Design and application of Teaching Case of Authentication and Data Security Mechanism Based on Blockchain

Fang Li, Wenju Liu, Ze Wang

Abstract— **The Internet provides us with rich data and services. Identity authentication and resource access authorization are key technologies in the field of network services and management. To realize the transmission of multi-domain identity information with only one cross-domain request process, we make full use of the characteristics of distributed consistency, combine the teaching experience of cross-domain identity authentication and data security in recent years, we propose a certificateless cross-domain identity authentication scheme based on master-slave chain. The scheme provides reference for the application teaching reform of data security by discussing the case design of cross-domain identity authentication.**

Index Terms—**Certificateless Cryptosystem, Cross-domain authentication, Master-slave blockchain, Teaching case**

I. INTRODUCTION

Information security is an indispensable security technology foundation for the development of information society, in which identity authentication technology is one of the important security technologies to ensure information security. At present, the main identity authentication technologies are based on the following systems: Public Key Infrastructure (PKI) [1] based on digital certificates. Its advantages lie in its extensive use and mature system scheme, but there are problems such as low efficiency of certificate management, center malfeasance and single point failure. Identity Based Cryptography (IBC) does not need to issue and manage certificates. Instead of certificate authentication, the IBC solves the problem of low efficiency of certificate management. However, there are still some problems such as low efficiency, key escrow and single point of failure caused by high computation and communication. The Certificateless Cryptography (CLC) [6] effectively solves the problems of complex certificate management in PKI and key escrow in IBC [7].

In a widely used distributed environment, different organizations establish trust domains according to their own systems. In the trust domain, proxy servers are used for authorization and authentication of users in the domain [8]. However, as the range of information interaction becomes wider and wider, the service provided by a single trust domain has obvious limitations and can no longer meet the needs of users. Therefore, the demand for cross-domain access arises. The emergence of identity authentication technology effectively breaks the existing information island problem and solves the problem of cross-domain identity authentication between different trust domains [9]. Zhang et al. [10] solved the problem of cross domain key negotiation and authentication between trust domains at the same level. However, the client needs to carry too much computation, which makes certificate management difficult and costly. References [11][12] introduced signcryption scheme to realize cross-domain authentication, but the scheme has high requirements on the performance of the authentication authority. Once overload or attack occurs, it is easy to cause single point failure verification failure. Literature [13][14] proposes a cross-domain identity authentication scheme based on strong unforgeable proxy re-signature technology, which improves the anonymity of user identity, but it has the problem of efficiency and server single point attack. The above schemes can solve the needs of users for cross-domain authentication function, but there are problems such as high cost of use, low work efficiency and inability to resist the inherent single-point vulnerability of centralized identity authentication scheme, which aggravate the risk of data privacy leakage of users or servers.

Based on the above reasons, an authentication scheme different from the central mode is needed at present, and the introduction of blockchain technology with decentralized performance can effectively solve the corresponding problem. Blockchain is a new data transmission method that integrates cryptography, distributed storage and consensus mechanism and other technologies. Its core advantages lie in its decentralization, non-tampering and group consensus characteristics, which can improve the problems of single point failure, inter-subject trust and certificate management in a variety of information service technologies.

At present, some scholars have studied decentralized identity authentication schemes. Their schemes can solve some task requirements, but there are still some performance problems. Wang et al. [15] proposed an access scheme based on distributed specific applications, but did not consider the issue of trust. Dong et al. [16] proposed a PKI technology authentication scheme based on block chain. By associating identity and certificate in the form of block chain transaction, the registration and update of certificate can be realized. However, there are privacy leakage problems caused by the disclosure of on-chain ledger transactions. Li et al. [17] introduced a cross-domain authentication scheme for

Manuscript received October 05, 2022.
Fang Li, School of Computer Science and Technology, Tiangong University, Tianjin, China.
Wenju Liu, School of Computer Science and Technology, Tiangong University, Tianjin, China.
Ze Wang, School of Computer Science and Technology, Tiangong University, Tianjin, China.

wireless access based on blockchain, which realized cross-domain authentication by replacing the original communication protocol with blockchain, but did not realize the communication between different trust domains. In reference [18], the association chain technology is used to realize the security authentication of the service entity between different domains, and the re-authentication protocol is designed to relieve the burden of the server. However, this scheme has a large amount of computation on the entity side of the information service, and fails to solve the problem of updating and revocation of user identity certificates on the blockchain. With the increase of information on the blockchain, the system overhead gradually increases. In reference [19], without changing the authentication model of PKI system in the domain, BCCA trust model is introduced into the alliance chain to realize bidirectional cross-domain authentication. Although the re-authentication scheme is designed, the read performance of the system is low and there are performance defects for frequent re-authentication operations. Aiming at the above problems, we design a certificateless cross-domain authentication scheme based on the master-slave chain model for teaching research.

The teaching case is mainly divided into the following parts: Firstly, the concept of blockchain and identity authentication technology and its significance and development status in the field of data security are described. Secondly, it introduces the basic knowledge involved in the teaching cases, such as certificateless public key cryptosystem and blockchain technology. Then, the design principle and detailed design of cross-domain identity authentication scheme based on master-slave chain are introduced in detail. Finally, the security and performance of the scheme are proved by literature comparison.

II. PREPARATION

A. *Certificateless Cryptosystem*

At present, although the traditional public key system based on PKI is widely used, there are many problems such as the difficulty of certificate management. To overcome the huge overhead problem of certificate management, researchers put forward identity-based cryptosystem, which eliminates the problems of certificate management and storage by associating the public key with the user's identity information. However, a trusted third party is required to act as the private key Generation center (PKG), which is easy to cause a single point of trust problem. The Certificateless Cryptosystem improves the identity-based cryptosystem. The Key Generation Center (KGC) generates a part of the user's private key, and a secret value selected by the user is used as another part of the private Key. The two private keys together form the final private Key, and PKG is not required to participate in the process of Key Generation. KGC can only calculate part of the user's private key through the identity information sent to it by the user and its own system master key, but does not know all the user's private key, which improves the security of the key. At the same time, the Certificateless Cryptosystem overcomes the problem of high cost of certificate management, solves the problem of key escrow, and is a kind of public key cryptosystem with good performance and high security.

B. *Blockchain technology*

Blockchain technology first emerged as the underlying technology for Bitcoin. Using near-zero credit costs, blockchain technology is a new way of data transmission that enables large-scale collaboration by building trust and consensus. Its core advantage is that it breaks through the traditional centralized system architecture and stores data in the nodes on the chain. Through the characteristics of collective maintenance, non-tampering, openness and transparency, the integrity and transparency of information on the chain are guaranteed, and the problem of system collapse caused by single point failure of traditional central network is effectively avoided. This case is designed based on the consortium blockchain, which is between the public blockchain and the private blockchain. Consortium blockchain has certain access authority, and needs to be jointly managed by the organization or several members of the blockchain.

III. CROSS-DOMAIN IDENTITY AUTHENTICATION SCHEME

A. *Design ideal*

Based on the problems of the above schemes, a concrete scheme to realize cross-domain authentication access between two different trust domains is proposed based on master-slave chain and certificateless cryptosystem.

Based on the characteristics of blockchain decentralization, tamper-proof content and data consistency, we propose a cross-domain authentication model based on the master-slave chain. The master chain is responsible for communication and storage of important resources between blockchains, and the slave chain nodes are responsible for user identity authentication and some data storage. Among them, the master chain nodes are elected by the slave chain nodes, and the master chain nodes will re-elect the slave chain nodes through the consensus mechanism after a fixed time interval. The scheme can effectively solve the security problems such as single point overload or single point attack caused by the centralized cross-domain authentication scheme.

The cross-domain access scheme algorithm is constructed by combining the master-slave chain mechanism and identity certificate, which can effectively reduce the redundant storage of blockchain data, simplify the number of signatures and authentication times, the number of hash functions and the interaction times of authentication process. By comparison, the overall computation cost of this case is relatively small, and it can improve the efficiency of identity authentication while still having better confidentiality, availability and consistency.

B. *Detailed design of case*

Assume that each domain has been initialized and each user node has completed identity registration before cross-domain authentication. This section uses user U in trust domain A to access resources in trust domain B as an example to construct the first cross-domain authentication scheme. Figure 3-1 shows the scheme model.

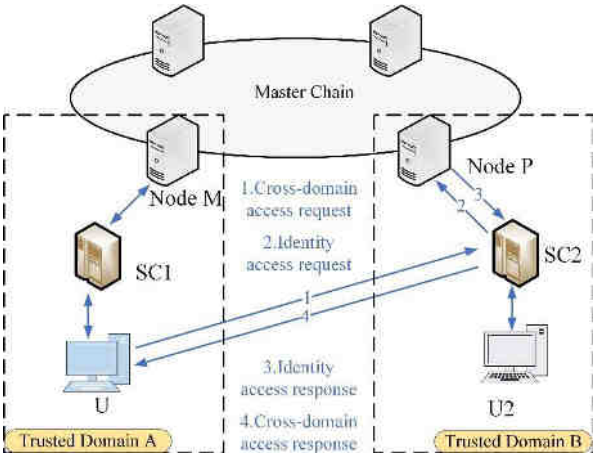

Fig 1. Cross-domain access authentication model

User U selects a random number x and uses its own private key SK_U to calculate the key negotiation parameters $X' = g^x$ for resource access information interaction. Send the access request message $\{PK_U, Re_1, PK_{SC2}, Q, ID_U, ID_{SC2}, N_{U1}, T_{11}, X'\}$ to the slave node SC2, where T_{11} is the locally obtained timestamp and N_{U1} is a random parameter to keep the message fresh.

After receiving user U's access request message from the chain node SC2, it decrypts the message with its own private key, confirms user U's identity, and performs the following operations: SC2 determines whether Re_1 is the cross-domain access request identifier and checks the freshness of timestamp T_{11}. If the authentication fails, the access will be terminated. Otherwise, Cert1 will be parsed to check the validity period, and $Hash(Cert1)$ will be obtained according to the Hash algorithm used by the blockchain. Get the result of the query on the blockchain.

If the authentication is successful, SC2 select the local timestamp T_{12} and send the access request message $\{PK_{SC2}, Re_2, PK_{SC1}, Q, ID_{SC2}, PK_U, T_{12}, expire2\}$ for user U to the master chain node P. expire2 indicates the user's identity expiration time and $\{PK_{SC1}, Q, PK_U, T_{12}, expire1, unknown2\}$ is stored locally. unknow2 indicates the unknown request status.

After receiving the message, the master chain node P decrypts the message, confirms the identity of the slave chain node SC2, checks the freshness of timestamp T_{12}, determines that Re_2 is the identity access request identifier, writes the information $\{PK_{SC2}, ID_U, PK_{SC1}, ID_{SC2}, PK_U, Cert1, expire2\}$ in the local block, passes the information to other nodes on the master chain through the consensus mechanism of the block chain, and reads the local timestamp T_{13}. Return message $\{PK_P, Ask_1, ID_U, PK_U T_{13}\}$ to slave node SC2.

After receiving the message, SC2 decrypts the message, confirms the identity of the master chain node P, checks the freshness of T_{13}, and determines Ask_1 as the request response identifier. SC2 selects a random number w locally, and calculates the key negotiation parameter $W' = g^w$ with its own private key. The local timestamp T_{14} is read, and the verification result $\{PK_{SC2}, Ask_2, ID_{SC2}, ID_U, PK_P T_{14}, N_{U1}, W'\}$ is returned to user U from SC2, and the local state unknow2 is changed to continue2. continue2 indicates that the access qualification of user U is acceptable, and the session key $K_{SC2\to U} = (PK_U)^{SK_{SC2}}(X')^W$ is calculated.

After receiving the message, user U decrypts the message, confirms the identity of slave node SC2, checks whether the timestamp T_{14} is fresh, checks whether N_{U1} in the message is the same as that in the sent authentication request message, and determines Ask_2 as the request response identifier. If any authentication fails, the authentication fails. Otherwise, save $\{ID_{SC2}, PK_{SC2}, PK_P\}$ to the local authentication list, and $K_{U\to SC2} = (PK_{SC2})^{SK_U}(W')^X$, user U and slave node SC2 successfully establish a resource access connection.

IV. PERFORMANCE EVALUATION

A. *Safety analysis*

In view of the possible attack forms in the process of cross-domain identity authentication, the proposed scheme in Table 1 compares the traditional cross-domain authentication scheme in recent years and the cross-domain authentication scheme introducing blockchain structure. The security of the proposed scheme is compared in five aspects, such as two-way entity authentication, anti-replay attack and anti-replacement attack. The results show that this scheme has relatively high security against authentication attacks. In the table, √ indicates that the solution has the performance, and × indicates that the solution does not have the performance.

Table 1 Security comparison of cross-domain authentication schemes

Schemes	[12]	[13]	[18]	[20]	[21]	Ours
Two-way entity authentication	×	√	×	×	×	√
Resistance to replay attack	√	√	√	√	√	√
Resistance to replacement attack	√	×	√	√	√	√
Resistance to DDoS attack	×	√	√	×	×	√
Resistance to man-in-the-middle attack	√	×	√	√	√	√

As shown in table 4-1, compared with reference [12], [18], the proposed scheme establishes the trust relationship between two trust domains by introducing the root certificate as the trust certificate for accessing foreign resources, and realizes two-way entity authentication. Compared with reference [13], the attacker in this scheme cannot obtain the private key of user U, cannot form the signature of the message, and cannot successfully verify the message when authenticating the message from the chain node, thus resisting the replacement attack. The proposed scheme can

resist man-in-the-middle attack by encrypting and signing messages with public keys. Compared with reference [12], [20], [21], the scheme in this paper uses the scheme that introduces the combination of master and slave chains of blockchain, and takes advantage of its decentralized characteristics to solve the single point of failure problem and resist distributed denial of service attacks.

B. *Efficiency evaluation*

This case compares the computational overhead with other cross-domain authentication schemes, ignoring the influence of factors unrelated to cross-domain authentication, and specifically describes the number of signatures and authentications, the number of hash operations, and the number of interaction rounds. The comparison results are shown in Fig 2.

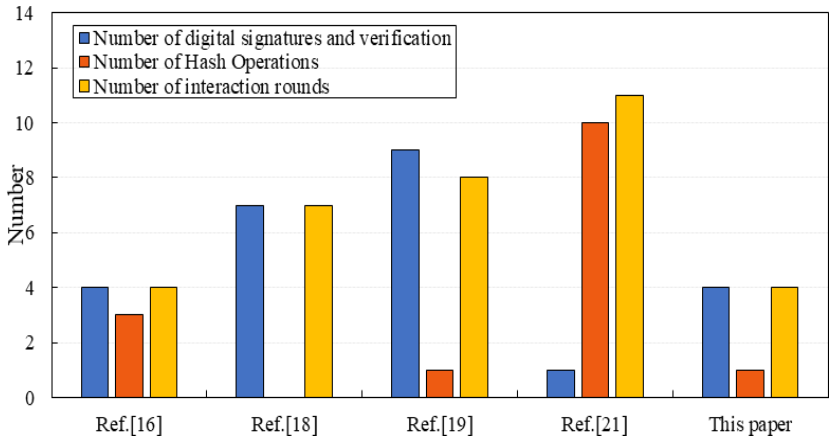

Fig 2. Comparison of computational overhead of cross-domain identity authentication schemes

As shown in Figure 4-1, during the transmission of the cross-domain authentication scheme, signature and verification are added to the four ciphertext transmissions to ensure the reliability of data sources. When querying the status, the blockchain certificate is hashed, and the final hash value is used to query the status result queried on the blockchain. Therefore, this case only needs four signature and verification processes and one hash operation process, and the interaction theory number is four rounds. Compared with reference [13], [18], [19], [21], the overall computational cost of this paper is relatively small and the efficiency is high. This scheme with the traditional centralized cross-domain authentication scheme [13], [21] contrast, although on the number of signature and verification were similar, but the hash operation times and interaction on the round number has a larger advantage obviously, so cross-domain authentication phase in this paper, the overall operation efficiency is higher, and the decentralized scheme is more security. Compared with the cross-domain schemes related to blockchain [18] [19], the scheme in this paper uses the combination of master and slave chains to simplify the authentication process through the division of labor and cooperation between master and slave chain nodes, which effectively improves the efficiency of solving cross-domain authentication problems, and improves the number of signatures and verification and the number of interaction rounds to varying degrees.

V. CONCLUSION

This teaching case summarizes the research status of cross-domain identity authentication and its significance in the field of data security. Aiming at the problems of centralization in the existing cross-domain identity authentication, we propose a certificateless cross-domain identity authentication scheme based on master-slave blockchain. We use master-slave blockchain technology to realize trust transfer between the trust domains of certificateless public key cryptosystem, and realize identity authentication and authorization between two different trust domains. Through teaching theory analysis and simulation experiments, it is proved that the proposed scheme can simplify the times of signature and authentication, the Times of using hash function and the interaction times of authentication process.

REFERENCES

[1] J. Lin, J. Wu, Q. Zhang, et al, A review of recent research on PKI technology, J. Cryptogr. 2 (6) (2015) 487-496.
[2] X. Tang, Y. Yu, T. Chen, et al, An analysis of cross-domain authentication scheme based on blockchain technology, Netw.Secur.Technol.Appl. (09) (2019) 22-25.
[3] Z. Chen, Y. Qiu, J. Liu, et al, Incentive mechanism for selfish nodes in wireless sensor networks based on evolutionary game, Comput. Math. Appl. 62 (9) (2011) 3378-3388.
[4] J. Tian, K. Sun, Trust-Distributed-Based Authentication Mechanism Using Hierarchical Identity-Based Cryptography, J. Comput. Res. Dev. 52 (07) (2015) 1660-1671.
[5] M. Guan, S. He, B. Song, et al, A fault-tolerant ad hoc network node cooperation strategy based on repeated games, J Chongqing Univ Posts Telecommun (Nat Sci Ed). 28 (3) (2016) 342-348.
[6] M. Zhang, Theory and application of certificate-free cryptosystem, J. Xidian. Univ. (2013).
[7] Z. Wang, Z. Han, J. LIU, et al, Authentication scheme based on PTPM and certificate-free public key in cloud environment, J. Softw. 27 (6) (2016) 1523-1537.
[8] Y. Ga, Research on Trusted Identity Issuance and Cross-Domain Authentication of Information Service Entities, J. Xidian. Univ. (2019). https://doi.org/10.27389/d.cnki.gxadu.2019.000326.
[9] H. Zhang, X. Chen, X. Lan, et al, BTCAS: A Blockchain-Based Thoroughly Cross-Domain Authentication Scheme, J. InF. Secur. Appl. 55 (2020) 102538.
[10] C. Yuan, W. Zhang, X. Wang, EIMAKP: Heterogeneous Cross-Domain Authenticated Key Agreement Protocols in the EIM System, Arab. J. Sci. Eng. 42(8) (2017) 3275–3287.

[11] J. Liu, L. Zhang, R. Sun, A two-way signature encryption scheme Under heterogeneous systems, J. Electron. Inf. Technol. 38 (11) (2016) 2948-2953.
[12] Z. Jiang, J. Xu, A heterogeneous cross-domain authentication scheme based on signature-encryption in cloud environment, J. Comput. Appl. 40 (03) (2020) 740-746.
[13] S. Yang, F. An, P. Yang, et al, A cross-domain authentication scheme based on proxy re-signature in cloud environment, Chin. J. Comput. 42 (04) (2019) 756-771.
[14] Y. Lv, W. Liu, Z. Wang, Heterogeneous Cross-Domain Identity Authentication Scheme Based on Proxy Resignature in Cloud Environment, Math. Probl. Eng. (2020).
[15] X. Wang, F. Gao, J. Zhang, et al, Cross-domain authentication mechanism for power terminals based on blockchain and credibility evaluation, 2020 5th Int. Conf. Comput. Commun. Syst. ICCCS. (2020) 936–940.
[16] G. Dong, Y. Chen, Z. Zhang, et al, Research on identity management authentication based on blockchain, Cmput. Sci. 45 (11) (2018) 52-59.
[17] C. Li, Q. Wu, H. Li, et al, Trustroam: A Novel Blockchain-Based Cross-Domain Authentication Scheme for Wi-Fi Access, Springer Int Publ, (2019).
[18] X. Ma, W. Ma, X. Liu, A cross-domain authentication scheme based on blockchain technology, Electron. Sin. 46 (11) (2018) 2571-2579.
[19] [19] Z. Zhou, L. Li, Z. Li, An efficient cross-domain authentication scheme based on blockchain technology, J. Comput. Appl. 38 (02) (2018)316-320+326.
[20] Y Chen, Dong G, Bai JS, et al. Trust Enhancement Scheme for Cross Domain Authentication of PKI System[C]// 2019 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC). 2019.
[21] Jia X , Hu N , Su S , et al. IRBA: An Identity-Based Cross-Domain Authentication Scheme for the Internet of Things[J]. Electronics, 2020, 9(4):634.