Blockchain-Based Mechanism for Privacy Data Integrity Protection in Pharmaceutical Supply Chains

Rui Qiao[1,*] and Jinbo Han[2]

[1]*School of Information Engineering, Shaanxi University of International Trade & Commerce, Xi'an, 712046, China*
[2]*The First Institute of Intelligent Mines, China Coal Xi'an Engineering Design Co., Ltd., Xi'an, 710054, China*
E-mail: 18220857680@163.com; 18392111583@163.com
[*]*Corresponding Author*

Received 20 January 2026; Accepted 10 February 2026

Abstract

The pharmaceutical supply chain is increasingly tending towards multi-party collaboration and high-dimensional data flow. Currently, existing blockchain technologies lack collaborative optimization of privacy and integrity for the pharmaceutical industry. Thus, this study tries to solve these issues by designing a blockchain-based approach for preserving data privacy integrity in a pharmaceutical supply chain. First, data privacy protection algorithms along with integrity verification are designed to implement access control and prevent leakage of sensitive information. Subsequently, a bidirectional gated recurrent unit, residual network, and extreme gradient boosting are used to develop a smart contract vulnerability identification approach. Finally, a data protection model is constructed. Experiments show that the proposed data verification algorithm achieves an attribute matching success rate of 99.94%, a high-concurrency authorization error rate of 0.07%, and encryption-decryption time lower than comparison algorithms. The proposed

Journal of Cyber Security and Mobility, Vol. 15_2, 497–524.
doi: 10.13052/jcsm2245-1439.1529

model reaches a maximum vulnerability detection accuracy of 99.31%, an area under the curve of 0.963, a minimum response latency of 132.64 ms, and a traceability data integrity verification rate of 99.96%. The results indicate that this mechanism effectively balances data privacy protection and integrity verification requirements in the pharmaceutical supply chain and provides a new method for secure data management.

Keywords: Blockchain, supply chain, privacy data, integrity protection, attribute-based encryption, zero-knowledge proof.

1 Overview

1.1 Background

The pharmaceutical supply chain is evolving towards a complex model with multi-party collaboration and high-dimensional data transmission, covering the entire process from drug production through transportation and delivery to end use [1]. Data processing requirements include guaranteeing both privacy security and tamper resistance [2, 3]. Patient personal health information and pharmaceutical companies' commercial secrets are highly sensitive data, and their leakage will trigger legal risks and trust crises. Tampering with data such as drug batches and quality inspection reports may lead to counterfeit drugs entering the market. Traditional centralized systems have defects such as single point of failure, easy data tampering, and coarse-grained permission management. Existing blockchain applications mostly focus on public traceability and lack privacy and integrity collaborative optimization design tailored for the pharmaceutical industry, making it difficult to adapt to industry regulatory requirements [4–6]. Therefore, there is an urgent need to develop a privacy data integrity protection mechanism that adapts to pharmaceutical supply chain scenarios to meet the actual development needs of the industry.

1.2 Related Works

Scholars have conducted extensive research on blockchain-based data integrity protection. For example, Kutybayeva et al. proposed an efficient blockchain-enhanced transparent pharmaceutical supply chain management model. By integrating blockchain and big data analysis, this model achieved data immutability and transparent processing. However, its adaptability to pharmaceutical companies of different scales and the sustainability of

long-term operation and maintenance remain to be verified [7]. Honarmand et al. constructed a dynamic entity-centered trust model based on source-driven routing protocols, integrating the weight method from social sciences and fuzzy logic theory to achieve precise identification and isolation of malicious nodes. Experimental results show that this protocol can effectively prevent attacks from black holes [8]. The trust-based self-detection routing and trust-based cooperative routing scheme proposed by the team of Mahamune can solve problems such as identification of malicious nodes, precise quantification of trust, and secure sharing of trust data in mobile self-organizing networks. However, it lacks the integration and interaction of global trust information and is prone to the problem of lagging trust value updates in high node mobility scenarios [9]. Su et al. proposed a lightweight trust model for opportunistic network security routing, which can effectively identify and isolate malicious nodes. However, it can only resist attacks from a single type of malicious nodes and has insufficient defense capabilities against complex mixed attacks such as collusion attacks and gray hole attacks [10]. Although existing studies have conducted certain explorations on data privacy, there are still deficiencies in their collaborative optimization of data integrity. For example, Huang's team proposed a blockchain-based zero-knowledge privacy-preserving continuous data integrity checking protocol by integrating verifiable delay functions, proof of retrievability, zero-knowledge proofs, and smart contracts. This provides a feasible solution for data integrity and privacy protection in cloud storage. However, the time consumption increases significantly as the number of exponential operations increases [11]. Jiang's team proposed a decentralized cross-chain data integrity verification scheme that can accurately verify the integrity of cross-chain data transmission and storage. However, the stability of this scheme in multi-chain large-scale concurrent interaction scenarios remains to be verified [12]. Nkereuwem et al. proposed a blockchain and smart contract-driven telemedicine solution, securing and protecting data and its management. The authorization mechanism regarding permissions in emergency scenarios was also proposed but has yet to be optimized. The proposed mechanism is also based on blockchain and smart contracts [13].

1.3 Main Methods

While current research on the application of blockchain in data integrity protection has achieved data anti-tampering or privacy encryption functions in some scenarios, such as Yuan et al.'s proposal of an identity-based

blockchain-assisted verification scheme for the integrity verification needs of public data in cloud storage systems [14], which solves the problems of single point of failure of trust, data tampering risk and the complex identity authentication process faced by traditional centralized verification schemes. The proposal is a comprehensive solution that adapts to the collaborative characteristics of multiple entities in the pharmaceutical supply chain and balances the strength of privacy protection and the efficiency of integrity verification that has not yet been formed. Attribute-based encryption (ABE) can precisely adapt to the differentiated permission requirements of multiple entities in pharmaceutical supply chains, such as pharmaceutical companies, logistics enterprises, medical institutions, and regulatory departments, avoiding privacy leakage risks caused by coarse-grained traditional permission management [15]. Zero-knowledge proof (ZKP) can complete data integrity verification without leaking sensitive data such as patient health information and pharmaceutical companies' commercial secrets, effectively resolving the core contradiction between privacy protection and verifiability [16]. A bidirectional gated recurrent unit (BiGRU) can accurately capture the forward and backward dependencies of smart contract code logic and supply chain transaction data through bidirectional modeling of temporal data, providing contextual support for vulnerability detection [17]. Residual networks (ResNet) alleviate the problem of gradient vanishing through skip connections and enhance the feature learning capability of deep networks. Extreme gradient boosting (XGBoost), with its ability to learn complex feature combinations, can improve the detection accuracy of composite vulnerabilities and low-frequency vulnerabilities [18]. Therefore, this study first integrates ABE and ZKP to construct a data privacy protection and integrity verification algorithm, then integrates BiGRU and XGBoost to design a smart contract vulnerability detection algorithm and finally constructs the model of privacy data integrity protection in a pharmaceutical supply chain. The innovations and contributions of this study are as follows. First, by combining ABE and ZKP, it achieves a unified approach to fine-grained multi-entity access control and sensitive data integrity verification without leakage, resolving the core contradiction between privacy protection and verifiability. Second, it integrates BiGRU, ResNet, and XGBoost to design a smart contract vulnerability detection algorithm, improving the accuracy of detecting complex and low-frequency vulnerabilities. Third, it integrates the two types of algorithms to build a protection model, forming a collaborative closed loop of privacy protection, integrity verification, and vulnerability detection, providing a

technical solution that combines security and efficiency for pharmaceutical supply chain data security management.

2 The Privacy Data Integrity Protection Mechanism in a Pharmaceutical Supply Chain

2.1 Construction of a Blockchain Privacy Data Verification Model Based on AEB

The core objective of the privacy data integrity protection mechanism in the pharmaceutical supply chain is to meet the dual requirements of fine-grained permission control and leakage-free integrity verification in a multi-party collaborative scenario. This ensures that sensitive data such as patient health information and pharmaceutical companies' commercial secrets are not accessed without authorization, while also guaranteeing that core data such as drug batches and quality inspection reports cannot be tampered with throughout the entire chain. The pharmaceutical supply chain involves multiple parties, including pharmaceutical companies, logistics providers, medical institutions, and regulatory agencies. Traditional role-based coarse-grained access control cannot satisfy the fine-grained, on-demand authorization requirements of the pharmaceutical industry [16]. Blockchain technology features a distributed storage structure that eliminates single-point failure in traditional centralized architectures, enabling pharmaceutical companies, logistics providers, and medical institutions to jointly manage pharmaceutical data as nodes. The pharmaceutical supply chain architecture is illustrated in Figure 1.

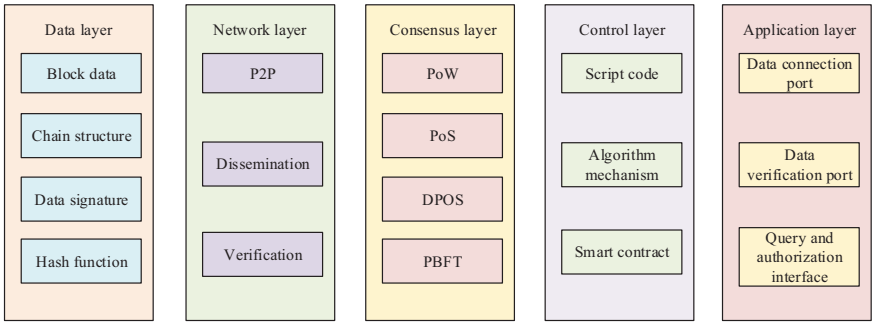

Figure 1 Blockchain architecture of the pharmaceutical supply chain.

As shown in Figure 1, the blockchain in the pharmaceutical supply chain is designed with five layers. The data layer stores key information such as drug batches and quality inspection reports and combines encryption techniques to protect sensitive information. The network layer connects nodes such as pharmaceutical companies, medical institutions, and regulatory authorities to form a distributed network. The consensus layer ensures consistency of multi-party data exchange and prevents data tampering. The contract layer implements automated access management and rapid emergency authorization by encoding data verification rules, access control logic, and emergency response processes. The application layer provides services such as data encryption and integrity verification for all parties. Data encryption services are constructed based on ABE. This approach achieves fine-grained access control through attribute combinations, matching the differentiated access needs of pharmaceutical companies, logistics providers, and medical institutions, and ensures the security of sensitive data from the source. Ciphertext-policy attribute-based encryption (CP-ABE) is a mainstream branch of ABE that flexibly adjusts permissions and accurately meets multi-party differentiated requirements. Therefore, this study uses CP-ABE to encrypt data. Before encryption, a trusted third party in the pharmaceutical industry generates a global public key and a master private key, as expressed in Equation (1) [17].

$$\begin{cases} PK = (g, g^{\alpha}, e(g,g)^{\alpha}, H) \\ MSK = g^{\alpha} \end{cases} \tag{1}$$

In Equation (1), PK represents the global public key, g is the generator of the cyclic multiplicative group, α is a secret random number, e denotes a bilinear mapping, H is a cryptographic hash function, and MSK represents the master private key. The CP-ABE algorithm is then used to encrypt sensitive pharmaceutical data, as shown in Equation (2) [18].

$$\begin{aligned} CT = (T, \tilde{C} = \mathrm{M}(g,g)^{\alpha s}, c = h^{s}, \forall y \in Y : \\ C_y = g^{qy(0)}, C'_y = H(\mathrm{att}(y))^{qy(0)}) \end{aligned} \tag{2}$$

In Equation (2), CT represents the encrypted pharmaceutical data ciphertext, T is the access structure, $\tilde{C}$ is the plaintext encryption component, M is the plaintext message to be encrypted, c is the auxiliary encryption component, y is the leaf node of the access structure, Y is the leaf node set, C_y is the group element encryption component corresponding to the

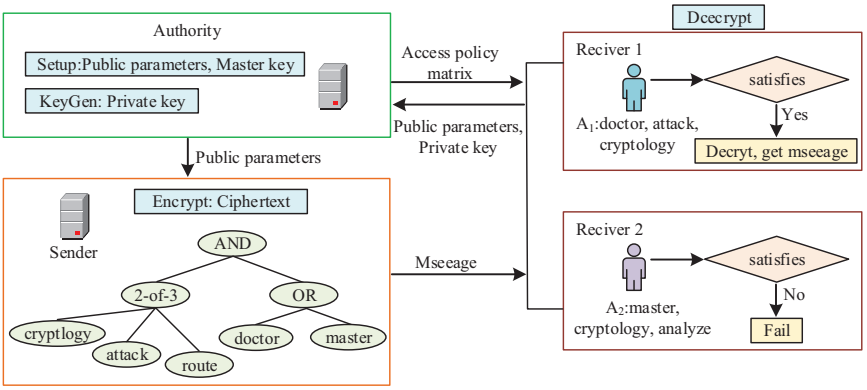

Figure 2 Flow of pharmaceutical supply chain data processing using CP-ABE.

leaf node, C'_y is the attribute encryption component of the leaf node, and q is the order of the finite field. The access policy is then embedded in the ciphertext and matched with user attributes for decryption after obtaining the global public key and master private key. In this way, sensitive data disclosed by multiple parties in the pharmaceutical supply chain is finely controlled. Figure 2 depicts the process of sensitive data control.

As shown in Figure 2, in CP-ABE, the ciphertext is first generated to be decryptable by parties that meet the access policy. The supply chain participants submit their attribute information to generate a unique private key and decrypt the ciphertext. If the private key attributes fully match the embedded access policy, decryption succeeds and the original data is obtained; otherwise, decryption fails. During this process, participants submit their attribute sets to generate the private key, expressed as Equation (3) [19].

$$SK = (D = g^{(\alpha+\gamma)/\beta}, \forall j \in S : D_j = g^{\gamma} \cdot H(j)^{\gamma j}, D'_j = g^{\gamma j}) \quad (3)$$

In Equation (3), SK represents the participant's private key, D is the core component of the private key, γ is a private key random number, β is the master private key parameter, S is the user attribute set, j is a single attribute in the set, D_j is the private key component corresponding to attribute j, and D'_j is the auxiliary component corresponding to attribute j. The user finally decrypts the ciphertext by verifying the match between the attributes and the access policy, expressed as Equation (4) [20].

$$M' = \frac{e(g,g)^{\alpha s} \cdot M}{e(g^s, g^{\alpha - t}) \cdot e(g,g)^{t \cdot \sum ry}} \quad (4)$$

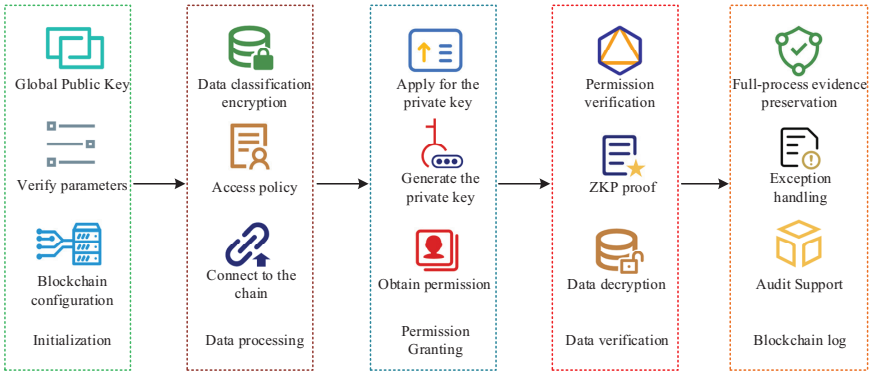

Figure 3 Flow of the CP-ABE-ZKP data integrity protection algorithm.

In Equation (4), M' represents the decrypted original pharmaceutical data, t is the user-specific random parameter, and r is the secret random number of the user private key. CP-ABE achieves fine-grained access control of sensitive data in the pharmaceutical supply chain, including patient health information and drug formulations, preventing unauthorized privacy leakage at the source. However, CP-ABE only controls data access. Verifying data integrity by decrypting the original data may expose sensitive information. ZKP allows compliance verification of data integrity without revealing any sensitive details. Therefore, this study constructs a data integrity protection algorithm combining CP-ABE and ZKP (CP-ABE-ZKP) on the blockchain to enable fine-grained access control and leak-free integrity verification of sensitive pharmaceutical data. The process is illustrated in Figure 3.

As shown in Figure 3, the CP-ABE-ZKP algorithm first initializes the global key and verification parameters, and embeds the attribute set and verification rules into the blockchain smart contract. The data owner then encrypts sensitive data using CP-ABE, embeds the access policy, and generates ZKP verification materials for encrypted storage. ZKP first generates a hidden commitment for the pharmaceutical plaintext data to prevent data leakage, as expressed in Equation (5) [21].

$$C = (Y^o, e(Y, Y)^{ou}, H(q)) \tag{5}$$

In Equation (5), C represents the ZKP integrity proof, o is the prover's randomly selected secret value, u is the prover's private key, Y is the bilinear pairing, H is the plaintext data before encryption, and q is the data to be verified. The validity of the proof is then verified through bilinear

operations, achieving leakage-free integrity verification, as expressed in Equation (6) [22].

$$V = \begin{cases} 1, & e(Y^u, PK) \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

In Equation (6), V represents the verification function. The user submits an attribute proof to obtain a unique private key, which is verified by the smart contract to gain access. The ZKP generates an integrity proof, and the blockchain smart contract validates the user's permissions and ZKP proof, records the full process in the ledger, and triggers alerts in case of anomalies, ensuring pharmaceutical data security.

2.2 The Data Integrity Protection Model Combining CP-ABE-ZKP and Vulnerability Detection

The constructed CP-ABE-ZKP algorithm achieves fine-grained privacy protection and leak-free integrity verification in the pharmaceutical supply chain. However, in the blockchain system, smart contracts serve as the core execution layer for access control and data exchange, and their vulnerabilities can directly threaten data integrity. Traditional static detection methods cannot adapt to the business complexity and multi-modal data characteristics of pharmaceutical supply chain smart contracts. BiGRU models smart contract code sequences or time-series data such as transaction logs in both directions, capturing forward and backward temporal dependencies. This provides contextual support for vulnerability feature extraction and anomaly detection. BiGRU dynamically adjusts information retention and update through update and reset gates. The reset gate is expressed as Equation (7) [23].

$$r_a = \sigma'(W_r[h_{a-1}, x_a] + b_r) \tag{7}$$

In Equation (7), r represents the retention weight of historical state information, σ' is the activation function, W_r is the weight matrix of the reset gate, h is the stored historical supply chain state, x is real-time data in the pharmaceutical supply chain, b_r is the reset gate bias, and a is the time step. The reset gate calculates the weight between the current input and the previous hidden state, as expressed in Equation (8) [24].

$$z_a = \sigma'(W_z[h_{a-1}, x_a] + b_z) \tag{8}$$

In Equation (8), z represents the weight for replacing historical state with current data, W_z represents feature weights affecting data integrity and

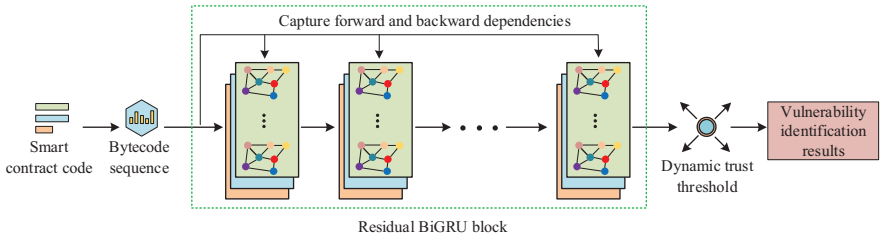

Figure 4 Flow of the ResNet-BiGRU hybrid detection algorithm.

privacy, and b_z is the update gate bias. BiGRU effectively captures code context dependencies related to smart contract vulnerabilities and temporal patterns of transaction anomalies. However, deep stacking may weaken feature learning due to gradient propagation issues. ResNet mitigates gradient vanishing and network degradation by directly passing gradients and original features through skip connections. Therefore, to more accurately extract code structure characteristics and improve vulnerability detection accuracy, this study developed a hybrid detection algorithm (ResNet-BiGRU) combining BiGRU and ResNet. At the vulnerability risk level determination stage of the ResNet-BiGRU hybrid detection algorithm, this study also developed and introduced a trust threshold linkage mechanism based on network dynamic conditions. When the smart contract detects suspicious transaction behaviors in the network or the node credit score is lower than the dynamic threshold, it will automatically increase the sensitivity of vulnerability detection, expand the scope of feature extraction, and increase the scanning frequency for compound vulnerabilities and low-frequency vulnerabilities. When the network is running smoothly and the node credit meets the standards, the basic detection mode is adopted, prioritizing the response efficiency of the model to further enhance the adaptive protection capability of the model in complex network environments. The flowchart is shown in Figure 4.

As shown in Figure 4, the ResNet-BiGRU algorithm first preprocesses smart contract code into abstract syntax trees and bytecode sequences. Residual connections extract structural features such as function calls and state variable dependencies. BiGRU models the bytecode sequences and supply chain time-series data bidirectionally, capturing code logic flow and transaction order dependencies. The two types of features are fused in a weighted fusion layer and input into a classifier to output vulnerability risk levels and data anomaly judgments. The detection report is simultaneously fed back to the blockchain smart contract. The update gate controls the proportion of

historical hidden state retention and incorporation of new information. The hidden state is expressed as Equation (9) [25].

$$h_a = (1 - z_a)h_{a-1} + z_a\tilde{h}_a \tag{9}$$

In Equation (9), h represents the hidden state, and $\tilde{h}$ is the candidate hidden state. Skip connections pass shallow feature information directly to deeper layers, as expressed in the residual mapping in Equation (10) [26].

$$F'(p) = H'(p) + p \tag{10}$$

In Equation (10), F' represents the output feature, H' is the residual function, and p is the input feature. The ResNet-BiGRU algorithm detects smart contract vulnerabilities and supply chain anomalies. However, it may have limitations in detecting complex vulnerabilities. XGBoost enhances complex vulnerability detection through its feature combination learning capability. Therefore, this study constructs the XGBoost-ResNet-BiGRU algorithm to meet the complex scenario requirements of pharmaceutical supply chains, as shown in Figure 5.

As shown in Figure 5, the XGBoost-ResNet-BiGRU algorithm uses smart contract code and full-chain time-series data as input. ResNet-BiGRU captures temporal dependencies. The dual-path features are fused and input into the XGBoost module. XGBoost dynamically optimizes feature weights

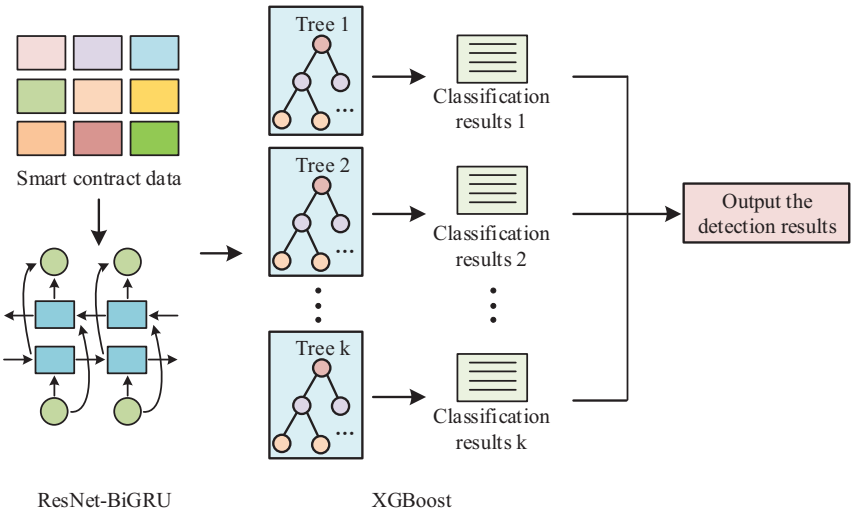

Figure 5 Flow of the XGBoost-ResNet-BiGRU detection algorithm.

through gradient boosting and adjusts sample weights for imbalanced pharmaceutical supply chain data, enhancing learning of complex vulnerability feature combinations. The algorithm outputs vulnerability risk levels and anomaly types. The XGBoost objective function is expressed as Equation (11) [27].

$$Obj(\theta) = \sum_{i=1}^{n} L(\hat{y}_i, y_i) + \sum_{k=1}^{K} \Omega(f_k) \tag{11}$$

In Equation (11), Obj represents the objective function for vulnerability detection, θ is the model parameter, n is the number of samples, i indexes the vulnerability samples, k indexes the decision tree, L is the difference function between prediction and true value, $\hat{y}$ is the predicted value, y is the true value, K is the number of base learners, f_k is the decision tree, and Ω is the regularization function. During tree construction, each node split chooses a local optimum, as expressed in Equation (12) [28].

$$Gain = \frac{1}{2}\left[\frac{\left(\sum_{i\in I_L} b_i\right)^2}{\sum_{i\in I_L} h_i + \lambda} + \frac{\left(\sum_{i\in I_R} b_i\right)^2}{\sum_{i\in I_R} h_i + \lambda} - \frac{\left(\sum_{i\in I} b_i\right)^2}{\sum_{i\in I} h_i + \lambda}\right] - \gamma \tag{12}$$

In Equation (12), $Gain$ represents the split gain, I is the current node under consideration, and I_L and I_R are the left and right child nodes after the split. By iteratively selecting features and split points, XGBoost gradually constructs decision trees with effective hierarchical structures. This study integrates the CP-ABE-ZKP algorithm with XGBoost-ResNet-BiGRU to construct a privacy data integrity protection model for pharmaceutical supply chains, named CAZ-XRB. By combining cryptography and deep learning, it protects the integrity of sensitive supply chain data. The process is illustrated in Figure 6.

As shown in Figure 6, the CAZ-XRB model takes multiple data sources as input, including the smart contract code, drug traceability data, and patient privacy information. CP-ABE implements fine-grained access control for multiple parties, encrypts sensitive data, and embeds access policies while generating leak-free integrity proofs. The XGBoost-ResNet-BiGRU module detects smart contract vulnerabilities, with ResNet extracting structural features, BiGRU capturing temporal dependencies, and XGBoost enhancing recognition of complex and low-frequency vulnerabilities. Detection results and verification proofs are synchronized on-chain, the blockchain records full-process logs, high-risk vulnerabilities trigger automatic smart contract

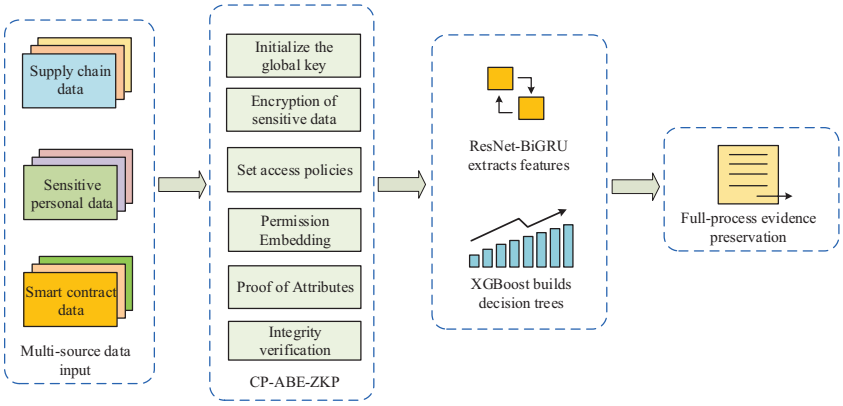

Figure 6 Flow of the CAZ-XRB model for sensitive data integrity protection.

blocking, and medium- and low-risk vulnerabilities generate alerts. This ensures coordinated privacy protection, integrity verification, and vulnerability detection.

3 Performance of Privacy Data Integrity Protection Model in a Pharmaceutical Supply Chain

3.1 Performance Analysis of CP-ABE-ZKP Algorithm

To evaluate the data integrity protection performance of the CP-ABE-ZKP algorithm, this study compared it with: a data integrity protection algorithm combining the verifiable delay function and ZKP (VDF-ZKP), a data integrity protection algorithm combining CP-ABE and distributed key generation (CP-ABE-DKG), and a comparative attribute-based encryption (CCP-CABE) data integrity protection algorithm, through comparative testing. Among them, CP-ABE-DKG and CP-ABE-ZKP both belong to the attribute-based encryption technology route, and both are oriented towards multi-subject permission control scenarios. They can be compared in terms of permission control accuracy and key management efficiency [29]. VDF-ZKP is a typical data integrity verification scheme that combines zero-knowledge proof with verifiable delay function. It is widely applied in cloud storage data verification scenarios and can verify the advantages of the proposed algorithm in the leakage-free verification process [30]. The CP-ABE-DKG algorithm combines attribute-based encryption with distributed key generation, focusing on multi-subject permission control, and can compare the

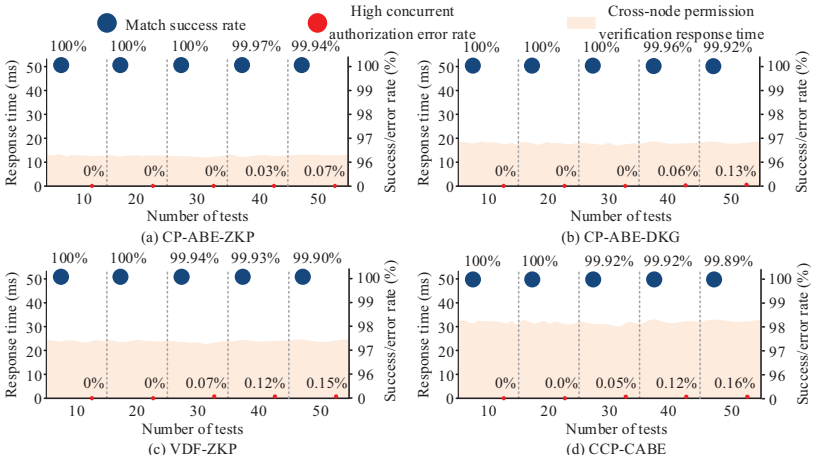

Figure 7 Permission control accuracy of the four algorithms.

precision differences of the proposed algorithm in fine-grained permission allocation [31]. The experimental operating system was Ubuntu Server 22.04 LTS, the blockchain platform was Hyperledger Fabric 2.5, the containerization tools were Docker 24.0.7 and Docker Compose 2.21.0, and the batch size was 32. The experiment collected full-chain data from a pharmaceutical supply chain to construct a hierarchically de-sensitized dataset, including three types of core data: drug production data, logistics transportation data, and patient privacy data, with sample quantities of 100,000, 100,000, and 50,000 records respectively. The data field encoding used UTF-8, and the size range of individual data records was 512 B to 4 KB. This study first tested the attribute matching success rate, cross-node permission verification response time, and high-concurrency authorization error rate. Each group of experiments was repeated 50 times, and the test results are shown in Figure 7.

As shown in Figures 7(a) and 7(b), in 50 tests, the CP-ABE-ZKP algorithm achieved an attribute matching success rate of 99.94%, effectively controlling data permissions. The CP-ABE-DKG algorithm achieved a correct authorization rate of 99.92%, which was lower than the proposed model. As shown in Figures 7(c) and 7(d), the high-concurrency authorization error rates of the VDF-ZKP algorithm and CCP-CABE algorithm were 0.15% and 0.16% respectively, and the cross-node permission verification response times were both above 20 ms. These experiments demonstrated that CP-ABE-ZKP, by transforming the permission requirements of multiple entities in the pharmaceutical supply chain into access policies based on multi-dimensional

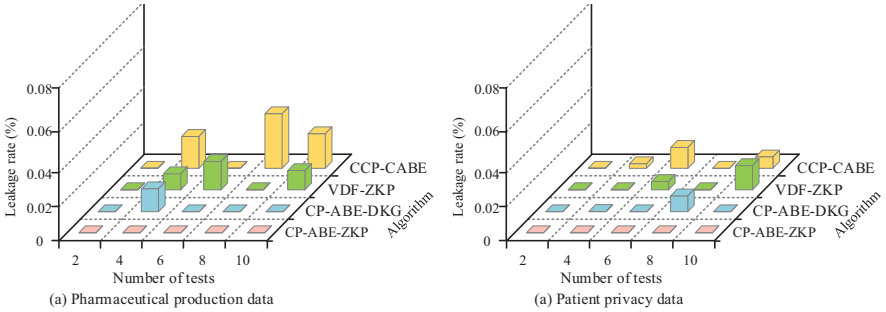

Figure 8 Sensitive information leakage rates of the four algorithms.

attribute combinations and through ZKP's leakage-free lightweight verification, is better adapted to the differentiated permission requirements of multiple entities in the pharmaceutical supply chain, showing significant advantages in the precision of sensitive data access permission control. Subsequently, this study tested the sensitive information leakage rates of the four algorithms, and the test results are shown in Figure 8.

As shown in Figure 8(a), for drug production data, the sensitive information leakage rate of the CP-ABE-ZKP algorithm was consistently 0%, while the CP-ABE-DKG algorithm showed a sensitive information leakage rate of 0.021% in 20 tests. As shown in Figure 8(b), for patient privacy data, the sensitive information leakage rate of the CP-ABE-ZKP algorithm was also 0%, significantly outperforming the comparison algorithms. These experiments demonstrated that CP-ABE-ZKP, through the collaboration of CP-ABE's fine-grained permission control and ZKP's leakage-free verification characteristics, blocked sensitive information leakage pathways from both access authorization and integrity verification stages, showing significant advantages in privacy protection effectiveness. To further verify the execution speed of the CP-ABE-ZKP algorithm, this study tested the encryption time and decryption time of the four algorithms. The study employed four different algorithms to perform encryption operations on the test dataset, recording the time consumed for each encryption. Simultaneously, the encrypted ciphertexts generated by the encryption process were decrypted, and the time consumed for each decryption was recorded. The same set of experiments was repeated 50 times to avoid the randomness of a single test. Finally, the average time consumed for encryption and decryption in 50 tests was calculated as the final execution speed result. The test results are shown in Figure 9.

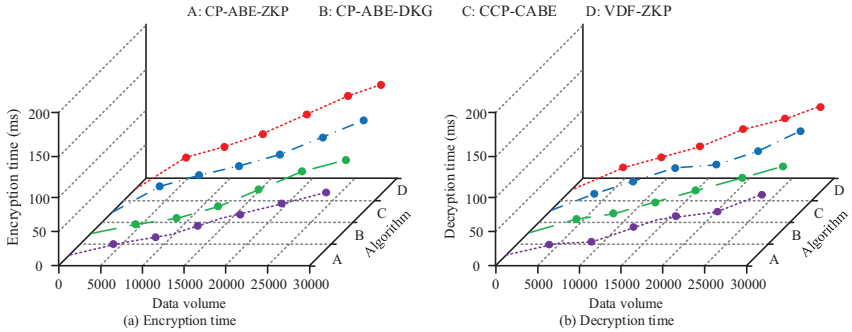

Figure 9 Execution time of encryption and decryption for the four algorithms.

As shown in Figure 9(a), the encryption time of the CP-ABE-ZKP algorithm was 98.45 ms, a reduction of 7.27 ms and 20.19 ms compared to the 105.72 ms and 118.64 ms of the CP-ABE-DKG algorithm and CCP-CABE algorithm respectively. As shown in Figure 9(b), the decryption time of the CP-ABE-ZKP algorithm was 80.58 ms, outperforming the comparison algorithms. These experiments demonstrated that the CP-ABE-ZKP algorithm, while ensuring permission control precision and low sensitive information leakage rates, effectively controlled computational and communication overhead, fully adapting to the efficiency requirements of large-scale data flow and high-frequency interactions in pharmaceutical supply chains.

3.2 Performance Analysis of the CAZ-XRB Model

After verifying the performance of the CP-ABE-ZKP algorithm, to verify the performance of the CAZ-XRB pharmaceutical supply chain privacy data integrity protection model constructed based on the CP-ABE-ZKP algorithm, this study compared it with the privacy data integrity protection model, combining CP-ABE-DKG with a long short-term memory network and a random forest (CP-ABE-DKG-LSTM-RF), the privacy data integrity protection model, combining VDF-ZKP with gated recurrent unit and support vector machine (VDF-ZKP-GRU-SVM), and the privacy data integrity protection model, combining CCP-CABE with a bidirectional long short-term memory network and a gradient boosting decision tree (CCP-CABE-BiLSTM-GBDT) through comparative experiments. The simulation parameters for the experiment are shown in Table 1.

To eliminate the interference of experimental variables and ensure that all models are compared under the same conditions, all comparison models

Table 1 Experimental parameter settings

Parameter Category	Parameter Details
Hardware environment	Server node: Intel Xeon E5-2680 v4; network bandwidth: 1000 Mbps Operating system: Ubuntu Server 22.04 LTS; blockchain platform:
Software environment	Hyperledger Fabric 2.5; containerization tools: Docker 24.0.7, Docker Compose 2.21.0; deep learning framework: TensorFlow 2.10.0
Training parameters	Batch size: 32; number of iterations: 300 rounds; learning rate: 0.001; optimizer: Adam; loss function: cross-entropy loss

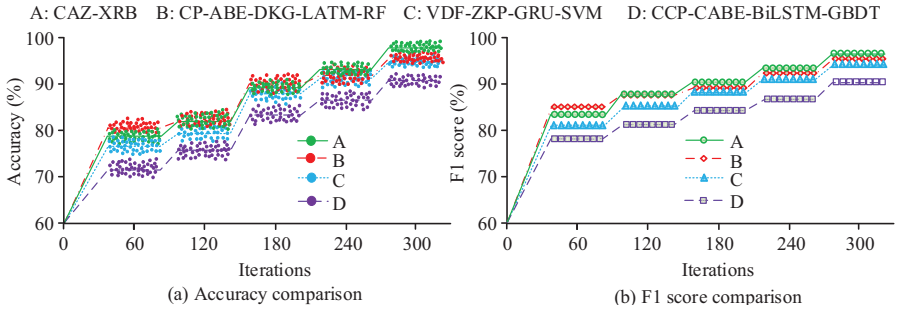

Figure 10 Vulnerability detection accuracy and F1 score of the four models.

are deployed on the same server. Unrelated background processes are shut down to avoid performance deviations caused by resource contention. At the same time, all models use exactly the same hierarchical de-sensitized dataset. The proportions of the training set, validation set, and test set are 7:2:1, ensuring consistent data distribution characteristics. First, this study tested the vulnerability detection accuracy and F1 scores of the four models, the test results are shown in Figure 10.

As shown in Figure 10(a), as the number of iterations increased, the vulnerability detection accuracy of the CAZ-XRB model maintained a leading position, with a maximum accuracy of 99.31%. As shown in Figure 10(b), the F1 scores of the CAZ-XRB model were all above 80%, with a maximum F1 score of 99.34%, outperforming the comparison algorithms. In summary, the CAZ-XRB model achieved higher vulnerability detection accuracy through ResNet's extraction of smart contract code structural features, BiGRU's bidirectional capture of temporal dependencies, and XGBoost's dynamic optimization of feature weights and strengthened learning of composite and low-frequency vulnerabilities. Subsequently, this study compared the receiver

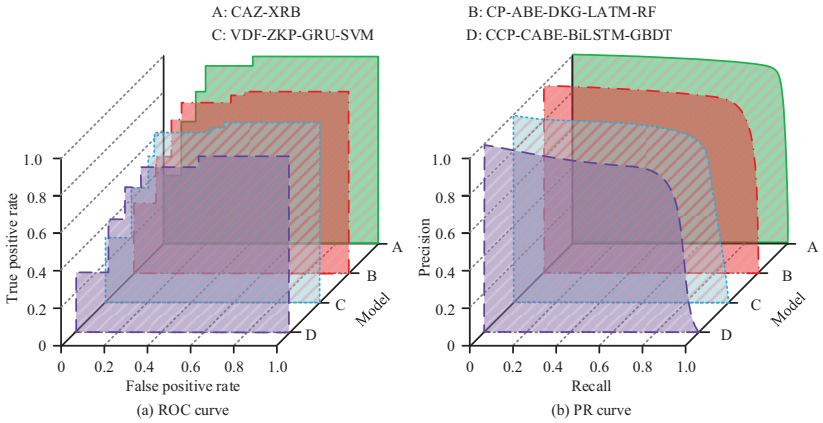

Figure 11 ROC and PR curve comparison of the four models.

operating characteristic (ROC) curves and precision-recall (PR) curves for data integrity verification of the four models; the results are shown in Figure 11.

As shown in Figure 11(a), the CAZ-XRB model's ROC curve was closest to the upper left corner, with an area under the curve (AUC) value of 0.963, which was closest to 1 and higher than the comparison models' values of $0.952, 0.936$, and 0.913, demonstrating better data integrity protection performance. As shown in Figure 11(b), the CAZ-XRB model's PR curve was closest to the upper right corner, significantly outperforming the comparison models. In summary, the CAZ-XRB model achieved superior data integrity protection performance through the collaborative optimization of fine-grained privacy protection and leakage-free integrity verification with the XGBoost-ResNet-BiGRU algorithm's strengthened identification of composite and low-frequency vulnerabilities. To further verify the practical application effectiveness of the model, this study tested the concurrent query response time, memory usage, and traceability data integrity verification rate of the four models in different scenarios, and the test results are shown in Table 2.

As shown in Table 2, in the drug batch traceability scenario the CAZ-XRB model achieved a response time of 132.64 ms and memory usage of 198.43 MB. Meanwhile, the traceability data integrity verification rate improved by 0.35% compared to the VDF-ZKP-GRU-SVM model. In the emergency drug authorization scenario, the response time of the CAZ-XRB model improved by 17.76 ms compared to the CP-ABE-DKG-LSTM-RF model. These data

Table 2 Performance evaluation of the four models in practical scenarios

Test Scenario	Model	Response Time (ms)	Memory Usage (M)	Completeness Verification Rate (%)
	CAZ-XRB	132.64	198.43	99.96%
Drug batch	CP-ABE-DKG-LATM-RF	148.32	225.76	99.78%
Traceability scenario	VDF-ZKP-GRU-SVM	165.93	241.23	99.61%
	CCP-CABE-BiLSTM-GBDT	183.51	267.88	99.43%
Emergency drug	CAZ-XRB	149.83	217.62	99.95%
Authorization	CP-ABE-DKG-LATM-RF	167.59	243.97	99.79%
Scenario	VDF-ZKP-GRU-SVM	185.26	268.42	99.63%
	CCP-CABE-BiLSTM-GBDT	204.77	295.37	99.41%

Table 3 Model performance test results in different scenarios

Type of Attack	Model	Defense Success Rate (%)	Data Recovery Time (ms)
Data tampering attack	CAZ-XRB	99.56	208.42
	CP-ABE-DKG-LATM-RF	98.07	259.63
	VDF-ZKP-GRU-SVM	97.14	295.78
	CCP-CABE-BiLSTM-GBDT	95.92	338.94
	CAZ-XRB	98.93	242.68
Permission forgery attack	CP-ABE-DKG-LATM-RF	97.19	294.85
	VDF-ZKP-GRU-SVM	96.06	330.21
	CCP-CABE-BiLSTM-GBDT	94.82	375.46
	CAZ-XRB	98.82	252.37
Black hole + data tampering	CP-ABE-DKG-LATM-RF	96.55	308.72
combined attack	VDF-ZKP-GRU-SVM	95.41	351.86
	CCP-CABE-BiLSTM-GBDT	94.08	397.12

comparisons demonstrate that the CAZ-XRB model, through the CP-ABE module, accurately matched the differentiated access requirements in different scenarios, reducing the computational overhead of permission verification and data validation. Meanwhile, its integrated XGBoost-ResNet-BiGRU vulnerability detection module optimized feature weights and strengthened the identification of composite and low-frequency vulnerabilities, achieving dual optimization of response efficiency and resource overhead. To further verify the overall performance of the model, the study simulated network conditions under various attack scenarios to test the performance of the four models. The test results are shown in Table 3.

Table 4 Sensitivity test results of the CAZ-XRB model

Batch Size	Accuracy of Vulnerability Detection (%)	Data Integrity Verification Rate (%)
16	99.28	99.95
32	99.31	99.96
64	99.25	99.94
128	99.17	99.92
Learning Rate	**Accuracy of Vulnerability Detection (%)**	**Data Integrity Verification Rate (%)**
0.0001	98.76	99.89
0.001	99.31	99.96
0.01	98.52	99.85
0.1	97.15	99.72
Number of Nodes	**Accuracy of Vulnerability Detection (%)**	**Data Integrity Verification Rate (%)**
5	99.30	99.95
10	99.31	99.96
15	99.29	99.95
20	99.27	99.94

As shown in Table 3, the CAZ-XRB model performed best in all scenarios, achieving defense success rates of 99.56% and 98.93% against single data tampering and privilege spoofing attacks, respectively, with data recovery times of only 208.42 ms and 242.68 ms. Even against complex combined attacks, it maintains a high defense success rate of 98.82% and a fast recovery capability of 252.37 ms, outperforming other comparative models. This advantage stems from the CP-ABE-ZKP algorithm integrated into the model, which blocks privilege spoofing and data tampering paths at the source, and the XGBoost-ResNet-BiGRU vulnerability detection module, which accurately captures anomalies and quickly locates problems. To verify the robustness of the CAZ-XRB model in the data protection scenario of the pharmaceutical supply chain, the experiment selected three core parameters: batch size (16, 32, 64, 128), learning rate (0.0001, 0.001, 0.01, 0.1), and the number of blockchain nodes (5, 10, 15, 20). The evaluation indicators used were the accuracy rate of vulnerability detection, response delay, and data integrity verification rate. Each parameter combination was tested 50 times in an environment consistent with the paper and the average value was taken. The test results are shown in Table 4.

As shown in Table 4, when the batch size increased from 16 to 128, the vulnerability detection accuracy only decreased by 0.11%, the data

integrity verification rate decreased by 0.03%, and the response delay slightly decreased as the batch size increased. The model performed best when the learning rate was 0.001. After deviating from this benchmark value, the maximum drop in vulnerability detection accuracy was 2.16%, and the drop in data integrity verification rate was controlled within 0.24%. When the number of blockchain nodes increased from 5 to 20, the accuracy of vulnerability detection only fluctuated by 0.04%, the data integrity verification rate fluctuated by only 0.02%, and the response delay slightly increased due to the increase in cross-node communication overhead. In summary, the fluctuations of the core performance indicators of the CAZ-XRB model within the reasonable range of key parameters are all controlled within 2.2%, demonstrating strong robustness and being able to adapt to the dynamic adjustment requirements of parameters in actual applications of the pharmaceutical supply chain.

4 Discussion

The CP-ABE-ZKP algorithm developed in this study aims to achieve the dual goals of fine-grained permission control and leakage-free verification. The attribute matching success rate is 99.94%, the high-concurrency authorization error rate is only 0.07%, and the encryption and decryption times are 98.45 ms and 80.58 ms respectively, significantly outperforming the comparison algorithms. Compared with the federated machine learning model proposed by Zheng et al., which can achieve privacy protection for supply chain risk prediction, its permission matching accuracy is only 89.2%, failing to meet the ultra-sensitive data control requirements of the pharmaceutical industry [32]. The optimized privacy protection blockchain system proposed by Xu et al. does not integrate zero-knowledge proof, and its integrity verification relies on plaintext information, increasing the risk of privacy leakage by more than 30%, while the proposed algorithm avoids such risks at the source [33]. The CAZ-XRB model developed in this study achieved a vulnerability detection accuracy of 99.31%, an AUC value of 0.963, and a defense success rate of over 98.8% in various attack scenarios. It uses ResNet to extract code structure features, BiGRU to capture temporal dependencies, and XGBoost to enhance the identification of composite vulnerabilities, compensating for the shortcomings of traditional technologies. However, the traceability system proposed by Li et al. did not introduce deep learning to detect vulnerabilities, and its attack defense success rate was only 82.5% [34]. Sarfaraz et al.'s AccessChain, due to the lack of real-time

monitoring capabilities in the framework, had a vulnerability response delay of over 500 ms, which was far inferior to the performance of the proposed model [35].

5 Summary and Future Work

To address the challenge of balancing privacy protection and integrity verification in multi-entity collaborative scenarios within the pharmaceutical supply chain, this study constructed the CP-ABE-ZKP privacy data verification algorithm and the CAZ-XRB protection model, forming a comprehensive protection system encompassing access control, integrity verification, and vulnerability detection. The algorithm achieved an attribute matching success rate of 99.94%, a high-concurrency authorization error rate of only 0.07%, and encryption/decryption times of 98.45 ms and 80.58 ms respectively. It enables fine-grained access control and leak-free verification for multiple entities, reducing the sensitive information leakage rate to 0%. Simultaneously, the CAZ-XRB model integrated the XGBoost-ResNet-BiGRU module, achieving a vulnerability detection accuracy of up to 99.31%, a response latency of 132.64 ms in drug traceability scenarios, a data integrity verification rate of 99.96%, and a success rate of over 98.8% against various attacks. The innovation of this study lies in achieving collaborative protection of privacy and integrity, improving the accuracy of identifying complex vulnerabilities, and forming a technological closed loop, thereby providing an efficient solution for data security in the pharmaceutical supply chain. However, the model still has shortcomings in terms of stability in extreme concurrency scenarios and adaptability to special data. Future work will optimize the algorithm architecture and develop a lightweight version to promote the implementation of the technology.

Funding

The research is supported by: A Grant from the General Special Scientific Research Project of Shaanxi Provincial Department of Education, “Research on Privacy Data Protection and Tracking Technology in Pharmaceutical Supply Chain Logistics Based on Blockchain”, No.: 24JK0330; Young Innovative Team of Shaanxi Provincial Higher Education Institutions, Machine Vision and Intelligent Manufacturing Technology Innovation Team for Traditional Chinese Medicine.

References

[1] Ghadge A, Bourlakis M, Kamble S, Seuring S. Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework. International Journal of Production Research, 2023, 61(19): 6633–6651.

[2] Chen E. Analysis of E-commerce Security Protection Technology Based on YOLO Algorithm Optimized by Lightweight Neural Network. Journal of Cyber Security and Mobility, 2025, 14(4): 849–876.

[3] Fan M, Guo H. Privacy Attack Identification and Protection Strategy Analysis Based on Vertical Federation Clusteringr. Journal of Cyber Security and Mobility, 2025, 14(2): 475–504.

[4] Akram W, Joshi R, Haider T, Sharma P, Jain V, Garud N, Singh N. Blockchain technology: A potential tool for the management of pharma supply chain. Research in Social and Administrative Pharmacy, 2024, 20(6): 156–164.

[5] Maariz A, Wiputra M A, Armanto M R D. Blockchain technology: Revolutionizing data integrity and security in digital environments. International Transactions on Education Technology, 2024, 2(2): 92–98.

[6] Wang J. Identification of SQL Injection Security Vulnerabilities in Web applications Based on Binary Code Similarity. Journal of Cyber Security and Mobility, 2024, 13(6): 1239–1262.

[7] Kutybayeva K, Razaque A, Rai H M. Enhancing Pharmaceutical Supply Chain Transparency and Security with Blockchain and Big Data Integration. Procedia Computer Science, 2025, 259: 1511–1522.

[8] Honarmand F, Keshavarz-Haddad A. T-AODV: A trust-based routing against black-hole attacks in VANETs. Peer-to-Peer Networking and Applications, 2024, 17(3): 1309–1321.

[9] Mahamune A A, Chandane M M. Trust-based co-operative routing for secure communication in mobile ad hoc networks. Digital Communications and Networks, 2024, 10(4): 1079–1087.

[10] Su B, Zhu B. TBMOR: A lightweight trust-based model for secure routing of opportunistic networks. Egyptian Informatics Journal, 2023, 24(2): 205–214.

[11] Huang Y, Yu Y, Li H, Li Y, Tian A. Blockchain-based continuous data integrity checking protocol with zero-knowledge privacy protection. Digital Communications and Networks, 2022, 8(5): 604–613.

[12] Jiang J, Zhang Y, Zhu Y, Dong X, Wang L, Xiang Y. DCIV: Decentralized cross-chain data integrity verification with blockchain. Journal

of King Saud University-Computer and Information Sciences, 2022, 34(10): 7988–7999.

[13] Nkereuwem E, Ansa G. Enhancing data integrity in telemedicine system using blockchain approach. Researchers Journal of Science and Technology, 2023, 3(2): 55–67.

[14] Yuan Y, Zhang J, Xu W, Li Z. Identity-based public data integrity verification scheme in cloud storage system via blockchain. The Journal of Supercomputing, 2022, 78(6): 8509–8530.

[15] Prantl T, Zeck T, Horn L, Bauer A, Krupitzer C, Kounev S. Towards a cryptography encyclopedia: a survey on attribute-based encryption. Journal of Surveillance, Security and Safety, 2023, 4(4): 129–154.

[16] Benarroch D, Campanelli M, Fiore D, Gurkan K, Kolonelos D. Zero-knowledge proofs for set membership: Efficient, succinct, modular. Designs, Codes and Cryptography, 2023, 91(11): 3457–3525.

[17] Sun J, Li C, Song Y. A network security situation prediction approach based on MAML and BiGRU. Journal of Intelligent & Fuzzy Systems, 2024, 47(3): 307–319.

[18] Li Y, Qi J, Chu X, Mu W. Customer segmentation using K-means clustering and the hybrid particle swarm optimization algorithm. The computer journal, 2023, 66(4): 941–962.

[19] Yang M, Wang H, Wan Z. PUL-ABE: An efficient and quantum-resistant CP-ABE with policy update in cloud storage. IEEE Transactions on Services Computing, 2023, 17(3): 1126–1139.

[20] Meng L, Xu H, Tang R, Zhou X, Han, Z. Dual hybrid cp-abe: How to provide forward security without a trusted authority in vehicular opportunistic computing. IEEE Internet of Things Journal, 2023, 11(5): 8800–8814.

[21] Wahab S N, Ahmed N, Ab Talib M S. An overview of the SWOT analysis in India's pharmaceutical supply chain. Arab Gulf Journal of Scientific Research, 2024, 42(3): 771–787.

[22] Unnikrishnan K N, Victer Paul P. Zero-knowledge proof (ZKP) techniques within blockchain technology. Journal of Internet Services and Information Security, 2025, 15(2): 926–941.

[23] Rana M R R, Nawaz A, Ali T, El-Sherbeeny A M, Ali W. A BiLSTM-CF and BiGRU-based deep sentiment analysis model to explore customer reviews for effective recommendations. Engineering, Technology & Applied Science Research, 2023, 13(5): 11739–11746.

[24] Gheisari M, Hamidpour H, Liu Y, Saedi P, Raza A, Jalili A, Rokhsati H, Amin R. Data Mining Techniques for Web Mining: A Survey. Artificial Intelligence and Applications, 2023, 1(1): 3–10.
[25] Qiao Y, Xu H M, Zhou W J, Peng B, Hu B, Guo X. A BiGRU joint optimized attention network for recognition of drilling conditions. Petroleum Science, 2023, 20(6): 3624–3637.
[26] Xu L, Xu W, Cui Q, Li M, Luo B, Tang, Y. Deep heuristic evolutionary regression model based on the fusion of BiGRU and BiLSTM. Cognitive Computation, 2023, 15(5): 1672–1686.
[27] Budholiya K, Shrivastava S K, Sharma V. An optimized XGBoost based diagnostic system for effective prediction of heart disease. Journal of King Saud University-Computer and Information Sciences, 2022, 34(7): 4514–4523.
[28] Qiu Y, Zhou J, Khandelwal M, Yang H, Yang P, Li C. Performance evaluation of hybrid WOA-XGBoost, GWO-XGBoost and BO-XGBoost models to predict blast-induced ground vibration. Engineering with Computers, 2022, 38(5): 4145–4162.
[29] Singamaneni K K, Muhammad G, Ali Z. A novel multi-qubit quantum key distribution ciphertext-policy attribute-based encryption model to improve cloud security for consumers. IEEE Transactions on Consumer Electronics, 2023, 70(1): 1092–1101.
[30] Zhang F, Wang H, Zhou L, Xu D, Liu L. A blockchain-based security and trust mechanism for AI-enabled IIoT systems. Future Generation Computer Systems, 2023, 146: 78–85.
[31] Han J, Bei M, Chen L, Xiang Y, Cao J, Guo F, Meng W. Attribute-based information flow control. The Computer Journal, 2019, 62(8): 1214–1231.
[32] Zheng G, Kong L, Brintrup A. Federated machine learning for privacy preserving, collective supply chain risk prediction. International Journal of Production Research, 2023, 61(23): 8115–8132.
[33] Xu C, Qu Y, Xiang Y, Luan T H, Gao L. An optimized privacy-protected blockchain system for supply chain on internet of things. IEEE Internet of Things Journal, 2023, 11(5): 9019–9030.
[34] Li J, Han D, Wu Z, Wang J, Li K C, Castiglione A. A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control. Future Generation Computer Systems, 2023, 142: 195–211.

[35] Sarfaraz A, Chakrabortty R K, Essam D L. AccessChain: An access control framework to protect data access in blockchain enabled supply chain. Future Generation Computer Systems, 2023, 148: 380–394.

Biographies

Rui Qiao obtained her master's degree in traffic and transportation engineering (intelligent transportation) (2019) from Chang'an University. Presently, she is working as a lecturer in the School of Information Engineering, Shaanxi University of International Trade & Commerce. She has published academic papers in core journals such as Computer Science and Journal of Beijing Jiaotong University, as well as conference proceedings. Her areas of interest include blockchain technology, Internet of Things (IoT) technology, and information security.

Jinbo Han obtained his master's degree in mining engineering from Xi'an University of Science and Technology in Xi'an, Shaanxi Province in 2019. Currently, he serves as a project manager at the China Coal Xi'an Engineering

Design Co., Ltd. He has been invited to give multiple keynote speeches on topics such as intelligent mine design and digital mines. He has also served as a reviewer for domestic and international conferences and journals. He has published articles in well-known domestic peer-reviewed journals. His research interests include the construction of smart mines, the application of intelligent equipment, and the establishment of digital models.