Secure Sharing and Encryption Control of E-commerce Data Information Based on Blockchain Technology

Yongxing You

Basic Course Teaching Department, Hubei University of Police, Wuhan, 430034, China
E-mail: zlh30619@126.com

Received 08 April 2025; Accepted 05 September 2025

Abstract

The rapid development of e-commerce has led to a significant increase in the risk of sensitive data leakage, such as user transaction records, payment details, and identity information. Information security issues are becoming increasingly severe, especially in scenarios that rely on centralized cloud storage architectures, facing core challenges such as single point of failure leakage risks, lack of fine-grained access control in cross organizational data sharing, high encryption computing costs, rigid existing access control policies, and the contradiction between privacy protection and data sharing efficiency. In view of this, research has proposed and validated an innovative solution that integrates blockchain technology. Specifically, the study proposes a data security protocol based on attribute proxy re encryption and a data security sharing model based on blockchain. The data security protocol adopts ciphertext policy attribute encryption and introduces attribute proxy re encryption technology to re encrypt ciphertext through proxy nodes, solving the privacy protection problem of data transmission and sharing. The data security sharing model utilizes blockchain to store shared data, designs detailed access control policies and data encryption and decryption control mechanisms, and constructs a data security sharing system under

Journal of Cyber Security and Mobility, Vol. 14_4, 1007–1032.
doi: 10.13052/jcsm2245-1439.14410

a multi-layer architecture. In the experimental section, a simulated attack environment was constructed to test data security protocols. The results showed that compared with protocols such as SRAAP, TEE Oracle, Pedersen link Schnorr, etc., the blockchain data sharing protocol designed in this study achieved a 'high' level in terms of resistance to 51% attacks and resistance to general attacks (better than the 'medium' level of SRAAP protocol). The encryption time for privacy identity data was only 2.84ms (lower than SRAAP's 5.20ms and TEE Oracle's 7.46ms), and the maximum encryption time was controlled at 32ms. When processing a large amount of private data, the indexing time of the encryption control algorithm did not exceed 0.4 seconds, far lower than B-SEM algorithm's 0.79s and CAB algorithm's 0.91s. Moreover, the average memory occupation of the research scheme was only 18.54%, significantly lower than F-SEM algorithm. In the verification of blockchain data sharing platforms, compared with data sharing schemes such as BDAE, BF, RAISE, etc., the data control error rate of the research model does not exceed 3%, the accuracy of privacy data transmission is close to 95%, the data search and encryption performance is excellent (average search time of 1.35ms, shortest encryption time), and the access control cost is lower than other models. The research method combines blockchain technology and attribute proxy re encryption technology to effectively improve the privacy protection and control performance of shared data. It is significantly better than existing mainstream solutions in terms of computing efficiency, resource consumption, security strength, and control accuracy, effectively solving the inherent defects of centralized cloud storage, providing enhanced privacy protection, access control, and secure sharing capabilities for e-commerce data, ensuring data integrity and confidentiality, and reducing the threat risk of privacy sensitive data.

Keywords: Blockchain, privacy protection, attribute encryption, access control, searchable-encrypted, safety, data sharing.

1 Introduction

The advancement of information technology has made e-commerce an indispensable part of the global economy, which has completely changed the traditional business operation mode with its characteristics of efficiency, convenience, and globalization. E-commerce information, as a bridge connecting buyers and sellers, covers sensitive data such as product information, transaction records, user preferences, and payment details. These pieces of

information are not only important basis for business operation decisions, but also the key to consumer privacy protection [1, 2]. The rise of e-commerce benefits from the popularization of Internet technology and the acceleration of digital process, but its development is also faced with problems such as privacy information disclosure, opaque logistics process, etc. On the one hand, e-commerce platforms store a large amount of user data. These data have become key targets of hacker attacks and online fraud, with frequent incidents of data breaches, identity theft, payment fraud, and other serious threats to users' property security and privacy rights [3]. On the other hand, the cloud storage model dominated by centralized management no longer allows data owners to have complete control over the data, making it difficult to share dispersed data and causing serious data silos, making it difficult to form effective management mechanisms [4]. In addition, existing information security protection relies heavily on one-way encryption control strategies, making it inadequate in the face of increasingly complex network environments. The privacy breaches and sharing difficulties in data management urgently need to be addressed. In e-commerce, information security sharing and encryption control are not only important means to protect user privacy and enterprise assets but also key to promoting the healthy development of the data economy and enhancing market competitiveness [5]. Previous studies have made numerous attempts in the information security sharing and encryption control of e-commerce data, such as Role-based Access Control (RBAC) and Attribute-based Access Control (ABAC). These methods have improved data security to some extent, but there are still limitations. For example, the RBAC model is relatively rigid in permission management and difficult to adapt to the dynamically changing e-commerce environment. Although ABAC has higher flexibility, it is more complex in attribute definition and policy management, and its performance is limited in large-scale data sharing scenarios. In addition, traditional encryption techniques such as symmetric encryption and asymmetric encryption also face challenges in key management and data decryption efficiency, making it difficult to meet the requirements of efficient and secure data sharing [6]. Therefore, this study relies on blockchain technology and designs a data sharing model under Ciphertext Policy Attribute-Based Encryption Proxy Re-Encryption (CP-ABE-PRE) from the perspective of information security sharing and encryption control, to meet diverse data sharing and privacy data encryption control needs.

The innovation is reflected in two points. Firstly, considering the diversity of e-commerce data subjects, a blockchain-based consortium chain is

proposed to manage and maintain information and store block information, and an architecture system for data sharing is designed. Secondly, considering the drawbacks of data management in cloud computing, a combination of blockchain technology and proxy re-encryption technology is proposed, and a blockchain data sharing protocol is designed to protect data privacy while also achieving secure data sharing.

2 Related Works

Traditional data sharing is mostly stored on third-party storage platforms, which poses significant risks of intentional data leakage and tampering, and makes it difficult for multiple parties to participate in data sharing. T. Guo et al. proposed using blockchain to implement architecture construction and designed a hybrid concurrency control protocol to improve the success rate of data sharing. This system had good scalability and can achieve data sharing on the EasyBuy blockchain [7]. However, its hybrid concurrency control protocol does not take into account the dynamic changes in attributes, making it difficult to adapt to the frequent changes in e-commerce user roles. To ensure secure data sharing, Y. Dong et al. proposed implementing behavior control and access control using a centralized consortium blockchain system. This method could achieve editable and secure data access for blockchain [8]. However, there is still a risk of single point of failure in centralized architecture, and the problem of centralized data access control has not been fundamentally resolved. Strengthening the security of e-commerce data is crucial. Z. Morić et al. proposed using integrated privacy enhancement technology to protect personal data sharing, and designed a comprehensive framework to collaborate legal, technological, and procedural elements to enhance trust in the digital market. This method provided a safeguard approach for data security in e-commerce [9]. P. Prathap Nayudu et al. proposed using hash algorithm to hide access policy to solve the data privacy leakage problem of CP-ABE (attribute-based encryption with ciphertext policy). This method could effectively resist attacks in the Internet of Things and had high adaptive security [10]. In response to the issue of data privacy protection in e-commerce, Y. Shu et al. proposed using a symmetric balanced funnel P5 model to implement data encryption protection and gradually enhance encryption strength. This model provided balanced protection for data exchange and enhanced the overall data security of e-commerce [11]. Z. Guan et al. proposed the use of integrated blockchain and searchable encryption models to improve the protection of sensitive data in order to meet

the storage and search needs of e-commerce data, and set up proxy roles to divide search tasks and virtual resources. This method had high reliability and safety [12]. However, the division of its proxy roles results in lower indexing efficiency, and the ciphertext query time significantly increases with the growth of data volume. S. Bharany proposed using asymmetric encryption algorithm (Rivest Shamir Adleman, RSA) to achieve sensitive data sharing and security protection, and utilizing cryptographic secure hash functions for digital signature formulation. The RSA algorithm had good encryption control performance [13].

Data privacy is crucial for social security, but the transparency of blockchain transaction information poses privacy challenges. T. Feng et al. used searchable attribute encryption methods to achieve blockchain data privacy protection and verified user access control. This method effectively solved the problems of privacy exposure and private key leakage risk [14]. The CP-ABE-PRE strategy posed security and performance challenges to a single authority dependency, and has high computational costs. Therefore, Y. Shuangxi proposed a data sharing scheme based on blockchain and decentralized attribute encryption to achieve integrated joint control. This method effectively achieved tamper proof and auditable data sharing [15]. The access control scheme based on blockchain and ciphertext policy attribute encryption poses new challenges such as information leakage and low consensus efficiency in cloud storage environments. Y. Lu et al. proposed a fine-grained access control method to update permissions through proxy re encryption. This method could effectively meet the requirements of information access control and had higher application efficiency [16]. H. Tang et al. proposed the construction of a secure storage and sharing framework using blockchain technology to address privacy breaches in centralized information storage. This framework improved the security and efficiency of information storage [17]. The traditional network transmission model does not fully consider the information security issues under the Internet environment. N. Hu et al. proposed an elastic anonymous information sharing environment method, which uses a blockchain consortium to control clusters and core exchange networks to achieve traffic segmentation, encryption, and other processing, solving the problems of anti tracking and traffic hijacking. This method could achieve high-performance network transmission and ensure network communication security [18]. Considering the risks of unauthorized destruction and low detection efficiency of blockchain in distributed networks, A. Baseera et al. proposed the Pisces hybrid technology to achieve efficient data transmission. This technology could effectively solve the problem of

distributed network vulnerabilities with the help of ripple consistency algorithm [19]. V. Mannayee et al. proposed a distributed management framework for dynamic access management and system governance of blockchain technology and peer-to-peer networks. This method had good storage transaction performance, with an average throughput far exceeding 95% [20].

The core challenge facing current e-commerce data sharing is that traditional centralized storage platforms have a single point of failure risk, weak multi-party collaborative sharing mechanisms, and existing blockchain solutions still have significant limitations in dealing with diversified e-commerce data scenarios. Through systematic analysis of cutting-edge research, it was found that in the security architecture design, Guo et al. [7] utilized blockchain to enhance sharing scalability, but their hybrid concurrent protocol did not solve the problem of fine-grained access control, making it difficult to adapt to the frequent changes in e-commerce user roles; The centralized consortium chain proposed by Dong et al. [8] achieves data editability, but the single point authoritative architecture is prone to performance bottlenecks and security risks (such as centralized private key management). In contrast, research on the use of distributed attribute proxy re encryption mechanism ensures fine-grained control while completely avoiding single point of failure. In terms of privacy encryption, Nayudu et al. [10] did not optimize the issue of high computational overhead; The decryption delay and memory usage of Lu et al. [16] still constrain real-time e-commerce scenarios. The design scheme proposed by Bharany et al. [13] is not suitable for dynamic access policies and its random security needs to be verified. And Guan et al. [12]'s searchable encryption model has significant indexing efficiency and ciphertext query latency. Although progress has been made in some areas of the current work, there are still issues such as the imbalance between computational efficiency and security, insufficient dynamic permission management, unsuitability to distribution vendor data characteristics, and poor latency encryption performance. In response to the above gaps, a research proposes an attribute encryption protocol that integrates proxy re encryption. Compared with references [10] and [16], it introduces dynamic re encryption of proxy nodes, which can reduce policy update overhead and support instant user revocation. The shared model proposed by combining IPFS distributed storage and smart contract automation control is more efficient than literature [12] and [17], which can improve indexing efficiency and data transmission accuracy. It also achieves a thorough decentralized design compared to literature [8] and [15], providing a secure and efficient solution for high concurrency, multi-agent e-commerce data sharing scenarios.

3 Electronic Commerce Data Information Security Sharing and Encryption Control

3.1 Data Security Protocol Based on CP-ABE-PRE

E-commerce breaks the temporal and spatial limitations of consumer activities, while expanding the boundaries of the e-commerce market, it also promotes economic growth and efficiency improvement of the entire society. However, its vigorous development has also led to increasingly prominent security risks in the form of information leakage and data tampering [21]. The centralized control mode of e-commerce systems can improve operational efficiency, but it also makes it difficult to effectively safeguard user information security. Once the platform data system is breached, a large amount of user information will face the risk of leakage. To address this challenge, blockchain technology has emerged, providing strong support for the transformation of e-commerce. CP-ABE can effectively achieve specific access based on data attributes, making it more suitable for data sharing scenarios. Considering the large number of data subjects in e-commerce and the special and complex nature of shared data, this study adopts the consortium chain form of blockchain to achieve information management, maintenance, and storage of block information. On the CP-ABE scheme, a blockchain data sharing protocol called Proxy Re-Encryption (PRE) is proposed. The PRE algorithm can achieve ciphertext transmission between data senders and receivers. As a third-party access to data, the proxy can ensure the integrity and security of the data. Figure 1 shows the design process of the PRE algorithm scheme.

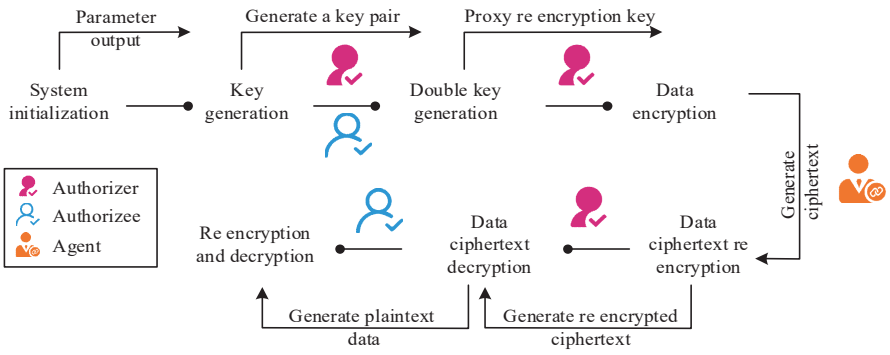

Figure 1 The design process of the RE algorithm scheme.

In Figure 1, the key distribution center generates keys for the data owner and requester based on the system's common parameters. Afterwards, the data owner generates a set of re encryption keys using their own private key and receiver's public key, as well as the number and threshold of proxy nodes [22]. The owner encrypts plaintext data into ciphertext using their own public key and sends the ciphertext to the proxy node. The proxy node uses the re encryption key to re encrypt the received ciphertext and obtain the re encrypted ciphertext. This ciphertext can only be decrypted by the requester's private key. This study is based on the PRE algorithm and introduces blockchain technology to achieve privacy protection and control of shared data. The design is based on access permissions, data storage, and traceability. Specifically, the protocol under PRE defines access policies and attributes to ensure the relative independence of encryption and decryption, and distributed file systems can achieve data storage. Each file has a unique hash value, avoiding the limitations of traditional cloud storage centralized access control. Figure 2 is a schematic diagram of the shared protocol model design.

In Figure 2, the data owner encrypts the shared data and uploads it to the interstellar file system, while developing access control policies and storing them on the blockchain. The data user obtains encrypted ciphertext through data requests and access control policies, decrypts it with a private key obtained from a trusted authorization node, and ultimately downloads and decrypts the data from the interstellar file system. The interstellar file system is mainly responsible for storing and retrieving data ciphertext and hash values. The trusted authorization node is responsible for system establishment, public key generation, and user private key distribution. Proxy

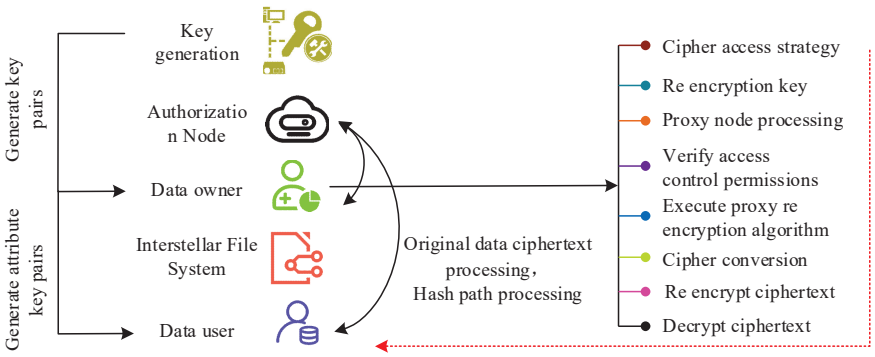

Figure 2 Schematic diagram of shared protocol model design.

nodes are responsible for storing metadata ciphertext and access policies on the blockchain, verifying data owner attributes, and performing re encryption operations when conditions are met. They serve as a bridge between the blockchain and data users. The various parts in this protocol are closely related and can effectively achieve secure data sharing and access control.

3.2 Design of Data Security Protocol Structure

The protocol construction part is designed from the aspects of system initialization, key generation, data storage, data access, and control. After selecting parameters, trusted authorization nodes can generate system public keys and system master keys using multiplication loop groups. Afterwards, the authorized node will initiate the registration process after verifying the identity IDi of user i, as expressed mathematically in equation (**??**).

$$Request_T(IDi) \rightarrow (Ecertsi, (UPK, USKi), ui) \tag{1}$$

In equation (1), $(UPK, USKi)$ is the user's public-private key pair. ui is a set of attributes. $Ecertsi$is the user certificate issued by the trusted authorization node [23]. When designing a blockchain data security protocol, the attribute proxy re encryption algorithm first uses a trusted authorization node to perform initialization steps, and then outputs the system public key and system master key. Afterwards, the user initiates a registration request $Request_T(IDi)$ to the certificate authority, and after verifying the user's identity, issues an authorization certificate, user public-private key pair, and corresponding authorization attribute set. Data users can initiate attribute private key requests to authorized nodes to generate private key $SKDU$, as shown in equation (2).

$$\begin{aligned} SKDU = \{&D = g^{(a+r)/\beta}, \forall i \in P : Dy = g^r \cdot H(hi)^{hi}, \\ &Di' = g^{hi}, Di'' = H(hi)^{\beta}\} \end{aligned} \tag{2}$$

In equation (2), D is the target group, a is the primary key, g is the public key component, and $H(\cdot)$ is the hash function. r is a random number, β is a system parameter, hi is an attribute-related parameter, and P is an attribute set. Di' is the basic component directly associated with the random number in the user's private key, used for matching and verifying with the corresponding item in the ciphertext during decryption. Di'' is a key component for implementing fine-grained access control based on attributes, ensuring the correspondence between private keys and user attributes. This formula defines how the private key for data user attributes is generated. By

combining system parameters, random numbers, and attribute hash values to construct the private key, it enables fine-grained permission control based on attributes, ensuring that only users who meet the attribute conditions can decrypt the data. This study utilizes public key encryption mechanism to achieve private key encryption, and RSA algorithm to achieve encryption Enc and decryption Dnc, as shown in equation (3).

$$\begin{cases} Enc = (SK_{DU}, U_{PKDU}) \rightarrow CSKDU \\ Dnc = (C_{SKDU}, U_{PKDU}) \rightarrow SK_{DU} \end{cases} \tag{3}$$

In equation (3), U_{PKDU} is the user's public key, and C_{SKDU} is the decryption private key ciphertext. In the attribute encryption and storage part of shared data, the data owner encrypts the plaintext of the shared data and then stores it through the interstellar file system. This study implements access in the form of an access structure tree, as shown in equation (4).

$$\begin{aligned} C_{DU} = \{\Phi, C* = (DK + H_W) \cdot e(g,g)^{\alpha s}, C = h^s, \\ \forall y \in Y : C_y = g^{qy(0)}, C_y = H(att(y))^{qy(0)}\} \end{aligned} \tag{4}$$

In equation (4), C is the challenger, Φ is the access policy, and att is the set of user attributes. $q(y)$ is a polynomial constructed from the set of node attributes y in the structural tree. s is the secret value, C_{DU} is the ciphertext, and Y is the public key, $H(w)$ is the index of the storage location of the shared data ciphertext in the interstellar file system, and C_y is the attribute encryption component in the ciphertext. $e(,)$ is a bilinear mapping function, and α is a key parameter in the system master key [24]. The ciphertext expression is a key parameter in attribute-based encryption for decryption verification, used to verify the match between user attributes and access policies during the decryption phase. Only when the attributes meet the conditions can the correct decryption result be calculated using this parameter, ensuring that data is only accessed by authorized users. Access permissions will limit access conditions to ensure data security, such as user roles, time, location, etc. In the data access section, the user sends a request to the blockchain proxy node and triggers the access control contract $Request_{data}(u_{DU}, C_{DU})$. The control contract will verify the user's attributes, and when the attribute set is 1, successful decryption can be achieved. The public key of the blockchain proxy node encrypts the generated re encryption key $RK_{DO \rightarrow DU}$ to obtain the re encryption key ciphertext CRk, as shown in equation (5).

$$\begin{cases} RK_{DO \rightarrow DU} = k_i (k_i \in Z_p) \\ Enc(RK_{DO \rightarrow DU}, U_{PKPN}) \rightarrow C_{Rk} \end{cases} \tag{5}$$

In equation (5), p is the order of the multiplication loop group, and ki is the node threshold. $Zp$is a finite field, $Enc(\cdot)$ is an encryption function, U_{PKPN} is the public key of the proxy node, and C_{Rk} is the re-encryption key ciphertext. After decrypting the encrypted key ciphertext with its own private key, the plaintext obtained will be stored in the file system along with the symmetric key and shared data. The data user implements attribute private key decryption based on recursive decryption, that is, inputs the decryption private key C_{DU}, attribute ciphertext SK, and node x of the access structure tree, and uses equation (6) for calculation.

$$DecryptNode(C_{DU}, SK, x) = \begin{cases} e(g,g)^{r \cdot qx(0)}, & i \in Y \\ \emptyset, & other \end{cases} \tag{6}$$

In equation (6), $DecryptNode()$ is the node decryption function. q_x is the polynomial of the node, and r is the root node of the tree. The node decryption function describes the decryption calculation logic for accessing structure tree nodes. When user attributes meet node requirements, decryption parameters can be generated through bilinear mapping and polynomial values. By introducing Lagrange coefficients into the equation, decryption can be achieved based on the value of the root node. The blockchain proxy node also supports attribute revocation while ensuring the encryption and decryption processing of shared data, effectively reducing computational overhead and improving the flexibility of access control.

3.3 A Data Security Sharing Model Based on Blockchain

Traditional e-commerce data are mostly distributed in a decentralized form, making it difficult to achieve centralized management, inevitably leading to data silos and exposure risks, and its shared model is difficult to achieve auditing and tracing of accessed data [25]. To ensure data privacy and integrity, this study proposes a blockchain based data security sharing model, which is designed from two aspects: data storage and access control. A decentralized file system can store data on multiple nodes, with blockchain primarily storing metadata information for shared data. Its integration with the file system enables participants to search for and access shared data blocks. The access control section combines the proxy re-encryption mentioned above with attribute based encryption. Figure 3 shows the design diagram of the data security sharing model.

In Figure 3, the data owner and data user interact through data encryption, data storage, proxy re encryption, access control, and other means. The

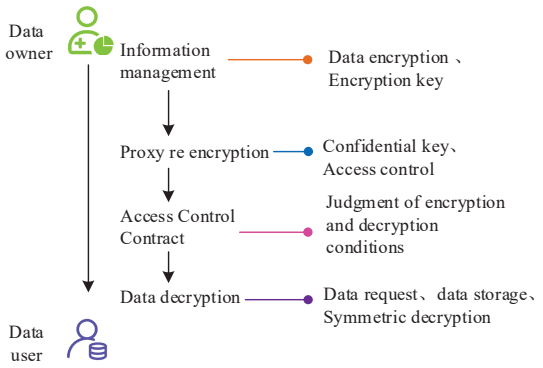

Figure 3 Schematic diagram of data security sharing model design.

information management section includes managing and updating participant identity information and transaction data. The data encryption module encrypts shared data and metadata attributes, while the proxy re encryption module implements re encryption of blockchain proxy nodes. Participants can use access control to achieve blockchain verification. Only when the encryption and decryption conditions are met, the data user and owner have corresponding authorization [26]. In the model, data owners utilize smart contracts and access policies to achieve ownership and control of shared data. Data users can initiate requests to the blockchain based on their attribute sets to obtain plaintext information for shared data. Figure 4 shows the process of data security sharing.

In Figure 4, the main focus is on symmetric encryption of shared data, data storage, data sharing, data management, re encryption operations, access control, and data decryption. The design of shared system architecture includes storage layer, network layer, engine layer, contract layer, interface layer, and application layer. The storage layer includes a decentralized network to store data and combines multiple database formats to meet file size requirements. The data content includes symmetric key ciphertext, metadata, data owner, identity information, etc. The network layer is mainly responsible for data transmission and communication, and its Hyperledger Fabric architecture ensures the flexibility of access control mechanisms, including Peer nodes, Orderer nodes, CA nodes, and client nodes [27]. The engine layer mainly performs functions such as executing transactions, managing ledger status, and providing query services. The interaction between the contract layer and the underlying consortium chain enables the management of business data, identity, access control, keys, and other contracts.

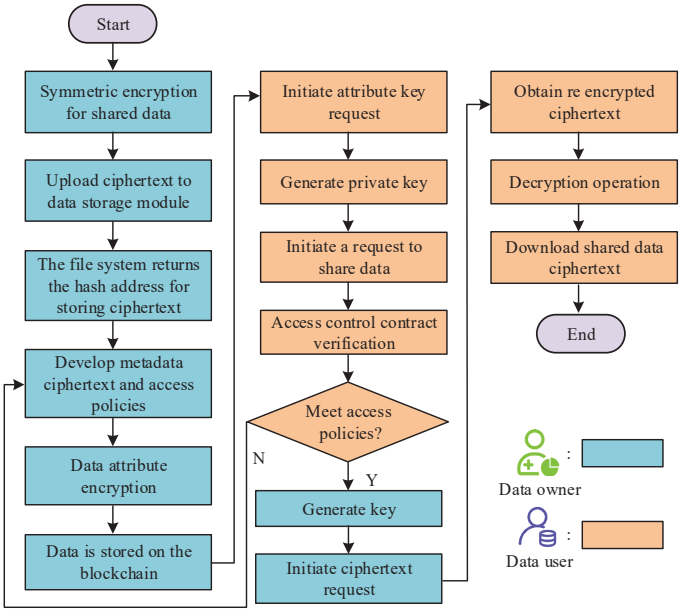

Figure 4 Schematic diagram of data security sharing process.

4 Analysis of Data Information Security Sharing and Encryption Control Results

4.1 Performance Analysis of E-Commerce Data Information Security Encryption

Under the data security sharing system, this study deploys the operating environment and adopts a front-end and back-end separation mode to achieve technical and functional design. The front-end and back-end frameworks use Layui technology and SpringBoot technology respectively to store the system's business data in a MySQL database. The underlying blockchain system is Hyperledger Fabrinch1.4. The experimental results are implemented using the Win10 operating system (Intel (R) Core (TM) i5-10210U, 16GB of memory and 512GB of hardware capacity) and the Ubuntu 18.04 LTS 64 bit blockchain operating system (Dockercompose 1.12.0 version). The design of blockchain networks uses Raft as the consensus algorithm to configure certificates, create initial blocks, configure channels, and download IPFS file systems from the official website. The experiment obtains e-commerce data from Taobao and JD.com. Firstly, a security comparison analysis is conducted between the proposed data security protocol and the

Table 1 Security analysis of different protocols

Agreement	Resist 51% of attacks	Resistance to attacks	Transaction throughput	Waste block rate	Computational overhead
SRAAP	Medium	Medium	High	Medium	Medium
TEE-Oracle	Low	Low	Low	Low	Medium
Pedersen-link-Schnorr	Medium	Medium	Medium	Medium	High
Blockchain Data Sharing Protocol	High	High	Medium	Low	Low

Selective Revocation Anonymous Authentication Protocol (SRAAP) [28], Trusted Execution Environment-Oracle (TEE Oracle) [29], and Pedersen-link-Schnorr (PLS) [30], as shown in Table 1.

In Table 1, the designed data security protocol is secure in the event of an attack, and its computational cost is significantly lower than the other three protocols. The second most secure protocol is the SRAAP protocol. Afterwards, a functional analysis is conducted on the above protocol, including two parts: privacy transaction data and privacy identity data, as shown in Figure 5.

In Figure 5, the encryption efficiency of the proposed protocol is relatively high on privacy transaction data, and its running time under different attribute numbers is smaller than other protocols, and the overall curve growth is relatively small. Secondly, PLS protocol and SRAAP protocol perform

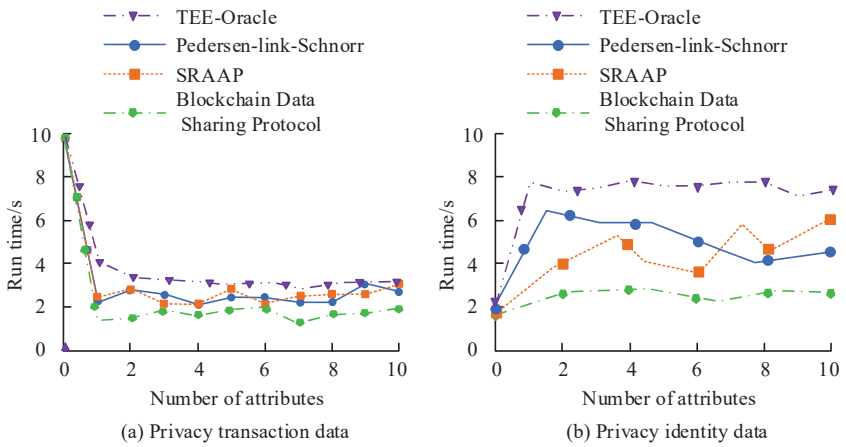

Figure 5 Running results of privacy transaction data and privacy identity data under different protocols.

well, with a running time of no more than 4 seconds in the later stage. In terms of privacy identity data encryption, when the number of attributes reaches 8, the encryption time spent by SRAAP, TEE-Oracle, PLS, and research protocols is 5.20ms, 7.46ms, 4.02ms, and 2.84ms. The research protocol makes its access control more flexible by adding proxy nodes and supporting user data revocation. Afterwards, the data sharing and permission control effects of the proposed CP-ABE-PRE algorithm are analyzed, and compared with the Centralized Alliance Blockchain (CAB) in reference [8], the Blockchain-Searchable Encryption Model (B-SEM) in reference [12], the Rivest-Shamir-Adleman (RSA) in reference [13], and the Fine-grained Proxy Re-Encryption (F-PRE) in reference [16].

In Figure 6(a), there is a significant fluctuation in the encryption time curves of CAB and RSA, with the maximum encryption time approaching 45ms, while the maximum encryption time of B-SEM and F-PRE also exceeds 50ms, far higher than the research algorithm. The encryption time of the research algorithm varies slightly at different times, with a maximum encryption time of only 32ms. In Figure 6(b), the decryption time consumption of the research algorithm is relatively similar to that of F-PRE, both of which introduce proxy re encryption, which to some extent increases the decryption time cost, but the overall variation is smaller than other algorithms. The maximum decryption time for B-SEM and RSA reaches 0.95ms and 0.84ms. Table 2 presents a random security analysis of the aforementioned algorithm.

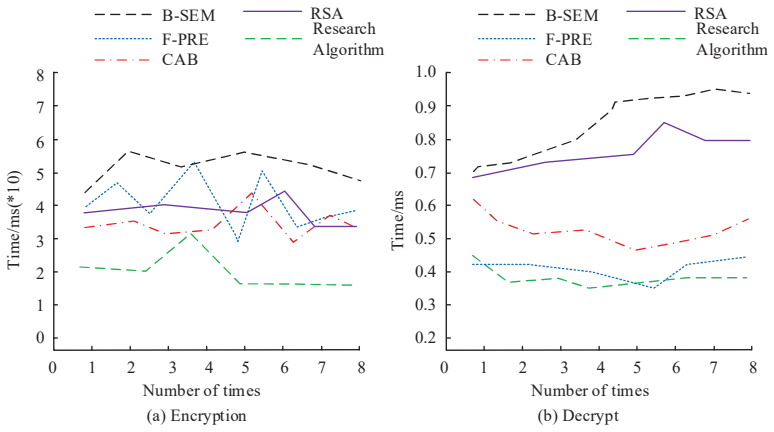

Figure 6 Time consumption of encryption and decryption for different algorithms.

Table 2 Randomness test results

Model	CP-ABE-PRE		F-PRE		CAB		RSA		B-SEM	
	P value	Result	P value	Result	P value	Result	P value	Result	P value	Result
1	0.31044	Pass	0.50434	Pass	0.51883	Pass	0.56381	Pass	0.34024	Pass
2	0.33019	Pass	0.52409	Fail	0.53881	Pass	0.58379	Pass	0.35999	Pass
3	0.40272	Pass	0.59662	Pass	0.60312	Pass	0.6481	Pass	0.43252	Pass
4	0.27182	Pass	0.46572	Pass	0.38127	Fail	0.42625	Fail	0.30162	Fail
5	0.31301	Pass	0.50691	Pass	0.56016	Pass	0.60514	Pass	0.34281	Pass
6	0.28403	Pass	0.47793	Fail	0.33199	Fail	0.37697	Pass	0.31383	Pass
7	0.34156	Pass	0.53546	Pass	0.26012	Pass	0.3051	Fail	0.37136	Fail
8	0.39873	Pass	0.59263	Pass	0.52179	Pass	0.56677	Fail	0.42853	Pass

Test items 1–8 in Table 2 represent frequency checks, intra block frequency tests, run tests, overlapping module matching tests, linear complexity tests, sequential tests, approximate entropy tests, and random walk tests. The proposed CP-ABE-PRE algorithm has passed the key stream sequence testing project. F-PRE did not pass the inspection on projects 2 and 6. There are many failed test projects for RSA [31, 32]. There is a significant difference in numerical values between CP-ABE-PRE and other algorithms, and its values in the project do not exceed 0.45, indicating that it has high randomness and security. Figure 7 shows the analysis results of the secure indexing time and ciphertext query time for the above algorithm.

In Figure 7, the indexing time of CP-ABE-PRE under maximum privacy data quantity does not exceed 0.4s, which is much higher than B-SEM's

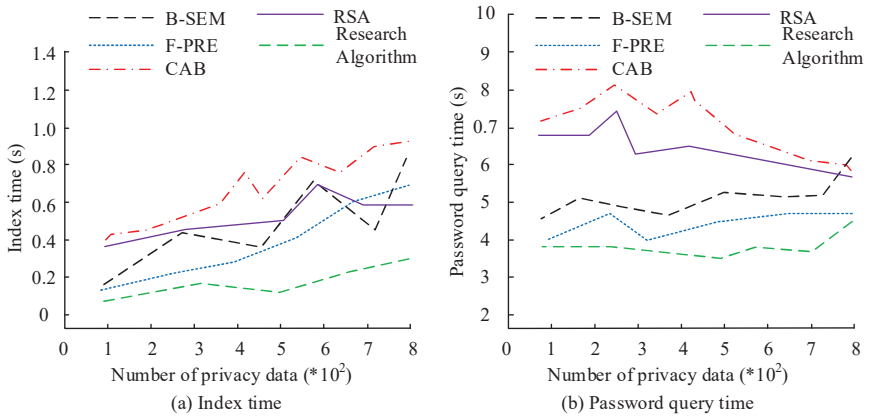

Figure 7 Security index time and ciphertext query time.

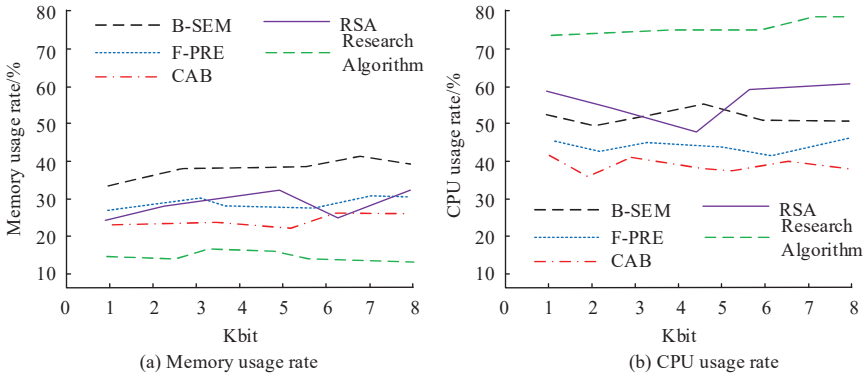

Figure 8 Results of different algorithms processing sensitive e-commerce data.

0.79s, F-PRE's 0.64s, CAB's 0.91s, and RSA's 0.58s. Under ciphertext query time, the slope of the query time curve of CP-ABE-PRE is smaller than other algorithms, and its maximum query time does not exceed 4.5 seconds. Figure 8 shows the results of using different algorithms to process sensitive data in e-commerce.

In Figure 8, the average memory usage rate of CP-ABE-PRE is 18.54%, while the average memory usage rates of F-PRE, CAB, RSA, and B-SEM are 29.68%, 27.34%, 28.25%, and 38.33%, showing some similarity. The CPU utilization of CP-ABE-PRE exceeds 75%, significantly higher than the comparison algorithm. This indicates that CP-ABE-PRE still has a high usage effect while ensuring data security.

4.2 Performance Testing of E-Commerce Data Information Security Sharing Model

Blockchain has brought revolutionary changes to e-commerce with its characteristics of network wide consensus, decentralization, programmability, and tamper resistance. Its decentralized nature breaks the monopoly of traditional e-commerce platforms, making transactions fairer and more transparent. The blockchain, a chain like data structure, requires the transaction information contained to be linked in block form. Each change in block data will result in a corresponding change in its hash value, which has high reliability and security. This study tested the proposed blockchain data sharing platform and compared its functional and data results with the Blockchain-Based and Decentralized Attribute-Based Encryption Scheme (BDAE) in reference [15], the Blockchain-Based Framework (BF) in reference [17], and the Resilient

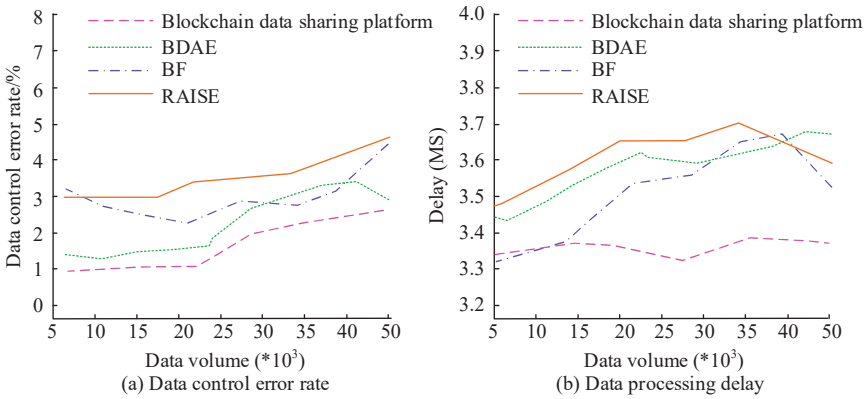

Figure 9 Data processing delay and control results of different schemes.

Anonymous Information Sharing Environment (RAISE) in reference [18], as shown in Figure 9.

In Figure 9(a), the maximum data control error rate for the four processing schemes does not exceed 5%. The data control effect of the research model and BDAE is relatively high, with similar trends and a maximum error rate of no more than 3%. The fluctuation of RAISE's error curve is slightly higher than other comparison schemes. In Figure 9(b), the data processing delay of the research model is the smallest and less affected by the amount of data, while the other three methods show varying degrees of delay, with the maximum value approaching 3.70ms. Figure 10 shows the results of privacy data transmission performance analysis of the above method.

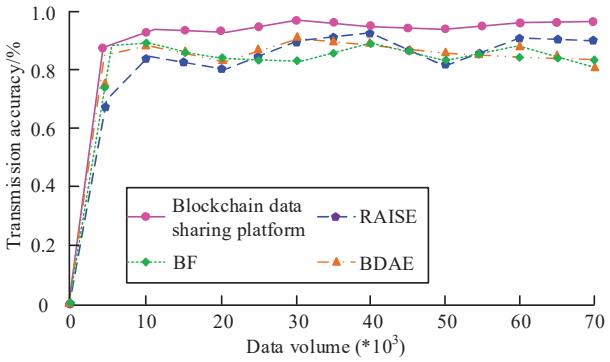

Figure 10 Privacy data transmission performance.

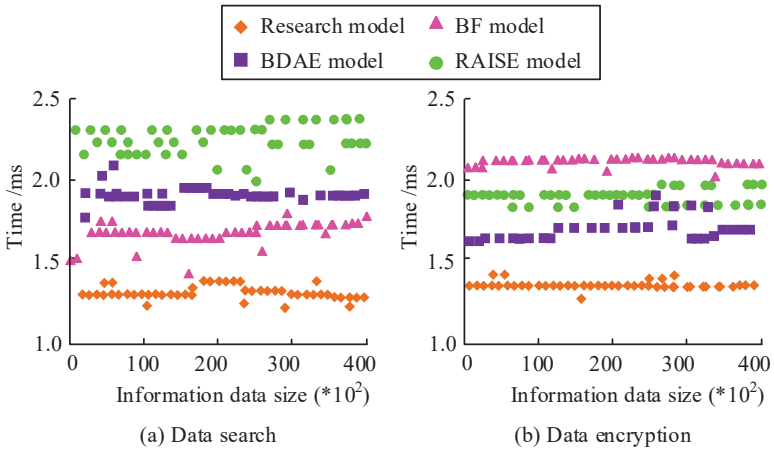

Figure 11 Data search and encryption scenarios for different schemes.

In Figure 10, the data transmission accuracy of the research model is relatively high, with privacy data transmission accuracy exceeding 85% under different document data, and the maximum value approaching 95%. The average transmission accuracy of BDAE, BF, and RAISE is 88.12%, 85.67%, and 89.33%. Figure 11 shows the data search and encryption performance analysis of the above method.

In Figure 11(a), the average data search time for the research model, BDAE, BF, and RAISE is approximately 1.35ms, 1.92ms, 1.73ms, and 2.23ms. There is a significant fluctuation in the search time spent by RAISE. In Figure 11(b), the research model<BDAE<RAISE<BF is obtained based on the cost of data encryption time from small to large. The data processing effect of the research model is good. Figure 12 analyzes the encryption performance of the model on identity data and transaction data in e-commerce.

In Figure 12(a), when the sample size exceeds 1200, the data encryption security values of the research model are all greater than 0.975, significantly higher than other algorithms. Next is BDAE, whose identity data encryption security value exceeds 0.97. On Figure 12(b), the encryption security of the research model is higher than that of other models, with an average value of 0.982. BDAE, BF, and RAISE are significantly affected by the sample size of the data, and their maximum values do not exceed 0.98. Table 3 provides a systematic analysis of the proposed shared model, including data processing speed, throughput, and data query efficiency.

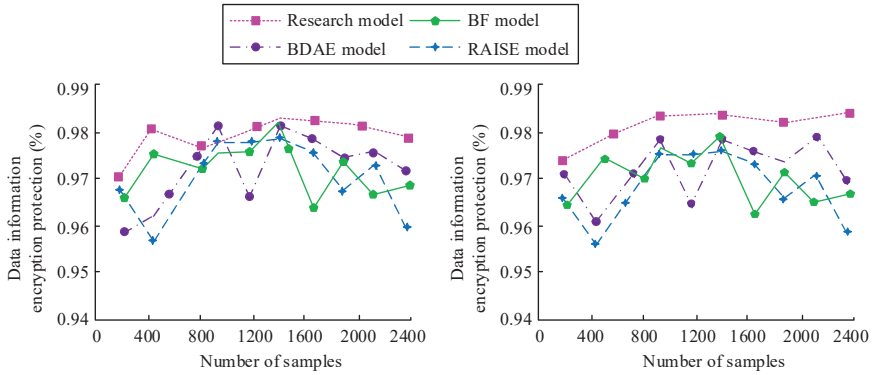

Figure 12 Encryption performance of identity data and transaction data.

Table 3 Application effect of data sharing model system

Model	Data size (MB)	Time (s)	Average speed (MB/s)	Throughput (tps/s)	Access control cost	
					Index re encryption communication cost (kb)	Key generation communication cost (kb)
BDAE	256	8.25	12.41	1736	2.33	3.67
BF	256	10.34	20.26	1857	2.57	4.18
RAISE	256	7.67	36.28	2043	3.16	3.25
Research model	256	4.38	63.17	2215	0.74	2.83

In Table 3, the BDAE, BF, and RAISE models all take over 5 seconds to complete, with average speeds of 12.41MB/s, 20.26MB/s, and 36.28MB/s, indicating slow performance. In terms of system throughput and access control cost, the numerical values of the research model are significantly better than other comparative models. The communication cost of re-encrypting the index and generating the key reaches 0.74kb and 2.83kb, with good access control costs and good application performance.

5 Conclusion

To ensure the privacy, security, and effective control of e-commerce data during the sharing process, this study proposed an encryption algorithm based

on blockchain technology and designed security controls based on CP-ABE. In the verification of the proposed encryption algorithm and secure sharing model, the designed data security protocol was secure under attack, and its computational cost was significantly lower than SRAA, TEE-Oracle, and Pedersen-link-Schnorr. The encryption efficiency of the proposed protocol was relatively high, and the running time on private transaction data and the encryption time on private identity data were both lower than other compared protocols. In the results of data sharing and permission control, there were significant fluctuations in the encryption time curves of CAB and RSA algorithms, with their maximum encryption time approaching 45ms, while the maximum encryption time of B-SEM and F-PRE was much higher than that of the research algorithms. The encryption time of the research algorithm varied slightly at different times, with a maximum encryption time of only 32ms. The proposed CP-ABE-PRE-has passed the key stream sequence testing project, with high randomness and security, and its indexing time under maximum privacy data quantity does not exceed 0.4s, far higher than other algorithms. The slope of the ciphertext query time curve for CP-ABE-PRE-was smaller than that of the comparison algorithm, and the average memory utilization was 18.54%. The average memory usage of F-PRE, CAB, RSA, and B-SEM exceeded 25%, and the CPU usage was relatively low. In the verification of the blockchain data sharing platform, the research model and BDAE showed high data control effectiveness, with a maximum error rate of no more than 3%. The data processing delay of the research model was the smallest, while the maximum values of the other three methods approached 3.70ms. The maximum transmission accuracy of the privacy data of the model under different document data approached 95%, and the data search was well encrypted, with data encryption security values all greater than 0.975. The average data search time for the other comparison models was over 1.5ms. The designed shared model had significantly better values in system throughput and access control costs than other models, with lower access control costs. The average speed of the other models was above 12MB/s, and their operating efficiency was relatively slow.

The blockchain data security protocol proposed in the study is superior to existing protocols such as SRAAP and TEE Oracle in terms of attack resistance and computational overhead. It has a 'high' level of resistance to 51% attacks and significantly reduces computational overhead; The CP-ABE-PRE encryption algorithm has a maximum encryption time of 32ms and a maximum indexing time of 0.4s, with an average memory usage rate of less than 20%, achieving a balance between security and efficiency; The

maximum error rate of data control in the blockchain sharing model is $\leq 3\%$, the accuracy of privacy data transmission approaches 95%, and the cost of access control is significantly reduced, effectively improving transmission efficiency and cost-effectiveness. For the first time, this study deeply couples proxy re encryption with the multi-layered architecture of blockchain, providing an industrial grade solution that combines strong security and low overhead for high concurrency and multi role e-commerce data sharing scenarios. The proposed blockchain based data security sharing architecture effectively solves the problems of data leakage and tampering in e-commerce data sharing platforms, and improves the effectiveness of data encryption and storage security.The limitations of the research include: firstly, it does not support cross chain data sharing, and its data interoperability mechanism with public or heterogeneous chains has not been verified, which restricts the flow of data in multi platform e-commerce, and the adaptability of multi platform e-commerce data interoperability scenarios is poor; Secondly, the system lacks interactivity, and the delay of re encryption of proxy nodes slightly increases with the growth of user volume. The elastic scalability of sudden traffic needs to be verified; Thirdly, the integration degree with the existing e-commerce information security system is relatively low, and the encryption efficiency of unstructured data has not been optimized, making it difficult to cover all types of e-commerce data. Future work will further focus on building cross chain data sharing mechanisms to achieve zero knowledge proof verification between heterogeneous blockchains; Optimize the parallel computing capability of proxy nodes and optimize resource allocation in high concurrency scenarios based on reinforcement learning; Explore hybrid encryption frameworks and integrate homomorphic encryption technologies to enhance the flexibility of data analysis, thereby providing security for e-commerce sharing in the commercial ecosystem.

References

[1] S. A. Ali. “Designing Secure and Robust E-Commerce Platform for Public Cloud,” The Asian Bulletin of Big Data Management., vol. 3, no. 1, pp. 164–189, November, 2023, DOI: 10.62019/abbdm.v3i1.56.

[2] H. Jebamikyous, M. Li, Y. Suhas and R. Kashef. “Leveraging machine learning and blockchain in E-commerce and beyond: benefits, models, and application,” Discover Artificial Intelligence., vol. 3, no. 1, p. 3, January, 2023, DOI: 10.1007/s44163-022-00046-0.

[3] C. Cho, B. Kim, H. Cho and T. Y. Youn. "A New Encryption Mechanism Supporting the Update of Encrypted Data for Secure and Efficient Collaboration in the Cloud Environment," CMES-COMP MODEL ENG., vol. 142, no. 1, pp. 813–834, January, 2025, DOI: 10.32604/cmes.2024.056952.

[4] P. Zhang and L. Xu. "Design and implementation of mobile e-commerce application built on WAP mobile payment system," WIREL NETW., vol. 30, no. 6, pp. 6089–6104, June, 2024, DOI: 10.1007/s11276-023-03409-2.

[5] Z. Lu and H. Mohamed. "A Complex Encryption System Design Implemented by AES," INT J INF SECUR., vol. 12, no. 2, pp. 177–187, April, 2021, DOI: 10.4236/jis.2021.122009.

[6] N. Pacharla and K. S. Reddy. "Trusted Certified Auditor Using Cryptography for Secure Data Outsourcing and Privacy Preservation in Fog-Enabled VANETs," CMC-COMPUT MATER CON., vol. 79, no. 5, pp. 3089–3110, May, 2024, DOI: 10.32604/cmc.2024.048133.

[7] T. Guo, Z. Zhang, Y. Yuan, X. Yang and G. Wang. "Hybrid concurrency control protocol for data sharing among heterogeneous blockchains," FRONT COMPUT SCI-CHI., vol. 18, no. 3, pp. 1–12, January, 2024, DOI: 10.1007/s11704-022-2327-7.

[8] Y. Dong, Y. Li, Y. Cheng and D. Yu. "Redactable consortium blockchain with access control: Leveraging chameleon hash and multi-authority attribute-based encryption," HIGH-CONFID COMPUT., vol. 4, no. 1, pp. 14–23, March, 2024, DOI: 10.1016/j.hcc.2023.100168.

[9] Z. Morić,V. Dakic,D. Djekic and D. Regvart. "Protection of Personal Data in the Context of E-Commerce," Journal of cybersecurity and privacy., vol. 4, no. 3, pp. 731–761, September, 2024, DOI: 10.3390/jcp4030034.

[10] P. Prathap Nayudu and K. R. Sekhar. "Secured Access Policy in Ciphertext-Policy Attribute-Based Encryption for Cloud Environment," COMPUT SYST SCI ENG., vol. 46, no. 7, pp. 1079–1092, December, 2023, DOI:10.3390/math10010068.

[11] Y. Shu and W. Wang. "Innovative research on encryption and protection of e-commerce with big data analysis," INT J DATA SCI ANAL., vol. 9, no. 2, pp. 123–142, July, 2024, DOI: 10.1504/IJDS.2024.139805.

[12] Z. Guan, N. Wang, X. Fan, X. Liu, L. Wu and S. Wan. "Achieving secure search over encrypted data for e-commerce: a blockchain approach," ACM T INTERNET TECHN., vol.21, no. 1, pp. 1–17, December, 2020, DOI: 10.1145/3408309.

[13] S. Bharany. "Secure Sensitive Data Sharing Using RSA and ElGamal Cryptographic Algorithms with Hash Functions," Information., vol. 13, no. 10, pp. 442, September, 2022, DOI: 10.3390/info13100442.
[14] T. Feng, H. Pei, R. Ma, Y. Tian and X. Feng. "Blockchain Data Privacy Access Control Based on Searchable Attribute Encryption," COMPUT MATER CON., vol. 66, no. 1, pp. 871–884, August, 2021, DOI: 10.32604/cmc.2020.012146.
[15] Y. Shuangxi. "BDAE: A Blockchain-Based and Decentralized Attribute-Based EncryptionScheme for Secure Data Sharing," Wuhan Univ. J. Nat. Sci., vol. 29, no. 3, pp. 228–238, June, 2024, DOI: 10.1051/wujns/2024293228.
[16] Y. Lu, T. Feng, C. Liu and W. Zhang. "A Blockchain and CP-ABE Based Access Control Scheme with Fine-Grained Revocation of Attributes in Cloud Health," COMPUT MATER CON., vol. 78, no. 2, pp. 2787–2811, February, 2024, DOI: 10.32604/cmc.2023.046106.
[17] H. Tang, C. Hu, T. Liu and J. Ouyang. "A Blockchain-Based Framework for Secure Storage and Sharing of Resumes," COMPUT MATER CON., no. 9, pp. 5395–5413, March, 2022, DOI: 10.32604/cmc.2022.028284.
[18] N. Hu, L. Liu, X. Liu, K. Wu, and Y. Zhao. "RAISE: A Resilient Anonymous Information Sharing Environment," COMP MODEL ENG., vol. 137, no. 12, pp. 2743–2759, August, 2023, DOI: 10.32604/cmes.2023.026939.
[19] A. Baseera and A. A. Alsadhan. "Enhancing Blockchain Security Using Ripple Consensus Algorithm," COMPUT MATER CON., vol. 73, no. 3, pp. 4713–4726, April, 2022, DOI: 10.32604/cmc.2022.029538.
[20] V. Mannayee and T. Ramanathan. "An Efficient SDFRM Security System for Blockchain Based Internet of Things," INTELL AUTOM SOFT CO., vol. 35, no. 2, pp. 1545–1563, March, 2023, DOI: 10.32604/iasc.2023.027675.
[21] K. Zhou. "Financial Model Construction of a Cross-Border E-Commerce Platform Based on Machine Learning," Neural Computing and Applications., vol. 35, no. 36, pp. 25189–25199, March., 2023, DOI: 10.1007/s00521-023-08456-6.
[22] H. Ping. "Network information security data protection based on data encryption technology," WIRELESS PERS COMMUN., vol. 126, no. 3, pp. 2719–2729, June,2022, DOI: 10.1007/s11277-022-09838-0.
[23] L. Zhao, B. Li and H. Yuan. "Cloud edge integrated security architecture of new cloud manufacturing system," J SYST ENG

ELECTRON., vol. 35, no. 5, pp. 1177–1189, October, 2024, DOI: 10.23919/JSEE.2024.000112.

[24] C. Guo, P. Weijun, W. Jing, F. Youxuan, Y. Keke and X. Yanshuang. "A blockchain-based proxy re-encryption scheme with conditional privacy protection and auditability," CHINA COMMUN., vol. 21, no. 7, pp. 267–277, July, 2024, DOI: 10.23919/JCC.fa.2022-0863.202407.

[25] S. Shunmuganathan, S. Kannan, M. R. TV, K. Ambika and T. Jayasankar. "Improved Secure Identification-Based Multilevel Structure of Data Sharing in Cloud Environments," COMPUT SYST SCI ENG., vol. 43, no. 11, pp. 785–801, November, 2022, DOI: 10.32604/csse.2022.022424.

[26] R. B. Salem, E. Aimeur and H. Hage. "A Multi-Party Agent for Privacy Preference Elicitation," Artificial Intelligence and Applications., vol. 1, no. 2, pp. 98–105, November, 2023, DOI: 10.47852/bonviewAIA2202514.

[27] X. Yang and P. Zhao. "A Lightweight, Searchable, and Controllable EMR Sharing Scheme," CMC-Comput. Mater. Con., vol. 79, no. 4, pp. 1521–1538, April, 2024, DOI: 10.32604/cmc.2024.047666.

[28] K. Yang, B. Yang, T. Wang and Y. Zhou. "Zero-cerd: A self-blindable anonymous authentication system based on blockchain," Chinese Journal of Electronics., vol. 32, no. 3, pp. 587–596, May, 2023, DOI: 10.23919/cje.2022.00.047.

[29] Y. Xian, L. Zhou, J. Jiang, B. Wang, H. Huo and P. Liu. "A distributed efficient blockchain oracle scheme for internet of things," IEICE T COMMUN., vol. 107, no. 9, pp. 573–582, September, 2024, DOI: 10.23919/transcom.2023EBP3156.

[30] D. Pengfei, M. Zhaofeng, Z. Yuqing, W. Jingyu and L. Shoushan. "Blockchain-Enabled Privacy Protection and Access Control Scheme Towards Sensitive Digital Assets Management," China Commun., vol. 21, no. 7, pp. 224–236, July, 2024, DOI: 10.23919/JCC.2022.ja.0740.

[31] Y. Dang, "Research on Collaborative Positioning Algorithm of Wireless Sensor Network Security Under Strong Topology Relation", JCSANDM, vol. 14, no. 01, pp. 25–46, Feb. 2025.

[32] J. K. Dawson, F. Twum, J. B. H. Acquah, and Y. M. Missah, "Cryptographic Solutions for Data Security in Cloud Computing: : A Run Time Trend-based Comparison of NCS, ERSA, and EHS", JCSANDM, vol. 13, no. 2, pp. 265–282, Feb. 2024.

Biography

Yongxing You obtained his MSc in Basic Mathematics (2003) from WHU, Wuhan. Presently, he is working as a Associate Professor in the Basic Course Teaching Department, Hubei University of Police, Wuhan. His areas of interest include machine learning and information security.