A Cross-Domain Authentication Scheme Based Master-Slave Chain in Edge Computing

Zhiyuan Li(✉) and Zhenjiang Zhang

Department of Electronic and Information Engineering, Key Laboratory of Communication and Information Systems, Beijing Municipal Commission of Education, Beijing Jiaotong University, Beijing 100044, China

{19120091,zhangzhenjiang}@bjtu.edu.cn

Abstract. As an emerging technology, edge computing can solve the problem of limited computing resources of IoT devices under the premise of lower latency. However, the existing mobile edge computing architecture cannot well solve the security problem of the identity authentication of the terminal device. In particular, the cross-domain authentication of the device cannot be completed efficiently when the device is switched between different IoT domains. To address these challenging issues, in this article, a lightweight edge computing cross-domain identity authentication scheme which combines edge computing with blockchain based on master-slave chain is proposed. The scheme uses the consortium blockchain as the master chain, that is, a decentralized authentication platform, realizes cross-domain authentication when the device switches domains, and can also solve the single point of failure problem of traditional authentication. The slave chain is maintained by edge computing nodes and terminal devices in each domain. When devices in the domain are mutually authenticated, the efficiency of authentication can be improved. During authentication, ring signature technology is used to ensure the security of the system, and at the same time, it can effectively save the storage space of the blockchain. Finally, the performance evaluation and security analysis of this scheme have been carried out to prove the safety and effectiveness of our scheme.

Keywords: Edge Computing · Master-slave chain · Ring Signature · Cross-domain authentication

1 Introduction

The appearance of edge computing can share the computing pressure of terminal devices, improve the quality of service (QoS), and respond to users' needs more quickly. However, the security problems caused by edge computing can not be ignored. Specifically, in the current edge computing system framework, edge node deployment is very flexible, and part of terminal device movement in the area covered by edge node is common. This brings new challenges to maintaining the security of equipment in the system and preventing it from external attacks [1].

D.-J. Deng et al. (Eds.): SGIoT 2022, LNICST 497, pp. 48–57, 2023.
https://doi.org/10.1007/978-3-031-31275-5_5

Identity authentication plays an important role in ensuring the safe operation of the whole system. In the current mature cloud computing architecture, cloud location is relatively fixed and centralized, which is convenient for cloud service providers to strictly protect cloud infrastructure and network [2]. However, the existing mature cloud computing security solutions cannot be directly extended to edge computing because the deployment characteristics and operating environment of edge computing are quite different from cloud computing.

Blockchains have a specially designed distributed ledger structure that connects blocks in chronological order. All nodes in a decentralized environment share and maintain the saved data. The main advantages of blockchain are decentralization, open autonomy and anonymous traceability [3]. However, the existing blockchain authentication scheme is not efficient and vulnerable to external threats.

The primary goal of this paper is to propose a cross-domain authentication scheme based on blockchain in edge computing environments. The main contributions of this paper are as follows:

1. An efficient cross-domain authentication scheme is designed in which blockchain is used to replace trusted third parties and can resist single point of failure. Specifically, a master-slave blockchain architecture is designed to store certificate information for devices and assist in cross-domain authentication. Slave chains are used to maintain intra-domain devices and implement intra-domain authentication.
2. Based on this scheme, ring signature technology is used to guarantee the validity of authentication, which improves the verification efficiency of each node in the consensus stage of block generation. Effectively resist malicious attacks inside the system, for the authentication process, can trace the source of the signer.
3. Security analysis and extensive performance evaluations demonstrate the effectiveness and the efficiency of our proposed schemes. Specifically, on the premise of realizing multiple security indexes and resisting threat attack, the authentication performance of our scheme is excellent.

The remainder of this article is organized as follows. Section 2 presents the related work of authentication. In Sect. 3, we describe the master-slave architecture. Detailed authentication scheme based on master-slave chain is proposed in Sect. 4. The security analysis and performance are described in Sect. 5. Section 6 is the conclusion.

2 Related Work

In view of the identity authentication technology of edge computing, some improved authentication schemes applied to edge are proposed based on joint cloud computing and P2P computing. For example, Donald et al. designed a centralized authentication mechanism for mobile cloud computing [4], but this method requires authentication services to be accessible all the time, resulting in limited availability. AMOR et al. proposed an authentication system that allows any fog computing user and fog node to authenticate each other [5], but this system forces all nodes to store the certificate information of all users in the trusted domain. Shouhuai et al. put forward the concept

of situational authentication [6], based on different time, place and interacting objects such as situational use different authentication methods. However, these schemes usually need to be connected to a centralized authentication server, so the performance can be improved to some extent.

At present, with the maturity of blockchain technology, it is a research idea to combine blockchain to realize trusted authentication. In [7, 8], Satoshi Nakamoto proposed a decentralized peer-to-peer (P2P) network platform that verifies the integrity and validity of the network through computationally intensive tasks such as proof of work. In [9], Almadhoun et al. applied blockchain authentication to iot scenarios. In [10], Dorri et al. proposed the application of blockchain technology to protect Internet of Things security and privacy technology in smart home scenarios. In [11], Li et al. applied blockchain to large-scale data storage and protection. In [12], Bao et al. constructed a three-tier security authentication architecture based on blockchain. In [13], Zhouglin et al. proposed a security authentication scheme for 5G super-dense network based on block chain to solve the identity authentication problem of mobile edge computing. In [14], Wang et al. proposed a cross-domain authentication model based on blockchain in a distributed environment. However, these studies do not put forward higher requirements for the performance of the system, which cannot meet the real-time requirements of edge computing scenarios.

3 System Architecture

According to the background proposed in Sect. 1, the edge computing authentication architecture based on the master-slave chain is shown in Fig. 1. The architecture is a two-tier architecture. The upper layer consists of multiple edge computing nodes to form a consortium chain for device management; the lower layer consists of edge computing nodes and devices distributed in different domains. The edge computing nodes in the domain form a blockchain to assist devices to achieve intra-domain authentication and cross-domain authentication. The functions of each part are described as follows:

1. Master chain node: Record the device certificate and other information on the blockchain after reaching a consensus. Therefore, when the device sends an authentication request, the query function is provided through the smart contract.
2. Slave chain node: Realize the management of the devices in the domain, and write the information into the blockchain through the consensus mechanism. It communicates with the master node and assist the device with authentication.
3. Device: Implement active application to join a domain and complete the identity registration and authentication process.

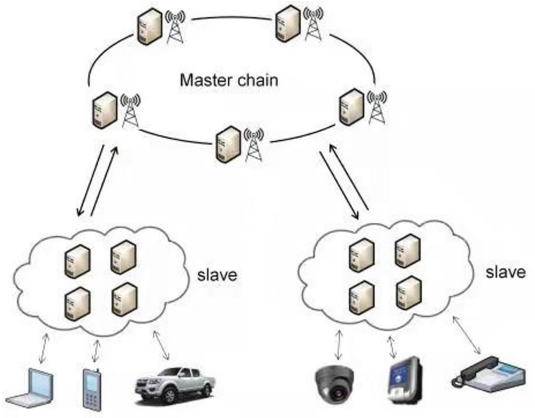

Fig. 1. Overview of the master-slave chain system architecture

4 Proposed Authentication Scheme Based on Master-Slave Chain

This section proposes the detailed process of device registration, intra-domain authentication and cross-domain authentication based on the master-slave chain system architecture. All the used notations are listed in Table 1.

Table 1. Notation description

Parameters	Description
d_{ij}	The j-th device in domain i
SE_j^i	The j-th slave chain edge server in domain i
ME_i	The i-th master chain edge server
ID_{ij}	Identity of d_{ij}
ID_{sij}	Identity of SE_j^i
SK_{ij}	Secret key of d_{ij}
SK_{sij}	Secret key of SE_j^i
SK_{mij}	Secret key of ME_i
PK_{ij}	Public key of d_{ij}
PK_{sij}	Public key of SE_j^i
PK_{dij}	Public key of ME_i
K	The key for the temporary session
Ring{*}	2n + 1 tuple of the ring signature
TS	Timestamp

4.1 Device Registration Process

If a new device wants to join an edge computing domain, it needs to send a request to a nearby edge computing node, as shown in Fig. 2. The process is as follows:

1. Apply to SE_j^i. A new d_{ij} sends ID_{dij} and PK_{dij} signed by SK_{dij} to SE_j^i, and SE_j^i verifies whether d_{ij} can join the domain. The registration result is then sent to ME_i and d_{ij}. Finally, the result is written to the blockchain.
2. ME_i Stores authentication information. After receiving the ID_{dij} sent by SE_j^i, ME_i will query whether the d_{ij} is a newly added device, then bind ID_{dij} and ID_{Sij} into the blockchain. If the device is moved from another domain, modify the binding information between d_{ij} and ME_i.
3. Check ID_{Sij}. After ID_{dij} receives ID_{Sij} sent by the SE_j^i and ME_i, the authentication of the slave chain is completed by comparison.

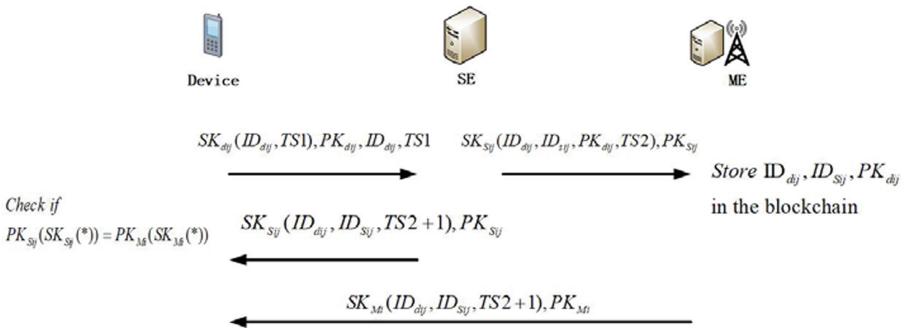

Fig. 2. Registration process for a new device

4.2 Intra-domain Authentication Process

After the registration is completed, the device can achieve mutual authentication with another device through the slave chain node in the domain as required, as shown in Fig. 3. The certification process is as follows:

1. Apply to SE_j^i. d_{ij} Sends ID_{dij} and ID_{dik} to SE_j^i through PK_{Sij} encryption, and applies for authentication with d_{ik}.
2. Send to d_{ik}. SE_j^i checks whether d_{ij} and d_{ik} are successfully registered devices in this domain. If d_{ik} is not a device in this domain, apply for cross-domain authentication to ME_i. This part is explained in cross-domain authentication. If d_{ik} is a device in this domain. Then ID_{dij} and PK_{dij} are encrypted by PK_{dik} and sent to d_{ij}.
3. Key agreement between d_{ij} and d_{ik}. d_{ik} Generates a session key K randomly, and encrypts ID_{dik} and K by PK_{dij} and sends it to d_{ij}. Complete the authentication of two devices in the domain.

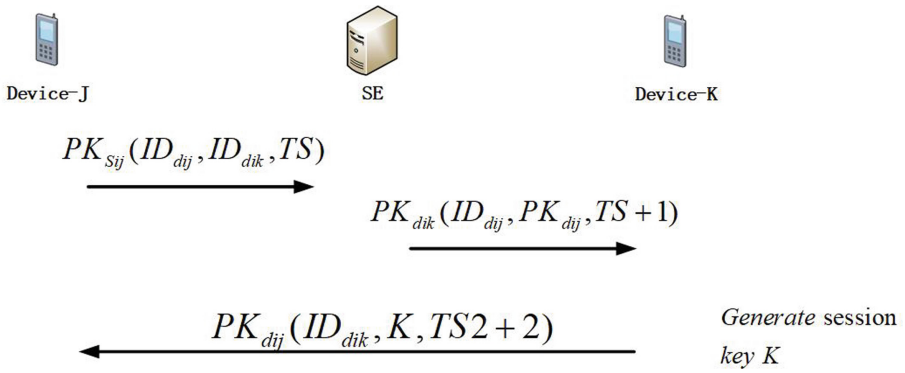

Fig. 3. Intra-domain authentication process between two devices

4.3 Cross-Domain Authentication Process

If the registered device wants to request data across domains, it needs the assistance of the slave chain node to complete the communication with the master chain. After that, the master chain node sends a request to the target device, as shown in Fig. 4. In the process of cross-domain authentication, the ring signature can realize the anonymity of the request initiator under the premise of ensuring the correctness of the signature. The specific certification process is as follows:

1. d_{ij} Applies to SE_j^i. Similar to the intra-domain authentication step 1, d_{ij} sends the ID_{dmn} and request *message*1 encrypted by PK_{Sij} to SE_j^i.
2. SE_j^i Generates ring signature. If d_{mn} is found not in this domain after the query, a ring signature will be generated to ensure the anonymity of d_{ij}. The process is as follows:

   a. Generate a symmetric k from *message*1 through a hash function:

   $$\mathrm{k} = hash(\mathrm{message1}) \tag{1}$$

   b. Generate a random number r.
   c. Randomly generate n-1 values $\{x_1, x_2, \ldots, x_{n-1}\}$. Use the public keys of other n-1 slave chain nodes to encrypt separately, and calculate $y_i = PK_i(x_i)$. Aggregate to get $\{y_1, y_2, \ldots, y_{n-1}\}$.
   d. Substitute k, r and $\{y_1, y_2, \ldots, y_{n-1}, y_n\}$ into the function $C_{k,r}()$ to solve for y_n.

   $$\mathrm{C}_{k,r}(y_1, y_2, \ldots, y_n) = r \tag{2}$$

   The solution process is as follows:

$$\mathrm{C}_{k,r}(y_1, y_2, \ldots, y_n) = \mathrm{E}_k(y_n \oplus E_k(y_{n-1} \oplus E_k(\cdots \oplus E_k(y_1 \oplus r)\ldots))) = r$$

$$y_n \oplus E_k(y_{n-1} \oplus E_k(\cdots \oplus E_k(y_1 \oplus r)\ldots)) = D_k(r)$$

$$y_n = D_k(r) \oplus E_k(y_{n-1} \oplus E_k(\cdots \oplus E_k(y_1 \oplus r)\ldots))$$

E_k means use k for encryption, D_k means use k for decryption.

e. Decrypt y_n through SK_{Sij} to get $x_n = SK_{Sij}(y_n)$
f. The obtained 2n + 1 tuple $Ring\{PK_1, PK_2, \ldots, PK_n; r; x_1, x_2, \ldots, x_n\}$ is the result of the ring signature.

3. SE_j^i sends $Ring\{*\}$, ID_{dmn} and $message1$ to ME_k. And ME_k sends the information encrypted by PK_{Smn} to SE_n^m.
4. SE_n^m verifies ring signature. Verification of the ring signature result can determine whether the signature is correct, and the sender of the message cannot be determined. The verification process is as follows:

   a. Encrypt y_i through PK_i to get $y_i = PK_i(X_i)$. Therefore, it can be obtained $\{y_1, y_2, \ldots, y_n\}$.
   b. Substitute $message1$ into Eq. (1) to get k.
   c. Verify the Eq. (2) holds.

5. SE_n^m sends request to d_{mn}. After completing the ring signature verification, SE_n^m sends the information encrypted by PK_{dmn} to d_{mn}.
6. d_{mn} replies to request. d_{mn} Generates a response $message2$ and sends $message2$ back through the above steps.

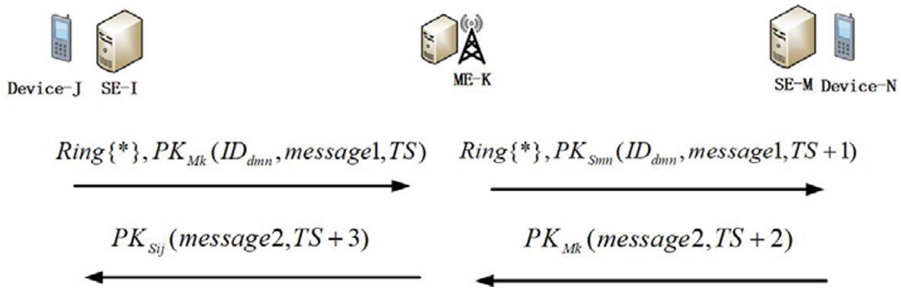

Fig. 4. Cross-domain authentication process between two devices

5 Security and Performance

In this section, the performance and security of the proposed master-slave chain authentication scheme will be analyzed. The feasibility of the scheme will be evaluated by comparing the schemes in other references.

5.1 Performance Evaluation

This section compares the computational overheads of the other three references for performance analysis. The overheads of different authentication schemes are shown in

Table 2. The values in the table represent the cumulative operation times of a certain operation.

Table 2. Calculation cost comparison

Scheme	Digital Signature and Verification	Hash Operation	Public Key Encryption and Decryption	Bilinear Pair	Exponential Operation
[9]	2	4	4	6	4
[11]	6	2	8	2	8
[12]	8	3	4	2	4
Our Scheme	5	2	7	0	3

According to the data in Table 2, our scheme performs less times for some operations with high computational cost (e.g. bilinear pair and exponential operation). To sum up, the implementation efficiency of our scheme is higher than that of other schemes.

5.2 Security Analysis

This paper analyzes the impact of various common attack methods on this scheme, and compares other reference schemes, as shown in Table 3. Through analysis, it is concluded that the safety indicators listed in this paper can be realized in our scheme. The specific analysis contents are as follows:

1. Anonymity: This scheme uses ring signatures to ensure that the verifier cannot determine the sender of the message on the premise of ensuring the accuracy of the information.
2. Mutual authentication: we use the master chain node to realize the mutual authentication between the slave chain node and the device when the device is registered. In the identity authentication stage, the mutual authentication between different devices is realized by using the slave chain nodes.
3. Message substitution: In the registration phase, the information of the device is digitally signed to ensure that it is not tampered with by attackers during the transmission process.
4. Cross-domain authentication: This article uses a two-tier blockchain to ensure efficient cross-domain authentication between devices belonging to different IoT domains.
5. Data security: Before the message is transmitted, the asymmetric key will be generated through the elliptic curve, and the public key will be transmitted through the master-slave chain. After that, the two sides negotiate the session key and encrypt the message to ensure the security of data transmission.

6. Message replay: A timestamp is added to each transmitted datagram to prevent frequent message sending and to ensure that the entire architecture is resistant to message replay attacks.

Table 3. Security comparison of different schemes

Attacks	[9]	[11]	[12]	Our Scheme
Anonymity	×	×	×	√
Mutual authentication	×	×	√	√
Message substitution	√	√	√	√
Cross-domain authentication	×	√	×	√
Data security	√	√	√	√
Message replay	√	×	√	√

6 Conclusion

In this article, we expound the potential security risks of current IoT device authentication, and propose a cross-domain authentication scheme based on master-slave chain and edge computing. In this scheme, the device registration process is lightweight, so that the device can quickly join an IoT domain, and the mobility of the device is considered. At the same time, this scheme can also realize intra-domain authentication and cross-domain authentication between different devices. A ring signature method is proposed to ensure the anonymity of the authentication process. Compared with the existing IoT device authentication schemes, the scheme proposed in this paper has less computational overhead and can resist a variety of common threat attacks. It is suitable for resource-constrained devices for registration and identity authentication.

In the future, we will make a more comprehensive evaluation of the performance for our scheme. Besides, we will focus on the privacy protection issue after the device is authenticated, making the architecture proposed in this paper more practical.

Acknowledgement. The authors gratefully acknowledge the support and financial assistance provided by the National Natural Science Foundation under Grant No. 62173026. The authors thank the anonymous reviewers who provided constructive feedback on earlier work of this paper.

References

1. Mao, Y., You, C., Zhang, J., Huang, K., Letaief, K.B.: A survey on mobile edge computing: the communication perspective. IEEE Commun. Surv. Tutor. **19**(4), 2322–2358 (2017)
2. Mukherjee, M., et al.: Security and privacy in fog computing: challenges. IEEE Access **5**, 19293–19304 (2017)

3. Ma, L., Pei, Q., Qu, Y., Fan, K., Lai, X.: Decentralized privacy-preserving reputation management for mobile crowdsensing. In: Chen, S., Choo, K.-K.R., Fu, X., Lou, W., Mohaisen, A. (eds.) SecureComm 2019. LNICSSITE, vol. 304, pp. 532–548. Springer, Cham (2019). https://doi.org/10.1007/978-3-030-37228-6_26
4. Donald, A.C., Arockiam, L.: A secure authentication scheme for MobiCloud. In: 2015 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore (2015)
5. Amor, A.B., Abid, M., Meddeb, A.: SAMAFog: service-aware mutual authentication fog-based protocol. In: 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC), Tangier, Morocco (2019)
6. Zhu, S., Xu, S., Setia, S., et al.: LHAP: a lightweight network access control protocol for ad hoc networks. Ad Hoc Netw. **4**(5), 567–585 (2006)
7. Zheng, Z., Xie, S., Dai, H., Chen, X., Wang, H.: An overview of blockchain technology: architecture consensus and future trends. In: Proceedings of the IEEE International Congress on Big Data, pp. 557–564 (2017)
8. Nakamoto, S.: Bit coin: a peer to peer electronic cash system (2009)
9. Almadhoun, R., Kadadha, M., Alhemeiri, M., et al.: A user authentication scheme of IoT devices using blockchain-enabled fog nodes. In: 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA). IEEE (2018)
10. Dorri, A., Kanhere, S.S., Jurdak, R., Gauravaram, P.: Blockchain for IoT security and privacy: the case study of a smart home. In: Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops, pp. 618–623 (2017)
11. Li, R., Song, T., Mei, B., et al.: Blockchain for large-scale internet of things data storage and protection. IEEE Trans. Serv. Comput. **12**, 762–771 (2018)
12. Bao, Z., Shi, W., He, D., et al.: IoTChain: a three-tier blockchain-based IoT security architecture (2018)
13. Chen, Z., Chen, S., Xu, H., Hu, B.: A security authentication scheme of 5G ultra-dense network based on block chain. IEEE Access **6**, 55372–55379 (2018)
14. Wang, W., Hu, N., Liu, X.: BlockCAM: a blockchain-based cross-domain authentication model. In: Proceedings of the IEEE 3rd International Conference on Data Science Cyberspace (DSC), pp. 896–901 (2018)