Journal of Artificial Intelligence and Technology, 2021, 1, 92-100
https://doi.org/10.37965/jait.2020.0060

ISTP
RESEARCH ARTICLE

Cross-heterogeneous Domain Authentication Scheme Based on Blockchain

Jing Liu,[1,2] Yixin Liu,[1] Yingxu Lai,[1,3,4] Rongchen Li,[5] Siyu Wu,[5] and Sami Mian[6]

[1]College of Computer Science, Faculty of Information Technology, Beijing University of Technology, Beijing 100124, China

[2]Shaanxi Key Laboratory of Network and System Security, Xi'an 710071, China

[3]Science and Technology on Information Assurance Laboratory, Beijing 100072, China

[4]Engineering Research Center of Intelligent Perception and Autonomous Control, Ministry of Education, Beijing 100124, China

[5]Fan Gongxiu Honors College, Beijing University of Technology, Beijing 100124, China

[6]University of Pittsburgh, Pittsburgh, PA 15260, USA

(Received 31 July 2020; Revised 24 January 2021; Accepted 10 March 2021; Published online 23 March 2021)

Abstract: With the rising popularity of the Internet and the development of big data technology, an increasing number of organizations are opting to cooperate across domains to maximize their benefits. Most organizations use public key infrastructure to ensure security in accessing their data and applications. However, with the continuous development of identity-based encryption (IBE) technology, small- and medium-sized enterprises are increasingly using IBE to deploy internal authentication systems. To solve the problems that arise when crossing heterogeneous authentication domains and to guarantee the security of the certification process, we propose using blockchain technology to establish a reliable cross-domain authentication scheme. Using the distributed and tamper-resistant characteristics of the blockchain, we design a cross-domain authentication model based on blockchain to guarantee the security of the heterogeneous authentication process and present a cross-domain authentication protocol based on blockchain. This model does not change the internal trust structure of each authentication domain and is highly scalable. Furthermore, on the premise of ensuring security, the process of verifying the signature of the root certificate in the traditional cross-domain authentication protocol is improved to verify the hash value of the root certificate, thereby improving the authentication efficiency. The developed prototype exhibits generality and simplicity compared to previous methods.

Key words: public key infrastructure; identity-based encryption; cross-domain authentication; blockchain

I. INTRODUCTION

With the development of Internet technology, organizations or service providers have an increasing amount of applications and information. Security is the premise and guarantee of the healthy development of the Internet platform, and the network communication environment that establishes a reliable and secure network is a significant problem [1] that needs to be solved. To prevent unauthorized users from accessing these data and applications, organizations usually utilize authentication techniques [2] and manage their users by establishing an authentication server to form a relatively independent trust domain. Public key infrastructure (PKI) [3] is the most commonly used identity authentication technology to ensure security in cyberspace. Numerous PKI-based identity management systems have been implemented in enterprises, hospitals, authentication domains, and government departments. However, with the development of identity-based encryption (IBE) technology [4,5], more small- and medium-sized enterprises are using IBE to deploy internal authentication systems. This is mainly because the IBE system largely solves the problem of certificate authority (CA) center construction in PKI technology and does not need to manage a large number of certificates, thereby reducing the operating costs. Moreover, PKI uses public key certificates to bind the public key of the client and its attribute information, which requires the digital certificate store certificate revocation list (CRL) under the PKI system to be updated in real time and run online. The IBE system does not need to use a public key digital certificate to authenticate a user. The identifiers of the users serve as their public keys in the decryption process, and the corresponding private key only needs to be obtained once, which can achieve the purpose of offline authentication. These organizations based on PKI and IBE systems are usually centralized, and the authentication structures and infrastructures in the PKI and IBE domains differ. Each organization may even design the identification or certificates of the authentication system differently. Moreover, it is important to note that the trust domains are isolated from one another. However, users may wish to access applications in other authentication domains to obtain superior services and a wider range of data. IBE has exhibited a good development trend, but with the current domestic network system architecture, the IBE system architecture cannot be fully applied nationwide. Therefore,

Corresponding author: Yingxu Lai (e-mail: laiyingxu@bjut.edu.cn).

the phenomenon of the coexistence of PKI and IBE system architecture will exist. Different domains generally use a heterogeneous trust system to provide security guarantees. Owing to the increasing demand for collaboration, trusted interconnections and trusted management among heterogeneous domains [6] are faced with three urgent problems: (1) ensuring that the entity is authentic and credible in the mutual access of heterogeneous domains, (2) how to authorize the legal entity property, and (3) how to determine the responsibility of the entity. Therefore, effectively dealing with the problem of information transfer among different authentication systems is an inevitable trend in current network development.

Blockchain technology [7] is causing substantial changes in the global financial field, and these changes will affect all other industries as profoundly as Internet technology. The blockchain is essentially a distributed recorded public ledger database of transactions or digital events that all transaction participants have executed and shared [8]. Every transaction in the public ledger is verified by the consensus of most participants in the system [9]. Furthermore, once the transaction has been completed, the information will always exist; that is, a solid and verifiable record of every transaction is contained in the blockchain. At present, the distributed feature of blockchain has been applied in many fields [10]. We consider the use of blockchain technology to establish a cross-domain authentication process between the PKI and IBE domains. The solution to the cross-heterogeneous domain authentication problem mainly involves improving the structure of the authentication process system. We combine the cross-heterogeneous domain authentication system, and the decentralized and naturally credible features of the blockchain platform to design an authentication system that does not change the internal architecture of each trust domain. The system is highly scalable and reduces the number of signature verifications, thereby reducing the authentication complexity. A blockchain certificate is designed to manage the trust relationship between domains, and the certificate is stored in a tamper-resistant blockchain to ensure security.

The main contributions of this study are as follows:

(1) Use blockchain to securely and reliably manage trust relationships: We propose a blockchain certificate called BCert for building a cross-domain authentication based on blockchain network. We designed a transaction with BCert as the key data to publish the trust relationship and certificate information on the blockchain. Trust relationships are securely and reliably managed by recording these transactions on a tamper-proof blockchain trusted and maintained by all members.

(2) Strong scalability: Only inter-domain authentication servers need to join the blockchain network, connecting the trust domains of different organizations through the alliance blockchain platform. The scheme ensures that the internal trust structure and logic of each trust domain remain unchanged, and the hierarchy structure is clear. The model has high scalability and flexibility.

(3) Reduce the amount of computation during authentication: This model builds a blockchain network and records the hash value of the blockchain certificate in the form of a transaction. Query BCert transactions on the blockchain to confirm the trust of both parties and realize cross-domain authentication. This solution further improves efficiency by converting the original process of issuing certificates and verifying signatures to a more efficient process of verifying certificate hashes.

The remainder of this paper is organized as follows: Section II introduces related work, Section II presents the proposed scheme, and Section IV discusses the experiment and results, and outlines the performance evaluation. Finally, Section V summarizes the paper.

II. MOTIVATION

A. RELATED WORK

As no uniform standard exists for transferring identities between different trust domains, user operations encounter many inconveniences in specific cross-authentication domain applications. To access applications and data in another trusted domain, users need to register their identities repeatedly in different trust domains. The same problem exists on the service provider side, as it is difficult to prove the validity of an identity certificate issued by a different domain. Existing cross-domain authentication solutions based on PKI are relatively mature and widely used applications include trust lists, cross-authentication, and bridge authentication [11]. PKI-based solutions use third-party proof to solve the problem of identity and key binding, revealing the third party's legal status and resulting in increased communication. The IBE system is a new and developing public-key cryptosystem. In IBE, users directly provide their e-mail address, phone number, and other information that can uniquely identify their identity as the public key, and the private key is generated based thereon. Therefore, compared to PKI, IBE avoids the problem of numerous resources being required for maintenance and certificate management. The authors of [12] proposed a PKI-based cross-heterogeneous domain authentication model to achieve cross-domain authentication among PKI domains. Peng [13] proposed an identity-based signcryption scheme and presented a model for multidomain mutual authentication on this foundation. The authors of [14] proposed a new and efficient certifiable key agreement protocol, which can convert between PKI domains and can effectively resist various active attacks. Huang *et al*. [15] proposed a heterogeneous signcryption scheme in which the sender is in an IBE environment and the receiver is in a PKI environment.

With the development of blockchain technology, research in the field of identity authentication has been undertaken by many institutions. The white paper of the Ministry of Industry and Information Technology [16] pointed out that the development of blockchain technology has substantially promoted the development and application of digital certificates. To manage user identity verification between authentication domains in a distributed manner, Grabatin and Hommel [17] proposed a cross-domain authentication model based on this method, which can access resources in different domains safely and effectively, and is superior to existing PKI cross-domain authentication. Moreover, simulations of the transmission overhead of receiving and dealing with the authentication messages demonstrate that the scheme is more effective [18]. Axon and Goldsmith [19] proposed a new scheme by improving Certcoin and designed a PKI authentication system with privacy protection. Lewison and Corella [20] proposed a certificate-based PKI authentication system based on the Ethereum blockchain, which solves the problems of excessive communication in traditional PKI certificate management and the use of CRLs. Zhang *et al*. [21] solved the centralization problem of the traditional PKI system by using blockchain technology. In their framework, users store their identities on the blockchain and attach a smart contract to grant different permissions for each site or application,

thereby enabling an entirely distributed user authentication framework. The authors of [22] proposed a PKI cross-domain authentication scheme based on blockchain technology. The scheme includes the trust model and the architecture of the Blockchain Certification Center, ensuring security and efficiency. Abdullah *et al.* [23] proposed a blockchain-based method for enhancing big data verification in a distributed environment. We have found through research that although the blockchain-based authentication scheme can solve several problems in the traditional authentication architecture, it generally exhibits the defects that the configuration process is cumbersome and unsuitable.

B. PROBLEM ANALYSIS

1) Authentication across heterogeneous domains. IBE systems and PKI systems have different authentication logics and authentication credentials; the existing authentication solutions across heterogeneous domains are faced with the problems of centralization and complex authentication process at the same time. Therefore, further research on heterogeneous domain authentication process is needed. At the same time, with the continuous growth of cooperation requirements, the trusted interconnection and management between heterogeneous domains are facing problems, and it is necessary to improve the security in the authentication process of heterogeneous trusted systems.

2) Implementation resistance. Blockchain technology originates from the financial field, and the research on its application in the field of authentication is not mature enough and lacks practical experience. The existing blockchain-based solutions do not take into account the bearing capacity of the nodes in the system and the complexity of the system caused by the characteristics of blockchain itself. Therefore, blockchain-based solutions should focus on improving system availability, compatibility with existing systems, reducing system deployment difficulties, and avoiding large-scale retrofits.

III. CROSS-DOMAIN AUTHENTICATION METHOD WITH BLOCKCHAIN

A. DESIGN GOALS

To make our system more usable, on the premise of using the authentication framework and the logic within each authentication domain, we use blockchain technology to establish authentication trust between authentication domains. Our system not only achieves the goal of cooperation but can also reduce system complexity and guarantee system security and traceability, while offering improved flexibility. To address the shortcomings of the cooperation model of heterogeneous authentication domains and the existing cross-heterogeneous domain authentication schemes, we propose an authentication scheme that is suitable for heterogeneous authentication domains across PKI and IBE based on blockchain technology. The interdomain interconnection module uses blockchain technology to establish trust connections and cross-heterogeneous domain authentication models. The design goals are as follows:

(1) Using the distributed and multicenter characteristics of the blockchain, we construct an authentication model that joins the consortium blockchain platform with the interdomain interconnection modules of multiple trust domains. On the premise of retaining the internal architecture and authentication logic of the original authentication domain, we ensure that the internal logic and hierarchy of each authentication domain is clear. Because the consortium blockchain is more centralized, and the chain is limited to members within the consortium, a consensus is reached when each authentication domain accesses the consortium chain; that is, the members of the access chain are all trusted members.

(2) Blockchain transactions are used to build trust and to ensure the security of certificates through transparent audits. The interdomain interconnection modules of multiple trust domains are used as the transaction initiator or receiver, which is published on the consortium blockchain platform to achieve authorized trust. Blocks are used to manage the trust and authorization in the form of recorded transactions. Each cross-domain authentication process can be traced back, and records cannot be tampered with.

(3) A unique blockchain certificate named BCert is designed for assembling the blockchain transactions. The BCert is recorded on the blockchain by recording transactions in the blockchain ledger. Because the blockchain is distributed and stored in all nodes of the blockchain network, the interdomain interconnection modules of multiple trust domains do not need to establish trust through trusted third parties. By simply querying and comparing the record stored on the blockchain issued by the interdomain interconnection module with the hash value of the BCert provided by the target domain, the purpose of verifying the authenticity of the certificate held by the target domain can be achieved. This solution not only simplifies the certification path in the cross-domain authentication process but can also reduce the number of verifications and improve the verification efficiency during cross-domain authentication.

B. SYSTEM MODEL

The overall system architecture is presented in Fig. 1. The system model includes a smart contract, blockchain ledger, entities, and interdomain interconnection module. The specific description of each part is as follows:

(1) Smart contract: The contracts to be followed by each domain are written into the blockchain, and these are transparent and executed automatically. The smart contracts are jointly supervised and maintained by members of the blockchain.

(2) Blockchain ledger: This is a distributed database that is jointly maintained by members of the blockchain. The

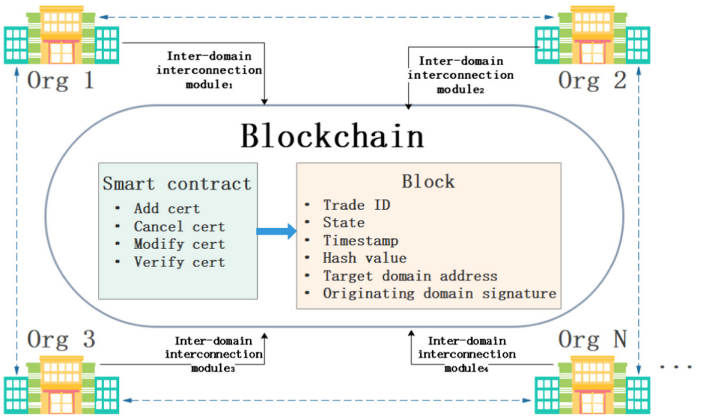

FIG. 1. Blockchain-based access authentication system model.

blockchain records the certificate information of the trust domain and provides public and tamper-resistant certificate records. Our blockchain system is constructed on the consortium chain [24]. As the consortium chain is only open to specific authentication domains, only the authorized interdomain interconnection module serves as the verification node of the consortium chain network. The blockchain certificate in the ledger records the authorization of one trust domain to another, and the blockchain certificate security is ensured by the tamper-resistant feature.

(3) Trust domain: The trust domain is divided into users and service providers. The user interacts with the interdomain interconnection module of the domain, in which the user is located through the terminal to realize the trust domain operation on the user registration, identity management, and authentication. If users wish to obtain cross-domain service, they need to pass the authentication within their trust domain and then request authentication from the service through the interdomain interconnection module.

(4) Interdomain interconnection module: The interdomain interconnection module server in each trust domain is the trusted source of this authentication domain and publishes the trust strategy of this trust domain. The interdomain interconnection module provides services for users and applications within its domain and manages and authenticates subordinate authentication servers as well as users. The interdomain interconnection module is the actual owner of the blockchain certificate in this system. The trust domain authorizes other domains by issuing transactions to the consortium chain.

C. BLOCKCHAIN-RELATED DESIGN

1) Data structure design.

BCert design. According to the specific functions of the system, the BCert certificate is improved with reference to the traditional X.509 certificate. The BCert is self-generated by the interdomain interconnection module added to the blockchain network. It is used to form transactions in the model. The BCert record as a credential for constructing the model is saved on the distributed blockchain. We design the BCert certificate with reference to the traditional X.509 certificate, with several improvements according to the relevant characteristics of this system. The details are presented in Fig. 2.

First, BCert has no signature or signature algorithm. To ensure the authenticity of the digital certificate and that the identity of the digital certificate holder and the public key is authentic and credible, traditional digital certificates mainly use digital signatures to determine whether a certificate has been tampered with. As the blockchain is a trusted machine, the data stored on the block exhibits the characteristics of being truly effective and tamper resistant. In this model, to verify the blockchain certificate, we only need to make a consistent hash value comparison between the obtained certificate following the hash operation and the certificate stored on the blockchain. Therefore, the BCert proposed in this model does not require signature and signature algorithm modules.

Second, no URL module exists in the format of the blockchain certificate proposed by this model because it is not necessary to provide CRL and OCSP management services to the BCert. Different BCert types are assembled into transactions and stored on a time-series and tamper-resistant blockchain. Therefore, the entire life cycle of the BCert can be recorded through the blockchain.

Blockchain data structure design. The data structure of this blockchain model is designed according to the design goals. By assembling the BCert hash into a transaction and recording the transaction on the tamper-resistant blockchain, the full life cycle of the BCert and trust relationships between multiple domains can be managed. The blockchain data structure is illustrated in Fig. 3.

The details of the blockchain data structure of this model are as follows:

Trade ID: The unique identifier of the transaction.

Status: The status of BCert, including *Issues*, *Revoke*, etc.

Timestamp: The time at which the transaction was initiated, which is used to sort the transaction to generate blocks.

Hash value: The hash value of BCert. In the model, the key data used to record transactions on the blockchain ledger is Cert hash.

Target domain address: The public key address of the domain authentication server. The public key address is usually obtained by hashing and encoding the public key. By attaching the public key address of the domain authentication server to the transaction, as the recipient of the transaction, the authentication server obtains ownership of this transaction. That is, the authentication server obtains the trust of the domain that issued this transaction.

Originating domain signature: The signature of the domain that issued the BCert.

2) Node topology structure design.

The topology structure of the network nodes is designed according to the node architecture of

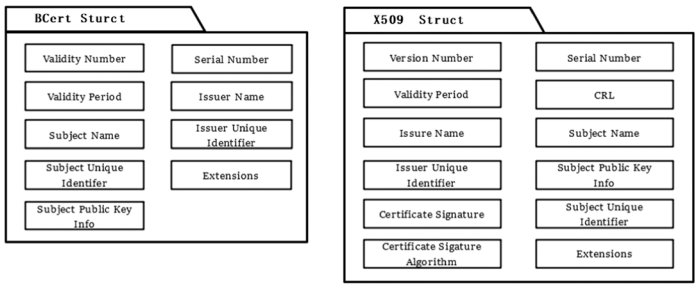

FIG. 2. Format comparison between X.509 certificate and BCert.

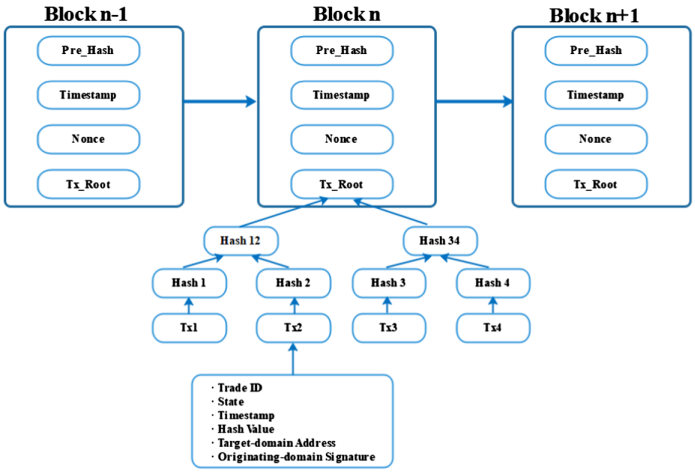

FIG. 3. Blockchain data structure.

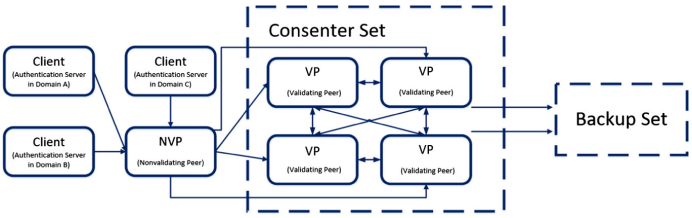

FIG. 4. Node topology.

the Hyperledger Fabric blockchain platform in combination with this model. The node structure in the blockchain is illustrated in Fig. 4.

Client: The client is assumed by the interdomain interconnection server of each trusted domain and submits and queries transactions to nonvalidating peers (NVPs).

NVP: NVPs are assumed by the servers of each trust domain. The NVP receives the transaction sent by the client, verifies the signature in the transaction, and sends the transaction in sequence, according to the timestamp, to the verification node for further processing. The NVP synchronizes the ledger data to provide rapid query services for clients.

Validating peer (VP): VPs are undertaken by the servers of each trust domain. The VP participates in the consensus process of the consensus algorithm. VPs are divided into master and slave nodes. The master node assembles the block to the transaction transmitted by the NVP broadcast, initiates a proposal, works with other VPs to reach a consensus on the block through a consensus algorithm, and connects the new block to the zone blockchain. The node collaboration in this model network is divided into three steps, as follows:

(1) After joining the network, the interdomain interconnection server, as a client of each trust domain, initiates a transaction with trust authorization regarding the BCert and sends it to the NVP.

(2) The NVP verifies the signature of the transaction received from the client, sorts the transaction according to the timestamp, and broadcasts it to the corresponding VP.

(3) The VP reaches consensus on the block according to the consensus algorithm and connects the blocks into a chain.

D. MODEL ARCHITECTURE

The design model architecture is presented in Fig. 5.

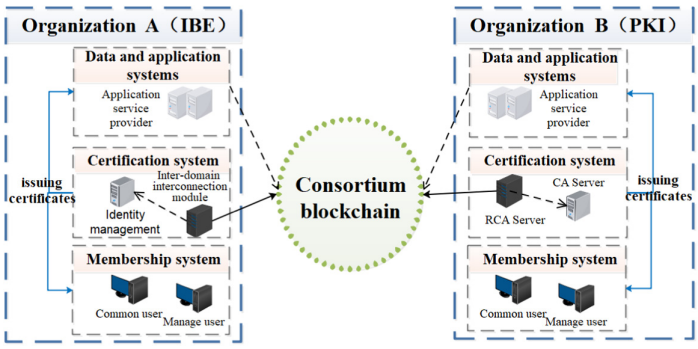

FIG. 5. Architecture struct.

In this model, the trust domain includes the PKI and IBE trust domains. Every trust domain includes an authentication system, a data and application system, and a membership system. In the PKI domain, the authentication system includes the root CA server and the subCA server. The data and application system includes the application servers, whereas the membership system includes the users (U) and administrator users (AD). The authentication system issues equipment certificates and user certificates for the data and application systems and membership systems, respectively. Therefore, based on the digital certificate technology, the security in the PKI authentication system of the user access to the application server is guaranteed. In the IBE domain, the authentication system includes an identity management server and an interdomain interconnection server. The data and application system includes application servers, whereas the membership system includes the U and AD. In this model, the blockchain is the trust-building machine, which is constructed by multiple trust domains. The root CA server in the PKI system and interdomain interconnection server in the IBE system are used to complete the interdomain authentication service. In the following description, we collectively refer to these as the interdomain authentication module.

The concept of cross-domain authentication in this model is as follows: Following social negotiation between domains A and *B*, it is assumed that domain B trusts domain A. The interdomain interconnection module of B domain assembles and generates a transaction that expresses the trust of domain A on the blockchain. The key information of this transaction is the hash value of BCert, which domain B issues to domain A. When U in domain A requests access to an application service in domain B, U needs to be authenticated across domains. First, the interdomain authentication module in domain A receives the access request from U, and subsequently, U sends the user certificate to the authentication server to verify their identity in this domain. If the authentication server passes the user certificate verification, the interdomain authentication module in domain A sends the BCert to the interdomain authentication module in domain B. Thereafter, domain B queries the hash transaction of this BCert through the blockchain client and parses and verifies the transaction. If it passes the validation, the cross-domain authentication is completed, and U in domain A can access the application server in domain B.

E. PROTOCOL OF CROSS-DOMAIN AUTHENTICATION

1) Overview of cross-heterogeneous domain authentication process. Figure 6 depicts the cross-domain authentication process of our scheme, as described in detail below:

Step 1: Build trust. Each trust domain publishes blockchain certificates for other domains on the blockchain through the interdomain interconnection module to establish trust relationships with the other domains.

Step 2: A user in the authentication domain interacts with the interdomain interconnection server or root CA in this domain to verify the domain identity.

Step 3: If the user identity in phase 2 is legal in this domain, the interdomain interconnection module of domain A sends the authentication and authorization certificate issued by B to A to the interdomain interconnection module of domain B.

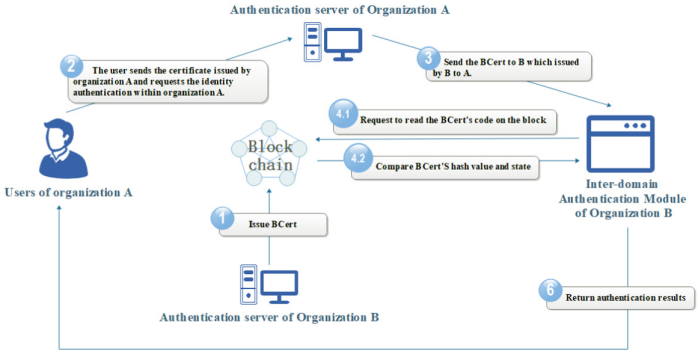

FIG. 6. Cross-domain authentication flow chart.

Step 4: The domain B server queries the transaction stored in the blockchain regarding the corresponding BCert. After hashing the certificate sent from domain A, it is compared with the hash value stored in the block, and the status of the certificate is verified to ensure that the certificate is valid.

Step 5: The domain B server returns the authentication result.

As the PKI domain and IBE domain authentication systems have different architectures, certain differences will exist in the cross-heterogeneous domain authentication process. The following describes the PKI/IBE authentication process in detail.

To facilitate the description of the authentication process, we define several symbolic representations in Table I.

2) PKI domain access to IBE domains. Figure 7 presents the cross-domain authentication process from the PKI domain to the IBE domain, as described in detail below:

Step 1: $U_A \rightarrow AS_P$: $\{Cert_A, sig(sk_A, timestamp), timestamp\}$: U_A sends the request and certification to AS_P for accessing IBE domain. U_A also sends the signature of the *timestamp* to guarantee safety.

Step 2: AS_P verifies U_A: AS_P uses $Cert_A$ and *timestamp* to verify that $sig(sk_A, timestamp)$ is correct. Thereafter, AS_P resolves $Cert_A$ and verifies the validity of the certificate, including whether it is within its validity period and the format is correct.

Step 3: $AS_P \rightarrow AS_I$: AS_P sends a request to AS_I.

Step 4: $AS_I \rightarrow AS_P$: $\{N\}$: AS_I accepts AS_P's request and returns a random number N.

Step 5: $AS_P \rightarrow AS_I$: $\{BCert_P, sig(sk_P,N), N\}$: AS_P sends $BCert_P$, the signature of N, and nonce N to AS_I.

Step 6: AS_I verify $sig(sk_P, N)$: AS_I uses $BCert_P$ and N to verify that $sig(sk_P, N)$ is correct. Thereafter, AS_I resolves $BCert_P$ and verifies the validity of the certificate, including whether it is within its validity period and the format is correct.

Step 7: $AS_I \rightarrow Blockchain$: Request $BCert_P$*'s* record.

Step 8: $Blockchain \rightarrow AS_I$: Return record: *Blockchain* returns the latest status of the record in the blockchain.

Step 9: Verify hash value: AS_I compares the record with the hash of $BCert_P$; if they are the same, AS_I authenticates U_A to access this domain.

Step 10: $AS_I \rightarrow U_A$: AS_I returns the validation results to U_A.

Step 11: Map to virtual user A': U_A maps to virtual user A' of the IBE domain.

Step 12: Unique identification: AS_I assigns the unique identification for user A'.

Step 13: $U_A \rightarrow ISE_I$: U_A obtains services from ISE_I.

Table I. Symbolic descriptions for authentication protocol

Symbol	Implication
U_X	User named X
AS_X	Authentication server in X domain
$Cert_X$	Certificate for user X in PKI domain
$BCert_X$	Blockchain certificate for X domain
$sig(sk_X, N)$	Result of signing N with private key of X
ISE_X	Information service entity in X domain

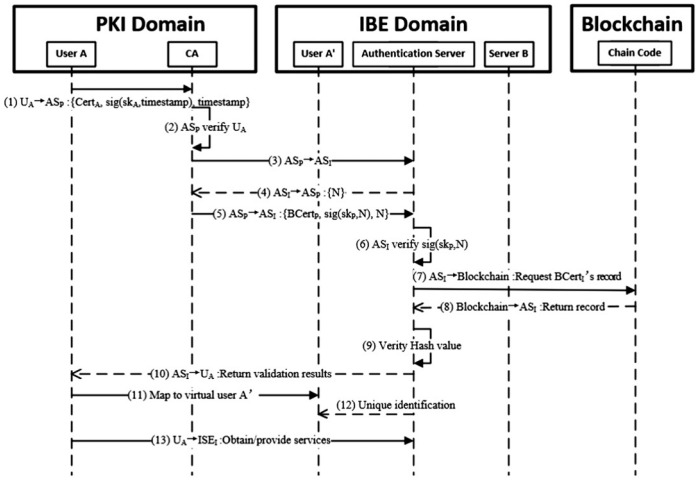

FIG. 7. PKI domain user access to services of IBE domain.

3) IBE domain access to PKI domains. Figure 8 depicts the cross-domain authentication process from the IBE domain to the PKI domain, as described in detail below:

Step 1: $U_B \rightarrow AS_I$: $\{Identification, sig(sk_B, timestamp), timestamp\}$: U_B sends *Identification* to AS_I for accessing the PKI

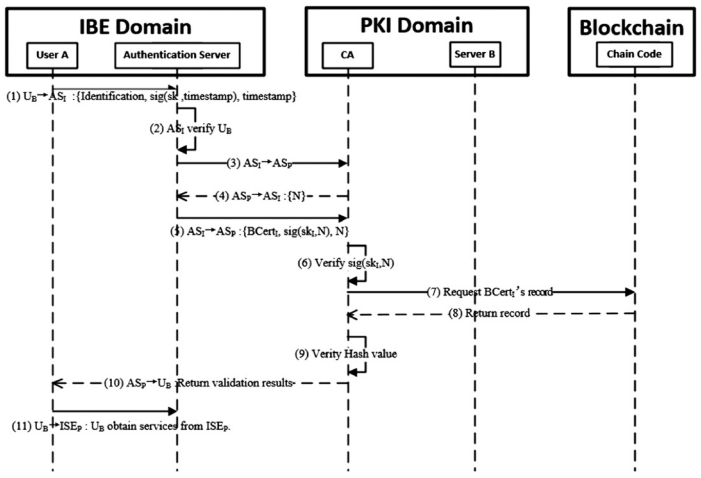

FIG. 8. IBE domain user access to services of PKI domain.

domain. U_B also sends the signature of *timestamp* to guarantee safety.

Step 2: AS_I verifies U_B: AS_I uses *Identification* and *timestamp* to verify that the *sig(sk$_B$, timestamp)* is correct. Thereafter, AS_I resolves $Cert_A$ and verifies the validity of *Identification*, including whether it is within its validity period and the format is correct.

Step 3: $AS_I \rightarrow AS_P$: AS_I sends a request to AS_P.

Step 4: $AS_P \rightarrow AS_I$: $\{N\}$: AS_P accepts AS_I's request, and returns a random number N.

Step 5: $AS_I \rightarrow AS_P$: $\{BCert_I, sig(sk_I, N), N\}$: AS_I sends $BCert_I$, the signature of N, and nonce N to AS_P.

Step 6: AS_P verifies $sig(sk_I, N)$: AS_P uses $BCert_I$ and N to verify that $sig(sk_I, N)$ is correct. Thereafter, AS_P resolves $BCert_I$ and verifies the validity of the certificate, including whether it is within its validity period and the format is correct.

Step 7: $AS_P \rightarrow$ *Blockchain*: Request $BCert_I$*'s* record.

Step 8: *Blockchain* $\rightarrow AS_P$: Return record: *Blockchain* returns the latest status of the record in the blockchain.

Step 9: Verify hash value: AS_P compares the record with the hash of $BCert_I$; if they are the same, AS_P authenticates U_I to access this domain.

Step 10: $AS_P \rightarrow U_B$: AS_P returns the validation results to U_B.

Step 11: $U_B \rightarrow ISE_P$: U_B obtains services from ISE_P.

F. MODEL FEATURES

A cross-domain authentication model is constructed based on the blockchain network, and a blockchain certificate named BCert is proposed for the authentication model. The transaction using BCert as key data is designed, indicating the trust relationships and certificate status posted on the blockchain. By recording these transactions on a blockchain that is maintained by all trust domains and cannot be tampered with, a management model of trust relationships between BCerts in different states and trust domains is realized.

1) The model levels are clear and exhibit scalability. This model connects each authentication domain through the blockchain platform and establishes trust relationships among domains by issuing authorized trust transactions in the blockchain network. This solution guarantees that the architecture and logic of the internal authentication of each trust domain remain unchanged. To achieve cross-heterogeneous domain authentication, it is only necessary to add the identity authentication server to the blockchain network to build a trust relationship. Furthermore, for cross-domain authentication requests to the IBE domain, the IBE domain also assigns the user identity within the domain following successful authentication to save on system resources when the user accesses it again.

2) The number of signature verifications during cross-domain authentication is reduced. This model constructs a blockchain network and records the hash value of the BCert in the form of a transaction on the blockchain. The transaction confirms that both parties are credible and realizes cross-domain authentication. This model solution transforms the original process of issuing a certificate to verify the signature into the more efficient process of verifying the certificate hash value. Furthermore, this process relies on a machine that is trusted by the blockchain and is proxied by the consortium blockchain platform to improve the efficiency further.

3) The BCert manages trust relationships among the trust domains. The BCert is proposed for the blockchain network by constructing a cross-domain authentication model based on blockchain. The BCert is designed as the key data, with transactions indicating the trust relationship and certificate status to be published in the blockchain. By recording these transactions on a blockchain that is jointly maintained by all trust domains and cannot be tampered with, the trust relationship between the BCert and trust domains in different states can be safely managed.

IV. SIMULATION EXPERIMENT AND RESULTS ANALYSIS

A. TECHNICAL PERFORMANCE ANALYSIS

The prototype of the scheme is based on the Hyperledger Fabric platform of the alliance blockchain. The blockchain consists of three nodes, including one order node and two peer nodes. Each node contains the same ledger.

In this study, the system performance was analyzed from the perspective of certificate proof relating to the above protocol, and the scheme was compared with that of [22] under the same conditions. The results are presented in Fig. 9. The *X*-axis indicates that several task queues are concurrent. Each task that is carried out in parallel is 1000 consecutive requests, whereas the task queue concurrency refers to a maximum of several tasks performing proof operations simultaneously. The *Y*-axis indicates the system throughput, which represents the rate of transactions submitted to the ledger. Table II displays the parameters of the experimental environment.

In the authentication stage, the new scheme performed better than that of [25] and provided higher throughput. This is because the blockchain is composed of three nodes, each of which has a complete ledger that can provide certification services. In this case, compared to the traditional scheme, its carrying capacity is 3:1, which means that if more nodes join the blockchain system, the system performance will be improved further, so it can perform better at this stage.

B. CALCULATION ANALYSIS

Compared with the method of [25], our scheme provided a reduction of 14 encryption and decryption operations, four digital signature and verification operations, and three bilinear mapping

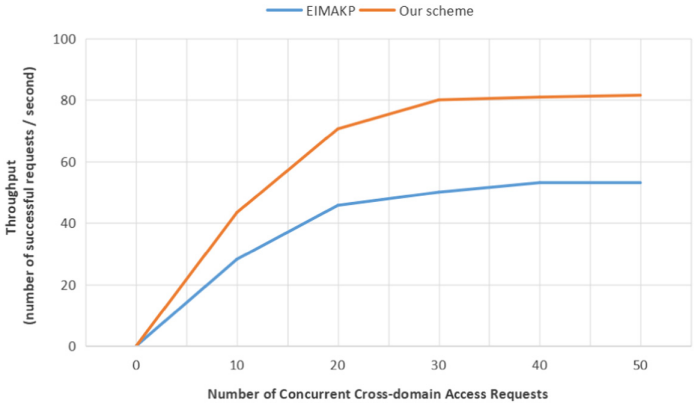

FIG. 9. Throughput experiment.

Table II. System parameters

Items	Explanation
Consensus algorithm	SOLO
Smart contract	Node SDK
Size	One orderer, two peers
Distribution	Single host

Table III. Calculation analysis

Scheme	Encryption/ decryption	Signature	Bilinear pairing	Hash
[25]	14	8	3	0
[26]	0	12	0	4
Our scheme	0	4	0	2

operations each time. Furthermore, our scheme added twice the hash algorithms. On the same configuration machine, the computing time of the 1024-bit RSA was approximately half of the 192-bit ECDSA, and that of the 256-bit Sha was approximately 1/101024-bit RSA. Therefore, the hash algorithm is more than a dozen times faster than the public key algorithm. Compared to the method of [26], our scheme reduced the number of digital signatures and verifications by eight times and reduced the hash algorithm twice each time.

The analysis in Table III demonstrates that the efficiency and carrying capacity of our scheme in achieving cross-domain authentication are considerable.

C. SECURITY ANALYSIS

1) Resisting internal attacks. In the blockchain, each block contains the hash value of the previous block. The block hash value will change if the transaction in the previous block is rolled back, deleted, or adjusted. Therefore, the consortium blockchain model exhibits tamper-resistant and traceability characteristics, which can guarantee the credibility of the node server and the security of the interdomain authentication process. Moreover, the proposed authentication scheme judges the validity of the identity by querying the BCerts and the BCert hash in each domain is stored in the blockchain. The hash function has unidirectional and anti-collision properties, thereby allowing any node connected to the blockchain to store trust credentials anonymously and securely. The authentication server submits the hash value of the file to the blockchain to provide the information and validity period in a timely manner.

2) Resisting man-in-the-middle attacks. During the authentication process, interactive messages between entities are signed by their private keys. If an attacker tampers with the message, the signed message cannot be verified by the receiver, thereby effectively resisting man-in-the-middle attacks.

3) Resisting counterfeit attacks. During the identity authentication between enterprises through the blockchain certificate, the attacker cannot imitate the user to obtain the information service. Furthermore, only after the signature verification is passed can the authenticated parties verify the identity of the other party. Therefore, an attacker cannot forge a valid signature message, and thus, cannot perform a forgery attack.

4) Resisting distributed denial of service attacks. As a type of trust credential, the blockchain exhibits the characteristics of multinode backup information. Even if an attacker destroys a node, the other nodes can still provide proof services to exchange commitments, which will effectively resist DDoS attacks and enhance system security. Therefore, even if certain nodes suffer DDoS attacks, the system can continue to operate normally.

5) Resisting replay attacks. The traditional challenge–response solution increases the system communication overheads, requiring at least three interactions between the sender and receiver. In the cross-domain authentication process of this solution, the interaction information between the interdomain interconnection module servers is guaranteed by the blockchain timestamp, which ensures the freshness of the message. Moreover, the authentication process uses a query–response handshake mechanism, which adds random numbers when passing messages. Before verifying the response message, the authentication server verifies the random number to ensure the correctness of the message. This solution uses a random number (the number used at one time) combined with a timestamp to ensure the same effect of challenge–response solution, while still reducing the number of interactions from three to two.

V. CONCLUSIONS

This paper has presented a blockchain model that can realize cross-domain authentication. Aimed at the frequent cross-authentication among different types of enterprises and users in large-scale heterogeneous networks, an efficient cross-domain authentication scheme based on blockchain has been designed. To overcome the disadvantage whereby IBE is not suitable for large-scale cross-domain architecture, this method introduces the blockchain without changing the existing PKI authentication model and proposes an authentication protocol combining the PKI environment and blockchain. It allows for communication across different IBE and PKI domains while ensuring the security of resource or service sharing in a distributed multidomain network environment. Moreover, it provides anonymity, as storing only the user's certificate hash in the blockchain can protect private information. The model offers good security and practicability, and it avoids the bottleneck of the traditional PKI model and complex authentication transfer. It is based on the blockchain design, with high scalability. We implemented a prototype system based on a hyper ledger structure to verify the proposed system. Compared to other methods, the computation and throughput are excellent, and our method offers the advantages of generality and simplicity.

In the future, we will strive to simplify the certification process and apply the proposed scheme in practice to identify and improve the shortcomings of the scheme, so as to achieve a more efficient cross-domain certification scheme.

Acknowledgment

This work was supported in part by Beijing Municipal Natural Science Foundation (19L2020), Foundation of Science and Technology on Information Assurance Laboratory (614211204031117), Industrial Internet Innovation and Development Project (Typical Application and Promotion Project of the Security Technology for the Electronics Industry) of the Ministry of Industry and Information Technology of China in 2018, Foundation of Shanxi Key Laboratory of Network and System Security (NSSOF1900105).

REFERENCES

[1] Y. X. Lai, Y. Liu, and J. Liu, "Trusted connection protocol between networks," Ruan Jian Xue Bao/J. Softw., 2019, 30(12): 3730–3749 (in Chinese). http://www.jos.org.cn/1000-9825/5603.htm

[2] Y. Liu, Y. X. Lai, S. Z. Yang and X. Lina, "Bilateral authentication protocol for WSN and certification by strand space model," Comput. Sci., vol. 46, no. 9, pp. 169–175, 2019.

[3] V. Lozupone, "Analyze encryption and public key infrastructure (PKI)," *Int. J. Inf. Manag.*, vol. 38, no. 1, pp. 42–44, Feb. 2018. DOI: 10.1016/j.ijinfomgt.2017.08.004.

[4] G. Enos and Y. Zheng, "An ID-based signcryption scheme with compartmented secret sharing for unsigncryption," *Inform. Process. Lett.*, vol. 115, no. 2, pp. 128–133, Feb. 2015. DOI: 10.1016/j.ipl.2014.08.002.

[5] Y. X. Sun, and L. I. Hui. "ID-based signcryption KEM to multiple recipients," Chin. J. Electron., vol. 20, no. 2, pp. 317–322, 2011.

[6] M. Alam, X. Zhang, K. Khan, and G. Ali, "xDAuth: a scalable and lightweight framework for cross domain access control and delegation," in SACMAT '11, Innsbruck, Austria, 2011. DOI: 10.1145/1998441.1998447.

[7] G. Miscione, R. Ziolkowski, L. Zavolokina, and G. Schwabe, "Tribal governance: the business of blockchain authentication," in HICSS 2018, Hawaii, USA, Jan. 2018. DOI: 10.2139/ssrn.3037853.

[8] Z. Guo, Z. Gao, H. Mei, M. Zhao, and J. Yang, "Design and optimization for storage mechanism of the public blockchain based on redundant residual number system," *IEEE Access*, vol. 7, pp. 98546–98554, 2019. DOI: 10.1109/ACCESS.2019.2930125.

[9] C. Cachin and M. Vukolić, "Blockchain consensus protocols in the wild," Keynote Talk, 2017.

[10] J. F. Lv, Y. X. Lai, and J. Liu, "Log security storage and retrieval based on combination of on-chain and off-chain," Comput. Sci., vol. 47, no. 3, pp. 298–303, 2019.

[11] M. R. Thompson, A. Essiari, and S. Mudumbai, "Certificate-based authorization policy in a PKI environment," *ACM TISSEC*, vol. 6, no. 4, pp. 566–588, Nov. 2003. DOI: 10.1145/950191.950196.

[12] Y. Yao, W. Xingwei, and S. Xiaoguang, "A cross heterogeneous domain authentication model based on PKI," in IEEE PAAP 2011, Tianjin, China, Dec. 2011, pp. 325–329. DOI: 10.1109/PAAP.2011.74.

[13] H.-X. Peng, "Identity-based authentication model for multi-domain," *Chin. J. Comput.*, vol. 29, no. 8, pp. 1271–1281, Aug. 2006.

[14] C. Wang, C. Liu, S. Niu, L. Chen, and X. Wang, "An authenticated key agreement protocol for cross-domain based on heterogeneous signcryption scheme," in 2017 13th IWCMC, Valencia, Spain, 2017, pp. 723–728. DOI: 10.1109/IWCMC.2017.7986374.

[15] Q. Huang, D. S. Wong, and G. Yang, "Heterogeneous signcryption with key privacy," *Comput. J.*, vol. 54, no. 4, pp. 525–536, Apr. 2011. DOI: 10.1093/comjnl/bxq095.

[16] Ministry of Industry and Information Technology, White paper on China's blockchain technology and application development, 2016.

[17] M. Grabatin and W. Hommel, "Reliability and scalability improvements to identity federations by managing SAML metadata with distributed ledger technology," in NOMS 2018, Taipei, Taiwan, Apr. 2018, pp. 1–6. DOI: 10.1109/NOMS.2018.8406310.

[18] W. Wang, N. Hu, and X. Liu, "BlockCAM: a blockchain-based cross-domain authentication model," in 2018 IEEE 3rd Int. Conf. DSC, Guangzhou, China, Jun. 2018. DOI: 10.1109/DSC.2018.00143.

[19] L. Axon and M. Goldsmith, "PB-PKI: a privacy-aware blockchain-based PKI," in SECRYPT 2017, Madrid, Spain, Jul. 2017, pp. 311–318. DOI: 10.5220/0006419203110318.

[20] K. Lewison and F. Corella, "Backing rich credentials with a blockchain PKI," Technical Report, Pomcor, Oct. 2016. https://pomcor.com/techreports/Blockchain%20PKI.pdf.

[21] L. Zhang, H. Li, L. Sun, Z. Shi, and Y. He, "Poster: towards fully distributed user authentication with blockchain," in 2017 IEEE Symp. PAC, Washington, DC, USA, Aug. 2017. DOI: 10.1109/PAC.2017.28.

[22] Z. Zhou, L. Li, and Z. Li, "Efficient cross-domain authentication scheme based on blockchain technology," *J. Comput. Appl.*, vol. 38, no. 02, pp. 316–320, 2018.

[23] N. Abdullah, A. Hakansson, and E. Moradian, "Blockchain based approach to enhance big data authentication in distributed environment," in IEEE 2017 9th ICUFN, Milan, Italy, Jul. 2017. DOI: 10.1109/ICUFN.2017.7993927.

[24] O. Ajayi, O. Igbe, and T. Saadawi. "Consortium blockchain-based architecture for cyber-attack signatures and features distribution," in 2019 IEEE 10th Annual UEMCON, 2019.

[25] C. Yuan, W. Zhang, and X. Wang, "EIMAKP: heterogeneous cross-domain authenticated key agreement protocols in the EIM system," *Arab. J. Sci. Eng.*, vol. 42, pp. 3275–3287, Feb. 2017. DOI: 10.1007/s13369-017-2447-9.

[26] W. Zhang, X. Wang, and M. K. Khan, "A virtual bridge certificate authority-based cross-domain authentication mechanism for distributed collaborative manufacturing systems," *Secur. Commun. Netw.*, vol. 8, no. 6, pp. 937–951, Jun. 2014. DOI: 10.1002/sec.1051.