Journal of Combinatorial Mathematics
and Combinatorial Computing
www.combinatorialpress.com/jcmcc

Combinatorial Press

Research on Network Data Security Integration Based on Blockchain Technology

Fang Yang[1,✉]

[1] *School of Computer Engineering, Shanxi Vocational University of Engineering Science and Technology, Jinzhong, Shanxi, 030606, China*

ABSTRACT

With the rapid development of informatization technology, the security of network data is more and more emphasized. In this study, ECDSA digital signature algorithm and PBET consensus algorithm are adopted to construct a network data security model based on blockchain technology. The system in this paper consists of three functional modules: application interaction client, federation chain Fabric module and data storage module DHT, which are further logically divided into five parts: initialization, identity registration, uploading data, querying data and permission revocation. The average CPU occupation of each component of the system ranges from 0.02% to 39.96%, which consumes low resources, and the maximum value of the time used by the system for data encryption and decryption and signature authentication is no more than 41ms, which is a relatively fast operation speed, and it can support the operation of the network data security system, and the designed system has relatively high security in resisting the attack of the authentication process, and it utilizes the decentralized characteristics of blockchain to resist the attacks of the distribution process, and it utilizes the blockchain to resist the attacks of the distribution process. Centrality to resist distributed denial of service (DDoS) attacks and replay attacks. This study provides lessons and references for the application of blockchain technology in network data security.

Keywords: Ecdsa digital signature, pbet consensus, blockchain, network data, security system

1. Introduction

The computer Internet brings great convenience to people's lives while leaving a greater security risks, network information contains many important personal information, once leaked will cause serious consequences that can not be estimated [1-2]. Nowadays, people's dependence on the Internet is increasing, and it is more important to do a good job of network information security management to prevent information leakage and improve information security [3-4].

✉ Corresponding author.
E-mail address: jshryf2021@163.com (F. Yang).
Received 05 March 2024; Revised 25 May 2024; Accepted 05 December 2024; Published Online 15 April 2025.
DOI: 10.61091/jcmcc127a-194

In the new era, in order to improve network security management, the use of blockchain technology has been a general trend [5]. The blockchain system adopts a partitioned data management structure, and carries out the operation of the refined contract mechanism [6], so as to complete the independent interaction of the nodes in the system, thus enabling the user to independently complete the storage and maintenance of data under the mechanism that does not require the participation of intermediaries [7], which has the characteristics of decentralization, and is capable of effectively preventing the loss of information and the leakage of information caused by accidental events, system intrusion and other security factors [8-9].

Blockchain network, as an important network distributed architecture, plays an important role in encryption algorithms and storing data [10]. By applying network database nodes and blockchain protocols, the encryption, updating and storage of network privacy data can be achieved to improve the efficiency of network decentralization [11] and minimize the cost of privacy data protection. The blockchain network architecture is mainly divided into two major parts: the support platform and the blockchain core, in which the blockchain core, as an important hierarchical structure, mainly contains the contract layer, the consensus layer, and the data layer. In this hierarchical structure, each layer has strength functions such as retrieval query and data encryption [12-13].

The blockchain-based network security technology is essentially a partitioned autonomous data management system, which emphasizes the security protection function of each node and is able to operate through an autonomous way in accordance with the relevant needs; it can be robustly prevented against malicious threats inside and outside the network [14]. This strict, rigorous, and scientific divisional autonomous data management system can also make full use of the blockchain security protection capability when facing insecure network environments, effectively blocking attacks from inside and outside, and maximizing the support of network data and information security [15].

Literature [16] proved experimentally that personal information can leak out. In the Internet environment, a large amount of sensitive data is transferred without adequate notification to the user, and the user's perception of risk to the Internet is lower than the perception of risk to the Internet. Literature [17] proposed a privacy-preserving blockchain-based model for secure data sharing in industrial IoT to ensure secure sharing of resources in industrial IoT, and under validation concluded that this model is correct and secure. Literature [18] suggests that in the Internet era, the key issue currently faced is the network-based IoT cybersecurity problem, and solving this problem which is of great significance for the future development of IoT cybersecurity. Literature [19] points out that more and more big data (including sensitive and confidential business data) are being accessed and stored by a range of IoT devices such as our mobile devices, and as a result, any vulnerabilities in IoT devices, operating systems or software may be exploited by cybercriminals in order to steal our data. Literature [20] provides a comprehensive survey of blockchain in smart grid cybersecurity, presenting the latest insights into ideas, architectures, and implementation techniques related to the use of blockchain in smart grid cybersecurity. Literature [21] points out that the inherent cryptographic properties of blockchain systems are sufficient to withstand constant hacking and security threats, but there are still many applications that fall victim to successful cyber-attacks. Literature [22] provides privacy and data protection of blockchain solutions in response to hacking incidents and relates it to regulatory framework provisions, and information about existing blockchain solutions. Literature [23] classifies blockchain attempts to overcome IoT limitations into four categories: end-to-end traceability, data privacy and anonymity, authentication and certification, and confidentiality, security and scalability.

Based on the network data sharing business scenario, this study proposes a new threshold signature scheme that can be compatible with the dynamic elliptic curve digital signature algorithm (ECDSA) of the current blockchain transaction system. It is also combined with the view transformation method of smart contracts based on the PBET consensus algorithm to build a network data security model and realize the distributed hosting of assets in the exchange. Meanwhile, the network data security system

based on blockchain technology is constructed on the basis of this algorithm. Finally, from the functional modules and logical architecture of the system, the performance of the system and the performance of network data security integration are tested, and the processes such as two-way entity authentication, tracking of the attacker's ID, defense against DDoS attacks, replay attacks and man-in-the-middle attacks, etc., are provided for the research of network data security.

2. Blockchain network data security model construction

The blockchain network data security model designed in this paper contains ECDSA digital signature algorithm and PBFT consensus algorithm, which serve to ensure the integrity and authenticity of the data during transmission with maintaining the consistency and integrity of the distributed ledger, respectively.

2.1. ECDSA digital signature algorithm

The steps of the algorithm are as follows:

Step1: Initialization Setup. Select an elliptic curve E/F_q, where $q = 2^m$, from which a set of ECDSA domain parameters $D=\left(E,\mathrm{F}_q,G,n\right)$ can be obtained, where G is the generating element on the curve and n is integrable q [24].

Step2: Key Generation KeyGen. Generate a public key based on the domain parameters selected in the Setup phase, select a random integer $x\in\left[1,n-1\right]$ as the key, and compute the public key:

$$Y = xG \tag{1}$$

Step3: Generate Signature Sig Gen. Sign message m with the key generated above. Choose a random integer $k\in\left[1,n-1\right]$ and compute it:

$$kG=\left(x_1,y_1\right) \tag{2}$$

Calculations:

$$r = x_1 \bmod n \tag{3}$$

Calculations:

$$h=H\left(m\right) \tag{4}$$

Where H is a one-way hash function, is computed:

$$s=k^{-4}\left(h+xr\right)\bmod n \tag{5}$$

Signature (r,s) is a tuple consisting of r and s.

Step4: Verify Verify. the user receives the verification data $(r,s)\|m$ and verifies the following signatures, checks the integers r and $s\in\left[1,n-1\right]$, and computes:

$$h=H\left(m\right) \tag{6}$$

Verify the signature by computing equation (7) below:

$$X=hs^{-1}G+rs^{-1}Y\left(\bmod n\right) \tag{7}$$

If:

$$x_i = r \bmod n \tag{8}$$

where x_1 is the x-coordinate of x, then the signature is accepted.

2.2. PBFT Consensus Algorithm

1) Overview of PBFT consensus algorithm. The PBFT algorithm is optimized on the basis of the BFT algorithm to reduce the complexity of the algorithm to polynomial level, which is able to tolerate a few node failures or evils, so that the distributed system can reach a consensus in this case[25].

The PBFT mechanism is able to tolerate $f=\left[(n-1)/3\right]$ incorrect node under the premise of guaranteeing security and system effectiveness, n denotes the total number of nodes, and f is the number of Byzantine nodes that can be tolerated. In other words, if there are f Byzantine nodes in the current distributed system, PBFT needs to be satisfied in the case of $n \geq 3f+1$ in order to ensure the consistency of the system.

2) Consistency protocol. Consistency protocol is one of the core protocols of PBFT consensus mechanism, which consists of three main phases: pre-preparation, preparation and submission. PBFT consensus mechanism can tolerate the nodes in the system to ensure the consistency and accuracy of message delivery in the event of failure, malicious behavior or inaction. In the consensus mechanism, the process of node consensus is the process of verifying the transactions in the chain and packing them into blocks, a block corresponds to multiple transactions that have been verified and passed by the nodes, and finally the blocks generated by consensus authentication are uploaded into the blockchain.

There are three main types of nodes in the PBFT mechanism: client nodes, master nodes and deputy nodes. Among them, Client is mainly responsible for sending the received request to the primary node, Primary is responsible for receiving the request and packing it, only one Primary node exists in one consensus process, and Replica is responsible for inter-block consensus. The consensus process of PBFT consensus mechanism is shown in Figure 1.

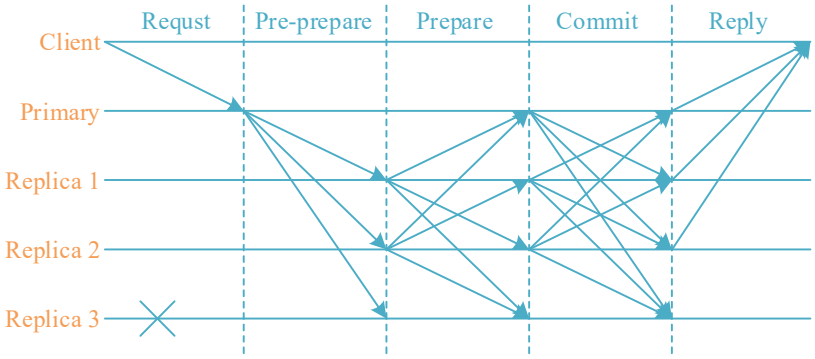

Fig. 1. Flow chart of the PBFT algorithm

3) View switching. When the PBFT consensus mechanism carries out data consensus, if the master node has a node failure or evil behavior and does not broadcast the request sent by the client within the specified time, resulting in the consensus process cannot be carried out normally. At this time, the slave node will trigger the view switching protocol and request to replace the master node. Once the nodes participating in the consensus receive $f+1$ view replacement message, the system will restart the election of a new master node to open a new round of consensus. The view number of the new master node is calculated as shown in equation (9):

$$p = v \bmod |R| \tag{9}$$

where v denotes the view number and $|R|$ denotes the total number of nodes.

3. Architecture design of blockchain-based network data security system

3.1. System Functional Module Design

The functional module design of this system is shown in Figure 2, which is divided into three modules: application interaction client, federation chain Fabric module and data storage module DHT. The role of each module is as follows:

The application client provides a friendly operation method for users, who interact with the blockchain module by calling the SDK through the client, and send the privacy data that need to be saved to the blockchain module after encrypting it through the client together with the access policy.

The blockchain module receives the client's request, executes the corresponding smart contract according to the request parameters, and writes the result of the execution into the blockchain ledger after passing the consensus according to the transaction process.

The data storage module DHT receives the request from the blockchain module to store data, stores the secret text in the DHT, receives the request from the blockchain module to query the data, and returns the corresponding secret text to the blockchain module.

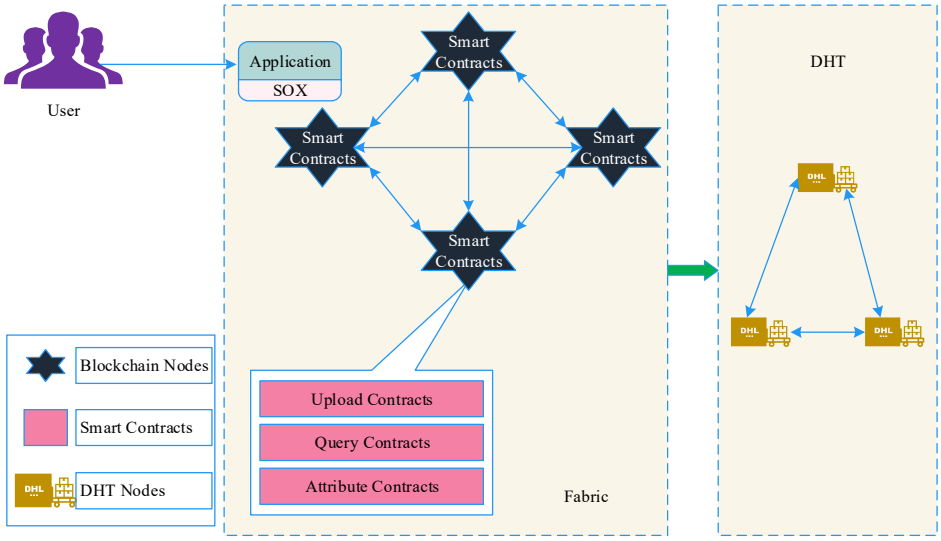

Fig. 2. System functional module design

The users in this system are data owner denoted by letter A and data requester denoted by letter I. The smart contracts are attribute contract, upload contract and query contract. The roles of the roles are as follows:

Attribute contract: adds or removes user data attributes and maintains the attribute list based on the request of the data owner.

Upload contract: uploads data into the DHT and maintains the upload list.

Query contract: when the data requester requests to view the ciphertext, verify the attribute set of the data requester, determine whether it satisfies the access privileges set by the data owner, and if it satisfies, decrypt the ciphertext for the first time and send the decryption result to the data requester. If it is not satisfied, the service is denied.

I: Provide identity information and apply for key. Query data.

A: Initialize the key. Based on the identity information of the data requester, issue the attribute key for it. Revoke the data requester's attribute. Upload encrypted data. Generate permission control tree.

3.2. System Logical Architecture

The whole system is divided into five parts, which are initialization, identity registration, uploading

data, querying data and permission revocation. The timing diagram of the whole system is shown in Fig. 3.

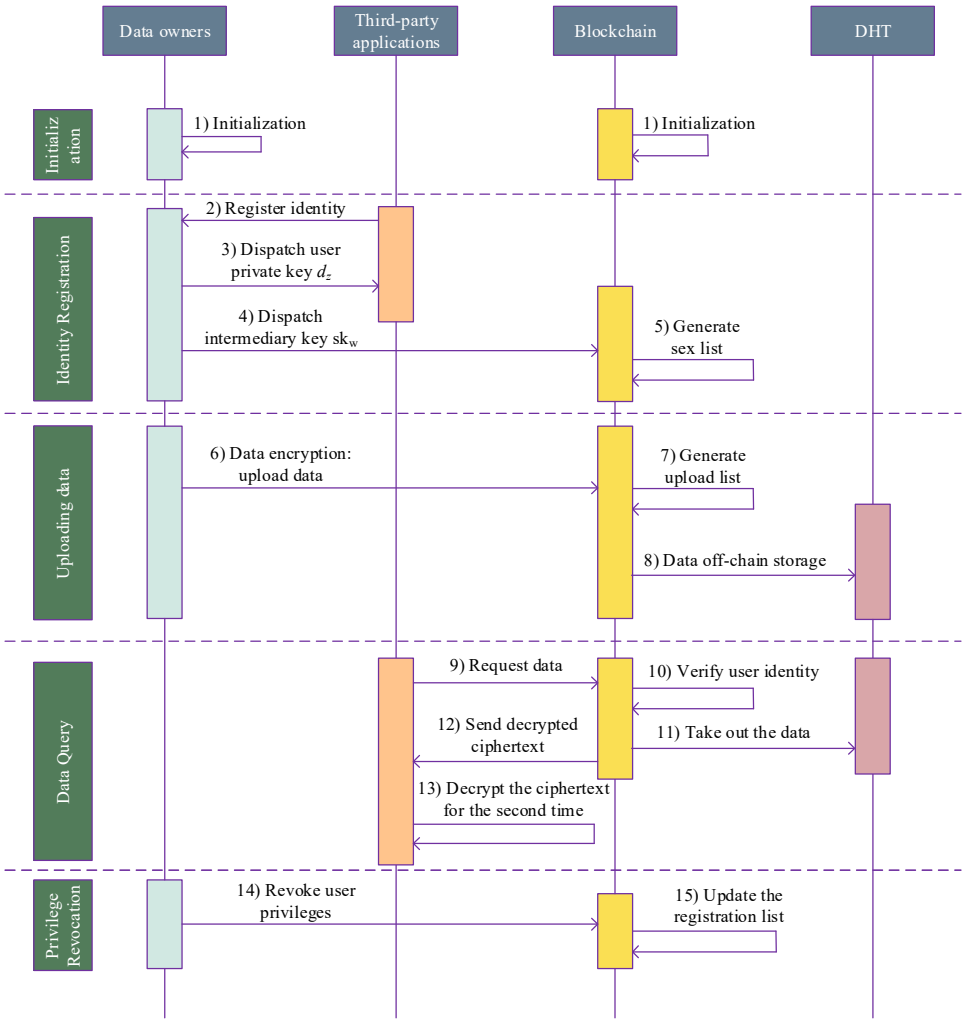

Fig. 3. Timing diagram of personal data protection

3.2.1. Initialization. The system initialization process is divided into two parts, one for the initialization of the Fabric network and the other for the initialization of the server. The details are as follows:
1) Fabric network initialization, start Fabric network nodes through Docker containers, write chaincode, i.e., smart contracts, package and show instantiated smart contracts, deploy instantiated smart contracts to Fabric network, and issue certificates for users in the system.
2) A generates a bilinear mapping based on the security parameters, performs Setup(k), generates the keys required by the system, the public key pk and the master-private key mk, and generates A's corresponding identity Auid.

3.2.2. Identity registration. Users in the system first need to register their identity and get their attribute key by providing their identity information. The detailed process is as follows:
1) I provide identity information Iu and attribute set ω.
2) A reviews the identity and attribute information provided by I and generates a unique identity Iuid for I after passing the review.
3) A enters the master key, the set of attributes of I, and the Iuid, and the client computes the private key $(sk_{\omega I_u,1}, sk_{\omega I_u,2}) = Keygen(mk, \omega, I_u)$ from the input.

4) A sends {Auid, Iuid, ω, $sk_{\omega I_u,1}$} to the blockchain attribute contract over a secure channel, and sends $sk_{\omega I_u,2}$ over a secure channel to I. The secure channel in this paper is implemented through the secure transport protocol TLS, which protects the confidentiality and integrity of information.
5) The client sends a registration request to the blockchain by calling SDK, and the blockchain executes the corresponding attribute smart contract according to the request information, generates the attribute list, and writes the content of the list to the ledger, in which the intermediary key is deposited in the form of a hash into the world ledger, and the real key is stored in the private dataset, which ensures the security of the private key. The attribute list is shown in Table 1.

Table 1. List of attributes

Serial number	Data Owner ID	Data requester ID	Attribute set	Mediation key
1	A_{uid}	I_{uid}	ω'	$H(sk_{\omega I_u,1})$

3.2.3. Data upload
1) A first performs an encryption operation on the data m to be uploaded and computes the ciphertext $c_\tau = Encrypt(m, \tau, pk)$.
2) A sends the identity Auid, the policy tree τ, the keyword of data m and the ciphertext c_τ to the upload contract.
3) The blockchain executes the transaction process, and the upload contract calculates the hash of the data keywords, i.e., it calculates $ht = SHA-256(m)$. ht as the key in the DHT and c_τ as the value in the DHT, and stores the data in the DHT. An upload list is generated and written to the blockchain ledger, and the contents of the list are shown in Table 2.

Table 2. List of attributes Serial number

	Data Owner ID	Data keywords	Privilege control tree
1	A_{uid}	$mKey$	τ

3.2.4. Access to data

1) I provides the identity I_{uid} and the keyword of data m and sends it to the query contract.

2) SDK calls the query contract to query the attribute list in the ledger based on I_{uid} and return I_{uid} the corresponding attribute set ω. Query the upload list based on the keyword hash of data m and return τ. Verify whether ω is satisfied τ, if so, take out the ciphertext c_τ from DHT and decrypt the ciphertext for the first time, i.e., execute the following algorithm:

$$c_\tau' = m\_Decrypt\left(c_\tau, sk_{\omega I_u,1}, I_u\right) \tag{10}$$

Return the result to I. If it is not satisfied, the service is denied.

3) I executes the following algorithm after getting the result returned by the query contract:

$$m = Decrypt\left(c_\tau', sk_{cI_u,2}\right) \tag{11}$$

Get plaintext m, or resubmit the request if you don't get a return result.

3.2.5. Revoking user privileges. When A needs to revoke the whole permission or part of the permission of I because of the change of demand, it initiates the transaction request of changing the attribute to the blockchain through SDK. Firstly, it finds the corresponding attribute record through the IDs of A and I, and then initiates the request to update the attribute record through the certificate of A. After the blockchain verifies the user's certificate, it updates the attribute list in the ledger, i.e., it modifies ω corresponding to I to ω', and ω' is the new set of attributes of I. If ω' is null, it means that the whole user's privilege has been revoked, and then after the coalition chain goes through the consensus algorithm, it writes the modified new attribute list into the block chain ledger. When I requests data again, the query contract queries the latest attribute list to determine whether I's attributes satisfy the access policy.

4. System testing and application analysis

4.1. System performance testing

This paper uses the Hyperledger Caliper test framework to test the performance of each part of the designed network data security system, this paper tested the blockchain network encryption and decryption, signature authentication performance through 60,000 data transaction information, and the test results are shown in Figure 4.

From Fig. 4, it can be seen that the system takes the shortest time to perform data decryption, and the minimum, average and maximum values are 1.1ms, 1.3ms and 1.5ms, respectively.The system takes the longest time to perform data signing, and the minimum, average and maximum values are 8ms, 18ms and 41ms, respectively.The system takes the maximum value of the time for data encryption, decryption and signature authentication which is not more than 41ms, and this system has high efficiency in integrating network data security.

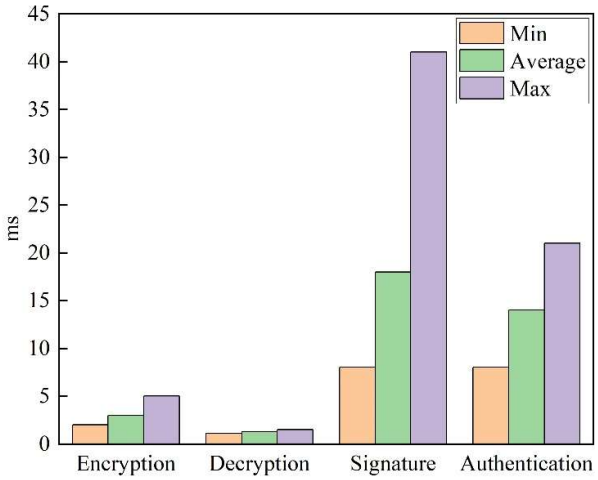

Fig. 4. Performance of system data encryption, decryption, signature, and authentication

The resource consumption index of the system in this paper is shown in Table 3. As shown in Table 3, when the system is running tests, the range of maximum and average memory values are 5.9M~361.4M and 5.9M~321.7M respectively, the range of maximum and average CPU occupancy are 0.23%~93.28% and 0.02%~39.96% respectively, and the range of traffic inflow and outflow are 2.2K~18.1M and 0.07K~31.2M. The component resource consumption is low and the system runs well.

Table 3. Resource consumption

Types	Memory(max)	Memory(avg)	CPU(max)	CPU(avg)	Flow in	Flow out
Process	-	-	NaN%	NaN%	-	-
Docker 1	361.4M	318.6M	18.29%	13.23%	18.1M	31.2M
Docker 2	352.2M	321.7M	19.34%	13.72%	16.9M	30.4M
Docker 3	8.1M	7.5M	5.25%	0.79%	6.8K	4.6K
Docker 4	5.9M	5.9M	0.23%	0.02%	2.2K	0.07K
Docker 5	20.5M	18.4M	3.98%	3.17%	4.1M	5.9M
Docker 6	111M	101M	57.56%	39.48%	4.5M	8.3M
Docker 7	108M	92M	52.46%	39.96%	4.7M	8.4M
Docker 8	129.3M	126.4M	87.48%	38.71%	5.5M	3.9M
Docker 9	148.8M	139.2M	93.28%	36.21%	5.9M	3.6M

Finally, the metrics of time spent for authentication, configuration file download and upload time in terms of system operation were measured and the results are shown in Table 4. From Table 4, it can be seen that in the system operation test, the time spent by the system in performing authentication, configuration file download and upload time ranges from [8ms, 19ms], [7ms, 10ms] and [369ms, 410ms] respectively. , the total time of system operation is in the range of 389~434ms, the system runs faster and performs well.

Table 4. Measurements of authentication, profile download, and upload times

Serial number	Verification/ms	Download/ms	Upload/ms	Total time/ms
1	8	7	410	425
2	12	9	394	415
3	13	7	369	389
4	19	8	382	409
5	18	9	407	434
6	13	10	410	433
7	11	9	354	374

From the analysis of the above data, while guaranteeing the safe storage and management of network data, the consumption of resources of each component is not very high, and the operation speed is fast, which can better support the operation of the network data security system.

4.2. System Security Analysis

4.2.1. Two-way entity authentication. The bi-directional entity authentication model is shown in Fig. 5, and entity authentication goes through four main parts: the master chain node MA distributes certificates to the UA within the domain, the intra-domain authentication process changes the certificate state to issue, the master chain consensus passes the message of the certificate state issue to the other slave chains corresponding to the master chain nodes by consensus, and the cross-domain authentication process changes the node UA's authentication privileges. The trust transfer completes the corresponding transformation from certificate state issue to node authentication authority executable continue1 through 11 steps. The systems designed in this paper all carry out two-way authentication communication between nodes, and the local storage device corresponding to each step node saves the relevant data of the node with which it communicates, which facilitates the efficient realization of authentication in the future reverse authentication process.

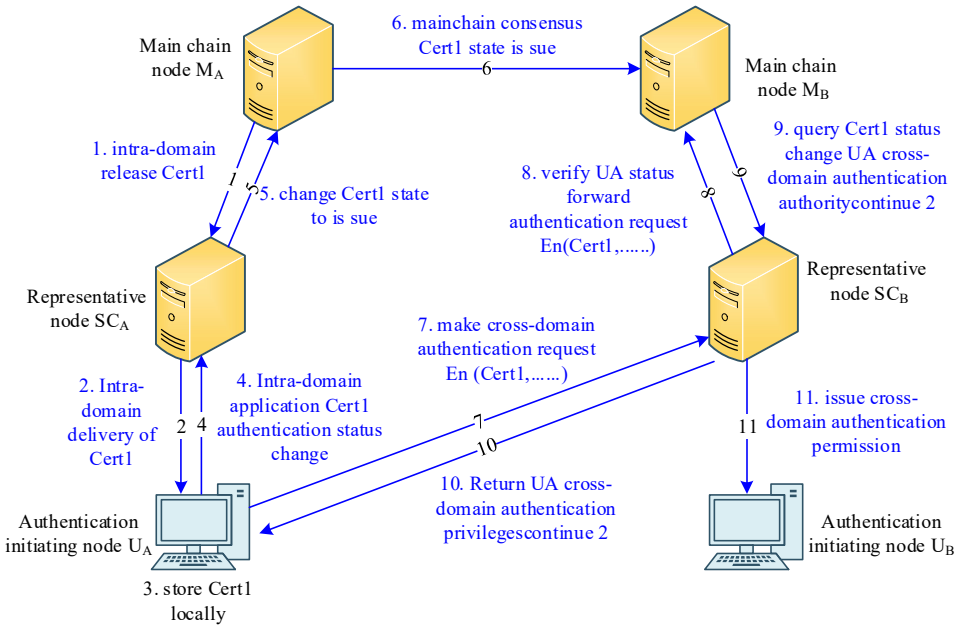

Fig. 5. Mutual entity authentication model

4.2.2. Identity tracking. The system determines whether the node is legitimate by the following ways: SCN uses its own private key to decrypt the encrypted message sent by UN, SCN calculates and obtains the true identity IDUN of node UA through its own DNSCA and the DNUA obtained by decryption, SCN

calculates the temporary identity of UN TIDUN2 through the formula, and compares it with the temporary identity TIDUN1 in the message sent by UN, if the two temporary identities are different, it is determined that the node is an illegal node, and the IDUN calculated in this process is the identity of the illegal node that is tracked, so the system can carry out identity anonymity tracking.

4.2.3. Resistance to Distributed Denial of Service (DDoS) Attacks. The system introduces blockchain technology, using its own characteristics, even if one or more nodes fail, as long as the number of valid nodes is within the threshold required by the PBFT consensus algorithm, the correct consensus mechanism can be completed, and the overall consensus results will not be affected, which can solve the problem of node failure caused by DDoS attacks. The introduction of blockchain scheme against denial of service attacks is much more flexible than the centralized system, once the node fails, the UN connected to the failed node will not be able to enter the system.

4.2.4. Resistance to replay attacks. The anti-replay attack model is shown in Fig. 6, if the attacker intercepts the message by eavesdropping or other means, and uses illegal means to obtain the function of this authentication message, he or she may obtain illegal privileges by re-sending the message. Therefore, the two sides of the system communication are first time synchronized to ensure that the timestamp selection is valid, and then the node adds a timestamp T to each message delivered in the authentication process, which is used to keep the message fresh. When the target node receives a message, it will verify the timestamp T. If the timestamp T in the message exceeds the validity period, it is recognized that it has received a replay attack and the authentication fails. Thus this system is effective against replay attacks.

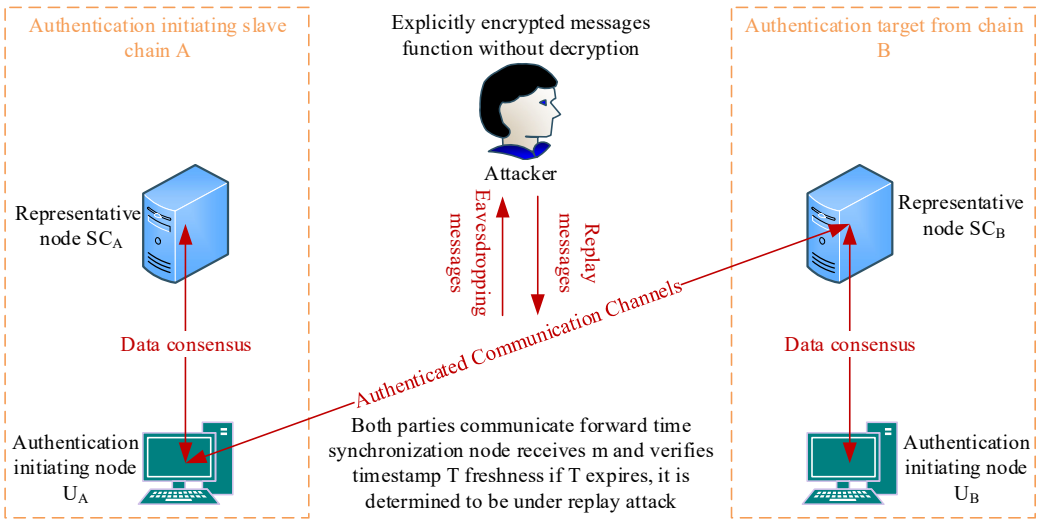

Fig. 6. Model of resisting replay attack

4.2.5. Resistance to man-in-the-middle attacks. Anti-Man-in-the-Middle Attack Model As shown in Fig. 7, the system may be subjected to man-in-the-middle attack without the knowledge of both nodes when they interact with each other for cross-domain authentication access. In this paper, the following two methods are used to solve this problem. On the one hand, a hybrid encryption algorithm combining symmetric encryption and asymmetric encryption is used to protect the message, as long as the security of the private key is ensured, the key security of the symmetric encryption algorithm is guaranteed, so that the adversary can not decrypt the ciphertext to obtain the data and tamper with the data, which ensures the authenticity of the transmitted message. On the other hand, digital signatures are added in the process of message transmission, even if the adversary intercepts the message, uses the receiver's public key to forge a new encrypted message, and passes it to the receiver,

the private key of the requesting party is unavailable, and therefore cannot form a signature on the message. Therefore, the system designed in this paper can resist man-in-the-middle attacks to some extent.

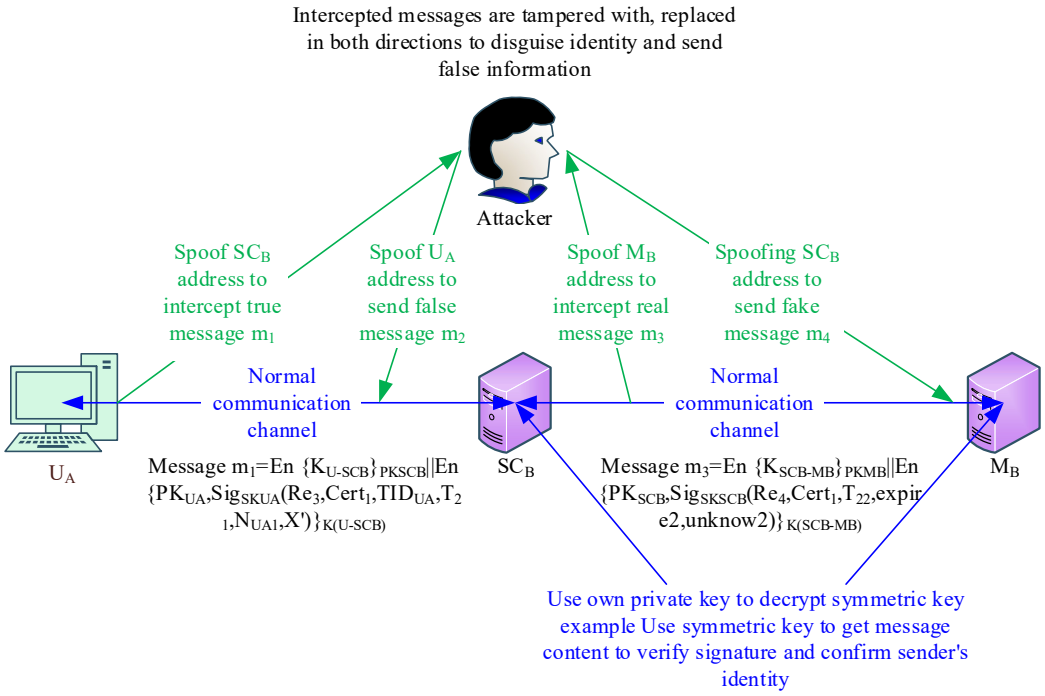

Fig. 7. Model of resistance to man-in-the-middle attack

The results show that the network data security system designed in this paper has relatively high security in resisting attacks on the authentication process. The system realized two-way entity authentication by introducing blockchain certificates as trust credentials for accessing heterogeneous resources and establishing a trust relationship between two trust domains. The system resists man-in-the-middle attacks by encrypting and signing messages with public keys. The system introduces temporary identity to achieve identity anonymity, and utilizes hierarchical ID tree to construct node UN identities, which realizes the tracking of attacker IDs. The scheme introduces a master-slave blockchain structure and resists distributed denial-of-service attacks by utilizing its own decentralized characteristics to solve the single-point-of-failure problem. The attacker cannot obtain the private key of the participating nodes, cannot decrypt to obtain the message content, and cannot form the signature of the message to verify its own identity; at the same time, the attacker cannot obtain the temporary identity TIDUN, and the slave chain representative node SCN cannot successfully verify the message when it verifies the message, and resists the replay attack.

5. Conclusion

This study combines ECDSA digital signature algorithm and PBET consensus algorithm to build a blockchain network data security model, constructs a network data security system based on blockchain technology, and tests the performance and security of the system.

The system in this paper consists of three functional modules: application interaction client, federation chain Fabric module and data storage module DHT, and the whole system is divided into five parts: initialization, identity registration, uploading data, querying data and authority revocation.

The performance test results show that the maximum value of the time used by the system for data encryption and decryption and signature authentication is no more than 41ms, and the maximum

value of the time used for identity verification, configuration file download and uploading time is 19ms, 10ms and 410ms respectively. this indicates that the system runs faster and has good performance. In the system operation test, the range of time spent by the system in performing authentication, configuration file download and upload time are [8ms, 19ms], [7ms, 10ms] and [369ms, 410ms] respectively. This indicates that the resource consumption of the components is low and the system runs well.

The system designed in this paper has relatively high security against attacks on the authentication process. The system utilizes blockchain decentralization and data encryption and authentication technology to achieve two-way entity authentication and tracking of attacker ID, resists man-in-the-middle attacks through public key encryption and signing of messages, solves the problem of single-point-of-failure, and resists distributed denial-of-service attacks and replay attacks, so the system has a high level of security.

The system in this paper guarantees the network data security storage and management while its various components consume less resources, run faster, can better support the operation of network data security system, can resist all kinds of attacks, has higher security, and can provide reference for the research of network data security.

In the system test section, although a series of performance indicators are provided, including the response time and resource consumption of the system, they lack the comparison data with their system. In the latter study, the comparison experiment was introduced to show the specific advantages of the system compared to other similar technologies.

References

[1] Singh, R. , Kumar, H. , Singla, R. K. , & Ketti, R. R. . (2017). Internet attacks and intrusion detection system: a review of the literature. Online Information Review, 41(2), 171-184.

[2] Song, I. H. . (2020). Positive and negative influences of the internet on suicide. Atherosclerosis, 151(1), 12.

[3] Li, R. , Tian, B. , Li, Y. , & Qu, Y. . (2019). Information security evaluation based on artificial neural network. International Journal of Performability Engineering(11), 15.

[4] Gao, H. , Wu, J. , Wei, C. , & Wei, G. . (2019). Madm method with interval-valued bipolar uncertain linguistic information for evaluating the computer network security. IEEE Access, 7(99), 151506-151524.

[5] Li, L. . (2017). Integration of information security and network data mining technology in the era of big data. Acta Technica CSAV (Ceskoslovensk Akademie Ved), 62(1), 157-165.

[6] Toyoda, K. , Mathiopoulos, P. T. , Sasase, I. , & Ohtsuki, T. . (2017). A novel blockchain-based product ownership management system (poms) for anti-counterfeits in the post supply chain. IEEE Access, 1-1.

[7] Zhen, H. , Zehua, W. , Wei, C. , & Victor, L. . (2017). Blockchain-empowered fair computational resource sharing system in the d2d network. Future Internet, 9(4), 85.

[8] Ma, C. , Huo, F. , & Shi, A. . (2023). Framework of interaction design method based on blockchain system. Journal of Internet Technology.

[9] Elagin, V. . (2021). Towards practical applications in modeling blockchain system. Future Internet, 13.

[10] Sato, T. , Shimosawa, T. , & Himura, Y. . (2022). Operations smart contract to realize decentralized system operations workflow for consortium blockchain. IEICE Transactions on communications(8), E105/B.

[11] Mladenov, V. , Chobanov, V. , Seritan, G. C. , Porumb, R. F. , Enache, B. A. , & Vita, V. , et al. (2022). A flexibility market platform for electricity system operators using blockchain technology. Energies, 15.

[12] Feng, L. , Zhang, H. , Tsai, W. T. , & Sun, S. . (2019). System architecture for high-performance

permissioned blockchains. Frontiers of Computer Science, 13(006), 1151-1165.

[13] A, J. W. , A, K. H. , B, A. A. , B, Z. C. , B, Z. Z. , & C, Y. P. , et al. (2020). A blockchain-based ehealthcare system interoperating with wbans. Future Generation Computer Systems, 110, 675-685.

[14] Park, Y. H. , Kim, Y. , & Shim, J. . (2021). Blockchain-based privacy-preserving system for genomic data management using local differential privacy. Electronics.

[15] He, J. , Zhang, Z. , Li, M. , Zhu, L. , & Hu, J. . (2018). Provable data integrity of cloud storage service with enhanced security in internet of things. IEEE Access, 6226-6239.

[16] Youngjoo, L. , Wonseok, Y. , & Taekyoung, K. . (2018). Data transfusion: pairing wearable devices and its implication on security for internet of things. IEEE Access, PP, 1-1.

[17] Zhang, Q. , Li, Y. , Wang, R. , Liu, L. , Yu‐an Tan, & Hu, J. . (2020). Data security sharing model based on privacy protection for blockchain‐enabled industrial internet of things. International Journal of Intelligent Systems.

[18] Jingtao, Y. , Li, Z. , & Junlei, Q. . (2018). Design of an internet of brain things network security system based on icn. IEEE Access, PP(99), 1-1.

[19] Christian J. D'Orazio, Choo, K. K. R. , & Yang, L. T. . (2017). Data exfiltration from internet of things devices: ios devices as case studies. IEEE Internet of Things Journal.

[20] Zhuang, P. , Zamir, T. , & Liang, H. . (2020). Blockchain for cyber security in smart grid: a comprehensive survey. IEEE Transactions on Industrial Informatics, PP(99), 1-1.

[21] Hasanova, H. , Baek, U. J. , Shin, M. G. , Cho, K. , & Kim, M. S. . (2019). A survey on blockchain cybersecurity vulnerabilities and possible countermeasures. International Journal of Network Management, 29(2), 1-36.

[22] Kolokotronis, N. , Limniotis, K. , Shiaeles, S. , & Griffiths, R. . (2019). Blockchain technologies for enhanced security and privacy in the internet of things. IEEE Consumer Electronics Magazine, 8(3).

[23] Alotaibi, B. . (2019). Utilizing blockchain to overcome cyber security concerns in the internet of things: a review. IEEE Sensors Journal, 19(23), 10953-10971.

[24] Jiby J. Puthiyidam, Shelbi Joseph & Bharat Bhushan. (2024). Temporal ECDSA: A timestamp and signature mask enabled ECDSA algorithm for IoT client node authentication. Computer Communications307-323.

[25] Liu Juan, Deng Xiaohong, Li Wangchun & Li Kangting. (2024). CG-PBFT: an efficient PBFT algorithm based on credit grouping.Journal of Cloud Computing(1).