the IEEE 802.15. 4 standard [18]. Each group represents a home, school, or office equipped with smart home equipment in real life.

Firstly, the adaptability of the signature scheme in a smart home environment is analyzed. According to the scheme proposed in this paper, the hardware of the smart home simulation system consists of an intelligent mobile terminal device and a home gateway server. The SM2 threshold group signature scheme is uplink on these devices, and the simulation test results in the following figure are obtained.

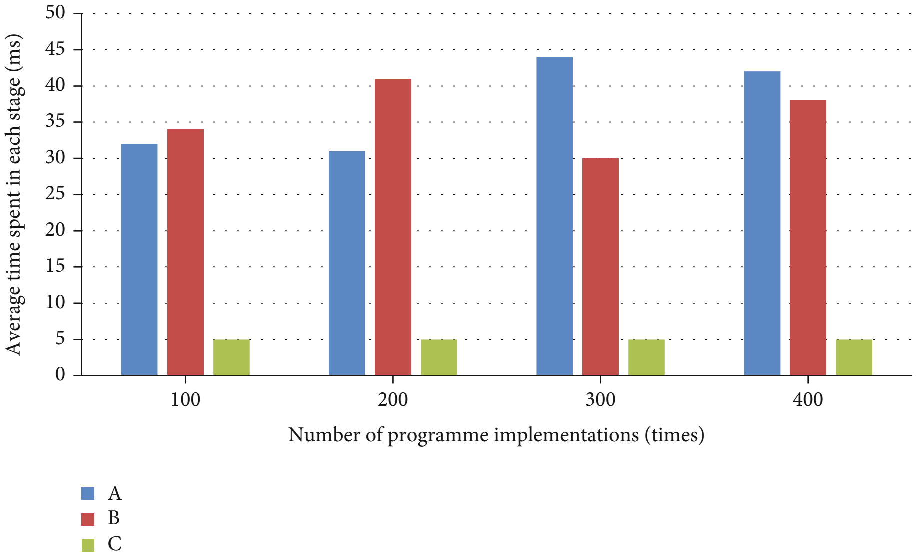

Figure 7: Average results of the signature scheme test performed by the home gateway server.

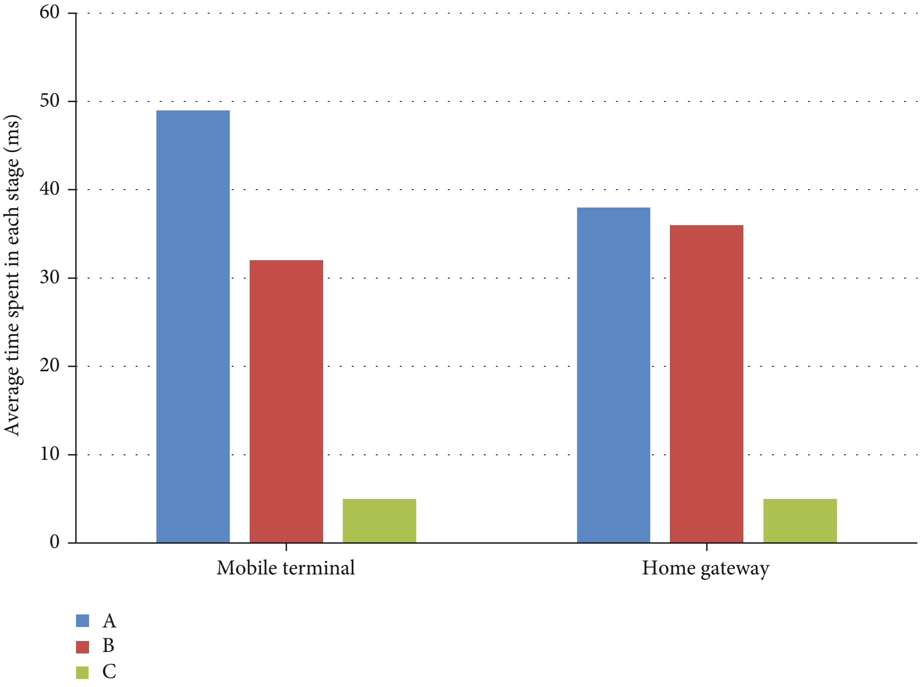

Figure 8: Average results of the signature scheme test performed by various devices in the smart home.

In Figures 6 and 7, the ordinate is the average time spent in different stages of the scheme during execution of 100, 200, 300, and 400 times and the abscissa A, B, and C represent the three stages of key generation, signature generation, and signature verification in the signature scheme, respectively. Figure 8 shows the total average time spent on each of the three phases performed on the two devices.

It can be clearly seen in Figures 6 and 7 that the time spent by the terminal equipment executing each stage of the signature scheme is similar to the average time spent in Figure 8, indicating that the signature scheme has good stability and is within the acceptable time range of practical application scenarios. It can be seen in Figure 8 that the signature scheme proposed in this paper has good performance on the premise of satisfying security characteristics and computational overhead. Therefore, the threshold group signature scheme based on SM2 proposed in this paper can meet the application requirements of smart home scenarios and has a good application prospect.

Next, in order to prove the practicability of the proposed scheme, a smart home access control system based on blockchain is implemented by using the simulation platform. In

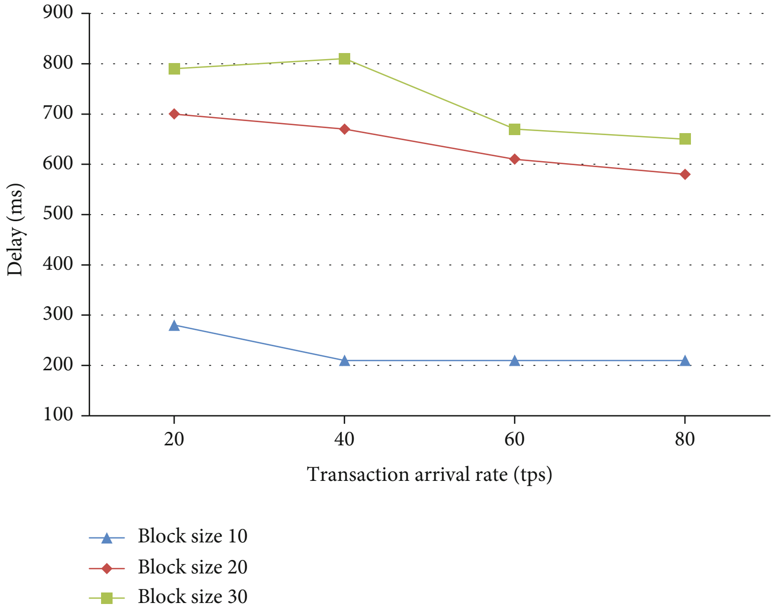

FIGURE 9: Property creation transaction delay.

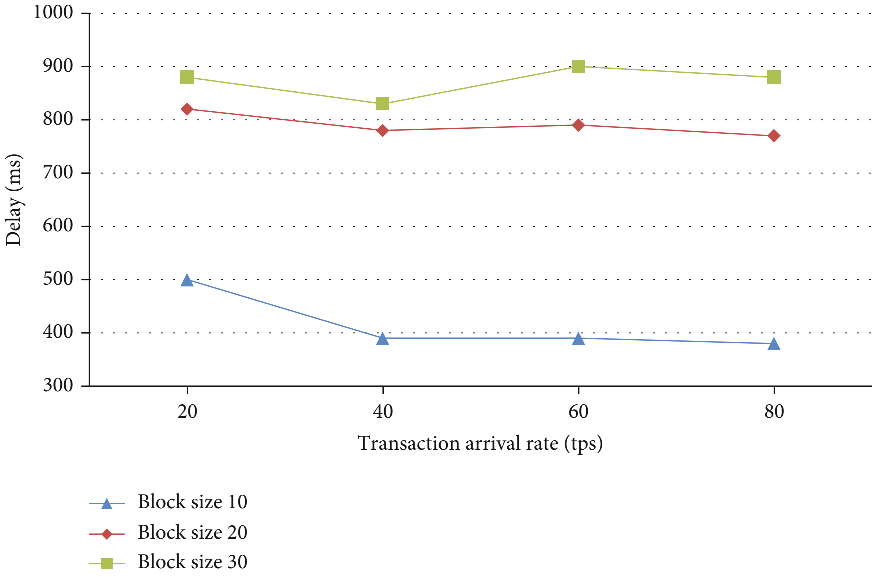

FIGURE 10: Attribute assignment transaction delay.

this section, we first introduce the implementation details, that is, the implementation of blockchain and a smart home platform. Then, the performance of the system is evaluated by simulation experiments.

4.3.2. Experimental Results. In the blockchain experiment, the timeout is set to 1 second. Examine the latency of attribute creation, attribute assignment, and policy creation operations for block size values of 10, 20, and 30 for four different transaction arrival rates (20, 40, 60, and 80 transactions per second).

It can be seen in Figures 9–11 that the delay increases as the block size increases. In Figure 9, if the arrival rate of the attribute generation is 40, the latency increases from 390 milliseconds to 830 milliseconds if the block size increases from 10 to 30. This is because the retained transactions will delay the writing speed of transactions within the blockchain as the block size increases and has to wait longer on the message queue.

Experimental results show that between attribute creation, attribute assignment, and policy creation, attribute assignment takes longer than the other two operations.

The experimental results of the test platform show that the access control performance of the blockchain network can be improved by finding the best parameter values of the blockchain network. The optimal parameters obtained

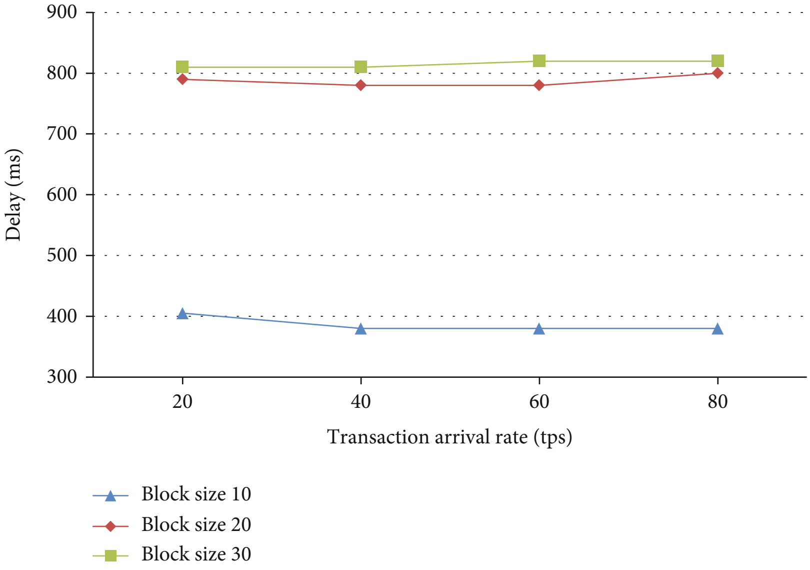

Figure 11: Policy creation transaction delay.

by experiments are block size 20 and 40 transactions per second, and the delay of data resource access is about 1 s.

5. Conclusion

Compared with the public blockchain, the scheme based on Hyperledger Fabric Alliance Chain proposed in this paper can serve smart home resource access requests faster. In addition, the more authentication peer nodes in the endorsement policy, the higher the security level of the system and the greater the communication and computational overhead. By setting appropriate security parameters, the balance between security and practicality can be realized in the smart home access control system. From the simulation results, the access control scheme proposed can meet the practical application requirements within the appropriate security parameters. Future research work will be in-depth study on parameter optimization, and multi-intelligent optimization algorithms will be applied to blockchain and cloud services to improve system performance.

Data Availability

The experimental data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declared that there are no conflicts of interest regarding this work.

References

[1] A. Mukherjee, M. Balachandra, C. Pujari, S. Tiwari, A. Nayar, and S. R. Payyavula, "Unified smart home resource access along with authentication using blockchain technology," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 29–34, 2021.

[2] M. Ammi, S. Alarabi, and E. Benkhelifa, "Customized blockchain-based architecture for secure smart home for lightweight IoT," *Information Processing & Management*, vol. 58, no. 3, article 102482, 2021.

[3] B. E. Sabir, M. Youssfi, O. Bouattane, and H. Allali, "Towards a new model to secure IoT-based smart home mobile agents using blockchain technology," *Engineering, Technology and Applied Science Research*, vol. 10, no. 2, pp. 5441–5447, 2020.

[4] M. Abunaser and A. A. Alkhatib, "Advanced survey of blockchain for the Internet of things smart home," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, pp. 58–62, Amman, Jordan, 2019.

[5] Y. Ren, Y. Leng, J. Qi et al., "Multiple cloud storage mechanism based on blockchain in smart homes," *Future Generation Computer Systems*, vol. 115, pp. 304–313, 2021.

[6] D. Schmelz, K. Pinter, S. Strobl, L. Zhu, P. Niemeier, and T. Grechenig, "Technical mechanics of a trans-border waste flow tracking solution based on blockchain technology," in *2019 IEEE 35th international conference on data engineering workshops (ICDEW)*, pp. 31–36, Macao, China, 2019.

[7] L. Liu and B. Xu, "Research on information security technology based on blockchain," in *2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA)*, pp. 380–384, Chengdu, China, 2018.

[8] A. A. Monrat, O. Schelen, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," *IEEE Access*, vol. 7, pp. 117134–117151, 2019.

[9] X. Zhu, "Research on blockchain consensus mechanism and implementation," *IOP Conference Series: Materials Science and Engineering*, vol. 569, no. 4, p. 042058, 2019.

[10] K. J. Kim and S. P. Hong, "Study on rule-based data protection system using blockchain in P2P distributed networks," *International Journal of Security and its Applications*, vol. 10, no. 11, pp. 201–210, 2016.

[11] S. J. Syscoin, "A peer-to-peer electronic cash system with blockchain-based services for E-business," in *2017 26th*

International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, Canada, 2017.

[12] W. S. Park, D. Y. Hwang, and K. H. Kim, “A TOTP-based two factor authentication scheme for hyperledger fabric blockchain,” in *Tenth International Conference on Ubiquitous and Future Networks (ICUFN).*, pp. 817–819, Prague, Czech Republic, 2018.

[13] P. Thakkar, S. Nathan, and B. Viswanathan, “Performance benchmarking and optimizing hyperledger fabric blockchain platform,” in *2018 IEEE 26th international symposium on modeling, analysis, and simulation of computer and telecommunication systems (MASCOTS)*, pp. 264–276, Milwaukee, WI, USA, 2018.

[14] W. Li, J. Liu, and G. Bai, “High-speed implementation of SM2 based on fast modulus inverse algorithm,” in *2018 China semiconductor technology international conference (CSTIC)*, Shanghai, China, 2018.

[15] H. Tian, X. Li, H. Quan, C. C. Chang, and T. Baker, “A lightweight attribute-based access control scheme for intelligent transportation system with full privacy protection,” *IEEE Sensors Journal*, vol. 21, no. 14, pp. 15793–15806, 2020.

[16] A. A. Jabal, E. Bertino, J. Lobo et al., “Polisma - a framework for learning attribute-based access control policies,” in *Computer Security–ESORICS 2020. ESORICS 2020*, L. Chen, N. Li, K. Liang, and S. Schneider, Eds., vol. 12308 of Lecture Notes in Computer Science, , Springer, Cham, 2020.

[17] M. Fazio, A. Celesti, F. G. Márquez, A. Glikson, and M. Villari, “Exploiting the FIWARE cloud platform to develop a remote patient monitoring system,,” in *2015 IEEE symposium on computers and communication (ISCC)*, pp. 264–270, Larnaca, Cyprus, 2015.

[18] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” in *Advances in Cryptology–EUROCRYPT 2017. EUROCRYPT 2017*, J. S. Coron and J. Nielsen, Eds., vol. 10211 of Lecture Notes in Computer Science, , Springer, Cham, 2017.