Research Article

Research on Multidomain Authentication of IoT Based on Cross-Chain Technology

Dawei Li^{1,2}, Jia Yu,³ Xue Gao,³ and Najla Al-Nabhan⁴

¹School of Computing Engineering, Nanjing Institute of Technology, Nanjing 211167, China

²Energy Research Institute, Nanjing Institute of Technology, Nanjing 211167, China

³State Grid Electric Power Research Institute, Nanjing, China

⁴Department of Computer Science, King Saud University, Riyadh, Saudi Arabia

Correspondence should be addressed to Dawei Li; lidw@njit.edu.cn

Received 22 October 2020; Revised 17 November 2020; Accepted 29 November 2020; Published 10 December 2020

Academic Editor: Zhaoqing Pan

Copyright © 2020 Dawei Li et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Blockchain is an innovated and revolutionized technology, which has attracted wide attention from academia and industry. At present, blockchain has been widely used in certificate management and credential delivery in network access authentication. In a large-scale multidomain Internet of Things (IoT) environment, one of the important issues is cross-domain key sharing and secure data exchange between different IoT. In this paper, aiming at the multidomain authentication requirements of the IoT, this paper introduces the blockchain cross-chain technology into the cross-domain authentication process of the IoT and proposes an effective cross-domain authentication scheme of the IoT based on the improved PBFT algorithm. First, an architecture of blockchain-based cross-domain authentication is proposed. Then, the block data structure is designed in order to enhance the function of access authentication. Third, the authentication process is realized by intelligent contract. The authentication information is encrypted and distributed by a key sharing method to ensure the security of authentication data. Simulation results show that the proposed scheme has significant advantages in security and availability.

1. Introduction

With the rapid development of 5G and other information and communication technologies (ICTs), the intelligence level as well as deployment scale of Internet of Things (IoT) is increased accordingly. In IoT application scenario, a large number of intelligent terminals work together to collect and process data. The wide area interconnection of IoT brings convenience to users; at the same time, it also brings security risks such as wide attack area, fuzzy security boundary, and poor node controllability [1–4].

The access control of terminals is a key aspect in the security of IoT [5]. With the expansion of the scale of the IoT, the secure access of IoT nodes is not limited to the small-scale trusted authentication of a single security domain, but multi security domain interactive authentication scenarios with business association are becoming more and more common [6–9].

In the traditional IoT authentication method based on centralization, there is an authentication center as an authoritative node for key escrow and certificate management. However, in the multidomain authentication scenario of the IoT, it is difficult to find a trusted authentication authority. A secure mechanism is needed to share the credentials in each security domain for cross domains [10–12].

The most common way of cross-domain authentication is to realize distributed public key authentication through digital certificate and PKI technology. But this method often involves complex certificate management process and has a large cost of computing and storage, which is not suitable for the deployment of low-power IoT systems [13].

In recent years, blockchain technology has been widely used in all walks of life and has produced huge economic and social benefits [14]. Especially in the field of IOT authentication [15], there have been many implementation schemes based on blockchain [16–18]. However, in the current

application scenario, each security domain often deploys blockchain system separately, and the blockchain architecture, data structure, and authentication certificate are different. In the large-scale IOT system with multidomain interconnection, there are challenges of authentication data communication and value transfer between public chain, private chain, and alliance chain with different architectures [19–22].

Cross-chain technology is the supporting technology of data asset interconnection and interworking in different blockchain systems. Through the establishment of cross-chain protocol between chains, the cross-domain transmission of data assets or value can be fully trusted. Cross-chain technology provides a feasible solution for the transfer of cross-domain authentication credentials in the IoT.

In order to meet the needs of large-scale multidomain authentication of the IoT, this paper applies the cross-chain technology to the cross-domain authentication certificate transfer, opens up the chain data channel in the authentication system of the IoT, and proposes an effective authentication scheme.

The motivation of the paper is that, on the one hand, the decentralized features of cross chain can decrease the overload of the CA and reduce the problem of single failure; on the other hand, the block chain can transfer cross-domain authentication credentials with the associated blocks in a credible and tamper proof way.

The contributions of the paper are as follows:

- (1) We analyze the security requirements of the IoT and propose a blockchain-based cross-domain authentication architecture.
- (2) We introduce the cross-chain technology into the multidomain authentication process of the IoT and realize the effective cross-domain transmission and use of the authentication certificate.
- (3) We design a block data structure in order to enhance the function of access authentication.
- (4) Based on cross-chain technology and distributed consensus mechanism, we realize the authentication process by intelligent contract.

2. Related Work

Compared with the traditional database-based data management, blockchain is a relatively closed system. At present, most of the security application scenarios based on blockchain use independent blockchain systems, which are isolated from each other and difficult to achieve interconnection and horizontal expansion, which hinders the effective transfer and circulation of digital assets between systems. With the popularity of blockchain applications and the complexity of its functions, more and more cross-chain requirements are proposed [23]. In the field of IoT access authentication, when the authentication requirements span multiple security domains of heterogeneous blockchain systems, the interoperability of cross-chain authentication data and remote authentication is particularly important

[24, 25]. However, there are few multidomain authentication solutions based on cross-chain technology.

Cross-chain technology can be divided into three mechanisms: notary schemes, side chains/relays, and hash locking. Different cross-chain methods are suitable for different application scenarios. The recommended cross-chain technology in multidomain authentication of the IoT is based on the side chain and relay chain [26]. This technology supports lightweight client-side verification. Through smart contract, it verifies the validity of cryptographic hash tree in the cross-chain system to determine the validity of a specific authentication event and state.

In terms of the implementation mechanism of cross-chain technology, Blockstream put forward the concept of pegged sidechain and studied the transfer mechanism between different blockchain assets in 2014 [26]. Jae and Ethan [27] proposed cosmos, an interoperability architecture between blockchains, which can access different blockchains through inter-blockchain communication protocol. In 2018, Joseph and Vitalik [28] proposed the blockchain expansion design mode for the 2-layer expansion of blockchain and designed the plasma cross-chain system framework with the main chain as the tree root and the slave chain as the branch, which has become the research foundation of many cross-chain technologies. Eykholt et al. [14] proposed an enterprise-level parallel cross-chain platform with high scalability. The platform runs smart contracts concurrently through RhoVM virtual machine and name space to realize multichain interoperability.

Cross-chain technology can realize data interoperability and interoperability between different blockchain systems. It is of great practical significance to apply it to the multidomain authentication field of the IoT. However, this research is still in its infancy, and no mature program has yet emerged.

IoT is an open system with distributed deployment, and its access security is particularly important; traditional access authentication is centralized scheme-based PKI [29–31]. At present, most of the common cross-domain authentication protocols of the IoT are based on distributed public key system, which uses digital certificate for identity authentication [32]. For example, literature [33] established the trust link based on the third-party trust CA to realize the cross-domain authentication of PKI. Literature [34] proposed the cross-domain trust model of PKI based on P2P grid network. Literature [13] proposed a public key infrastructure based on blockchain distributed ledger for the first time. On this basis, the follow-up researchers put forward various improvement schemes, such as PB-PKI [29].

The existing multidomain authentication of the IoT is a large-scale deployment of the same type of system, and the cross-domain authentication of heterogeneous systems is rarely involved. Especially for the IOT deployed with different blockchain platforms, the existing cross-domain authentication schemes are difficult to achieve satisfactory authentication effect.

So, aiming at the security issues in cross-domain authentication of IoT, based on cross-chain technology, we

improved the PBFT mechanism using secret sharing protocol and addressed the practical multidomain authentication scheme.

3. Algorithm Description

The basic idea of the proposed algorithm is to improve the traditional PBFT consensus mechanism through identity-based secret sharing algorithm to achieve group authentication for access requests. IBE algorithm is a common public key encryption algorithm in the field of Internet of Things. It can achieve high security strength with short key. As an encryption algorithm, public key and private key appear in pairs, which can only be used in point-to-point encryption and authentication scenarios. When IBE algorithm is applied to the IoT cross-domain distributed authentication scenario, it needs to combine a distributed key management scheme to fragment the single key. In this scheme, a secret sharing algorithm based on Lagrange interpolation is adopted, which encapsulates the key information as the authentication certificate to form a subkey, and each node takes the subkey as the voting basis in the PBFT consensus algorithm. If the node votes in favor, it submits the correct subkey. The number of votes that meet the threshold number indicates that the group authentication has passed.

4. Preparatory Knowledge

IBE public key encryption system takes the character string representing identity as the encryption public key [34, 35]. The algorithm can be implemented by elliptic curve and has the semantic security of adaptive selection ciphertext attack (IND-ID-CCA). The algorithm consists of four algorithms.

- (1) Setup: with the security parameter k , generate the system parameter params and master key. The system parameters determine the plaintext space M and ciphertext space C . The system parameters are published through public channels, while the system master key is only secretly stored by the key generation center (PKG).
- (2) Extract: with params and master key and identity $ID \in \{0, 1\}^*$ as input, the corresponding private key d is returned.
- (3) Encrypt: input params, ID, and plaintext $m \in M$ and output ciphertext $c \in C$.
- (4) Decrypt: input params, ciphertext $c \in C$, and private key d and output plaintext $m \in M$.

5. Authentication Mechanism

5.1. Authentication Scenario. In the scenario, terminals of the IoT are divided into several domains, and each domain has a local blockchain which contains the local authentication information of this domain. There is an alliance blockchain which stores metadata of local authentication data in each domain. If cross-domain authentication is required, the authenticator can read the metadata of the

authenticated terminal from the federation chain to confirm its access rights.

The common scenario of IoT is shown in Figure 1. The left side is two authentication domains, each maintaining a local authentication blockchain, and each domain has three Internet of Things terminals. On the right is the public authentication blockchain, whose form of existence is alliance chain.

When cross-domain interaction is needed, the local blockchain first verifies the identity of the requester. After the verification, the local authentication information is exchanged to the alliance chain through cross-chain technology. According to the authentication strategy and distributed authentication algorithm based PBFT, the public authentication blockchain completes the authentication of the requesting node. After the authentication is passed, the authentication information is recorded, and the authentication information is exchanged to the local chain of the other domain through the cross-chain technology so as to realize the transfer of the authentication certificate. The specific process of certification is described in detail below.

5.2. Cross-Chain Data Exchange. The data transfer between local chain and alliance chain is realized by side chain of cross-chain technology. Side chain is a technology that allows token to exchange assets safely between different blockchains. The side chain is connected with the main chain through a two-way pegging mechanism. After the connection, the assets on the main chain can be operated to a certain extent through the two-way peg technology.

Through side chain technology, digital assets can be transferred from the first blockchain to the second blockchain and can be safely returned from the second blockchain to the first blockchain at a later time point. The first block chain is usually called the main chain, and the second block chain is called the side chain. By connecting different blockchains together, side chain technology extends the technology of single blockchain, realizes the interoperability between accounts, and ensures the controllable sharing of information in the local domain. The advantage of side chain architecture is that the code and data are independent, do not increase the burden of the main chain, and avoid excessive data expansion. It is a natural fragmentation mechanism.

The core of side chain technology is to realize the co-operation and data interaction between the main chain and the slave chain, which is called “two-way peg.” Two-way peg realizes the flow of the same data assets on the main chain and side chain. When the assets on the main chain are locked, the equivalent side chain assets can be released on the side chain. When the assets on the side chain are locked, the equivalent assets on the main chain are released.

There are several ways to achieve two-way peg.

5.2.1. Symmetrical Mechanism. The main chain and side chain have equal data exchange mode. The two directions carry out equivalent simplified payment verification (SPV) to ensure the authenticity of data in a chain. In data

FIGURE 1: The proposed authentication scenario.

exchange, the status of the main chain and side chain is equal, so it is called symmetric two-way peg.

5.2.2. Asymmetric Mechanism. The information between the side chain and the main chain is asymmetric. The users on the side chain can fully verify the main chain, while the data on the main chain need to be verified by SPV when the data on the main chain are transferred to the side chain. In this mode, the verifier of the side chain needs to synchronize with the main chain.

5.2.3. Single Hosting Mode. A trustee is designated on the main chain to realize the information locking, asset synchronization, and unlocking functions when the side chain of the main chain is synchronized.

5.2.4. Joint Hosting Mode. In this mode, there are multiple hosting centers, and cross-chain data exchange is confirmed in a joint way. In order to achieve security, multisignature mechanism is often used.

5.2.5. SPV Mode. The user sends the data to the main chain. After the confirmation of six blocks on the main chain, the information in the ledger is stored as main chain block. The main chain starts the side chain data update by creating SPV verification.

5.2.6. Driving Chain Mode. Users drive the data interaction between the chains, monitor the status of the side chain, and ensure the data consistency through consensus algorithm.

In the cross-domain authentication of power IoT, each authentication domain has its own authentication policy and certificate, which is stored in the distributed ledger of local chain, namely, side chain. The power IoT system composed of multiple authentication domains maintains an authentication chain as the main chain of the system.

5.3. Data Structure. Block is a data structure for storing ledger. The cross-domain authentication credentials recorded in the block have publicly verifiable and unforgeable attributes. In the cross-chain authentication information exchange, the block data structure defines the description specification, security policy, and security level of authentication certificate.

Cross-domain authentication block is composed of header and data part. Header contains several fields, which are (1) the data used to connect the previous block and index the hash value from the parent block; (2) the timestamp to determine the session aging; (3) the random number used for authentication algorithm; and (4) Merkle tree root data that can summarize and verify all transaction data in the block. As a data carrier, block body stores authentication information through Merkle tree. The data structure is illustrated in Figure 2.

Smart contract of local chain calculates hash value of every node's certificate and forms Merkle tree in blocks.

FIGURE 2: The structure of the certified blockchain.

The certificate includes certificate serial number, public key information, issuer, validity period, signature information, domain ID, etc. Nodes in alliance chain store certification information of cross-domain authentication, and all the information is saved in Merkle tree of the block chain.

5.4. Certification Process. The cross-domain authentication process includes registration, authentication request, credential transfer, distributed authentication, and authentication passing, as shown in Figure 3.

5.4.1. Register. In the registration phase, terminal A in local domain A initiates registration according to the unique ID and triggers the smart contract on the local chain.

The system calls the smart contract and returns the registration information encrypted with A's public key, i.e., $\text{Res} = \text{EN}_{\text{Pub}_A}(\text{UUID}||\text{timestamp}||n_1||\text{cert}_A)$, where n_1 is a random number selected by the system.

Terminal A returns the digital signature, $\text{Sig}(\text{UUID}||\text{timestamp}||n_1)$, and completes the three handshake registration interaction processes, and the smart contract on the local chain A is activated and executes registration processing.

FIGURE 3: Access authentication process.

5.4.2. Authentication. When terminal A needs to access resources in remote domain B, terminal A initiates authentication request $\text{Request}(A, B) = \text{EN}_{\text{Pri}_A}(\text{ID}_A || \text{Pub}_A || \text{time_stamp} || \text{business_code})$, which includes local domain ID and remote domain ID, as well as business type.

After the local chain confirms, it initiates the two-way peg with the authentication alliance chain and transmits the authentication request information as well as certificate information of A to the alliance chain synchronously. Thus, the authentication certificate of terminal A and the cross-domain authentication request of A are in the alliance chain.

5.4.3. Verification. The smart contract on the alliance chain performs distributed authentication for the nodes applying for access. Firstly, the nodes meeting the threshold number are selected from the alliance chain to form the authentication group. Secondly, the optimized PBFT consensus algorithm is used for distributed authentication. Finally, the authentication results are stored in the chain. The optimized

PBFT consensus algorithm will be described in detail in the next section.

Trigger the smart contract and store the authentication results on the distributed ledger of the alliance chain. Then, the authentication credential information is transferred to the blockchain B in remote domain B by two-way peg. Therefore, the nodes in remote domain B also have the ability to authenticate A.

5.4.4. Connection Establishment. After node A in area A initiates a remote access request to terminal B in remote domain B, terminal B firstly verifies the request and calls smart contract of blockchain B to authenticate A's access request. Because there are communication permissions between A and B in blockchain B, based on the distributed consensus of the blockchain and the unforgeable security attribute, terminal B is very easy to confirm the identity and authority of terminal A, which can be established after authentication secure communication.

5.5. Optimized PBFT Algorithm. Practical Byzantine fault tolerance (PBFT) is a common consensus algorithm in many blockchain application scenarios. It solves the Byzantine error problem in a limited number of nodes by election, and the algorithm performance can be applied to mainstream IoT scenarios.

The distributed cross-domain authentication process of the IoT based on PBFT algorithm is divided into four steps: request, prepreparation, preparation, and submission, as shown in Figure 4.

In the initialization phase, the key management system generates identity-based encryption keys for each IoT terminal, as follows.

Given a security parameter κ , select the large prime number $p(\kappa\text{bit})$, find a hyper singular elliptic curve $E/GF(p)$ that satisfies the CDH security assumption, and generate the order $q(q > 2^\kappa)$ subgroup $(G, +)$ and its generator P ; bilinear mapping $\hat{e}: G \times G \rightarrow GF(P^2)^*$.

Select one-way hash functions H_1, H_2, H_3 :

$$H_1: \{0, 1\}^* \rightarrow G^*, H_2, H_3: GF(P^2)^* \rightarrow \{0, 1\}^l. \quad (1)$$

Select the master key $s \in Z_q^*$, calculate the system public key $P_{\text{pub}} = sP$, and return the system parameters: $\text{para} = (G, q, P, \hat{e}, H_1, H_2, H_3, P_{\text{pub}})$.

When the IoT terminal with ID as identification in the local domain makes an authentication request to the remote domain, it firstly generates request message by $X = E_{pk}(\text{ID})$, where pk is the public key of ID and $E(\cdot)$ represents the encryption function. The authentication request is transmitted to the master node of the remote domain through the cross-chain technology. The master node runs the smart contract to verify the authenticity of the authentication data transferred across the domain.

After accepting the authentication request, the primary node first finds the legitimate nodes in the security domain to form the authentication group $G = \{P_1, P_2, \dots, P_t\}$. The master node packages the authentication request data and publishes the subauthentication message to the members of the authentication group, and the system enters the prepreparation stage.

The (t, n) secret sharing mechanism is used to generate the subkey. Assuming that the number of members of the authentication group G is n and the authentication threshold is t , if and only if not less than t nodes submit confirmation, the authentication is deemed to have passed.

The subkey generation process is as follows.

Let IBE ciphertext be $C = \langle U, V \rangle = \langle rP, R \oplus H_2(g^r) \rangle$, where $\oplus$ is XOR operation. Choose $t-1$ elements randomly, i.e., $a_1, \dots, a_{t-1} \in Z_p^*$, and let Lagrange interpolation polynomial be $f(x) = sH_1(\text{ID}) + a_1x + a_2x^2 + \dots + a_{t-1}x^{t-1}$; for each voting node, calculate $S_i = f(x_i)$, $1 \leq i \leq n$ and send S_i and $y_i = \hat{e}(S_i, P)$ as subkeys.

Calculate and verify key $U_j = \hat{e}(a_j, P_{\text{pub}})$, where $1 \leq j \leq t-1$ and $U_0 = \hat{e}(sH_1(\text{ID}), P_{\text{pub}})$.

In the preparation stage, all nodes in the authentication group conduct P2P broadcast and exchange their own subkeys with each other. The rule is if the cross-domain authentication request of the IoT terminal is agreed and the

request information is verified, the subkey held by itself will be disclosed. All participating nodes collect the shared subkeys in the network. When a node in the authentication group collects more than the threshold number of subkeys, the authentication key can be recovered by secret sharing algorithm. At this time, the status is set to the submitted state.

Suppose the subkeys are $(x_1, y_1), \dots, (x_t, y_t)$, and let the authorization subset of t members be Φ . Subkey receiving node can be calculated as

$$R' = \prod_{j \in \Phi} \hat{e}(S_j, U)^{C_{0,j}^\Phi}, \quad (2)$$

where $C_{0,j}^\Phi$ is the Lagrange coefficient, defined as: $C_{x,j}^\Phi = \prod_{l \in \Phi, l \neq j} ((x-l)/(j-l)) \in Z_q$. Set $\Phi \subset \{1, 2, \dots, n\}$, $|\Phi| \geq t$.

According to IBE encryption algorithm, $R = V \oplus H_2(R')$.

6. Security Analysis

6.1. Correctness Analysis. If there is authorization subset in access structure Φ , satisfying $|\Phi| \geq t$, then the peer node decrypter can decrypt the ciphertext C to get R according to the shadow secret provided by the member in Φ .

The participant who needs to decrypt R sends the decryption request to the member of Φ and gets the verified shadow secret $\{S_i | i \in \Phi\}$ after the authentication.

Execute bilinear operation of U and S_i ; according to Lagrange interpolation theorem, we have

$$R' = \prod_{j \in \Phi} \hat{e}(S_j, U)^{C_{0,j}^\Phi} = \hat{e}\left(\sum_{j \in \Phi} C_{0,j}^\Phi S_j, U\right) = \hat{e}(D_{\text{ID}}, U). \quad (3)$$

Thus, $R = V \oplus H_2(R')$.

6.2. Security Analysis. The security analysis focuses on several attack types which are common in IoT systems. For example, internal and external data source attack, anti-counterfeiting attacks, mutual authentication, middleman attack, Sybil attack, generation attack, single point failure, and so on.

6.2.1. Anti-Internal and Anti-External Data Source Attacks.

Through the double-layer structure of local chain and alliance chain, data t_{pub} in the domain are stored in the local chain, and only metadata m_{pub} of local block are stored in the alliance chain, which can be controlled and retrieved through the smart contract using hash function $m_{\text{pub}} = H(t_{\text{pub}})$. The feature of this structure is that the searcher can query and parse the authentication information through metadata specification and get the results that can be publicly verified but cannot get the detailed data, thus protecting the sensitive information in the domain. In addition, the alliance chain uses hash function and other cryptographies to ensure data security and to prevent tampering by illegal users.

FIGURE 4: The core stages of consensus algorithm.

6.2.2. Anticounterfeiting Attack. The proposed scheme-based IBE threshold secret sharing encryption system can obtain high security with short key length. The digital certificates are encrypted and stored in distributed ledgers; because of the characteristics of blockchain, it is easy to verify the integrity of certificate. When the authentication group votes for distributed access authentication, the cross-domain authentication key can be calculated only when the adversary obtained more than the threshold number of subkeys, and the attack of malicious nodes can be effectively prevented as long as the threshold t is controlled within a reasonable range.

6.2.3. Antireplay Attack. Replay attack is one of the common attacks in IOT access authentication. By intercepting and resending the information, the adversary can cheat the system. There are three forms of replay attack: one is direct replay, that is, replay to the original verification end; the second is reverse replay, which replays the message originally sent to the receiver to the sender; the third is the third-party replay, which replays messages to other verifiers in the domain. In the scheme, there are timestamps and serial numbers as the basis of message freshness in different stages, such as cross-domain request, intradomain agent encapsulation, cross-domain authentication, etc. If the system finds that there are random replay numbers used before in the message, it can identify replay attacks easily.

6.2.4. Anti-Sybil Attack. In Sybil attacks, attackers rely on a single node with multiple identities and control most nodes of the system to gain the advantage of voting, which is a common attack in cooperative IOT scenarios. In the proposed scheme, the blockchain is a distributed database that only writes and does not delete. Through redundant data of multiple nodes, network security and nontamperability can be achieved. Multiple identity information of attacking nodes can be easily found by consensus algorithm.

In this scheme, the original PBFT consensus algorithm is improved so that the weight of verifier's voting corresponds to its historical trust value. When the threshold is set to be greater than $2/3$ of the number of nodes, it can effectively resist witch attacks. In addition, the verification message U_j

TABLE 1: Experimental system configuration.

Item	Configuration parameter
Blockchain platform	Hyper ledger Fabric
Docker version	18.06
Kubernetes	1.9
Operation system	CentOS 7
Authentication station	Intel i7 CPU 16 GB RAM
IoT terminal (type 1)	Raspberry pie 3b+ 1 GB LPDDR2

of voting broadcast in the proposed scheme can also effectively prevent witch attack.

7. Simulation Analysis

The proposed algorithm is based on alliance blockchain, which requires all the nodes and users to be authenticated and authorized. For example, there are ECert (Enrollment Cert), TCert (Transaction Cert), and TLSCert (Transport Layer Security Cert) integrated by CA of Membership component of Hyperledger Fabric. The ECert certificate is used for identity authentication, which can confirm the identity of nodes and users when logging in the system. TCert certificate is used for signature and verification of transactions. Each transaction contains the signature and transaction certificate of the sender. To ensure that the third party cannot trace the specific sender from the transaction certificate, different TCert certificates can be used for each transaction. TLSCert certificate is used for SSL/TLS communication between system components.

In the simulation environment, multiple x86 servers are used to simulate multiple blockchain nodes in the security domains. Each server is deployed with Hyperledger alliance chain system instance, and the data exchange between multiple instances is realized through cross chain. Each server is interconnected with its IoT terminals. The specific configuration parameters of the system are shown in Table 1.

The simulation environment is the application scenario of the IoT for video capture and monitoring, and the terminal is the camera. The remote camera must pass the cross-domain authentication before sharing data. The authentication scheme is the multidomain authentication scheme based on cross chain proposed above. The simulation topology is shown in Figure 5. Among them, Figure 5(a) shows the network connection mode. The four terminals belong to four authentication domains, respectively, and are connected through switches. The authentication application server is set on the uplink network node and managed and configured by the configuration terminal. Figure 5(b) shows the physical device diagram, including the IoT video terminal, authentication node, and authentication server.

Delay is an important indicator of the efficiency of IoT terminal multidomain access authentication, which directly affects the performance of the upper business system.

We use the scheme which is proposed by Chen et al. in literature [36] as a comparative scheme. Chen's scheme combines the key sharing and distribution protocol in secure multiparty computing with Hyperledger platform and addresses a trusted access authentication scheme for power IoT

FIGURE 5: Logical architecture and physical composition of the simulation IoT. (a) Logical architecture. (b) Physical composition.

FIGURE 6: Certification time curve.

terminals. We simulate the system of literature [36] and the proposed cross-chain system in the same environment. The simulation results are shown in Figure 6. From the simulation data, we can see that with the increase of concurrent access requests, the total delay of authentication presents an increasing trend. When the number of nodes increases from 0 to 12, the total delay increases from 2000 ms to 4000 ms. From the horizontal comparison of the three schemes, when the number of concurrent requests exceeds 3, the proposed scheme begins to have performance advantages, that is, in each concurrency level, the proposed scheme is better than the comparison scheme.

In terms of performance, we tested the CPU load in the experimental environment, and the test results are shown in Figure 7. When the number of concurrent nodes is from 0 to 15, the CPU load in the scheme proposed in this paper and in reference [36] increases to about 80%. The difference is that

the growth rate of the proposed scheme is slower than that of the comparison scheme. For example, under the condition of less than 5 concurrent nodes, the CPU load of the proposed scheme is less than 5%, but the load of the comparison scheme has increased to 60%. Obviously, the proposed scheme has advantages in the occupation of system resources.

Figure 8 shows the relationship between authentication threshold size and authentication delay. Generally, the larger the threshold value is, the more the legitimate nodes are required for authorization and credit endorsement, and the system security will be improved accordingly. However, the increase of information interaction between nodes in the system with large threshold will directly lead to the increase of authentication delay. In this experiment, the proposed scheme and the contrast scheme have the same change trend. About 10% of the proposed scheme is slightly better than the contrast scheme.

FIGURE 7: CPU load curve.

FIGURE 8: The impact of certification group size.

FIGURE 9: Block generation curve.

An important evaluation index in blockchain system is block speed, which is often associated with TPS. However, from the perspective of blockchain system performance, Figure 9 shows the time of block output under different blockchain heights. It can be seen that with the increase of the height of the blockchain, the retrieval and processing efficiency of the data on the chain decreases, leading to an upward trend in the time delay. Due to the improvement and optimization of the PBFT consensus mechanism, the reduction of the block speed is acceptable.

8. Conclusions

In this paper, a cross-domain authentication method and a model for distributed shared authentication factors are constructed by using the double blockchain structure. The scheme stores authentication data in untouchable blockchains and shares them through public alliance chains. It has high security and good system stability. It can be directly deployed in existing systems and is compatible with local systems. On the basis of ensuring security, it realizes the interoperability of cross-domain terminals.

Further research is to improve the consensus mechanism, improve the authentication efficiency, and adapt to 5G and other new IoT application scenarios. In addition, for the authentication mechanism, distributed identity (DID) and zero trust principle will be added to realize a more flexible authentication mechanism.

Data Availability

The processed data required to reproduce these findings cannot be shared at this time as the data also form part of an ongoing study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research was funded by the Talent Start-Up Project of Nanjing Institute of Technology (YKJ201721) and Natural Science Foundation of Colleges in Jiangsu Province (19KJB520036). The authors extend their appreciation to the Deanship of Scientific Research at King Saud University for funding this work through research group no. RG-1441-331.

References

- [1] B. Al-Otaibi, N. Al-Nabhan, and Y. Tian, "Privacy-preserving vehicular rogue node detection scheme for fog computing," *Sensors*, vol. 19, no. 4, 2019.
- [2] R. Aljably, Y. Tian, and M. Al-Rodhaan, "Preserving privacy in multimedia social networks using machine learning anomaly detection," *Security and Communication Networks*, vol. 2020, Article ID 5874935, 14 pages, 2020.
- [3] Y. Tian, M. M. Kaleemullah, M. A. Rodhaan, B. Song, A. Al-Dhelaan, and T. Ma, "A privacy preserving location service for cloud-of-things system," *Journal of Parallel and Distributed Computing*, vol. 123, pp. 215–222, 2019.
- [4] Y. Tian, B. Song, M. A. Rodhaan et al., "A stochastic location privacy protection scheme for edge computing," *Mathematical Biosciences and Engineering*, vol. 17, no. 3, pp. 2636–2649, 2020.
- [5] L. Zhang, H. Li, L. Sun, Z. Shi, and Y. He, "Poster: towards fully distributed user authentication with blockchain," in *Proceedings of the 2017 IEEE Symposium on Privacy-Aware Computing (PAC)*, Washington, DC, USA, August 2017.
- [6] O. Abdulkader, A. M. Bamhdi, V. Thayanathan, F. Elbouraey, and B. Al-Ghamdi, "A lightweight blockchain based cybersecurity for IoT environments," in *Proceedings of the The 6th IEEE International Conference on Cyber Security and Cloud Computing (IEEE CSCloud 2019)*, Paris, France, June 2019.
- [7] W. N. Qian, Q. F. Shao, Y. C. Zhu, C. Q. Jin, and A. Y. Zhou, "Research problems and methods in blockchain and trusted data management," *Journal of Software*, vol. 29, no. 1, pp. 150–159, 2018.
- [8] T. Ma, H. Rong, Y. Hao, J. Cao, Y. Tian, and M. A. Al-Rodhaan, "A novel sentiment polarity detection framework for Chinese," *IEEE Transactions on Affective Computing*, vol. 99, p. 1, 2019.
- [9] B. Song, et al., "A two-stage approach for task and resource management in multimedia cloud environment," *Computing*, vol. 98, no. 1–1, pp. 119–145, 2016.
- [10] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *Proceedings of the 2018 27th International Conference on Computer Communication and Networks (ICCCN)*, Hangzhou, China, July 2018.
- [11] Z. Liehuang, G. Feng, and S. Meng, "Survey on privacy preserving techniques for blockchain technology," *Journal of Computer Research and Development*, vol. 54, no. 10, pp. 2170–2186, 2017.
- [12] G. L. Millan, M. G. Perez, G. M. Perez, and A. F. G. Skarmeta, "PKI-based trust management in inter-domain scenarios," *Computers & Security*, vol. 29, no. 2, pp. 278–290, 2010.
- [13] C. Fromknecht, D. Velicanu, and S. Yakoubov, "CertCoin: a NameCoin based decentralized authentication system," 2014, <http://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf>.
- [14] E. Eykholt, L. Meredith, and J. Denman, "RChain architecture documentation," 2017, <https://media.readthedocs.org/pdf/rchain-architecture/stable/rchain-architecture.pdf>.
- [15] M. Samaniego, U. Jamsrandorj, and R. Deters, "Blockchain as a service for IoT," in *Proceedings of the 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, Chengdu, China, December 2016.
- [16] A. Ouaddah, A. Abou Elkalim, and A. Ait Ouahman, "FairAccess: a new Blockchain-based access control framework for the internet of things," *Security and Communication Networks*, vol. 9, no. 18, pp. 5943–5964, 2016.
- [17] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an internet of things environment," *The Journal of Supercomputing*, vol. 73, no. 3, pp. 1152–1167, 2017.
- [18] X. Chen, X. Hu, Y. Li, X. Gao, and D. Li, "A blockchain based access authentication scheme of energy internet," in *Proceedings of the 2018 2nd IEEE Conference on Energy Internet and Energy System Integration (EI2)*, Beijing, China, October 2018.
- [19] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the internet of

- things: a comprehensive survey,” *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2019.
- [20] A. Mohammed, V. Potdar, and L. Yang, “Key factors affecting blockchain adoption in organizations,” in *Big Data and Security. ICBDS 2019. Communications in Computer and Information Science* Springer, Singapore, 2020.
 - [21] C. Y. Guan Zhenyu, D. Li, W. Liu, and D. Yu, “A cross-domain authentication scheme for Internet of vehicles based on blockchain,” *Cyberspace Security*, vol. 11, no. 9, p. 8, 2020.
 - [22] A. Moinet, B. Darties, and J. L. Baril, “Blockchain based trust & authentication for decentralized sensor networks,” 2017, <https://arxiv.org/pdf/1706.01730.pdf>.
 - [23] S. Guo, X. Hu, S. Guo, X. Qiu, and F. Qi, “Blockchain meets edge computing: a distributed and trusted authentication system,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 3, pp. 1972–1983, 2020.
 - [24] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, G. Linchao, and H. Kai, “A multiple blockchains architecture on inter-blockchain communication,” in *Proceedings of the 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C)*, Lisbon, Portugal, July 2018.
 - [25] D. Li and X. Gao, “A blockchain based terminal security of IoT,” *ICBDS 2019, Communications in Computer and Information Science*, Springer, Singapore, pp. 445–454, 2020.
 - [26] B. A. Sidechains, et al., Enabling blockchain innovations with pegged sidechains,” 2014, <https://blockstream.com/sidechains.pdf>.
 - [27] K. Jae and B. Ethan, “Cosmos: a network of distributed ledgers,” 2020, <https://github.com/cosmos/cosmos/blob/master/WHITEPAPER.md>.
 - [28] P. Joseph and B. Vitalik, “Plasma: scalable autonomous smart contracts,” 2018, <https://plasma.io/plasma.pdf>.
 - [29] L. Axon, “Privacy-awareness in blockchain-based PKI,” 2015, https://ora.ox.ac.uk/objects/uuid:f8377b69-599b-4cae-8df0-f0cded53e63b/download_file?file_format=pdf&safe_filename=21-15.pdf&type_of_work=Working+paper.
 - [30] S. Matsumoto and R. M. Reischuk, “IKP: turning a PKI around with decentralized automated incentives,” in *Proceedings of the 2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, California, May 2017.
 - [31] H. Orman, “Blockchain: the emperors new PKI?” *IEEE Internet Computing*, vol. 22, no. 2, pp. 23–28, 2018.
 - [32] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, “A comprehensive survey of blockchain: from theory to IoT applications and beyond,” *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8114–8154, 2019.
 - [33] Z. Wen-Fang, W. Xiao-Min, G. Wei, and H. E. Da-Ke, “An efficient inter-enterprise authentication scheme for VE based on the elliptic curve cryptosystem,” *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol. 42, no. 6, pp. 1095–1102, 2014.
 - [34] X. M. Lu and D. G. Feng, “An identity-based authentication model for multi-domain grids,” *Tien Tzu Hsueh Pao/Acta Electronica Sinica*, vol. 34, pp. 577–582, 2006.
 - [35] B. Yang, G. Q. Chen, and Y. H. Sun, “Research of a new identity-based authentication model for multi-domain,” *Computer Security*, vol. 1, no. 8, pp. 15–18, 2010.
 - [36] X. Chen, X. Xiaohai, and G. Feng, “Research on distributed authentication of power IoT based on hyperledger blockchain,” *Application of Electronic Technique*, vol. 45, no. 5, pp. 57–60, 2019.