User Identity Confirmation Property Management System Based on State Secret Algorithm and Blockchain Technology

Xiao Tian[1]*, Xing Chen[2]
Nanyang Medical College, Nanyang 473000, China[1]
Henan Engineering Research Center of Intelligent Processing for Big Data of Digital Image-School of Artificial Intelligence and Software Engineering, Nanyang Normal University, Nanyang 473061, China[2]

***Abstract*—The existing user identity confirmation methods in property management systems are vulnerable to attacks and forgery, posing serious threats to system security and reliability. To address these issues, this study proposes a novel user identity confirmation method that combines the state secret SM9 algorithm with blockchain technology. The system utilizes blockchain for managing and verifying user identity information, while employing the SM9 algorithm for double encryption of user data. This approach ensures robust protection against identity theft and fraud, enhancing security and privacy. The proposed method was tested experimentally, and the results show that the model achieves an average communication connection and verification initiation time of approximately 11.07 ms, with a key negotiation success rate of 88.73%. Moreover, the model achieved a user identity confirmation accuracy of 90.41%, which is significantly higher than traditional methods. These findings highlight that the integration of the SM9 algorithm and blockchain technology offers high accuracy, low latency, and improved scalability, making it an ideal solution for enhancing the security and efficiency of property management systems.**

***Keywords*—User identification; state secret algorithm; blockchain technology; property management system; security**

I. Introduction

With the rapid advancement of internet technology, more users interact with the property management system through various online platforms. Ensuring the authenticity and security of user identities is essential for the smooth operation of these systems [1-2]. Traditional authentication methods, such as username-password combinations and dynamic tokens, are often vulnerable to hackers or malicious software attacks due to their simplicity and ease of use, making it difficult to meet current high-precision security and safety requirements [3-4]. Intelligent encryption algorithms and blockchain have brought new ideas for enhancing user privacy and security. The state secret SM9 algorithm is a national commercial cryptographic algorithm in China, which has significant application value in information encryption, digital signatures, and key exchange [5]. The SM9 algorithm is an identity-based cryptographic system used for message encryption, digital signatures, and key exchange. Key pairs are generated through a specific hash function using the user's identification information (such as email address or phone number) as the public key. SM9 uses smaller key sizes and faster encryption/decryption speeds, which makes it more suitable than asymmetric encryption algorithms in resource-constrained environments (e.g., Internet of Things (IoT) devices). SM9 provides security comparable to Elliptic Curve Cryptography (ECC), with a smaller key size. The ECC algorithm is a widely used public key cryptography based on the difficulty of large integer factorization. The SM9 algorithm is more efficient than ECC in resource-constrained environments (e.g., IoT devices) due to its smaller key size. The decentralized management and traceability of blockchain technology can meet the demand for tamper-proof property management systems. Blockchain technology, especially the technology used in cryptocurrencies such as Bitcoin, requires a significant amount of computing power to solve complex mathematical problems, verify transactions, and create new blocks. Each node in the blockchain network needs to store a copy of the entire transaction history, which requires a large amount of storage space as the blockchain grows. Therefore, this study proposes a novel SM9-Blockchain identity confirmation system that integrates the state secret SM9 algorithm with Distributed Ledger Technology (DLT) from blockchain.

Research question: This study aims to address the security vulnerabilities, vulnerabilities to attacks, and forgery in existing user identity verification methods for property management systems, and explore a more secure, efficient, and scalable authentication method.

Research objective: Propose a dual-encryption user authentication model that combines the state-secret SM9 algorithm with blockchain technology to enhance authentication security and privacy. Design and implement a user identity verification system based on the SM9 algorithm and blockchain technology to reduce system latency and improve authentication accuracy and efficiency.

Research significance: This study proposes a new dual-encryption authentication method by combining the state-secret SM9 algorithm with blockchain technology, providing a more secure solution for property management systems. This model not only effectively prevents identity forgery and information tampering, but also enhances system reliability and security through the decentralized and immutable nature of blockchain. Furthermore, this study explores how to optimize computational efficiency and communication latency during the authentication process in resource-constrained

*Corresponding author.

environments, which has important theoretical and practical implications.

The research's innovation is reflected in three key aspects. First, a dual-encryption identity authentication model was constructed, combining the state secret SM9 algorithm with blockchain DLT. This overcomes the limitations of existing methods that rely solely on a single encryption or storage mechanism. Second, a time-decay-based trust management mechanism for Certificate Authorities (CAs) was proposed. This mechanism dynamically adjusts the trustworthiness of CAs based on historical behavior, effectively suppressing the repeated issuance of certificates by low-reputation CAs and improving the reliability of the authentication system from the source. This design breaks away from the static model of traditional trust management methods, making the system more resilient to low-reputation CAs. Finally, the research introduced multi-layer blockchain data compression and snapshot technology, enabling efficient collaboration between the main chain and auxiliary chain/off-chain data.

The research's contribution lies in proposing a dual-encryption identity authentication framework that combines the SM9 identity-based encryption algorithm with blockchain-based DLT, overcoming the limitations of traditional single-layer encryption or storage mechanisms. In experiments, the SM9-blockchain model achieved a response latency of 6ms against SQL injection attacks, approximately 50% faster than traditional approaches, enhancing security and authentication efficiency. Secondly, the research designed a CA trust management mechanism based on time decay to dynamically adjust the CA's credibility and effectively prevent duplicate certificate issuance by low-reputation institutions. In experiments, the mis-issuance rate of certificates from low-reputation CAs was reduced from the traditional 20% to 12%, improving the reliability of the authentication system. Finally, a multi-layer blockchain data structure supporting compressed snapshots was constructed, improving data storage and processing efficiency in resource-constrained IoT scenarios. When processing 1,000 concurrent requests, the SM9-blockchain model achieved a response time of 11 ms, approximately 50% faster than traditional blockchain systems, while also reducing energy consumption by 30%.

The structure of the study is divided into six sections. Section II is a literature review. Section III is the methodology, which designs a user identity confirmation model based on DLT and state secret SM9 algorithms. Section IV is the performance validation, which analyzes the performance of the proposed model through experiments. Section V is a discussion, which analyzes the research results. Section VI is the conclusion, which summarizes the research results and shortcomings.

II. Related Work

As the Internet grows, there is an increase in the focus on user data security and privacy across fields like business registration and corporate governance [6]. Blockchain, a leading encryption and traceability tech, is under intensive study by researchers [7]. Attaran's research underscores blockchain's secure encryption, suggesting its use in crypto transactions. It notes that blockchain nearly prevents data alteration or removal without others' private keys, marking a key trend in future crypto security [8]. Li et al. suggested a blockchain framework for encrypting info exchanges among IoT devices, leveraging blockchain's consensus mechanism, encryption, and smart contracts to secure interactions between smart devices [9]. Panda et al. created a blockchain-IoT architecture that secures data privacy and IoT security by using hash chains for key management, eliminating the need for third-party key handlers. The scheme includes an efficient key generation method for mutual authentication through self-verification [10]. To address the limitation of lack of flexibility and responsiveness to dynamic changes of static smart contracts in blockchain applications, Saputra et al. based on the innovative concept of dynamic smart contracts in key-value format framework, AniraBlock, which enhances the data management and supply chain transparency, and achieves the optimisation of data integrity and operational efficiency in the agriculture sector [11]. Saputra et al. further proposed a blockchain-based key-value store that explores interoperability, dynamic data processing and performance testing of smart contracts, thereby enabling dynamic smart contract interactions in the agriculture sector [12].

State secret algorithms are cryptographic algorithms designed and developed independently by China, currently an open source including SM2 to SM9. There are a large number and wide range of SM9-based studies on the Internet. For example, Yang et al. proposed a novel identity-based blind signature scheme combined with message recovery technology to reduce the transmission bandwidth of the signature information by hiding the message in the signature in response to the problem of high resource consumption of the SM9 blind signature scheme in practical applications [13]. Lai et al. introduced an improved online/offline signature scheme for SM9 to accelerate its signing process. The new scheme boosts signature generation speed by 9.9%, reducing signature time to under 1 millisecond, and demonstrates superior performance over existing fast signature algorithms [14]. Aiming at the problem that civil navigation information of BeiDou satellite navigation system (BDS) is vulnerable to spoofing and replay attacks due to the lack of authentication mechanism, Wu et al. proposed a secure authentication protocol BDSec based on the design of China's SM series of algorithms [15]. Zhang and Ye developed a privacy-preserving method leveraging SM9 and blockchain. It employs conditional anonymous ring signatures for enhanced security and optimizes key negotiation using the discrete logarithm assumption, making it faster. The scheme proved to be effective and practical in experiments [16].

In summary, SM9 algorithm and blockchain technology are current research hotspots, and the combination of the two has great potential in protecting blockchain communication and data privacy. SM9 algorithm, as an identity-based cryptographic algorithm, provides a secure key negotiation and authentication mechanism. However, existing research has largely focused on using either the SM9 algorithm or blockchain technology alone, while the combination of the two has not been fully explored. The scalability and efficiency issues of combining the SM9 algorithm and blockchain technology in practical applications remain unaddressed. Furthermore, many studies assume an ideal network

environment, overlooking performance bottlenecks in resource-constrained and high-concurrency environments. Therefore, this research aims to combine the SM9 algorithm with blockchain technology to build a more efficient, secure, and scalable identity verification system, addressing the challenges faced by existing approaches in practical applications.

III. Identity Confirmation Property Management System Based on State Secret SM9 Algorithm and DLT

The study introduces a user identity verification model on DLT to ensure data integrity and accuracy through a decentralized network. It also incorporates the SM9 algorithm for double encryption of the identity verification model and uses asymmetric encryption to safeguard user identity information.

A. Construction of Identity Confirmation Property Management Model Based on DLT

DLT technology is a data storage and recording technology, which allows multiple participants to jointly maintain a growing list of data records. DLT ensures the data consistency of all participants through consensus mechanism. Blockchain DLT stores data in block form, with each block holding transactions and linked via hashing to the previous block, creating a chain structure [17-18]. Once data is recorded, all nodes synchronize it, making alterations to a single block ineffective [19]. DLT also features encryption for secure and confidential data storage. In this, the expression of DLT block is shown in Eq. (1):

$$block = h(data, timesiamp, previous\_hash, hash) \quad (1)$$

In Eq. (1), $data$ denotes data stored on the blockchain, which can be interpreted as user identity information or transaction records, etc. $timesiamp$ represents a timestamp used to maintain the order of blocks. $previous\_hash$ represent the hash value of the previous block; $hash$ represents the hash value of the current block; $h(.)$ represents the connection function between different blocks, which is used to link blocks and ensure that each block is closely connected to the previous block, forming a chain. Eq. (1) describes the structure and linkage of individual data blocks in a blockchain. In practice, each block is like a "ledger page", in which the user's identity data and operation records are recorded. By linking the hash value to the previous block, the data can be prevented from being tampered with in the middle of the process, thus guaranteeing the security and non-repudiation of the system. The blockchain architecture in this study is constructed based on the Hyperledger Fabric platform, adopting the coalition chain model, through the improved Byzantine Fault Tolerance (BFT) algorithm as the consensus mechanism, combined with the main chain-side chain structure and compressed snapshot technology, which improves the processing performance and data synchronization efficiency while ensuring that the transactions are not tampered with. Each node constructs the block header and synchronously updates the blockchain through the hash function, forming a complete DLT, according to a special combination, as shown in Fig. 1.

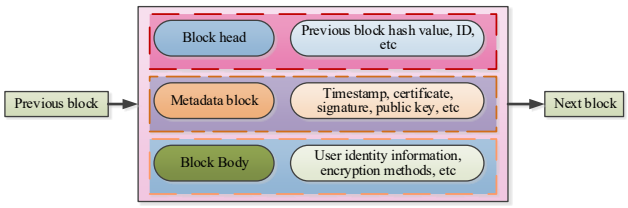


Fig. 1. Schematic diagram of blockchain combination structure.

From Fig. 1, it can be seen that in cross-system identification, the length of the authentication path and the size of the integer volume are the key factors affecting the difficulty of constructing the trust path. In order to adapt to the higher requirements of energy consumption and storage efficiency in large-scale application scenarios, the optimized DLT technology adopted by the institute introduces a lightweight consensus mechanism and compressed storage structure in its design. In terms of energy consumption control, the system adopts an improved BFT algorithm to replace the traditional proof-of-work mechanism to avoid a large number of invalid calculations. Compared with the traditional BFT algorithm, this study simplifies the node election and message transmission mechanisms by introducing pre-selected nodes, thereby reducing redundant broadcast communication and lowering network overhead while maintaining fault tolerance. Compared with commonly used consensus mechanisms such as Proof of Work (PoW) and Proof of Stake (PoS), BFT offers higher determinism and efficiency in consortium blockchain environments. Although PoW provides strong security, it relies heavily on computational resources and consumes a large amount of energy, making it unsuitable for identity authentication systems that require real-time response and resource efficiency. PoS, while improving performance to some extent, depends on economic assumptions in its incentive and security models, which are less compatible with uniformly managed system architectures. In contrast, BFT does not rely on computational competition and offers advantages such as low latency, high controllability, and strong determinism, making it more suitable for the trusted identity authentication model proposed in this study.

In terms of data storage, by setting the validity period and update cycle of identity data, and combining layered storage and snapshot mechanism, only key identity information and index data are retained on the main chain, while the rest of the auxiliary information is distributed to the side chain or off-chain storage. A snapshot mechanism is one that periodically records a full copy of the current state of the blockchain system and transfers the historical block data to off-chain or auxiliary chain storage. To optimize storage requirements, the system uses a snapshot mechanism. By periodically generating snapshots of the blockchain data, the system saves the current state and the historical data is transferred to off-chain storage or external storage. This strategy not only reduces the storage pressure on the blockchain main chain, but also ensures the consistency and integrity of the data through hash values and timestamps. While preserving the current valid data, the historical data can still be traced back through the verification

mechanism to ensure the security and traceability of the data, thus effectively reducing the storage requirements and improving the query efficiency.

In this way, while ensuring data integrity and traceability, it effectively reduces the local storage pressure and bandwidth demand of the nodes, and improves the scalability and green computing capability of the system. Among them, CA auditing is an important work in blockchain. If CA CA_1 has issued M certificates in a period of time, among which there are m legitimate certificates. The weight attenuation of CA certificates, the expression of the legitimacy probability of institutional certificates, and the calculation of credibility are shown in Eq. (2):

$$\begin{cases} f_{PRE}(CA) = \gamma^{t_n - t_{pre}} \\ P_{le} = \dfrac{M}{m}\gamma^{\frac{1}{M}} \\ P_{re} = \dfrac{1}{n}\sum_{i=1}^{n}\left[\alpha f_{PRE}(CA) t_{pre} + \beta P_{le}\right] \end{cases} \tag{2}$$

In Eq. (2), $f_{PRE}(CA)$ represents the CA's weight decay function, reflecting the gradual decrease in trust over time. γ indicates the decay factor; t_n indicates the current time; t_{pre} indicates the moment when the CA issues the last certificate. α, β represents the weight parameter, which has the relationship of $\alpha + \beta = 1$, and both parameters are constants greater than 0 and less than 1; n represents the number of times the organization has been audited. Eq. (2) is used to calculate the credibility of the CA. This equation is based on a time decay model. If the CA issues low-quality certificates or issues certificates frequently, the CA's credibility gradually declines over time. The study introduces a 'trust decay' mechanism for dynamically assessing the trustworthiness of CA organizations. The system records the frequency, legitimacy rate and historical behavior of certificate issuance by CAs, and sets a time decay factor to make the trust value of CAs decay naturally over time, so as to prevent the risk of abuse brought by long-term accumulation of trust. If a CA frequently issues illegal or low-quality certificates within a certain period, its weight will be rapidly reduced, and it will eventually be regarded by the system as a low-trust or failing organization. This mechanism improves the resilience and robustness of the certification system and effectively prevents the risk of a single point of failure of the authority center. The specific calculation equation is shown in Eq. (3):

$$\begin{cases} S = HA(s) \\ r = (S + x) \bmod n \\ k = (1+v)^{-1}(t - rt) \bmod n \end{cases} \tag{3}$$

In Eq. (3), S denotes the encrypted ciphertext; $HA(.)$ denotes the hash encryption function; s denotes the plaintext to be encrypted. x denotes the parameter of the public key; $\bmod n$ denotes that the mode of this calculation is elliptic curve. k denotes another parameter of elliptic curve digital signature, the larger the value, the higher the strength of the signature, and the higher the security. v denotes the parameter in the private key; t denotes the moment when this calculation is performed. Eq. (3) is the calculation for cryptographic signing of user identity information, which indicates that the user encrypts the information to be signed using a private key to generate a signature. The signature can be used to verify the legitimacy of the user's identity in subsequent steps. In practice, the user's identity information is converted into an encrypted digest, and the equation generates the signature parameter r. Once the server receives the signature, it can verify the legitimacy of the identity and avoid identity forgery. The proposed model uses digital signatures to verify user identities on the Public Key Infrastructure (PKI). PKI employs asymmetric encryption with a public-private key pair for secure data transmission, where the public key is shared for encryption and the private key is kept secret for decryption. Automated certificate lifecycle management in PKI systems reduces complexity and errors in manual operations. When a user from PKI domain 1 wants to authenticate with a server in domain 2, they must submit a certification request, including a digital signature and blockchain certificate to the server in domain 2. The server then verifies the user's identity with the certificate issuer [20]. Fig. 2 illustrates the steps of user authentication.

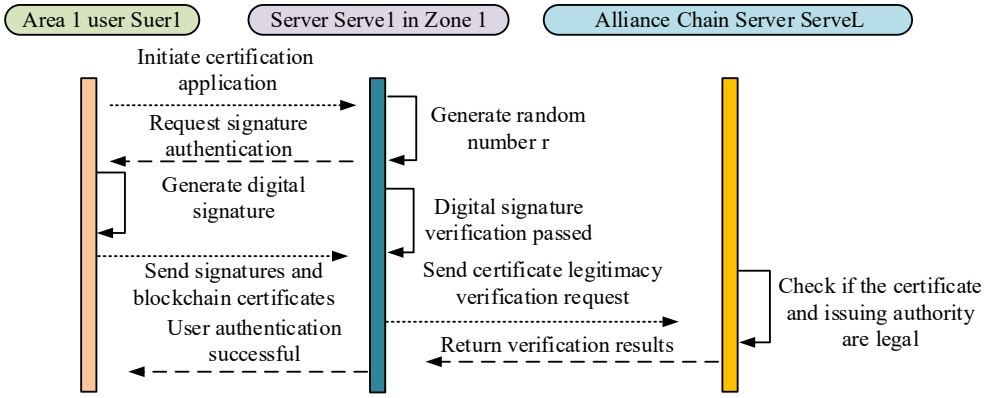


Fig. 2. Schematic diagram of user identity authentication process.

Fig. 2 illustrates the PKI encryption process: the sender gets the receiver's public key, encrypts data with it to create ciphertext, and sends the ciphertext. The decryption process involves the receiver using their private key to decrypt the ciphertext and retrieve the original data. Leveraging blockchain's decentralized and tamper-proof features, the study develops a secure user identification model offering efficient authentication, authorization, and protection of user privacy and security. The interaction mechanism between the blockchain and the SM9 algorithm is shown in Fig. 3.

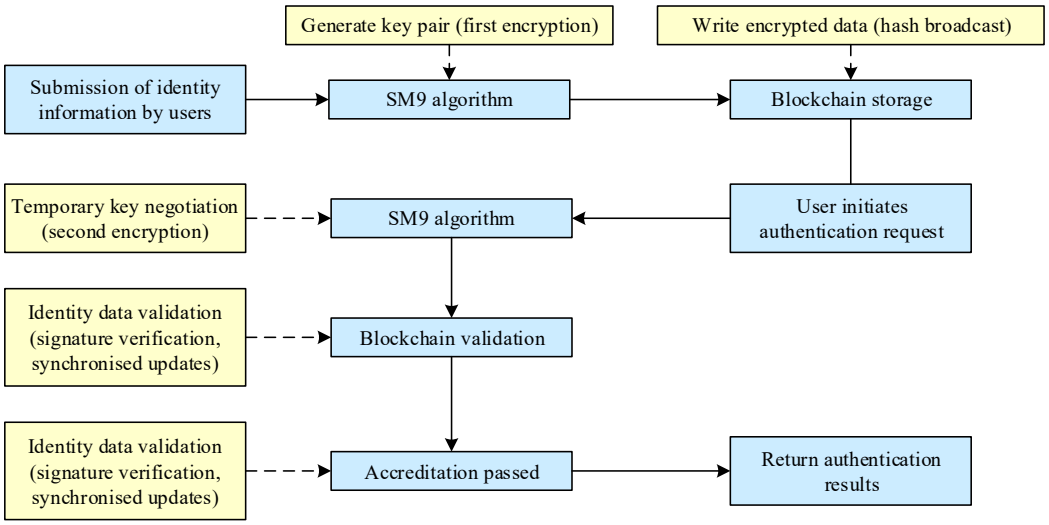


Fig. 3. Technical interaction mechanism between blockchain and the SM9 algorithm.

Fig. 3 shows how the SM9 algorithm generates key pairs and encrypts the data, how the blockchain stores the encrypted data and verifies it, and ultimately ensures the security and efficiency of the system through key negotiation and authentication. And in order to ensure the security of the off-chain data storage, the Institute lifting system has adopted a variety of technical measures. All off-chain data is encrypted before storage, and the SM9 algorithm is used for secondary encryption. At the same time, distributed storage and data slicing technologies are used to increase data redundancy and reliability and prevent a single point of failure. Managing permissions through role-based access control ensures that data access is restricted to authorized users only. In addition, the system introduces audit logs to record all data operations to ensure data traceability.

B. Secondary Encryption of Identity Confirmation Physical Model Based on SM9 Algorithm

In order to improve the encryption performance of the identity verification property management model, the use of the national security SM9 algorithm for secondary encryption is studied. The SM9 algorithm typically uses an asymmetric encryption system, also known as a public key cryptosystem, to generate identity-based public key encryption schemes to generate key pairs. Among them, the expressions for calculating the public and private keys are shown in Eq. (4):

$$\begin{cases} Pu_i = Hash(id_i) \\ Pr_i = \left(\dfrac{w}{w + Pu_i} \right) Pu_i \end{cases} \tag{4}$$

In Eq. (4), Pu_i denotes the public key of the first i user; $Hash(.)$ denotes the hash encryption function; id_i denotes the identity information of the first i user. w represents the master private key generated by the public key generator; Pr_i represents the private key of the i user. Eq. (4) is the basis for the SM9 algorithm to generate user public-private key pairs. The system generates its own encryption key based on the user's identity information, which is equivalent to "using identity information directly into a key". During key pair generation for user authentication, the IMS generates a random large prime number. This prime is used to create a temporary public and private key, as detailed in Eq. (5):

$$\begin{cases} \phi = N_1 Pu_i \\ \theta = N_2 \Pr_i \end{cases} \tag{5}$$

In Eq. (5), N_1 denotes the randomly generated large prime number; ϕ denotes the temporary public key. N_2 denotes the randomly generated large prime number, which is not necessarily the same as the value of N_1 ; θ denotes the temporary private key in the key negotiation process. During the key negotiation process, both parties generate temporary key pairs, which are used only for encryption tasks in the current session. The use of temporary keys reduces the security risks associated with using the same key for a long period of time. After generating the temporary key, the initiator sends the encrypted ciphertext and the temporary public key to the authenticator. The authenticator decrypts the message and checks the bilinear pairing conditions. If conditions are met, they calculate the session key, as detailed in Eq. (6).

$$\begin{cases} E(\theta, s' + Pu_i N_1) = E(\phi, s') \\ sk = Hash(id_i \| \phi \| \phi' \| \beta) \\ \partial = N_1 \phi \end{cases} \tag{6}$$

In Eq. (6), s' denotes the master public key generated by the public key generator. ϕ' denotes the temporary public key of the authentication server; ∂ denotes the private key base point in the system parameters. Generating the session key is the final step in the key negotiation phase, and the detailed flow of key negotiation is shown in Fig. 4.

Fig. 4 shows the detailed steps of the key negotiation process based on the SM9 algorithm. Firstly, both parties generate their own temporary public-private key pairs for initialization. Secondly, both parties exchange parameters for key negotiation in this phase, such as algorithm version or key size, to ensure that they are communicating under the same standard. Subsequently, in the 'Temporary Key Negotiation' phase, both parties generate a temporary key based on the exchanged parameters, which is only used for the current session to enhance the security of the communication. Verify that the temporary key is correctly authenticated by both parties. If the authentication fails, the process returns to the "Parameter Exchange" phase and restarts the entire process to prevent man-in-the-middle attacks and to ensure that the key is secure before it is used. If authentication passes, the process continues to the Key Negotiation Calculation phase, where both parties calculate the final shared key based on the temporary key and possibly other parameters, ensuring that the key is consistent between the parties and can be used for encrypted communication. In the 'Encrypted Communication' phase, both parties use the negotiated key for encrypted communication to ensure that the data is secure from unauthorised access during transmission. Subsequently, in the 'key validation' phase, the parties confirm that the key has been used correctly to ensure that there are no errors or tampering. At this point, the blockchain user identity confirmation property management model SM9-Blockchain optimized based on the SM9 algorithm runs, as shown in Fig. 5.

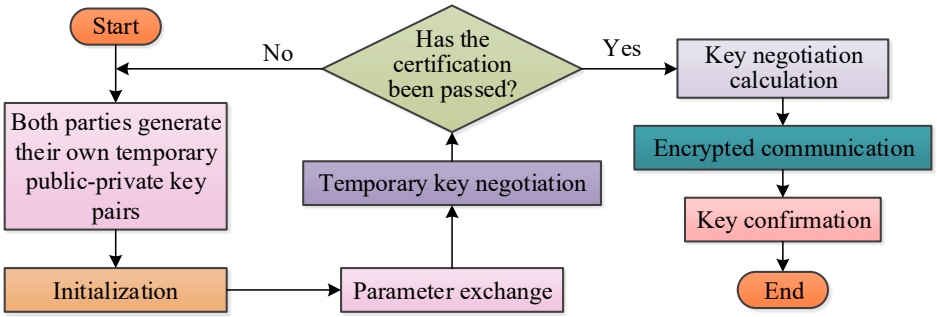


Fig. 4. Detailed process of key negotiation.

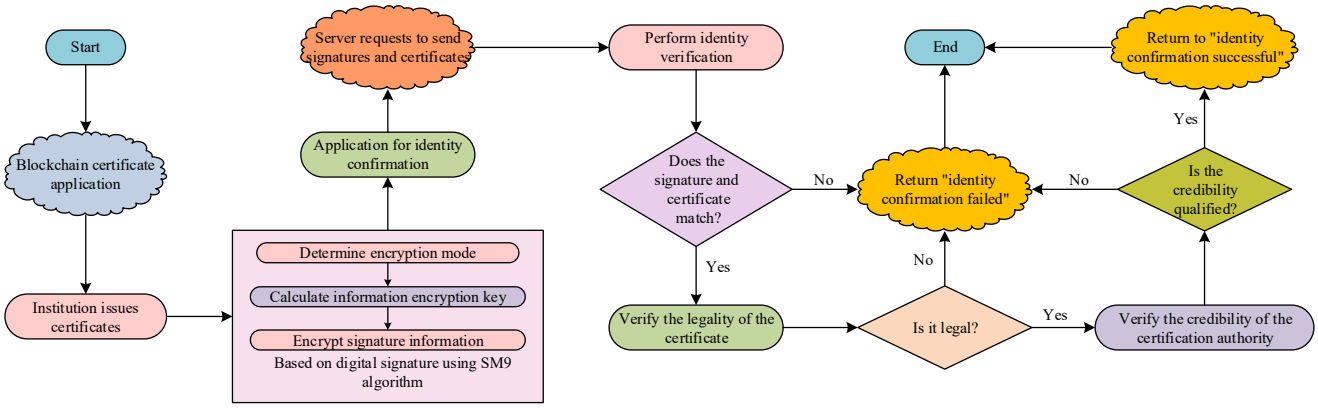


Fig. 5. SM9 blockchain model running process.

Fig. 5 shows the running process of the optimized SM9-blockchain model. First, the two parties exchange parameters used for key negotiation, and the user submits an authentication request through the blockchain to complete the authentication. At the same time, the system uses the SM9 algorithm to double-encrypt and verify the user's identity. After the authentication is passed, the user data is securely stored on the blockchain. Next, key negotiation is performed between the user and the system to generate a session key. Encrypted communication using the session key ensures the security of data transmission. This model makes use of the tamper resistance of blockchain and the encryption strength of SM9 algorithm to improve the security and efficiency of user authentication.

IV. SM-Blockchain Model Performance Validation

A. SM9-Blockchain Model Performance Validation

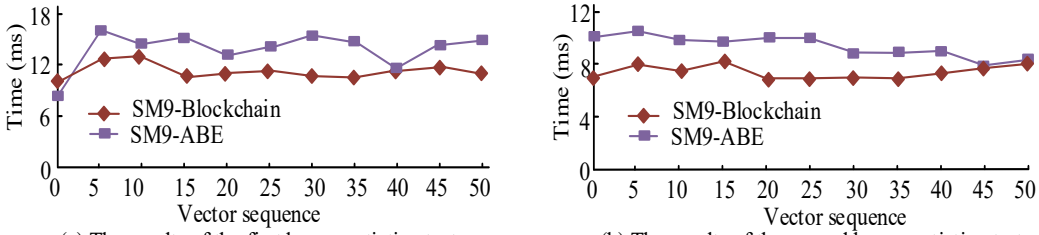
To validate the performance of the proposed model, the study conducted experiments in the hardware and software environments shown in Table I.

TABLE I. Configuration Table of Software/Hardware Experimental Environment

Item	Configuration	Item	Configuration
Operating system	Ubuntu 16.04	Programming language	Java
Processor	8-core CPU	Key generation tools	Cryptogen & Fabric-CA
Memory	16 GB RAM	Key generation method	Combination of static and dynamic
Blockchain platform	Hyperledger Fabric 1.4	Chaincode deployment	Automated via network.sh script

In this case, the decay factor γ is 0.1 and the weight parameter α, β is 0.5 [21-22]. The SM9 algorithm, as an identity-based cryptosystem, is faster in key generation and encryption and decryption than traditional public key systems. Therefore, the study chooses test values that can reflect the efficiency of the SM9 algorithm. The study follows the three principles of reproducibility, practicability, and comparability in the selection of test values. First, in order to ensure that the test data can truly reflect the performance of the algorithm, the parameters selected in the test (elliptic curve order, hash function bits, temporary key length, etc.) are based on the national commercial cryptography standard and the recommended configuration of Hyperledger Fabric. Second, when simulating the actual operating environment of the blockchain, a typical data load size is set to simulate the transmission performance under medium load in reality. Again, to enhance the interpretability of the results, the selected test vectors include Padding, Differential Analysis, and Random, and compare the commonly used model SM9-ABE. Parameter values that can simulate the actual blockchain operating environment were selected in the tests to evaluate the performance and energy consumption of the model in real applications. Parameter values that can ensure transaction security while minimizing the impact on system performance are selected.

The study evaluates the SM-Blockchain model's performance using three test vector sets: Padding Test Vectors (PTV) for testing encryption and decryption correctness and efficiency, Differential Cryptanalysis Test Vectors (DCTV) for assessing resistance to attacks, and Random Test Vectors (RTV) for performance and security. The above vectors are all derived from the publicly available national cryptography SM9 algorithm standard test set and open source implementation, mainly including the National Cryptography Administration SM9 standard and test vectors (http://www.gmbz.org.cn/main/viewfile/20180108015305901286.html) and the GmSSL open source national cryptography algorithm library (https://github.com/guanzhi/GmSSL). The SM9-ABE framework is included for comparison. Fig. 6(a) shows that the establishment of a communication connection or initiating a validation process speeds for SM9-ABE and SM9-Blockchain on various input vectors in the first test. SM9-Blockchain averages at 11.07 ms, while SM9-ABE at 14.11 ms. Fig. 6(b) reveals average times of 7.96 ms for SM9-Blockchain and 9.88 ms for SM9-ABE. This result shows that the SM9-Blockchain model is superior to the SM9-ABE model in the speed of establishing a communication connection or initiating a validation process. In addition, the research simulates different network conditions and data loads through automated scripts, which ensures the accuracy and reliability of test results.

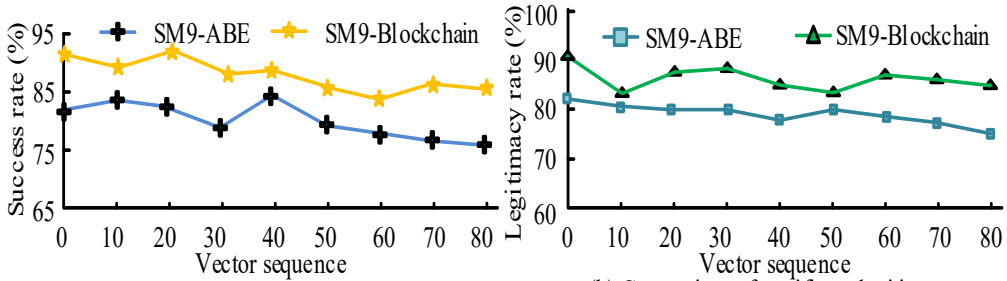


(a) The results of the first key negotiation test (b) The results of the second key negotiation test

Fig. 6. Comparison of models establishes a communication connection or initiates a validation process speed.

Fig. 7 illustrates the success and legitimacy rates for key negotiations in the SM9-ABE and SM9-Blockchain models under the PTV vector set. As can be seen from Fig. 7(a), the success rate of key negotiation of SM9-Blockchain model is 88.73%, which indicates that this model can effectively establish secure session keys between users in most cases. In contrast, the success rate of SM9-ABE model is 83.77%, which is slightly lower than that of SM9-Blockchain model. This may be because the SM9-Blockchain model adopts more optimized algorithms and protocols in the process of key exchange. The difference of success rate may be due to the fact that SM9-Blockchain model provides a more stable network environment and a more reliable data synchronization mechanism by using the distributed characteristics of blockchain technology, thus improving the stability and success rate of key agreement. In Fig. 7(b), the certificate validity rate of the SM9-Blockchain model is 87.51%, which means that the model can verify the validity and legality of the certificate with high accuracy. The certificate validity rate of SM9-ABE model is low, which may be due to some loopholes or deficiencies in the process of certificate management and verification, which leads to the decrease of the accuracy of validity verification. The high

certificate legitimacy rate of SM9-Blockchain model benefits from the non-tampering and transparency of the blockchain, and the issuance and status of each certificate can be tracked and verified on the blockchain, thus effectively preventing forgery and tampering.

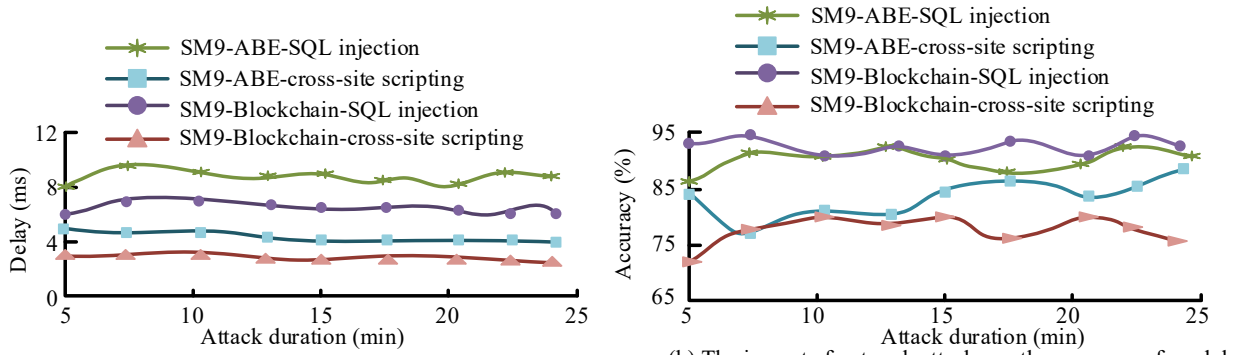


(a) Comparison of key negotiation success rates (b) Comparison of certificate legitimacy

Fig. 7. Comparison between the success rate of model key negotiation and the legality rate of certificates.

B. SM9-Blockchain Model Security Validation

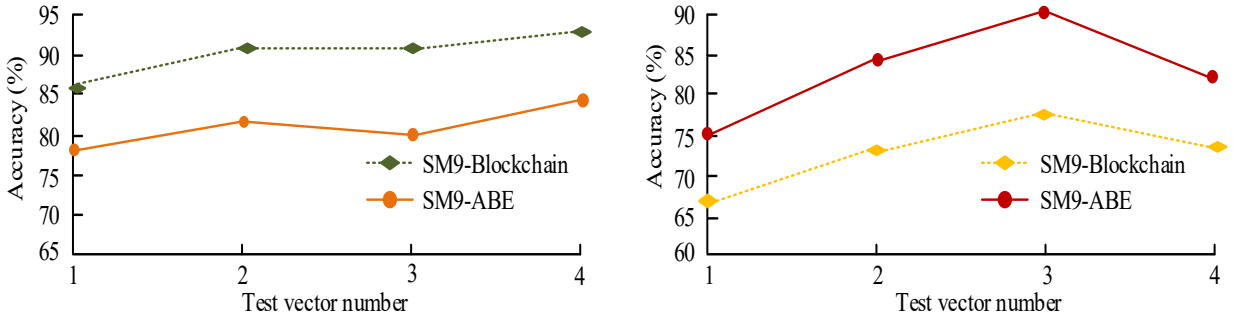
The study tests the model's security against SQL Injection and XSS attacks. Fig. 8(a) shows the SM9-Blockchain model experiences about a 6ms delay under SQL Injection and a 3ms delay under XSS attacks. Fig. 8(b) indicates that the SM9-Blockchain model has a higher average correct rate than the control model under various attacks.



(a) The impact of network attacks on model runtime latency (b) The impact of network attacks on the accuracy of model identity confirmation

Fig. 8. Model security verification.

To analyze the factors affecting user identity confirmation accuracy, the model uses PTV and RTV vectors. Fig. 9(a) shows that SM9-ABE has an average correct rate of 81.29%, while SM9-Blockchain has 90.41%. Fig. 9(b) reveals that SM9-ABE's average correctness is 71.81% and SM9-Blockchain's is 83.25%.



(a) The recognition accuracy of random vectors generated in RTV (b) The recognition accuracy of random vectors generated in PTV

Fig. 9. Comparison of user identity confirmation accuracy.

To analyze encryption and decryption delays in user identity confirmation under normal scenarios, experiments were conducted using the PTV vector set. In Fig. 10(a), the encryption delay of SM9-Blockchain model is about 0.35 ms lower than that of SM9-ABE model under the same conditions. This improvement may be attributed to the adoption of more efficient algorithm and optimized data structure in the encryption process of SM9-Blockchain model. The lower encryption delay means that the SM9-Blockchain model is faster in dealing with encryption tasks, which is especially

important for application scenarios that need rapid response, such as real-time communication and online transactions. The SM9 algorithm, the core cryptography of the model, is important for reducing latency due to its smaller key size and faster encryption/decryption speed. Lower cryptographic latency means that the SM9-Blockchain model is faster in processing cryptographic tasks, which is especially important for application scenarios that require fast responses (e.g., real-time communication and online transactions). The distributed architecture of blockchain technology, however, improves the efficiency and reliability of data synchronization, which reduces delays in the user identification process. Each node stores a copy of the blockchain, and this decentralized structure reduces the single point of failure and bottlenecks that can occur in centralized systems. It can also be seen from Fig. 10(b) that the delay of the proposed model is about 0.39ms lower than that of the SM9-ABE model. This shows that the SM9-Blockchain model not only performs well in the encryption stage, but also provides fast processing ability in the decryption stage. Decryption delay is very important to ensure real-time data and improve user experience, especially in the environment of frequent data exchange. In this study, several key security protocols are introduced in the contract design. First, when a user submits an authentication request, the system uses the signature verification function built into the on-chain contract to verify the request information to ensure that the request source is real and not forged. Second, by introducing the anti-replay mechanism based on timestamp and Nonce, attackers are effectively prevented from utilizing historical requests to initiate pseudo-authentication operations. In addition, the smart contract restricts the invocation scope of contract functions through role authority control to prevent illegal access to sensitive resources. To address the risk of contract logic vulnerabilities, Mythril, a static code analysis tool, is introduced to conduct vulnerability scanning before the system is deployed, and combined with the test network for simulated attack verification, to ensure that the contract has a strong anti-re-entry and anti-overflow capabilities. The above mechanisms together constitute the basic security protocol framework used in this system to defend against typical attacks, which improves the robustness and credibility of the system in real application scenarios.

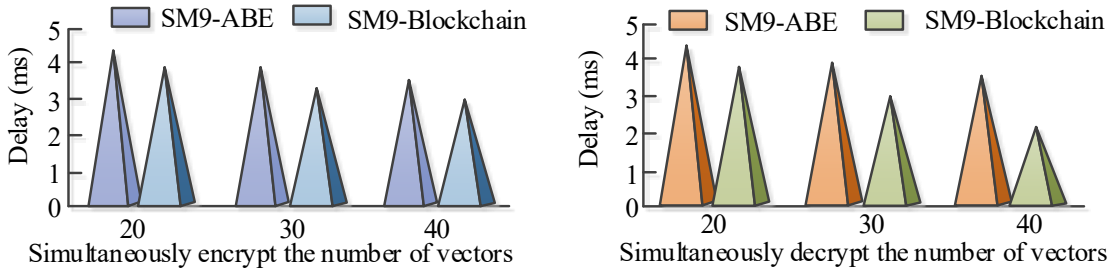


Fig. 10. Comparison of encryption and decryption latency among different models.

C. Performance Comparison of Different Methods

The study compares blockchain-based authentication management methods proposed by other scholars, including Miao et al.'s [23] blockchain-enabled privacy-preserving authentication management protocol for the Internet of Medical Things, Kumar et al.'s [24] blockchain-based authentication method, and Kang et al.'s [25] blockchain-based authentication scheme for an enhanced and lightweight medical sensor network. It benchmarks the time overhead for key generation, proving keys, and verifying keys in the PTV set for these methods. Details are shown in Fig. 11.

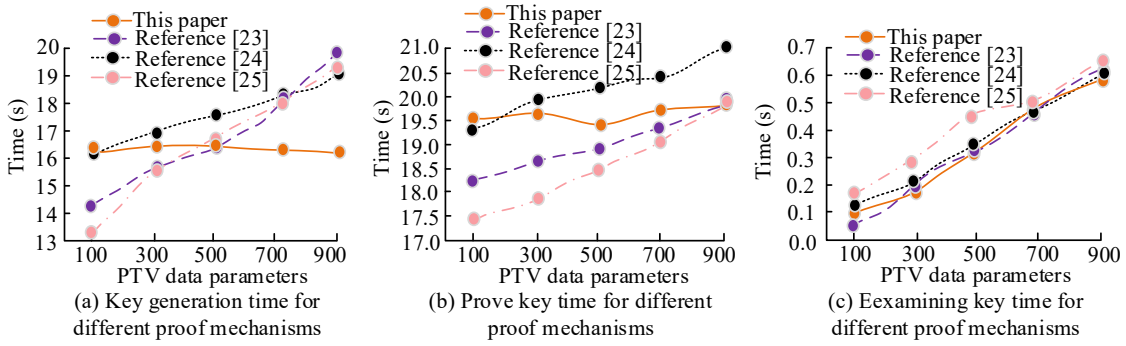


Fig. 11. Comparison of the time overhead required for key generation and verification under different authentication mechanisms.

Fig. 11(a) shows that SM9-Blockchain's key generation time is consistently around 16.29s, with an average reduction of 3.93%, 7.39%, and 1.51% compared to other methods. Fig. 11(b) indicates that SM9-Blockchain is least affected by data parameter size in key proving, while other methods show an increasing trend with larger parameter sizes, possibly due to larger proof key storage requirements. Fig. 11(c) shows that SM9-Blockchain's verification time is reduced by 4.84% on average when handling 900 PTV data parameters. These results demonstrate that SM9-Blockchain outperforms others in encryption and decryption time. The performance comparison results of key indicators of the four methods are shown in

Table II. To ensure the statistical reliability of the results, each test was conducted no fewer than twenty times under the same conditions, and all metrics are reported as mean ± standard deviation. Performance differences were evaluated for statistical significance using paired t-tests with a significance level of $\alpha = 0.05$.

TABLE II. PERFORMANCE COMPARISON RESULTS OF KEY INDICATORS OF FOUR METHODS

Index	SM9-Blockchain	Miao et al. [23]	Kumar et al. [24]	Kang et al. [25]
Average establish a communication connection or initiate a validation process time (ms)	11.07±0.22	14.52±0.48	12.31±0.35	13.83±0.41
Average key negotiation success rate (%)	88.73±1.15	85.20±1.60	87.11±1.42	86.54±1.51
User identity confirmation accuracy (%)	90.41±1.07	87.61±1.32	88.93±1.21	89.26±1.29
Delay time under SQL injection attack (ms)	6.00±0.31	8.22±0.37	7.52±0.29	7.81±0.33
Delay time under XSS attack (ms)	3.00±0.18	4.53±0.22	3.81±0.20	4.04±0.21
Average key generation time overhead (s)	16.29±0.47	18.51±0.55	17.10±0.52	17.94±0.54
Average key proof time overhead (s)	19.52±0.62	21.33±0.72	20.25±0.68	20.82±0.70
Average key verification time overhead (s)	0.36±0.05	0.45±0.06	0.40±0.05	0.42±0.06

Through the comparison in Table II, it can be seen that the SM9-Blockchain model performs better than other models in most key performance indicators. Especially in the accuracy of user identity confirmation and the delay time under SQL injection and XSS attacks, the SM9-Blockchain model shows obvious advantages. This shows that the SM9-Blockchain model has obvious advantages in improving security and efficiency. To further evaluate the performance advantages of the SM9 algorithm in identity authentication systems, this study conducts a comparative analysis with traditional encryption protocols, including Rivest–Shamir–Adleman (RSA) (1024-bit), Elliptic Curve Cryptography (ECC) (256-bit), and Advanced Encryption Standard (AES) (128-bit). All tests were conducted under the same environment and transaction volume. This is shown in Table III.

TABLE III. PERFORMANCE COMPARISON BETWEEN SM9 AND CONVENTIONAL ENCRYPTION ALGORITHMS

Algorithm	Key length	Key generation time (ms)	Encryption latency (ms)	Decryption latency (ms)	CPU utilisation (%)	Memory usage (MB)	Energy consumption (J)
SM9	256 bit	16.29	7.81	8.70	12.34	25.43	0.09
RSA	1024 bit	31.20	9.56	18.40	20.15	38.62	0.18
ECC	256 bit	23.45	8.63	12.51	17.98	33.24	0.12
AES	128 bit	1.52	4.13	4.05	8.56	14.79	0.03

As can be seen from Table III, RSA exhibits significantly higher average latency in key generation and decryption compared to SM9 (16.29 ms and 8.7 ms). ECC performs better than RSA but remains slightly slower than SM9 under concurrent transaction loads due to computational bottlenecks in key negotiation. AES, as a symmetric encryption algorithm, delivers excellent speed but lacks support for identity binding and key negotiation, making it unsuitable for standalone use in blockchain-based identity authentication. Although the symmetric encryption algorithm of AES has the lowest CPU usage (8.56%), considering the strong encryption strength provided by the SM9, the SM9's CPU usage is still within a reasonable range, which is a superior price/performance ratio, especially with its high level of security. Overall, SM9 strikes a balance between security and efficiency by enabling identity-based encryption, digital signature, and key exchange with smaller key sizes and lower latency. This makes it particularly suitable for resource-constrained environments, such as IoT devices and lightweight authentication terminals.

D. Practical Validation

To further evaluate the performance of the proposed authentication model in real-world and IoT scenarios, two experimental environments were designed: a real property management system and an IoT device environment. In the real property management system test, the model was deployed on an existing platform for limited-scale validation. The system included multiple users and multiple device nodes to simulate concurrent authentication requests. During deployment, the front-end authentication module interacted with the back-end RESTful API via the HTTPS protocol. The back-end invoked the SM9 double encryption module and Hyperledger Fabric nodes to perform on-chain authentication and verification. The property management system ran on real servers and client devices, with a local area network latency of approximately 20 ms and a bandwidth of 50 Mbps.

In the IoT device test, a Raspberry Pi 3 (1GB RAM, quad-core processor) was used as the end node, connected to IoT sensors and low-power devices. Communication was securely established with the IoT gateway via an MQTT protocol adapter, with the model also performing encryption, authentication, and verification in the back-end. The IoT devices are connected to the network via Wi-Fi, with a latency of approximately 50 ms and a bandwidth of 10 Mbps.

In both environments, the system first initialized and configured the hardware and network conditions, and then seamlessly integrated with the existing platform (including the PKI certificate system and device management platform) through an interface adaptation layer. The user-side authentication process was triggered with a single click, eliminating the need for manual key management or plugin installation. Interaction latency was kept to under 0.5 seconds,

and the interface style remained consistent with the existing system. Key performance indicators were measured in both environments. Detailed results are shown in Table IV.

TABLE IV. TEST RESULTS OF DIFFERENT ALGORITHMS IN VARIOUS ENVIRONMENTS

Experimental environments	Algorithm	Response time (ms)	Authentication success rate (%)	Network bandwidth consumption (KB/s)
Real-world	SM9	16.97	91.26	22.68
	RSA	28.74	81.32	36.48
	ECC	23.85	86.05	30.92
	AES	18.42	88.14	24.75
IoT	SM9	19.06	87.93	19,47
	RSA	39.21	74.81	30.67
	ECC	33.54	79.49	27.18
	AES	21.13	85.20	21.60

As shown in Table IV, in the real-world property management system test, the response time of the SM9 algorithm was 16.97 ms, which is 40.96%, 28.81%, and 7.88% faster than RSA, ECC, and AES, respectively. This indicates that SM9 has a clear advantage in processing efficiency within practical systems. The authentication success rate of SM9 in this environment reached as high as 91.26%. Combined with the results from the IoT device environment, the superiority of the proposed method is further demonstrated. In the resource-constrained IoT environment, SM9 achieved an authentication success rate of 87.93%, which is 17.52%, 10.62%, and 3.20% higher than RSA, ECC, and AES, respectively. This shows that the proposed method maintains strong authentication performance even on devices with limited resources. Finally, the study further selected two common and representative attack methods to evaluate the security of the system, namely the replay attack and the impersonation attack.

Replay attack refers to a situation where an attacker intercepts and records legitimate authentication requests from users and then resends the same data to the system in an attempt to bypass identity verification. Impersonation attack means that an attacker forges the identity or credentials of a legitimate user or node in order to obtain authentication privileges or access to sensitive resources. The study designed corresponding defense mechanisms based on the SM9-Blockchain model and conducted a comparative evaluation with traditional encryption systems, RSA and ECC. The details are shown in Table V.

TABLE V. SECURITY AND SCALABILITY COMPARISON UNDER REPLAY AND IMPERSONATION ATTACKS

Evaluation Metric	SM9-Blockchain	RSA	ECC
Replay attack detection rate (%)	99.82±0.14	87.20±1.40	91.45±1.25
Impersonation attack detection rate (%)	98.50±0.42	85.70±1.58	89.35±1.31
Authentication throughput (requests/s)	158.42±3.51	112.74±4.15	128.20±3.91
Average authentication latency (ms)	21.85±1.20	36.57±1.82	29.46±1.52
Max concurrent devices supported	1200	750	880

As can be seen from Table V, in the replay attack test, the SM9-Blockchain model achieves a 99.82% interception rate relying on the timestamp and session key mechanism, which has stronger anti-replay capability than RSA and ECC. In the impersonation attack test, SM9 achieves a 98.50% recognition rate based on the identity signature and certificate chain verification mechanism, which is significantly better than RSA and ECC. In addition, in a highly concurrent environment, SM9-Blockchain can still support 1,200 devices to authenticate concurrently, and the authentication throughput reaches 158.42 times/s, with an average latency of only 21.8 ms, which indicates that it has a superior ability to scale. The capability is more superior.

To fully validate the performance of the proposed model under scalability, extreme stress, and long-term operation conditions, the study designed three scenarios: concurrent expansion testing, stress testing, and long-term data accumulation simulation. In the scalability test, the number of concurrent device connections was gradually increased from 200 to 1600. In the stress test, the number of concurrent connections was further increased to 2000 to simulate peak load. In the long-term data accumulation simulation, nodes were continuously run and authentication transactions were continuously written. The storage growth rate and node synchronization latency were recorded after one, three, and six months. The experimental results are shown in Table VI.

TABLE VI. SM9-BLOCKCHAIN MODEL SCALABILITY VERIFICATION

Test scenario	Concurrency level / Duration	Avg. authentication latency (ms)	Authentication throughput (req/s)	Storage growth rate (%)	Node sync delay (ms)
Scalability test	200 devices	19.42 ± 0.38	155.12 ± 3.42	-	-
	800 devices	20.57 ± 0.41	154.03 ± 3.51	-	-
	1200 devices	21.85 ± 0.44	158.42 ± 3.51	-	-
	1600 devices	24.16 ± 0.50	149.35 ± 3.72	-	-
Stress test	2000 devices	27.94 ± 0.55	138.27 ± 3.85	-	-

Long-term data accumulation	1 month	-	-	8.53 ± 0.12	2.83 ± 0.05
	3 months	-	-	24.68 ± 0.21	3.12 ± 0.04
	6 months	-	-	42.37 ± 0.26	3.38 ± 0.06

Table VI shows that in the scalability test, when the number of concurrent devices increased from 200 to 1200, the average authentication latency increased only slightly, while the throughput fluctuated slightly and remained above 150 req/s, demonstrating that the system can operate stably under high concurrency conditions. In the stress test, when the number of concurrent accesses reached 2000, the latency increased to 27.94 ms and the throughput dropped to 138.27 req/s, demonstrating that the system still has sufficient processing capacity under extreme loads. In the long-term data accumulation test, thanks to the multi-layer blockchain and snapshot compression mechanism, the main chain storage growth rate was 42.37% over 6 months, and the node synchronization latency remained in the millisecond range with minimal increase. This demonstrates that the proposed model not only has good concurrency processing capabilities in the short term, but also maintains low resource consumption and stable performance in the long term.

V. Discussion

The SM9-Blockchain model proposed in the study excels in authentication accuracy, encryption and decryption efficiency, and resource adaptability. The constructed double encryption structure and traceable certificate mechanism guarantee the system's lower authentication latency and higher throughput rate in high concurrency and resource-constrained scenarios. In addition, compared with the RSA and ECC models, SM9-Blockchain achieves significant improvements in identity confirmation accuracy and key generation efficiency. From the perspective of mechanism design, the model integrates the structure of the main chain and auxiliary chain, and realizes the collaborative processing of identity authentication and data consistency through the on-chain trusted CA authorization and chain code execution mechanism; the CA trust decay mechanism effectively inhibits the repeated authorization of low-credibility nodes, and the chain code snapshot strategy improves the storage and response efficiency of the system while safeguarding the performance of the main chain. These designs enhance the system's adaptability to complex network environments while improving authentication accuracy. Furthermore, the model's design takes into account internal threats, CA compromise, and practical key management needs. Role-based access control and on-chain auditing are used to prevent internal unauthorized access, trust decay and certificate status broadcasting are used to address CA compromise, and key recovery and revocation mechanisms are provided to ensure long-term security.

In terms of practical application, the system still shows good scalability and platform compatibility. The system can be applied to intelligent communities, IoT terminal access, distributed identity management and other scenarios. Experimental results also demonstrate the model's adaptability and interoperability across diverse regulatory frameworks. Within China's national cryptographic system, SM9 enables authentication compliant with the Cryptography Law, whilst in the US FIPS 140-3 environment, it supports PKI systems including ECC and RSA. Concurrently, the model supports integration with global standards including X.509, OAuth 2.0, and FIDO, while enabling cross-chain interoperability across platforms such as Hyperledger Fabric and Ethereum. Its broad cross-platform and cross-domain applicability has been validated in smart community, IoT, and financial healthcare scenarios. However, with the continuous evolution of technology and the expansion of application scenarios, identity authentication models face new challenges and development requirements in real-world deployments. Firstly, in terms of security, the advancement of quantum computing poses potential threats to existing cryptographic systems. As an identity-based cryptographic scheme based on bilinear pairings, the SM9 algorithm relies on mathematical problems that may no longer be secure under quantum computing. In addition, the hash algorithms and digital signature mechanisms used in blockchain systems are also susceptible to quantum attacks. Therefore, to enhance the model's security adaptability in future quantum environments, it is advisable to introduce post-quantum cryptographic algorithms, such as lattice-based or hash-based signature schemes, in alignment with the standards currently being promoted by institutions such as the National Institute of Standards and Technology of the United States.

Secondly, although this model employs encryption mechanisms and role-based access control policies, there remains a potential risk of privacy leakage during data interaction between on-chain and off-chain environments. Future improvements could incorporate privacy-enhancing technologies such as anonymous credentials and zero-knowledge proofs to mitigate such issues. While blockchain achieves decentralized data storage, PKI still exhibits centralized tendencies during certificate issuance. To address this, the CA trust decay mechanism proposed in this study dynamically adjusts the trustworthiness of certificate authorities based on their historical behavior, thereby effectively reducing the risk of long-term trust monopolization by authoritative institutions. With the development of quantum computing, existing cryptographic algorithms such as SM9 and elliptic curve cryptography may face the threat of being cracked. To enhance the system's security adaptability in future environments, further research into integrating post-quantum cryptographic algorithms should be considered to strengthen the model's long-term robustness in identity authentication scenarios.

Finally, to improve the system's scalability and interoperability, future research will explore cross-chain integration capabilities with other blockchain platforms such as Ethereum and Hyperledger. Through techniques such as relay chains, hash time-locking, oracle services, or pluggable identity modules, the model can enable trusted identity data sharing and verification across multiple blockchains.

VI. Conclusion

This study proposes a dual-encryption authentication framework that combines the SM9 algorithm and blockchain technology. It also designs a time-decay-based CA trust management mechanism and a multi-layer blockchain architecture. Experimental validation demonstrates that the model demonstrates outstanding authentication security, responsiveness, and scalability, achieving a latency of 11.07 ms, a key agreement success rate of 88.73%, and an identity confirmation accuracy of 90.41%. The key contribution of this study lies in its breakthrough of the limitations of single encryption or storage mechanisms by innovatively proposing a dual-encryption authentication framework and optimizing storage and processing efficiency through a multi-layer blockchain architecture. However, the experiments were limited to a simulated environment. Future research could focus on further optimizing the model's performance in resource-constrained IoT environments and enhancing its applicability for large-scale deployments. In summary, this study provides a new solution for authentication in property management systems and IoT devices, improving security, reliability, and scalability, and laying the foundation for further research in related fields.

Acknowledgment

This study was supported by 2022 Nanyang Science and Technology Development Plan Project (NO. KJGG105); Nanyang Medical College 2022 Scientific Research Fund Project (grant No. 2022ZRKX005), Nanyang Science and Technology Plan Project for 2024-2025 (grant No. 24KJGG127).

References

[1] Yusuf M, Yusup M, Pramudya R D, Fauzi A Y, Rizky A, "Enhancing user login efficiency via single sign-on integration in internal quality assurance system (espmi)," International Transactions on Artificial Intelligence, vol. 2, no. 2, pp. 164-172, 2024.

[2] Selvam D, Khanna A, "Enhancing utility sector efficiency and security: Integrating digital identity systems amidst privacy and ransomware challenges," International Journal of Advanced Research in Science, Communication and Technology, vol. 4, no. 1, pp. 759-772, 2024.

[3] Rieger A, Roth T, Sedlmeir J, Fridgen G, Young A, "Organizational identity management policies," Journal of the Association for Information Systems, vol. 25, no. 3, pp. 522-527, 2024.

[4] Oduri S, "Continuous authentication and behavioral biometrics: Enhancing cybersecurity in the digital era," International Journal of Innovative Research in Science Engineering and Technology, vol. 13, no. 7, pp. 13632-13640, 2024.

[5] Fan Y, Li J, "Cross-chain transaction of notaries based on two-stage improved PageRank algorithm," International Journal of Network Security, vol. 27, no. 1, pp. 95-103, 2025.

[6] Aguilera R V, Ruiz Castillo M, "Toward an updated corporate governance framework: Fundamentals, disruptions, and future research," BRQ Business Research Quarterly, vol. 28, no. 2, pp. 336-348, 2025.

[7] Rijanto A, "Blockchain technology roles to overcome accounting, accountability and assurance barriers in supply chain finance," Asian Review of Accounting, vol. 32, no. 5, pp. 728-758, 2024.

[8] Attaran M, "Blockchain technology in healthcare: Challenges and opportunities," International Journal of Healthcare Management, vol. 15, no. 1, pp. 70- 83, 2022.

[9] Li D X, Lu Y, Li L, "Embedding blockchain technology into IoT for security: A survey," IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10452-10473, 2021.

[10] Panda S S, Jena D, Mohanta B K, Ramasubbareddy S, Daneshmand M, Gandomi A. H, "Authentication and key management in distributed IoT using blockchain technology," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12947-12954, 2021.

[11] Saputra I, Arkeman Y, Jaya I, Hermadi I, Akbar N A, Sutedja I, "AniraBlock: A leap towards dynamic smart contracts in agriculture using blockchain based key-value format framework," Communications in Science and Technology, vol. 8, no. 2, pp. 154-163, 2023.

[12] Saputra I, Arkeman Y, Jaya I, Hermadi I, Sutedja I, "Blockchain-based key-value store to support dynamic smart contract interaction in the agricultural sector," Indonesian Journal of Electrical Engineering and Computer Science, vol. 33, no. 1, pp. 622-633, 2024.

[13] Yang Y, Qiu Y, Cao J, Xiao S, "Identity-Based Blind Signature Scheme with Message Recovery over SM9," Chinese Journal of Electronics, vol. 34, no. 2, pp. 510-519, 2024.

[14] Lai J, Huang X, He D, Wu W, "Provably secure online/offline identity-based signature scheme based on SM9," The Computer Journal, vol. 65, no. 7, pp. 1692-1701, 2022.

[15] Wu Z J, Zhang Y, Yang Y M, Wang P, Meng Y, "BDSec: Security authentication protocol for BeiDou-II civil navigation message," China Communications, vol. 21, no. 6, pp. 206-218, 2024.

[16] Zhang X, Ye C, "A novel privacy protection of permissioned blockchains with conditionally anonymous ring signature," Cluster Computing, vol. 25, no. 2, pp. 1221-1235, 2022.

[17] Prabakaran D, Ramachandran S, "Multi-factor authentication for secured financial transactions in cloud environment," Computers, Materials & Continua, vol. 70, no. 1, pp. 1781-1798, 2022.

[18] Mokayed H, Quan T Z, Alkhaled L, Sivakumar V, "Real-time human detection and counting system using deep learning computer vision techniques," artificial Intelligence and Applications, vol. 1, no. 4, pp. 221-229, 2023.

[19] Gad A G, Mosa D T, Abualigah L, Abohany A A, "Emerging trends in blockchain technology and applications: a review and outlook," Journal of King Saud University-Computer and Information Sciences, vol. 34, no. 9, pp. 6719-6742, 2022.

[20] Mukherjee A, Balachandra M, Pujari C, Tiwari S, Nayar A, Payyavula S R, "Unified smart home resource access along with authentication using Blockchain technology," Global Transitions Proceedings, vol. 2, no. 1, pp. 29-34, 2021.

[21] Garba A, Chen Z, Guan Z, Srivastava G. "LightLedger: A novel blockchain-based domain certificate authentication and validation scheme," IEEE Transactions on Network Science and Engineering, vol. 8, no. 2, pp. 1698-1710, 2021.

[22] Anisetti M, Ardagna C A, Bena N, Damiani E. "Rethinking certification for trustworthy machine-learning-based applications," IEEE Internet Computing, vol. 27, no. 6, pp. 22-28, 2023.

[23] Miao J, Wang Z, Wu Z, Ning X, Tiwari P. A blockchain-enabled privacy-preserving authentication management protocol for Internet of Medical Things. Expert Systems with Applications, vol. 237, pp. 121329, 2024.

[24] Kumar R, Javeed D, Aljuhani A, Jolfaei A, Kumar P, Islam A N. Blockchain-based authentication and explainable AI for securing consumer IoT applications. IEEE Transactions on Consumer Electronics, vol. 70, no. 1, pp. 1145-1154, 2024.

[25] Kang T, Woo N, Ryu J. Enhanced lightweight medical sensor networks authentication scheme based on blockchain. IEEE Access, vol. 12, pp. 35612-35629, 2024.