A User Authentication Schema Under the Integration of Mobile Edge Computing and Blockchain Technology

Feng Xue, Zhengzhou University of Economics and Business, China*

Fangju Li, College of Computer and Artificial Intelligence, Zhengzhou University of Economics and Business, China

ABSTRACT

The safe and efficient authentication of users is the basis for the realization of the Internet of Things. A reliable and fast user authentication schema that combines mobile edge computing and blockchain technology is proposed. This schema adopts the polling hosting method to optimize the practical Byzantine Fault Tolerance (PBFT) algorithm, it reduces the impact of tokens in the algorithm, and ensures trusted authentication. The two-way authentication protocol between the cluster head and the base station, and the one-way authentication protocol between the base station and the sensor node are designed to effectively simplify the authentication process of sensor nodes, which further guarantees the security and speed of user authentication and effectively meets the security, reliability, and convenience requirements of the Internet of Things. Simulation experiments show that the schema can achieve efficient information verification, and the identity authentication time and protocol authentication times are only 23.58 ms and 25.06 ms, respectively, which has obvious performance advantages over the Paillier algorithm, the hybrid Paillier-blowfish algorithm, and the ElGamal algorithm.

KEYWORDS

bidirectional authentication protocol, blockchain, mobile edge computing, Internet of Things, practical Byzantine fault tolerant algorithm, smart contracts, user authentication

A USER AUTHENTICATION SCHEMA UNDER THE INTEGRATION OF MOBILE EDGE COMPUTING AND BLOCKCHAIN TECHNOLOGY

User identity authentication technology is used to identify entity identity in the network world. Correct identity authentication and identification are primary gateways of establishing information system protection; moreover, it is the fundament of building the mutual trust relationship between communication parties (Kaladevi et al., 2022; Su & Long, 2021; S. Wang et al., 2020).

DOI: 10.4018/IJACI.327027

*Corresponding Author

The mobile Internet of Things (IoT) has many problems in data sharing, for example, data redundancy, data security cannot be guaranteed, and a low efficiency of data sharing (Cui et al., 2022; Sandhiya et al., 2021).

Mobile edge computing can decentralize the computing and storage task of central nodes by using multiple edge nodes with the aim of reducing the burden of central nodes; it has been widely applied in mobile networks (Chen et al., 2021; H. Q. Liu et al., 2022; W. Zhang et al., 2022). As a result, it is crucial to introduce moving edge computing to propose an efficient user authentication algorithm.

Traditional user identity authentication schemes mainly include offline identity authentication and centralized electronic identity authentication (Z. Wang et al., 2020). Both have privacy problems that include excessive exposure of user information, which makes it easy to disclose a user's privacy information (Gao et al., 2021; Hongbin & Zhi, 2023).

The current rapid development of blockchain technology provides new methods to solve the above problems. The emergence of blockchain technology handles the trust problems that exist in traditional centralized applications, enabling all blockchain nodes to successfully complete data interaction without mutual trust. Many existing schemes often have the following problems (Chen et al. 2023): 1) Edge nodes lack reliable authentication protocols, which leads to certain security risks in the received data from terminals; 2) While ensuring trusted identity authentication, the blockchain network layer is prone to significant storage or computational burden; 3) The overall computational and communication costs of the system are difficult to balance, resulting in poor real-time service response.

Different strategies can be adopted in face of the previously mentioned three issues. Among these are:

Problem 1: It is necessary to design a reliable authentication protocol at the edge nodes.

Problem 2: It is necessary to adopt a suitable consensus mechanism that ensures the trustworthy performance of the network system while reducing the load on the blockchain network layer.

Problem 3: By optimizing each layer or the lightweight designing of each layer, computing and communication costs can be effectively reduced.

To better solve these problems in the existing schemes, an efficient user authentication scheme is proposed that integrates mobile edge computing and blockchain technologies. The main innovation points are as follows:

1) The Practical Byzantine Fault Tolerance (PBFT) algorithm (Garcia et al., 2022) is optimized, and the polling hosting method is used to eliminate the influence of tokens in the algorithm, reduce the storage and calculation burden of the blockchain, decrease the complexity of the algorithm, and enhance the computational efficiency of the algorithm.
2) The authentication protocol of mobile edge computing node is designed. The protocol includes a bidirectional authentication protocol between the cluster head and the base station, and a one-way authentication protocol of base station to sensor node. The protocol can effectively simplify the sensor node authentication process, further ensure the analysis speed of the authentication algorithm, and meet the safe, reliable, and real-time response requirements of the IoT effectively.

RELATED RESEARCH

IoT devices have also shown explosive growth in the era of the rapid development of hardware. Efficient authentication of device users is the basis of realizing the interconnection of everything in the IoT (Sun et al., 2022; M. Zhang et al., 2022).

A successful example of an offline identity verification method is the citizen ID card. However, the user is still required to carry a variety of information for identity verification, which brings with it the risk of excessive leakage of resident information (Prajapati, & Gupta, 2022).

Online centralized authentication has also made some progress (Zhao et al., 2022). Lv et al. (2020) relies on the proxy analysis mode and using the methods of "password-key" and "temporary identity-real identity" to realize the transformation of password signatures between cloud centers. Zheng et al. (2021) combines hash function with random numbers and other technologies to design an authentication protocol for telemedicine scenarios to ensure the security of users' private data. Digital ID is used as the global identifier of the network to ensure the anonymity and security of transaction information.

On the contrary, centralized electronic identity authentication has two main disadvantages:

1) Unified certification is difficult. The process of centralized electronic identity authentication is cumbersome, and there are problems such as slow interaction, time-consuming, and poor practicality, which makes the cross-domain authentication between platforms inefficient (Zhang et al., 2020).
2) Privacy protection is difficult (G. Zhang et al., 2022). Centralized electronic identity authentication relies on the credibility of the authentication center, to a large extent. User identity data needs to be uploaded and stored on the central server (Jia et al., 2020). Therefore, there are security threats such as user privacy information disclosure and malicious behavior of the central server.

Blockchain has unique technical rules and obvious advantages in data security and rights protection (J. Liu et al., 2022). Ren et al. (2020) endow each node in the distributed energy trading system with computing processing capability, which implements user authentication and logs recordings based on blockchain. Research by Zou et al. (2021) is aimed at the scenario of the power IoT, a digital authentication method with full cycle management designed to realize the independent authentication and security sharing management of heterogeneous users. Wang et al. (2022) adopted the method of regional connection to solve the problem of data islands; it also achieves secure access and authentication between multiple regions. M. Zhang et al. (2022) introduced blockchain technology into the research of Internet of Vehicles identity authentication, including identity registration and authentication, for the purpose of reducing the security risk of identity authentication. W. Zhang et al. (2022) proposed a Paillier homomorphic encryption-based blockchain audit scheme for IoT, which can effectively reduce communication costs and computation while ensuring high security. However, these schemes often fail to address the data storage pressure of blockchain (Zang et al., 2023).

The introduction of mobile edge computing can solve the storage pressure of the blockchain (Xia et al., 2021). Cheng et al. (2021) introduced blockchain technology, elliptic encryption algorithm, etc., to further ensure reliability and security on the basis of ensuring that edge computing releases the pressure of central verification processing. Table 1 is the characteristics comparison of methods from the abovementioned related references.

In the current IoT application scenario, in addition to the safe and reliable verification of users, the efficiency of analysis and processing needs to be ensured (Zhao et al., 2020; Ma et al., 2020). Therefore, it is necessary to effectively reduce the storage and computing burden of blockchain and realize lightweight user authentication.

Mobile edge computing can combine with blockchain and complement one another. This paper combines mobile edge computing and blockchain technology, proposes a reliable and fast user authentication algorithm, optimizes the PBFT algorithm, and designs an authentication protocol for mobile edge computing nodes, ensures trusted authentication, and effectively meets the security, reliability, and convenience requirements of the IoT.

Table 1. Characteristics comparison of methods from related references

Schemes	System Architecture	Authentication Method	Security	Service Response Real time
Lv et al., 2020	Cloud	Centralized	Medium	Low
Zheng et al., 2021	Cloud	Centralized	Medium	Low
Wang et al., 2022	Cloud	Centralized	High	Low
Ren et al., 2020	Blockchain	Distributed	Medium	Medium
Zou et al., 2021	Blockchain	Distributed	Medium	Medium
Wang et al., 2022	Blockchain	Distributed	High	Medium
M. Zhang et al., 2022	Blockchain	Distributed	High	Medium
W. Zhang et al., 2022	Blockchain	Distributed	High	High
Cheng et al., 2021	Edge Computing+ Blockchain	Distributed	High	High

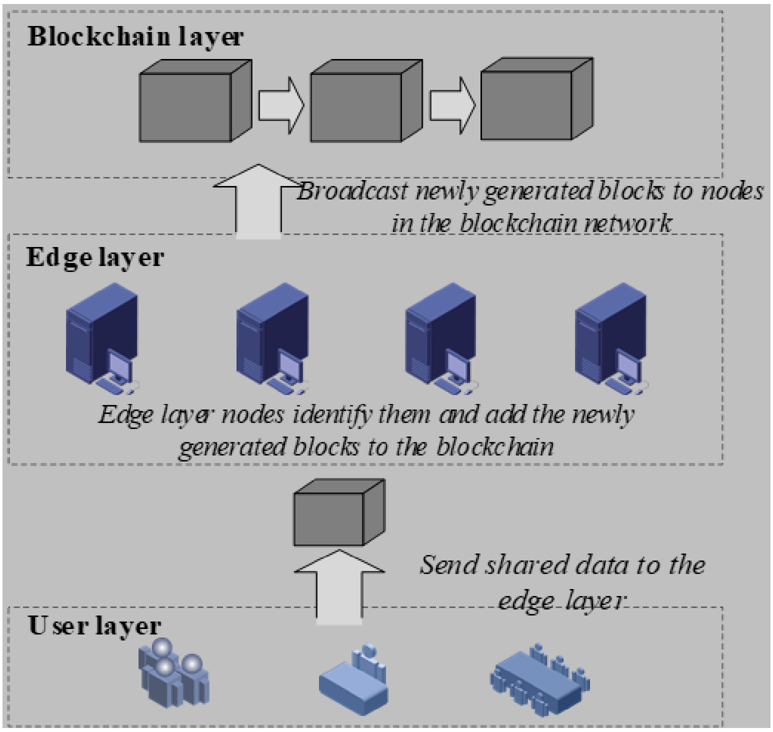
ALGORITHM MODEL OF MOBILE EDGE COMPUTING AND BLOCKCHAIN TECHNOLOGY INTEGRATION

Fusion Algorithm Framework Model

Aiming at the risk factors in edge networks, an efficient user authentication scheme based on blockchain and edge computing is proposed. Figure 1 is the framework, which is based on the public blockchain, including user layer, edge layer, and blockchain network layer.

1) **User Layer:** Many IoT terminal devices establish connections with edge nodes through the user layer. Due to the mobility and dispersion of edge nodes, the convergence of edge computing and blockchain can improve the real-time response capability of the system and the data security of edge nodes effectively. For example, in the intelligent connected vehicle system, the intelligent vehicle can perform real-time computing of the data in real time and transmit the data that has passed the security authentication to other nodes.
2) **Edge Layer:** The edge layer is mainly divided into two types of nodes, namely highly trusted server nodes and IoT edge nodes. The edge nodes of the Internet of Things are responsible for resolving domain names, verifying the identity of newly added nodes, conducting transactions, and submitting blocks to the blockchain network. Only through the authentication system can highly trusted server terminals provide data offloading services and synchronize authentication data in a timely manner to ensure the safe and reliable monitoring of edge nodes.
3) **Blockchain Network Layer:** The blockchain network stores terminal information and creates smart contracts through the Hyperledger Fabric to provide distributed services. When registering into the blockchain through the Internet of Things terminal, the terminal can select the nearest highly trusted node in the system to complete registration through the known domain name resolution protocol. In order to solve the threats posed by malicious and illegal terminals to data security and privacy, consensus algorithms are utilized at the blockchain network layer to ensure communication security and anonymity of terminal identity. In order to minimize the resource waste caused by repeated task offloading, the existing resources in the blockchain system are utilized to provide efficient services for blockchain terminals. The smart contract will add the results to the blockchain ledger after each task offloading and synchronously broadcast them to other blocks. In addition, in the proposed scheme, while verifying user information, it will also verify whether the data requested by the user has been stored in the blockchain. If so, caching can be directly requested without issuing an offload request to the base station.

Figure 1. Data sharing framework of edge network


Blockchain layer
Broadcast newly generated blocks to nodes in the blockchain network
Edge layer
Edge layer nodes identify them and add the newly generated blocks to the blockchain
Send shared data to the edge layer
User layer

User Authentication Layer

The purpose of the protocol in the user authentication layer is to ensure the legitimacy of the participants in the network and the confidentiality of the transmitted data.

According to the application scenario of the model, users need to communicate with sensors securely. Thus, the protocol also needs to negotiate session keys to ensure secure communication.

As shown in Figure 2, the model of the system is a single-mesh joint model. The contents are as follows:

The first part is the user. When it accesses the network, it needs to authenticate and negotiate the session key with the sensor node.

The second part is the gateway node, which represents the communication bridge between the sensor node and user. The gateway node has unlimited resources in communication, computing, storage, and other aspects, and is capable of performing various complex operations.

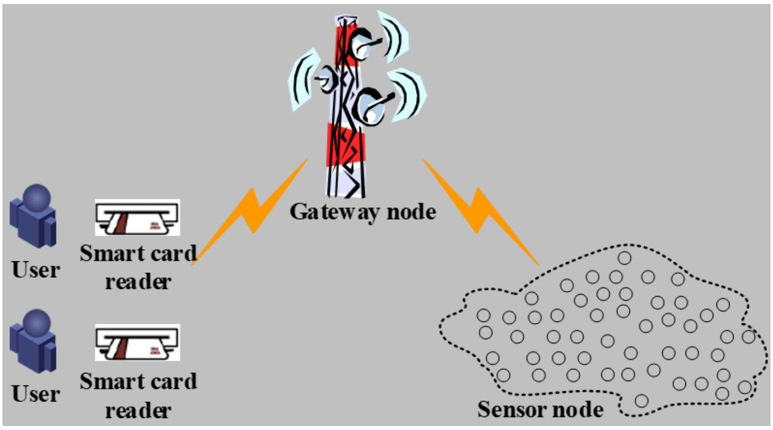
The third part is abundant sensor nodes in the environment to be monitored, which detect the environment and collect data. The resources of sensor nodes are limited, such as short communication distance and weak computing power.

Edge Layer

The existence of the mobile edge layer extends the connectivity of mobile devices and enhances data storage, processing, and management of users using the same connection. Edge computing can also handle some privacy and large-scale computing problems.

The edge server is close to the user device; its latency is usually lower than other computing platforms. Mobile devices do not have to wait for highly centralized platforms to provide services, so the demand rate of services in the edge network is higher.

Figure 2. Model diagram of user authentication layer



Blockchain Layer

The blockchain node will broadcast to other peers after generating blocks, so all peers will store the same data. When a node crashes, the system can connect to other nodes to work.

Figure 3 shows the structure of blocks in the blockchain. The block body stores data that needs to be recorded and cannot be changed. The node hashes these data to generate a Merkle tree, and finally obtains a Merkle tree root value. Due to the nature of Merkle tree, once the data is tampered with, the calculated root of the Merkle tree will change.

For the purpose of better ensuring the "decentralization" of blockchain, the smart contract model allows the system to automate traceable, irreversible, and secure transaction processes without the need for third-party audits. A smart contract contains all relevant information during the transaction process, and the requesting node can only execute consensus operations if it meets the established consensus conditions of the system. The essential difference from traditional paper contracts is that smart contracts are automatically generated by computers. Based on this, a new smart contract activation rule is proposed.

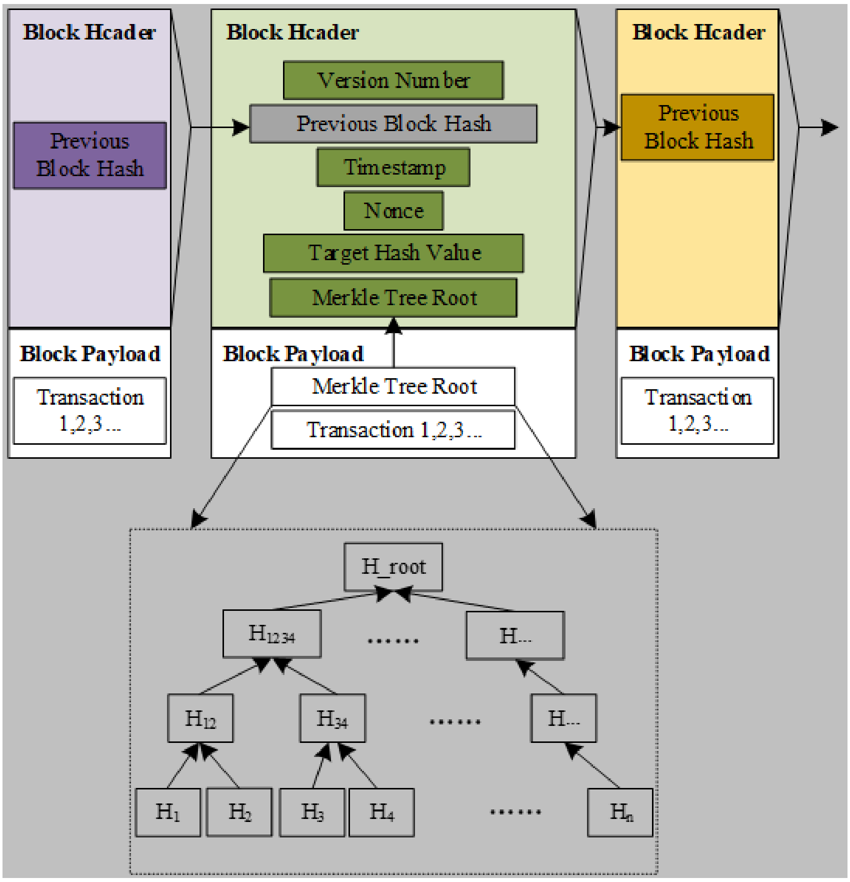
Blockchain has the characteristic of distributed storage. In order to better ensure the correctness and consistency of each node's ledger, the Practical Byzantine Fault Tolerance (PBFT) algorithm is selected as the consensus algorithm of the system.

Smart Contract Model

The blockchain network layer furnishes distributed services by storing terminal information and creating smart contracts through the Hyperledger Fabric (Melo et al., 2022). Hyperledger Fabric, also known as "chain codes," is a customizable blockchain platform that supports the creation of smart contracts. As a distributed vendor, Hyperledger Fabric uses optimized consensus algorithms to store authentication logs in an orderly manner. Each block records a timestamp and a unique password signature in the ledger, enabling traceability of terminal activities.

In addition to the consensus algorithm for security assurance, smart contracts are the most important core component in Hyperledger Fabric, which are mainly responsible for integrating various protocols in the IoT platform and developing practical and effective execution rules for consensus nodes. The proposed access mechanism for mobile edge computing nodes based on smart contracts is shown in Figure 4. The activation rules designed for highly trusted nodes and blockchain edge nodes are as follows:

Figure 3. Blockchain layer structure



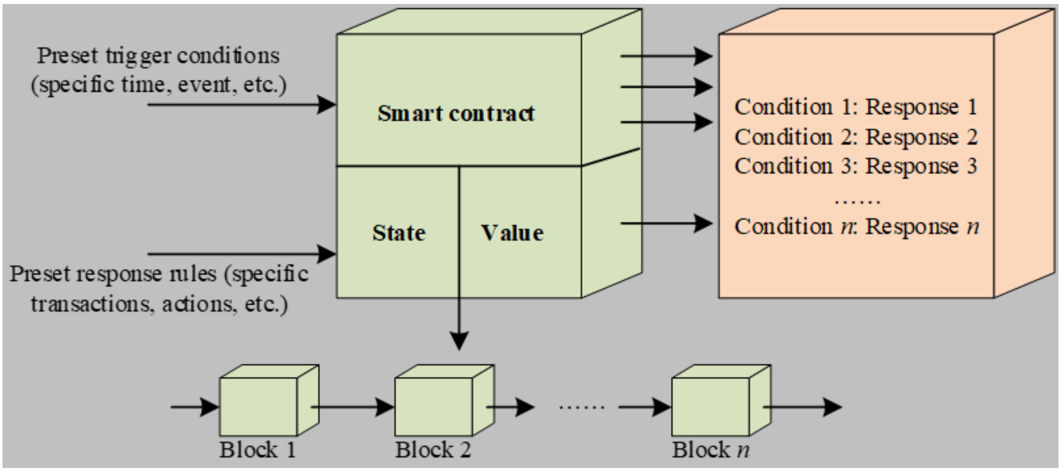
1) When the new node establishes communication with any node in the blockchain, the node encrypts its information, transmits it to the highly trusted node in the block for identity authentication, generates identity information, and broadcasts it to the whole network.
2) When a node with ID in the blockchain sends a task offload request to a highly trusted node, it needs to pass the consensus authentication of each blockchain edge node. The contract triggers the appropriate highly trusted node through the address resolution protocol after the verification of multiple nodes. When the trigger condition is met, the highly trusted node will automatically execute the task-unloading request.
3) The highly trusted node caches the result of the task-unloading request into the blockchain account book and synchronizes the whole network to facilitate the IoT terminals in the blockchain to obtain data.

N-PBFT Algorithm

Aiming to satisfy the requirements of high real-time performance, the No token required Practical Byzantine Fault Tolerance (N-PBFT) algorithm is adopted. The consensus process of N-PBFT is as follows:

Step 1: The client sends a request to the main node for performing an operation.

Figure 4. Execution mode of smart contract



Step 2: The main node sends over the request to all backup nodes.

Step 3: After receiving the preparation message, all backup nodes, including the primary node, verify the message, confirm that the information is correct, perform the operation, and inform the client of the result.

Step 4: When the client receives identical results from 3f+1 different nodes, the process ends, and the result is recognized as the final consensus. Among them, f represents the number of nodes allowed to fail.

The IoT terminals are scattered in the edge network, and it is hard to obtain their accurate IP address and identity information. In this case, the proposed N-PBFT algorithm can improve the trust efficiency.

After receiving the authentication result, the federation node writes the authentication log into the chain through the optimized consensus algorithm.

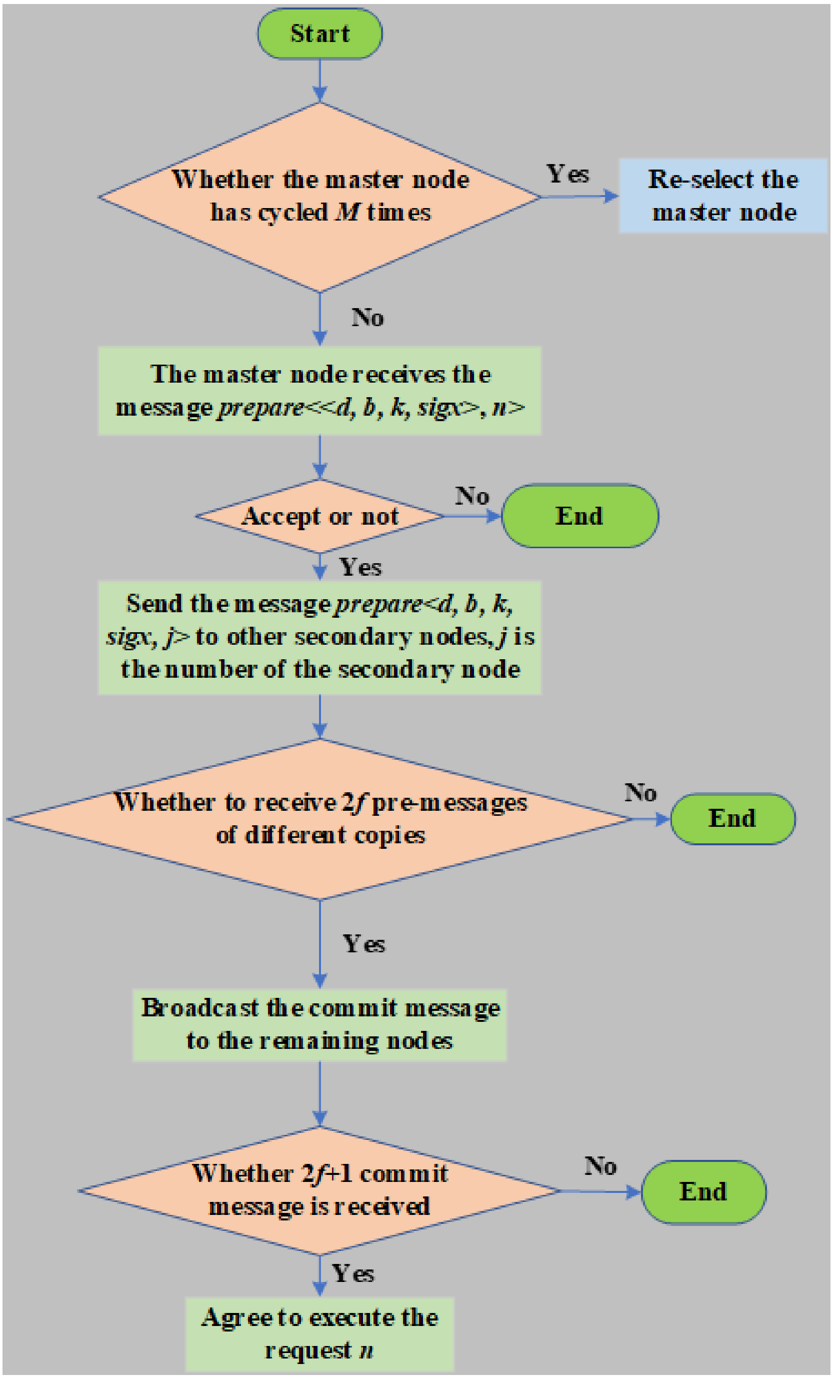
This paper assumes that there are a total of M nodes in the system. In the process of reaching consensus on each round, one node will be selected as the host and the other nodes as the member nodes. The chair does not have effect on the consensus results. The chair may participate in the consensus process on M times. After M times, the chair of the system will be replaced.

The host node M_i is selected by formula $i = (j \bmod M) + 1$, where j is the height of the current block. The edge node can send over the authentication results to the federation node.

Define j to represent the time interval for generating blocks. After the j interval, M_i broadcasts the message $preprepare < d, b, k, Sig_i >$ to all candidate nodes. d represents the viewing identity, b is the message summary, and Sig_i is the summary signature of the speech node, as shown in Figure 5.

After receiving the message $preprepare$ within the working times M of the primary node, judge the message credibility and send it to the secondary node to verify the message and signature. If the secondary node agrees that the message is true, M_j broadcasts the content $prepare < d, b, k, Sig_j >$ to the other nodes for authentication, and then continues to calculate the received messages from other member nodes. Sig_j represents the signature of the M_j node. If the message $prepare < d, b, k, Sig_j >$ is received by different member nodes than $2f + 1$, the number of witch nodes cannot exceed $f =| (M - 1) / 3 |$. When receiving more than $f + 1$ submission messages, the

Figure 5. N-PBFT algorithm flow


Start
Whether the master node has cycled *M* times
Yes
Re-select the master node
No
The master node receives the message *prepare<<d, b, k, sigx>, n>*
Accept or not
No
End
Yes
Send the message *prepare<d, b, k, sigx, j>* to other secondary nodes, *j* is the number of the secondary node
Whether to receive 2*f* pre-messages of different copies
No
End
Yes
Broadcast the commit message to the remaining nodes
Whether 2*f*+1 commit message is received
No
End
Yes
Agree to execute the request *n*

master node can identify that the consensus has been completed and generate a block in the blockchain ledger. The authentication log will send over in the edge node, update its ledger, and execute the request n . If the verification fails, the block will be discarded, then the next round of consensus will be fulfilled.

Network Authentication Protocol

In this certification scheme, it is mainly divided into two parts:

1) Authentication between the base station and the cluster head.
2) The base station appraises the sensor node and stores the authentication information of the sensor node in the blockchain safely after the authentication.

Authentication of Base Station and Cluster Head

In this scheme, by referencing the idea of the lightweight authentication center (LCA), the private key of the trusted LCA is used to sign the public key of the requesting node.

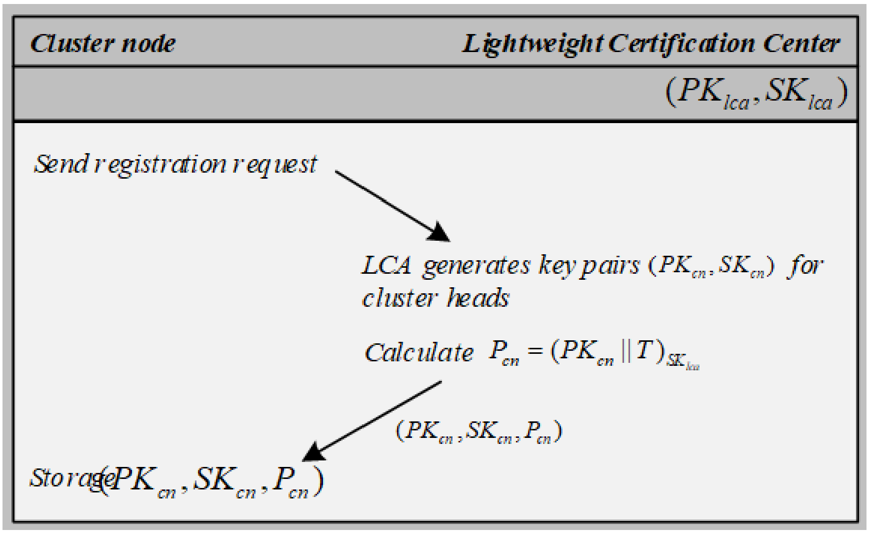
In the authentication process, if the public key signature of the node is signed by LCA and that node has a private key matching the public key, then it is proved that the node is a legal node. In this scheme, the public key cryptography algorithm of elliptic curve is used.

LCA registers the cluster head and the base station, that is, LCA signs the public key of the node. Figure 6 shows the offline operations for this phase.

The specific steps are as follows:

1) LCA selects an elliptic curve E, whose generator is G, and randomly selects a random number to generate the public and private key pair (PK_{lca}, SK_{lca}) of LCA.
2) After the LCA receives the application, it generates a pair of keys (PK_{cn}, SK_{cn}) for the cluster head, and then the LCA uses its own private key to sign $P_{cn} = (PK_{cn} \,||\, T)_{SK_{lca}}$ on the public key, where T is the valid time of PCN. Once the effective time is exceeded, LCA will send a re-sign request to ID_{cn} to change the P_{cn}, and the overdue P_{cn} cannot be used again.
3) The operation of the base station is the same as that of the cluster head, and the information $(PK_{bs}, SK_{bs}, P_{bs})$ is finally saved.

Figure 6. Node registration flow chart


Cluster node
Lightweight Certification Center
(PK_{lca}, SK_{lca})
Send registration request
LCA generates key pairs (PK_{cn}, SK_{cn}) for cluster heads
Calculate $P_{cn} = (PK_{cn} \,||\, T)_{SK_{lca}}$
$(PK_{cn}, SK_{cn}, P_{cn})$
Storage $(PK_{cn}, SK_{cn}, P_{cn})$

Before the network is deployed, the public keys of the base station and the cluster head nodes have been signed by LCA. It only needs to determine the validity and legitimacy of the signed public key to complete the authentication process .

The specific step is as follows:

(1) The cluster head node generates a random number C_1 and a timestamp T_1, and uses the elliptic curve to calculate $U_1 = (r(C_{cn} \mid\mid T_1))_{SK_{cn}}$ and $U_2 = (C_{cn} \mid\mid P_{cn})_{PK_{bs}}$. Then, the cluster head node sends the information (U_1, U_2, T_1) for authentication.

(2) After receiving the information, the BTS generates a random number C_2 and a timestamp T_2 to verify whether it is within the specified time range, then uses the public key PK_{lca} of LCA to calculate P_{cn} to get PK_{cn} and T, namely $(P_{cn})_{PK_{lca}} = (PK_{cn} \mid\mid T)$. Check whether it is within the valid time range. If it is not, stop the operation. Otherwise, calculate $r(C_{cn} \mid\mid T_1)$ and compare it with $(U_1)_{PK_{cn}}$. If it is not equal after comparison, it indicates that the private and public key pairs of the cluster head nodes do not match, or the message is tampered with by the attacker, and the operation is stopped. The base station calculates the authentication information $U_3 = (r(C_{bs} \mid\mid T_2))_{SK_{bs}}$, $U_4 = (C_{bs} \mid\mid P_{bs}))_{PK_{cn}}$ and $U_5 = r(Y \mid\mid T_2)$.

(3) After receiving the information, the cluster head node generates a timestamp T_3. Then, the node of cluster head decrypts the U_4 with the private key SK_{cn} to obtain C_{bs} and P_{bs}, and then calculates P_{bs} with the LCA's public key PK_{lca}, namely $(PK_{bs} \mid\mid T) = (P_{bs})_{PK_{lca}}$. Check whether it is within the valid time range, then calculate $r(C_{bs} \mid\mid T_2)$ and compare it with $(U_3)_{PK_{bs}}$. Then, calculate $Y = C_{bs}C_2$, $r(Y \mid\mid T_2)$ and compare it with U_5.

Authentication of Base Station and Sensor Node

In the scenario of user access authentication, the user finally communicates with the sensor node to obtain information. The network system model of this scheme is mainly used for sensors to collect information. The cluster head node then summarizes and processes such scenarios sent to the base station (Ma et al., 2020).

The first authentication and non-first authentication of sensor nodes is different. Before the network layout, the sensor node presets a secret parameter related to the base station. Therefore, when the sensor node performs the first authentication, it needs to forward information through the node of the cluster head and authenticate it with the base station.

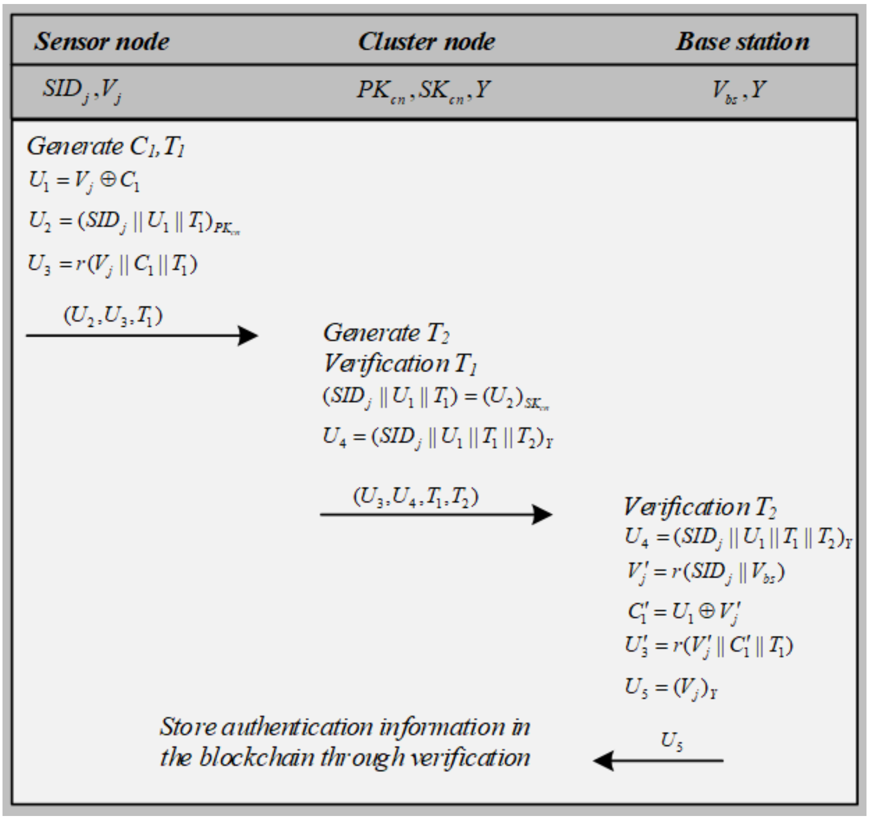
According to the unchangeable characteristics of the blockchain data, when the sensor node authenticates again, it can authenticate through the information stored on the blockchain. According to the distributed storage characteristics of the blockchain, sensor nodes that move across clusters can be authenticated no matter which cluster head node they are in.

Initialization phase: The base station generates a secret parameter V_{bs}.

Offline setting of sensor nodes: the base station selects an identity SID_j for each sensor node, calculates $V_j = r(SID_j \mid\mid V_{bs})$, and sends (SID_j, V_j) to the sensor node for saving.

Authentication phase: initial authentication of sensor nodes, as shown in Figure 7. The step is as follow:

Figure 7. Sensor node authentication diagram


Sensor node
Cluster node
Base station
SID_j, V_j
PK_{cn}, SK_{cn}, Y
V_{bs}, Y
Generate C_1, T_1
$U_1 = V_j \oplus C_1$
$U_2 = (SID_j \| U_1 \| T_1)_{PK_{cn}}$
$U_3 = r(V_j \| C_1 \| T_1)$
(U_2, U_3, T_1)
Generate T_2
Verification T_1
$(SID_j \| U_1 \| T_1) = (U_2)_{SK_{cn}}$
$U_4 = (SID_j \| U_1 \| T_1 \| T_2)_Y$
(U_3, U_4, T_1, T_2)
Verification T_2
$U_4 = (SID_j \| U_1 \| T_1 \| T_2)_Y$
$V_j' = r(SID_j \| V_{bs})$
$C_1' = U_1 \oplus V_j'$
$U_3' = r(V_j' \| C_1' \| T_1)$
$U_5 = (V_j)_Y$
U_5
Store authentication information in the blockchain through verification

(1) The sensor node generates random number C_1 and timestamp T_1 to calculate $U_1 = V_j \oplus C_1$. Then, uses the cluster head node's public key to encrypt and calculate $U_2 = (SID_j \| U_1 \| T_1)_{PK_{cn}}$ and $U_3 = r(V_j \| C_1 \| T_1)$.

(2) After receiving the information, the cluster head node generates a timestamp T_2 to verify whether it is within the specified time range. The cluster head decrypts U_2 with the private key to obtain SID_j, U_1 and T_1. Then, the session key Y between the node of the cluster head and the base station is used to symmetrically encrypt the information and calculate $U_4 = (SID_j \| U_1 \| T_1 \| T_2)_Y$, and a timestamp is added to the information to prevent replay attacks.

(3) After receiving the information, the base station verifies whether it is within the specified time range. Then, the U_4 is decrypted to obtain SID_j, U_1, T_1 and T_2. The base station uses the secret parameter V_{bs} to calculate $V_j' = r(SID_j \| V_{bs})$, and then calculates $C_1' = U_1 \oplus V_j'$ and $U_3' = r(V_j' \| C_1' \| T_1)$.

(4) The cluster head node calculates $r(V_j)$ and signs it with the private key. Then, the information is sent to the blockchain constructed by the cluster head. Other cluster heads verify the signature, use the consensus mechanism to generate blocks, and store the information in the blockchain.

The above authentication process is the first time that a sensor node enters the network for authentication, so the steps are relatively cumbersome. However, after that, the authentication information of sensor nodes is distributed and stored in the blockchain using the concept of the blockchain data structure model in the protocol. When the node is re-authenticated, the authentication information stored in the blockchain can be used for authentication.

SIMULATION ANALYSIS

Experimental Scenario

Experiment Configuration Table

The software and hardware environment for the simulation experiment is constructed according to Table 2, including the hardware test environment and software tool configurations. Among them, one CA node and three consensus nodes in the underlying blockchain platform are deployed on the following configured services. Meanwhile, the underlying platform of the blockchain uses RayBaaS. MySQL is used to store the information related to the DID under the chain, Httpd-tools is used for interface stress testing, and all services and applications are deployed and installed through Docker.

System Test Network Topology

The network topology of the simulation experiment is constructed. The network topology of the system test represents the physical or logical connection and arrangement of various nodes and devices in the system, which is shown in Figure 8.

Algorithm Training

Based on the above experimental environment, this paper analyzes and verifies the algorithm from the aspects of block generation efficiency, convergence, and algorithm overhead.

Convergence Analysis of the Algorithm

The convergence performance of the proposed schema is analyzed, which is shown in Figure 9.

As shown in Figure 9, the proposed schema can quickly jump out of the trap of early local optimization. The finite convergence is obtained after 100 iterations, and the consistency of global variables is maintained in the subsequent optimization iterations.

Table 2. Simulation experiment setup environment

Item	Parameter
CPU	Intel Core i5-8400
Memory	32 GB
Docker	17.03
Docker-Compose	1.20.0
JDK	1.6
Httpd-Tools	2.0.2.2
MySQL	4.8
RayBaaS	1.20.2

Figure 8. System test network topology

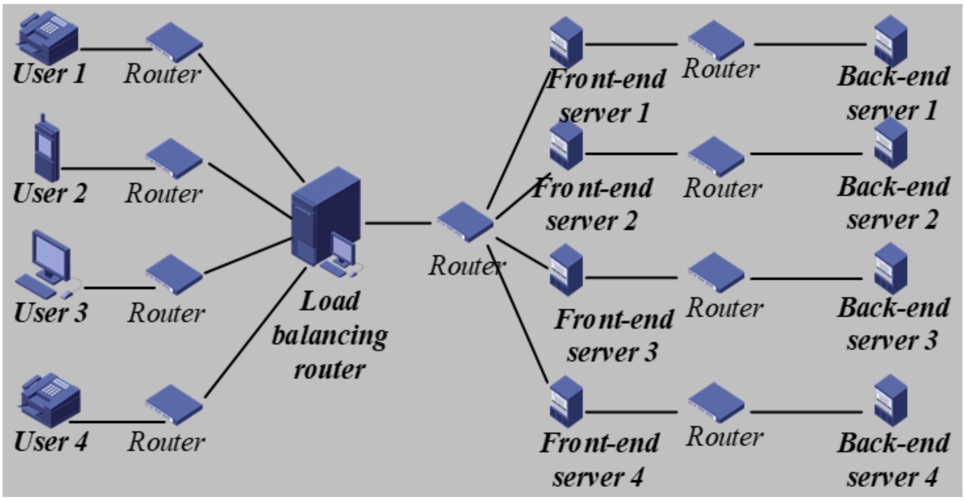
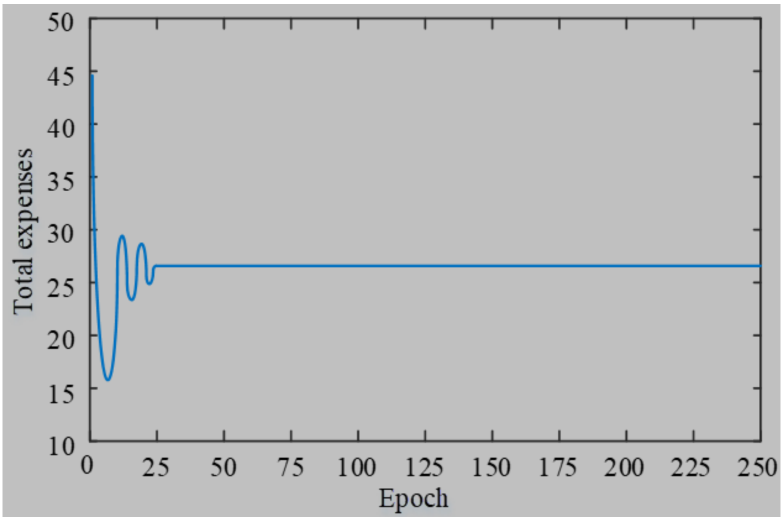


Figure 9. Convergence performance analysis of proposed schema

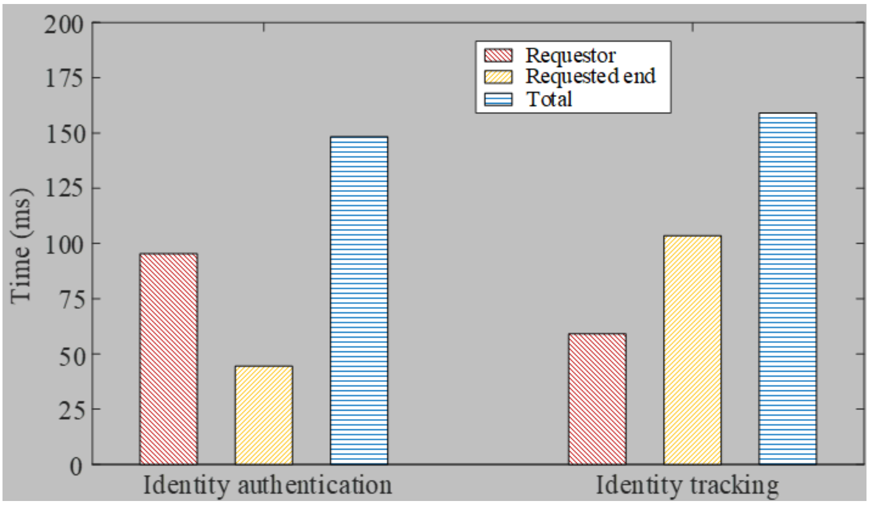


Time Consumption Analysis

Aiming to analyze the impact of identity authentication algorithm on the performance of the whole system, the algorithm overhead experiment takes the user as the requesting end and the client as the requested end, records the time consumption between the requesting end and the requested end, and obtains its average value, which is shown in Figure 10.

In Figure 10, the total time consumption of identity authentication is 145.98 ms, of which the time consumption of the requester is 92.15 ms and the time consumption of the requested end is 53.83 ms. In addition, the total time for identity tracking is 165.51 ms, including 63.22 ms for the requesting end and 102.29 ms for the requested end. The schema has less computational overhead, which also brings a certain improvement in system security.

Figure 10. Analysis of algorithm time consumption



Experimental Comparison

The use of dynamic encryption algorithms mainly includes the Paillier algorithm and the ElGamal algorithm. The Paillier encryption algorithm is a difficult problem based on the composite residue class. It is a homomorphic encryption algorithm that satisfies the addition (W. Zhang et al., 2022). The ElGamal algorithm is an encryption system based on a discrete logarithm problem, which can be used for data encryption and digital signature (Li et al., 2021).

For the purpose of verifying the performance superiority of the proposed algorithm, the Paillier algorithm (W. Zhang et al., 2022), the hybrid Paillier-blowfish algorithm (Bijeta et al., 2021), and the ElGamal algorithm (Li et al., 2021) are used as comparison methods, and the simulation experiments are carried out under the same operating environment.

Performance Comparison of Different Protocols

This paper analyzes the computational complexity of different algorithms. Table 3 shows the results.

In Table 3, the Paillier algorithm requires n times of encryption and one time of decryption for the receiving user, and 1 time of modular multiplication for the sending user, with a total of $2(n+1)\log n+1$ times of modular multiplication. The ElGamal algorithm requires n times of encryption and one time of decryption for the receiving user, and three times of modular multiplication for the sending user, with a total of $2(n+1)\log n+3$ times of modular multiplication. The algorithm

Table 3. Algorithm complexity

Algorithm	Complexity
The proposed algorithm	$6\log n$
Paillier (W. Zhang et al., 2022)	$2(n+1)\log n+1$
Paillier-blowfish (Bijeta et al., 2021)	$2(n+1)\log n+1$
ElGamal (Li et al., 2021)	$2(n+1)\log n+3$

of this protocol only needs to be encrypted twice and decrypted once, and the total number of modular multiplication operations is $6\log n$ times. Therefore, this paper proposes that the authentication algorithm has obvious advantages in computational efficiency.

Algorithm Authentication Time-Consuming Comparison

Additionally, the time-consuming of algorithm authentication in edge nodes are analyzed, which is mainly divided into two aspects: identity authentication and data authentication.

Table 4 shows the time consumption analysis of identity authentication under different algorithms.

As shown in Table 4, due to the introduction of blockchain edge nodes in the authentication algorithm, the authentication time between nodes is effectively reduced. Thus, the proposed authentication algorithm sinks the process of computing authentication to the user side to achieve fast information verification, and the calculation time is only 23.58 ms. On the contrary, the centralized operation authentication method is adopted in the Paillier algorithm, the hybrid Paillier-blowfish algorithm, and the ElGamal algorithm, which has no advantages in terms of computing costs, 26.58 ms, 34.27 ms, and 38.01 ms, respectively.

At the same time, a comparative analysis of data authentication time is also carried out.

As shown in Table 5, the data authentication time of the proposed algorithm is 25.06 ms, which is 2.51 ms, 8.17 ms, and 11.76 ms shorter than that of the Paillier algorithm, the Paillier-blowfish algorithm, and the ElGamal algorithm. One reason is that a lightweight authentication protocol is adopted by the proposed scheme at the edge nodes where each terminal device independently authenticates without queuing, which can improve the efficiency of identity authentication in distributed identity authentication systems significantly. Secondly, the base station will store the parameters related to the sensor nodes on the blockchain of the cluster head, which shortens the computational overhead.

Comparison of Certificate Certification Time

The efficiency of block generation is crucial to blockchain technology. In this paper, the traditional Proof of Work (PoW) algorithm is used as a comparison method, and the corresponding quantitative analysis of this index is carried out (Yin et al., 2022).

As shown in Figure 11, the block generation time has same direction as the number of blocks increases. When the number of blocks is below 500, the generation efficiency of traditional PoW algorithm is more than that of the proposed authentication algorithm. On the other hand, with the

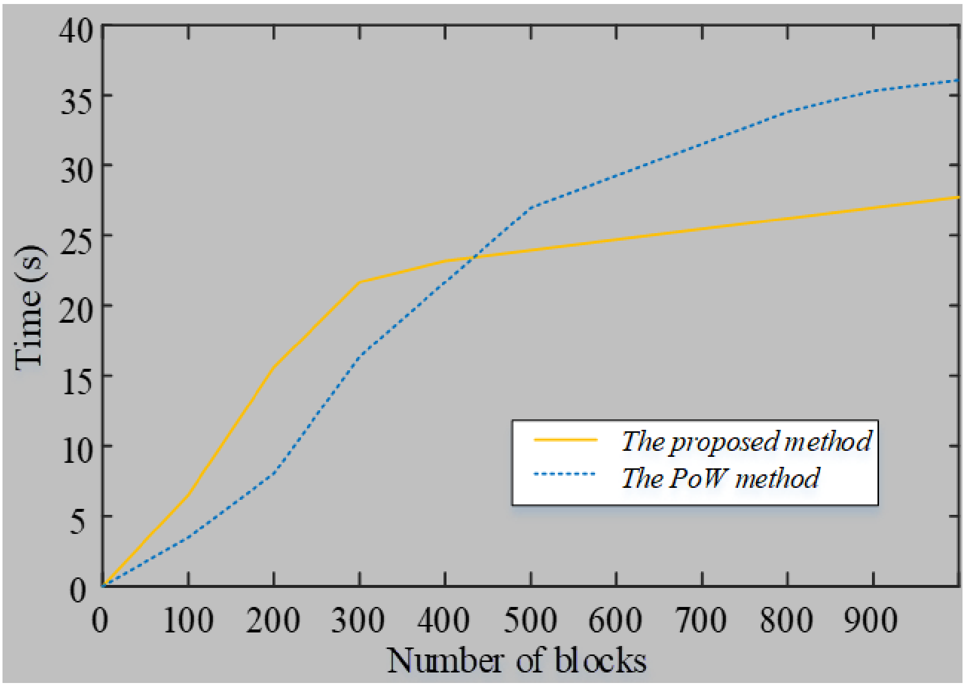
Table 4. Time consumption of identity authentication under different algorithms

Algorithm	Time (ms)
The proposed algorithm	23.58
Paillier (W. Zhang et al., 2022)	26.58
Paillier-blowfish (Bijeta et al., 2021)	34.27
ElGamal (Li et al., 2021)	38.01

Table 5. Time consumption of data authentication under different algorithms

Algorithm	Time (ms)
The proposed algorithm	25.06
Paillier (W. Zhang et al., 2022)	27.57
Paillier-blowfish (Bijeta et al., 2021)	33.23
ElGamal (Li et al., 2021)	36.83

Figure 11. Block generation time



number of blocks increases, the calculation time of the traditional method is more than that of the proposed verification method of the traditional method. When the number of blocks is 1000, the calculation cost of the proposed algorithm is only 27.91 s, while the time cost of PoW algorithm is 36.29 s. The PBFT algorithm does not require mining, and each consensus process does not require a large amount of electricity consumption like PoW. In addition, sending transactions in the PBFT algorithm does not require waiting for confirmation. If a block is recognized by the system through the PBFT algorithm, it will be recognized as the final block and will not be revoked. The blockchain maintained by PBFT is not prone to forking, and all nodes reach consensus at the same time without the need for additional waiting time. Therefore, the efficiency of PBFT is significantly higher than that of PoW mechanism.

CONCLUSION

A user authentication scheme combining mobile edge computing and blockchain was designed to meet the requirements of reliable and fast IoT scenarios. From the results of the experiment, it is easy to see that the proposed user authentication scheme can meet the requirements of reliable, secure, and real-time response of the IoT in multi-user grid connection scenarios. Thus, the following conclusions are drawn:

1) In the system architecture integrating edge computing and blockchain, the N-PBFT algorithm can not only ensure the trusted authentication of the blockchain layer, but it can also reduce the storage and computing burden of the blockchain.
2) By adopting the LCA concept to optimize the design of authentication protocols for edge nodes, while ensuring the security of edge node users and data, it can improve authentication efficiency

effectively, thereby better meeting the requirements of security, reliability, and real-time response of the IoT.

3) The proposed scheme can achieve better performance compared with other existing authentication schemes and consensus mechanisms. However, the blockchain layer of this scheme only considers smart contracts and consensus mechanisms, without considering incentive mechanisms, resulting in the inability to fully mobilize the enthusiasm of edge nodes to participate in blockchain.
4) The proposed scheme does not optimize the caching mechanism, in other words, there is still more space for improvement in real-time performance.
5) In the future, a series of incentive mechanisms (such as a computing consumption incentive) will be designed, and the Federated learning technology will be introduced to improve overall system security. Moreover, the caching mechanism will be optimized and designed to further improve the real-time of system service response.

AUTHOR NOTE

The data that used to support the findings of this study are included within the article.

The authors declare that there is no competing interest for this work and no funding was received.

This work was supported by Research on key technologies of authentication mechanism based on enhanced blockchain framework (No. 232102210197). Research on consistency checking algorithm of spatial direction relation in spatial database (No. 232102210085).

Correspondence concerning this article should be addressed to Feng Xue, Zhengzhou University of Economics and Business, China, Emai: xuefeng707@163.com

REFERENCES

Bijeta, Seth, K. (. (2021). Secure cloud data storage system using hybrid paillier-blowfish algorithm. *Computers, Materials & Continua*, *67*(01), 779–798. doi:10.32604/cmc.2021.014466

Chen, J., Zhang, J., Pu, C., Wang, P., Wei, M., & Hong, S. (2023). Distributed logistics resources allocation with blockchain, smart contract, and edge computing. *Journal of Circuits, Systems, and Computers*, *32*(7), 2350121. doi:10.1142/S0218126623501219

Chen, R., Shu, F., Huang, S., Huang, L., Liu, H., Liu, J., & Lei, K. (2021). BIdM: A blockchain-enabled cross-domain identity management system. *Journal of Communications and Information Networks*, *6*(1), 44–58. doi:10.23919/JCIN.2021.9387704

Cheng, G., Chen, Y., Deng, S., Gao, H., & Yin, J. (2021). A blockchain-based mutual authentication scheme for collaborative edge computing. *IEEE Transactions on Computational Social Systems*, *9*(1), 146–158. doi:10.1109/TCSS.2021.3056540

Cui, Z., Xue, F., Zhang, S., Cai, X., Cao, Y., Zhang, W., & Chen, J. (2020). A hybrid blockchain-based identity authentication scheme for multi-WSN. *IEEE Transactions on Services Computing*, *13*(2), 241–251. doi:10.1109/TSC.2020.2964537

Gao, S., Su, Q., Zhang, R., Zhu, J., Sui, Z., & Wang, J. (2021). A privacy-preserving identity authentication scheme based on the blockchain. *Security and Communication Networks*, *2021*, 1–10. doi:10.1155/2021/9992353

Garcia, R. D., Ramachandran, G., & Ueyama, J. (2022). Exploiting smart contracts in PBFT-based blockchains: A case study in medical prescription system. *Computer Networks*, *211*, 109003. doi:10.1016/j.comnet.2022.109003

Hongbin, F., & Zhi, Z. (2023). Privacy-preserving data aggregation scheme based on Federated Learning for IIoT. *Mathematics*, *11*(1), 214. doi:10.3390/math11010214

Jia, X., Hu, N., Yin, S., Zhao, Y., Zhang, C., & Cheng, X. (2020). A2 chain: A blockchain-based decentralized authentication scheme for 5G-enabled IoT. *Mobile Information Systems*, *2020*, 1–19. doi:10.1155/2020/8889192

Kaladevi, R., Gopirajan, P. V., Hariharan, S., Bhanu, P. A., & Sandhiya, B. (2022). Digital healthcare using blockchain. In *2022 1st International Conference on Computational Science and Technology (ICCST)*, (pp. 651-655).

Li, L., Zhang, F., & Zhang, W. Y. (2021). An ELGamal re encryption algorithm for database homomorphic computing. *Journal of Beijing Jiaotong University*, *45*(2), 127–134.

Liu, H. Q., Ai, M., Huang, R., Qiu, R., & Li, Y. (2022). Identity authentication for edge devices based on zero-trust architecture. *Concurrency and Computation*, *34*(23), e7198. doi:10.1002/cpe.7198

Liu, J., & Liu, R. C. (2022). 7 Lai, Y. (2022). Risk-based dynamic identity authentication method based on the UCON model. *Security and Communication Networks*.

Long, J., & Su, X. (2021). Anonymous chaotic-based identity authentication protocol in IoT. *International Journal of Embedded Systems*, *14*(2), 194–200. doi:10.1504/IJES.2021.113813

Lv, Y., Liu, W., & Wang, Z. (2020). Heterogeneous cross-domain identity authentication scheme based on proxy resignature in cloud environment. *Mathematical Problems in Engineering*, *2020*, 1–12. doi:10.1155/2020/2078032

Ma, Z., Meng, J., Wang, J., & Shan, Z. (2020). Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. *IEEE Internet of Things Journal*, *8*(4), 2116–2123.

Melo, W. S. Jr, dos Santos, L. S., de Souza Bento, L. M., & Nascimento, P. R. (2022). Using blockchains to protect critical infrastructures: A comparison between Ethereum and Hyperledger Fabric. *International Journal of Security and Networks*, *17*(2), 77. doi:10.1504/IJSN.2022.123294

Prajapati, V., Gupta, B. B., & Gupta, B. B. (2022). A robust authentication system with application anonymity in multiple identity smart cards. [JITR]. *Journal of Information Technology Research*, *15*(1), 1–12. doi:10.4018/JITR.2022010107

Ren, Y., Zhao, Q., Guan, H., & Lin, Z. (2020). A novel authentication scheme based on edge computing for blockchain-based distributed energy trading system. *EURASIP Journal on Wireless Communications and Networking*, *2020*(1), 152. doi:10.1186/s13638-020-01762-w

Sandhiya, B., Kaladevi, R., & Hariharan, S. (2021, December). Data security in healthcare using blockchain technology. In *2021 International Conference on Decision Aid Sciences and Application (DASA)*, Sakheer, Bahrain, (pp. 354-359). IEEE.

Sun, H., Tan, Y. A., Li, C., Lei, L., Zhang, Q., & Hu, J. (2022). An edge-cloud collaborative cross-domain identity-based authentication protocol with privacy protection. *Chinese Journal of Electronics*, *31*(4), 721–731. doi:10.1049/cje.2021.00.269

Wang, S., Ma, Z., Liu, J., & Luo, S. (2022). Research and Implementation of Cross-Chain Security Access and Identity Authentication Scheme of Blockchain [J]. *Information Network Security*, *06*(1), 61–72.

Wang, S., Mao, K. L., Zhan, F., & Liu, D. (2020). Hybrid conditional privacy-preserving authentication scheme for VANETs. *Peer-to-Peer Networking and Applications*, *13*(5), 1600–1615. doi:10.1007/s12083-020-00916-3

Wang, Z., Zhuang, Y., & Xia, Q. (2020). Mutual authentication-based RA scheme for embedded systems. *IET Information Security*, *14*(2), 232–240. doi:10.1049/iet-ifs.2019.0027

Xia, Z., Fang, Z., Gu, K., Wang, J., Tan, J., & Wang, G. (2021). Effective charging identity authentication scheme based on fog computing in V2G networks. *Journal of Information Security and Applications*, *58*, 102649. doi:10.1016/j.jisa.2020.102649

Yin, Y. Y., Ye, B. Y., & Liang, T. T. (2022). Research on multi-layer blockchain network model in edge computing. *Chinese Journal of Computers*, *45*(1), 115–134.

Zang, Y., Lv, G. Y., & Jia, D. X. (2023). Power transaction data encryption scheme based on paillier homomorphic encryption. *Electrical Automation*, *45*(1), 39–41.

Zhang, G., Zhao, X., Chen, M., & Ma, S. (2022). Efficient privacy protection authentication protocol for vehicle network in 5G. *Concurrency and Computation*, 7247. doi:10.1002/cpe.7247

Zhang, L. H., Hu, F. Z., & Huang, Y. (2020). Identity authentication protocol of micro-grid power based on consortium blockchain. *Journal of Applied Sciences*, *38*(1), 173–183.

Zhang, M., Mao, J., Ma, Y., Xu, L., Wang, C., Zhao, R., Li, Z., Chen, L., & Zhao, W. (2022). A CPK-based identity authentication scheme for IoT. *Computer Systems Science and Engineering*, *40*(3), 1217–1231. doi:10.32604/csse.2022.017657

Zhang, W., Bai, Y., & Feng, J. (2022). Tiia: A blockchain-enabled threat intelligence integrity audit scheme for IIoT. *Future Generation Computer Systems*, *132*, 254–265. doi:10.1016/j.future.2022.02.023

Zhao, B., Zhao, P., & Fan, P. (2020). ePUF: A lightweight double identity verification in IoT. *Tsinghua Science and Technology*, *25*(5), 625–635. doi:10.26599/TST.2019.9010072

Zhao, G., Di, B., & He, H. (2022). A novel decentralized cross-domain identity authentication protocol based on blockchain. *Transactions on Emerging Telecommunications Technologies*, *33*(1), e4377. doi:10.1002/ett.4377

Zheng, L., Song, C., Zhang, R., Lv, B., Liu, Y., Cui, M., & Meng, L. (2021). Design and analysis of telemedicine authentication protocol. *International Journal of Sensor Networks*, *37*(3), 198–208. doi:10.1504/IJSNET.2021.118878

Zou, J., He, D., Zeadally, S., Kumar, N., Wang, H., & Choo, K. R. (2021). Integrated blockchain and cloud computing systems: A systematic survey, solutions, and challenges [J]. *ACM Computing Surveys*, *54*(8), 1–36. doi:10.1145/3456628

Xue Feng, Associate Professor. Master's degree,Graduated from Liaoning Petrochemical University in 2010. Worked in Zhengzhou University of Economics and Business. His research interests include Algorithms, Computer applications.

Fangju Li, Professor, Master's degree, Graduated from Information Engineering University in 2000, Worked in Zhengzhou University of Economics and Business. Her research interests include Computer applications.