Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Data privacy and audit compliance of supply chain finance warehouse receipt pledge based on WSN federated edge learning

Ge Shankai
Shandong University of Technology
Xu Xintian
Shandong University of Technology
Chen Yingjie
Shandong University of Technology
Han Bopeng
Shandong University of Technology
Chen Huiyu
Shandong University of Technology
Ma Chuanjin
Machuanjin0826@outlook.com
Shandong University of Technology

Research Article

Keywords: Supply chain finance, Warehouse receipt pledge, Wireless sensor network, Federated edge learning, Privacy protection, Audit compliance

Posted Date: November 5th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-11285515/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Data privacy and audit compliance of supply chain finance warehouse receipt pledge based on WSN federated edge learning

Ge Shankai1, Xu Xintian1 ,Chen Yingjie1,Han Bopeng1,Chen Huiyu1,Ma Chuanjin*
1.Business School, Shandong University of Technology, Zibo, 255000,China
Ge Shankai email:17888339905@163.com
Xu Xintian email:18265373595@163.com
Chen Yingjie email:15106533286@163.com
Han Bopeng email:hanyoa7@163.com
Chen Huiyu email:13361057896@163.com
*Corresponding Author Email: machuanjin@sdut.edu.cn and Machuanjin0826@outlook.com

Abstract: In supply chain finance warehouse receipt pledge financing, the status of the pledged assets is difficult to verify in real time, the risk of privacy leakage of financing data is high, and the federal training process lacks verifiable audit trajectories for regulatory authorities. To achieve multi-warehouse collaborative risk control modeling under the condition of data not leaving the domain and meet the requirements of privacy protection and audit compliance, a method for privacy and audit compliance of supply chain finance warehouse receipt pledge data based on federated edge learning of wireless sensor networks is constructed. A pledge perception and digital warehouse receipt generation mechanism based on wireless sensor networks is designed. A federated edge learning architecture integrating trust and energy-aware weighted aggregation, federated proximal terms and communication compression is constructed. The study introduces a joint security aggregation mechanism of differential privacy and homomorphic encryption, as well as an audit compliance framework for blockchain smart contracts. The experimental results show that when the data heterogeneity parameter is 0.1, the test accuracy of the proposed method reaches 88.4%, which is 9.9% higher than the 78.5% of the federal average algorithm. In the ablation experiment, the F1 score of the complete method is 93.6%, while it drops to 88.9% after removing the federal proximal term. When the privacy budget is 0.10, the accuracy rate of the proposed method is 92.1%, which is 8.0% higher than the 84.1% of the federal average algorithm. The results show that the proposed method has stronger robustness under extreme non-independent homogeneous distribution conditions. Trust and energy-aware selection and federated proximal terms contribute significantly to accuracy, and the privacy enhancement mechanism achieves effective privacy protection with limited accuracy loss. This research provides a technical path that takes into account data privacy, model performance and audit compliance for the warehouse receipt pledge scenario in supply chain finance, which is conducive to promoting the compliant application of federated learning in supply chain finance risk control.

Keywords: Supply chain finance; Warehouse receipt pledge; Wireless sensor network; Federated edge learning; Privacy protection; Audit compliance

1. Introduction

Supply chain finance, as an important tool to alleviate the financing constraints of small and medium-sized enterprises, has achieved rapid development worldwide. Warehouse receipt pledge financing, as one of the core business models of supply chain finance, allows borrowing enterprises to apply for loans from banks with stored goods as collateral, effectively activating the inventory assets of enterprises [1-2]. However, traditional warehouse receipt pledge financing faces two core challenges in practice. One issue is that the status of the pledged property is difficult to verify in real time. Banks' monitoring of pledged assets mainly relies on manual inspections and regular inventories. Information updates are lagging behind, making it difficult to dynamically grasp the quantity, quality and physical condition changes of pledged assets. Meanwhile, the pledged data from multiple warehouses and institutions involves business secrets and sensitive enterprise information. Under the centralized data processing model, the risk of data leakage is high, and it is difficult for financial institutions to achieve collaborative risk control due to the "data silo" problem [3-4]. Meanwhile, regulatory authorities are increasingly strict in their auditing requirements for the data usage process. How to meet the compliance auditing requirements of traceability and verifiability while protecting data privacy has become a key issue that needs to be urgently addressed [5-6].

In response to the above issues, the academic community has carried out explorations from multiple technical directions such as blockchain, federated learning, the Internet of Things, and wireless sensor networks. Zhang J et al. proposed a warehouse receipt pledge financing model based on blockchain data assets. Through evolutionary game analysis, they revealed the impact of blockchain construction costs and information costs on banks' adoption of blockchain technology [7]. Kong L et al. proposed a federated machine learning framework for order-level risk prediction in supply chain financing, and verified the feasibility of federated learning in achieving order-level risk prediction while protecting data privacy in the aerospace industry case [8]. In terms of privacy protection in supply chain finance, Zheng G et al. proposed a supply chain collaborative risk prediction method based on federated machine learning, allowing supply chain members to collaboratively train the risk prediction model without sharing the original data. The effectiveness of federated learning in order delay risk prediction was verified in the aerospace industry case [9]. In terms of the integration of Wireless Sensor Network (WSN) and federated learning, Khraisat A et al. proposed a random forest intrusion detection architecture based on federated learning, achieving an accuracy rate of 99.67% on the WSN-DS dataset. The privacy protection and scalability of federated learning in resource-constrained WSN environments were verified [10]. Moudoud H et al. proposed a novel framework integrating federated learning and multi-agent deep reinforcement learning in response to the current situation of emerging security threats faced by wireless sensor networks. The results showed that in real WSN attack tests, this framework demonstrated secure and communicatively efficient federated edge learning capabilities [11].

Although the above studies achieve favorable results, most of them focus on credit risk assessment or financing decision modeling, and do not involve the real-time collection of the physical state of pledged assets and the generation of digital warehouse receipts at the WSN perception layer. On this basis, a data privacy and audit compliance method for warehouse receipt pledge in supply chain finance based on WSN federated edge learning is proposed. This method aims to solve the problem of multi-warehouse collaborative risk control modeling under the condition that pledged data does not leave the domain, and meets the dual requirements of privacy protection and audit compliance while realizing high-precision risk control model training. The

innovation of the study lies in the construction of a WSN-based pledged asset perception and digital warehouse receipt generation mechanism, which realizes the mapping of the physical state of pledged assets to trusted digital warehouse receipts through "object-information binding", and provides a trusted data source for federated edge learning. Meanwhile, a WSN federated edge learning architecture integrating trust and energy-aware weighted aggregation, federated proximal term and communication compression is designed, which realizes multi-warehouse collaborative risk control modeling with high precision, fast convergence, low communication and energy overhead under Non-Independent and Identically Distributed (Non-IID) pledged data.

2. Research methodology

2.1 A method for pledge perception and digital warehouse receipt generation based on WSN

Aiming at the problems that the status of the pledged goods is difficult to verify in a timely manner and the information of the warehouse receipts is prone to being tampered with in warehouse receipt pledge financing, a pledged goods perception and digital warehouse receipt generation method based on WSN is first constructed. Firstly, WSN nodes such as temperature and humidity, weight/liquid level, pressure, radio frequency identification, electronic fence and smart camera are deployed at the warehouse end to collect the status data of the pledged items at a fixed frequency. The edge gateway performs time synchronization, missing value handling and initial anomaly screening of data. On this basis, the WSN status data is bound with the business elements of warehouse receipts to generate digital warehouse receipts and store them on the chain for evidence. The "physical information binding" process is shown in Figure 1.

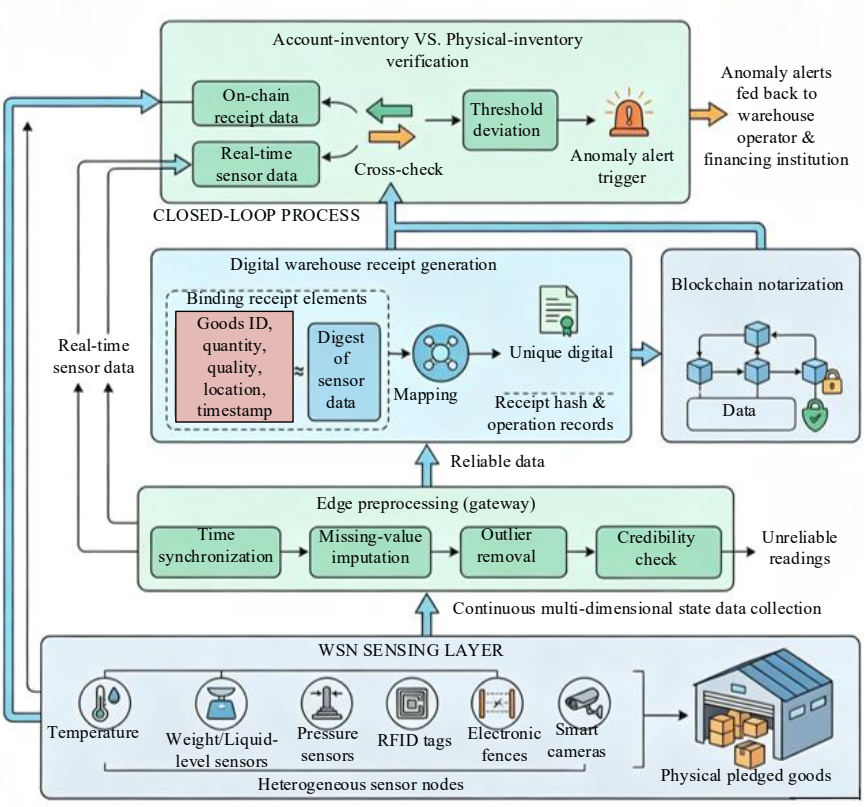


Fig. 1 WSN pledge asset perception and digital warehouse document "asset-information binding" generation mechanism diagram

In Figure 1, the perception layer of WSN is responsible for collecting the physical state of the collateral, while the edge gateway is responsible for cleaning, anomaly detection and physical

rationality verification. The digital warehouse receipt generation module binds elements such as the goods Identifier (ID), quantity, quality, location, status and timestamp with the sensor summary to form a digital warehouse receipt. The blockchain evidence storage module saves the hash of warehouse receipts and operation records. The account-inventory verification module cross-verifies the actual inventory sensor data with the account-inventory warehouse receipt data. If the deviation exceeds the threshold, an alarm will be triggered. The hash digest of a digital warehouse receipt can be represented by Formula (1).

$$H_t = Hash(C_t \| S_t \| T_t \| N_t) \quad (1)$$

In Formula (1), H_t represents the hash digest of the digital warehouse receipt at time t, C_t is the set of business elements of the warehouse receipt, S_t is the state vector of the pledged goods collected by WSN, T_t is the timestamp, N_t is the random number, $\|$ indicates the concatenation operation, and A $Hash$ is the anti-collision hash function. Formula (1) can ensure that the content of the warehouse receipt corresponds to the physical state and is difficult to tamper with.

Furthermore, to transform heterogeneous data into local samples available for federated edge learning, it is necessary to integrate real-time WSN data, warehouse receipt business data, logistics data, and quality inspection/contract data. This process is shown in Figure 2.

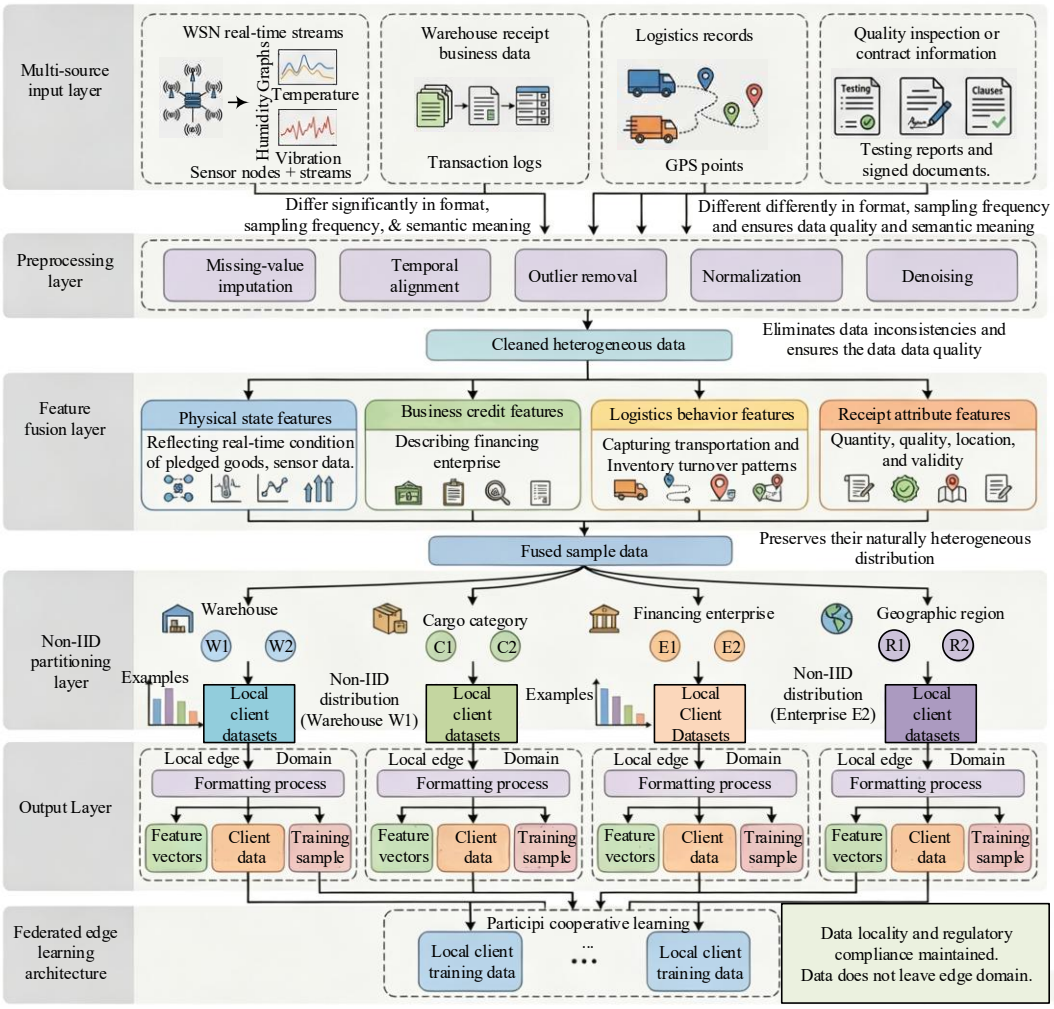


Fig. 2 Multi-source pledge data fusion and local federated sample construction mechanism diagram

In Figure 2, the multi-source input layer receives real-time WSN streams, inbound orders, quality inspection reports, contract information, transportation trajectories, and inbound and outbound records. The preprocessing layer performs missing value handling, time alignment, outlier elimination, and normalization [12-13]. The feature fusion layer constructs physical state features, business credit features, logistics behavior features and warehouse receipt attribute features. The Non-IID division layer divides the local client dataset by warehouse, goods category, financing enterprise and region. The output layer obtains the local feature vectors and the index of training samples, which are input into the subsequent federated edge learning architecture. The fusion features can be formalized and represented based on Formula (2).

$$z_i = f_{pre}(x_i^{WSN}, x_i^{biz}, x_i^{\log}, x_i^{qc}) \qquad (2)$$

In Formula (2), z_i represents the fusion feature problem of the i th pledged sample, with $x_i^{WSN}, x_i^{biz}, x_i^{\log}, x_i^{qc}$ representing the WSN status, warehouse receipt business, logistics, and quality inspection/contract features respectively. f_{pre} is the preprocessing and fusion function.

The local dataset of the k th edge client can be represented as $D_k = \{(z_i, y_u)\}_{i=1}^{n_k}$, where D_k is the local dataset of client k, n_k is the sample size, and y_i is the risk or compliance label. By physically perceiving trusted warehouse receipts and then constructing federated local samples, a data foundation can be provided for federated edge learning.

2.2 WSN federated edge learning architecture design

Based on completing the mapping of the physical state of the pledged goods to the trusted digital warehouse receipts and constructing the local Non-IID samples of each edge client, the WSN federated edge learning architecture is further designed to solve the problem of multi-warehouse collaborative risk control modeling under the condition that the pledged data does not leave the domain. The architecture and the collaborative training process are shown in Figure 3.

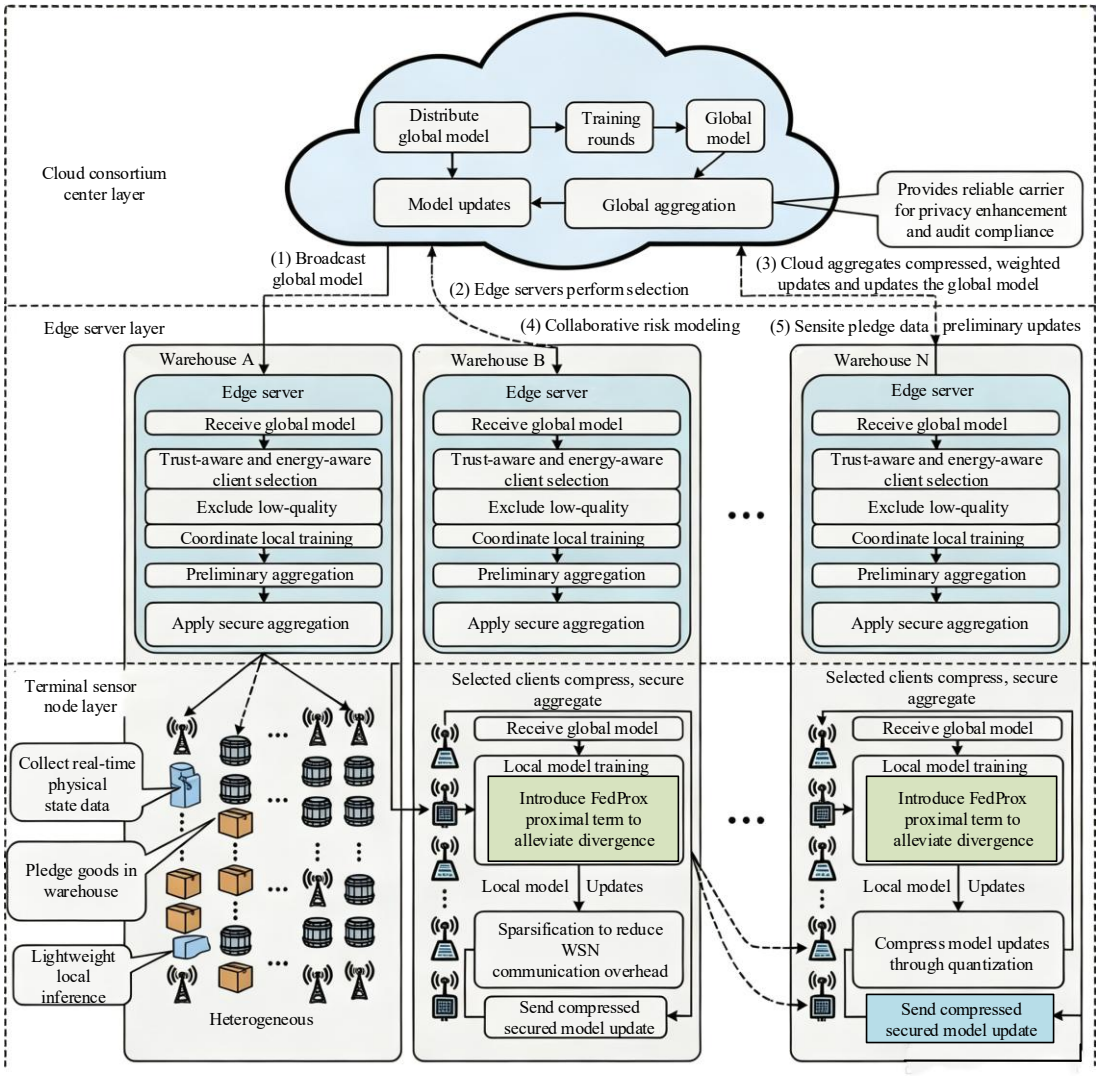


Fig. 3 Multi-source pledge data fusion and local federated sample construction mechanism diagram

In Figure 3, the terminal sensor node layer is responsible for collecting the state data of the pledged assets and conducting lightweight reasoning. The edge server layer is responsible for local model training, initial aggregation, as well as trust and energy evaluation. The cloud/alliance

center layer is responsible for global model aggregation, model distribution, and training scheduling [14-15]. The training loop includes: central initialization and distribution of the global model; The edge server performs trust and energy-aware client selection. Each client is locally trained and uses FedProx to alleviate Non-IID. The global model is updated and distributed. Let the global model of the t th round be $\boldsymbol{w}^t$ and the local dataset of the client k be D_k, then its local training objective can be expressed based on Formula (3).

$$\min_{\mathbf{w}} G_k(\mathbf{w}) = F_k(\mathbf{w}) + \frac{\mu}{2}\| \mathbf{w} - \mathbf{w}^t \|^2, \quad F_k(\mathbf{w}) = \frac{1}{n_k}\sum_{i=1}^{n_k} \ell(\mathbf{w}; \mathbf{z}_i, y_i) \qquad (3)$$

In Formula (3), $\mathbf{w}$ represents the parameters of the model to be optimized, $G_k(\mathbf{w})$ is the local objective function of the client k, $F_k(\mathbf{w})$ is the local empirical loss, and μ is the coefficient of the proximal term, which is used to control the deviation degree between the local model and the global model [16-17]. n_k is the number of local samples of client k; $\ell(\cdot)$ is the loss function, and $\boldsymbol{z}_i$ and y_i are the fusion features and labels of the i th sample, respectively.

To suppress low-quality nodes while taking into account the energy constraints of WSN, edge servers select clients based on trust scores and remaining energy and allocate aggregation weights, as shown in Formula (4).

$$\alpha_k = \frac{n_k \tau_k e_k}{\sum_{j \in S_t} n_j \tau_j e_j}, \quad k \in S_t \qquad (4)$$

In Formula (4), α_k represents the aggregation weight of client k, S_t is the set of clients participating in the aggregation in the t th round, τ_k is the trust score of client k, e_k is the normalized value of residual energy, and n_j, τ_j, e_j are the sample size, trust score, and normalized value of residual energy of client j, respectively. The global model can be updated based on Formula (5).

$$\mathbf{w}^{t+1} = \sum_{k \in S_t} \alpha_k \mathbf{w}_k^{t+1} \qquad (5)$$

In Formula (5), $\mathbf{w}^{t+1}$ represents the global model of round $t+1$, $\mathbf{w}_k^{t+1}$ is the locally updated model parameter uploaded by client k, and the meanings of S_t and α_k are the same as above. To reduce the communication overhead of WSN, quantization or sparsification $Q(\cdot)$ is performed on local updates before uploading, and only the compressed model updates are transmitted [18-19]. By repeating the above process until convergence, this architecture realizes multi-warehouse collaborative risk control modeling without data leaving the domain, and provides a training carrier for privacy enhancement and audit compliance.

2.3 Privacy enhancement mechanisms and audit compliance frameworks

Although the WSN federated edge learning architecture has achieved collaborative risk control modeling for staked data without leaving the domain, there is still a risk of privacy leakage in the uploaded model updates, and the training process lacks a verifiable audit trajectory for regulators. Therefore, a privacy enhancement mechanism and an audit compliance framework should be further constructed. To protect the local model updates uploaded, a combined security aggregation mechanism of differential privacy and homomorphic encryption is adopted, as shown in Figure 4.

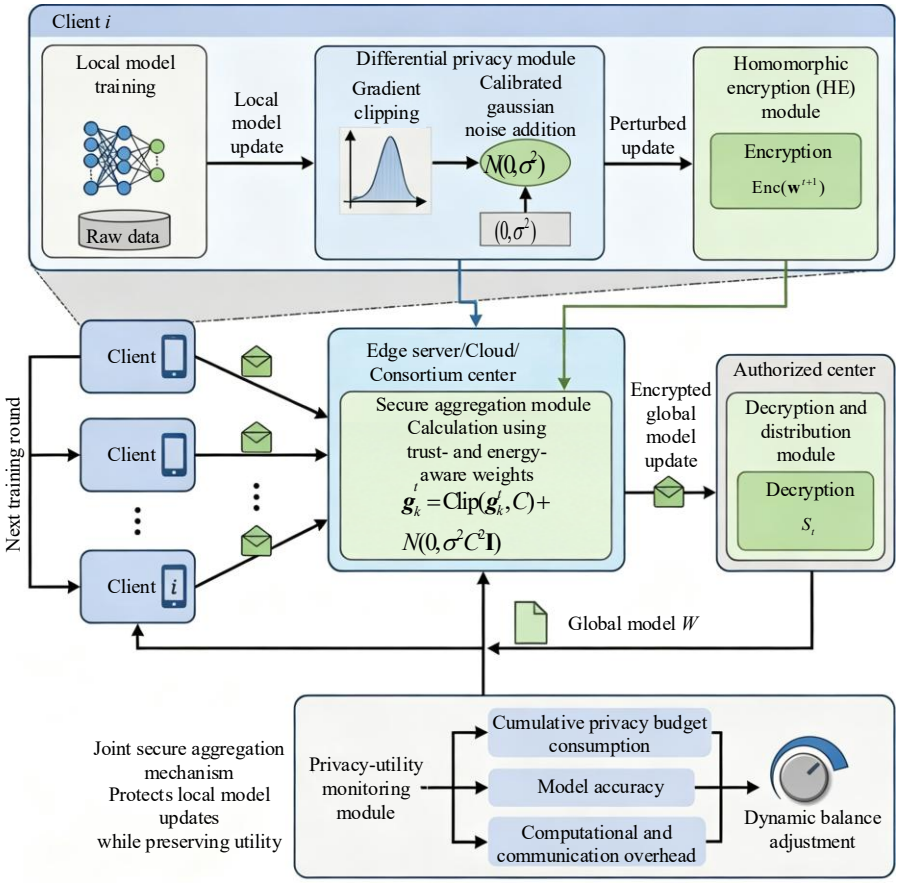


Fig. 4 Joint secure aggregation mechanism of differential privacy and homomorphic encryption

In Figure 4, the local training output first enters the differential privacy module to perform gradient clipping and noise addition; Then it enters the homomorphic encryption module to encrypt the noisy update; The security aggregation module accomplishes multi-client update aggregation in ciphertext state. The decryption and distribution module decrypts the global model by the authorization center and distributes it. The privacy-utility monitoring module continuously records privacy budget consumption, model accuracy, and computational communication overhead. The local update after adding noise can be based on Formula (6).

$$\boldsymbol{g}_k^t = \mathrm{Clip}(\mathbf{g}_k^t, C) + \mathrm{N}\ (0, \sigma^2 C^2 \mathbf{I}) \tag{6}$$

In Formula (6), $\boldsymbol{g}_k^t$ represents the model update of the client k after adding noise in the t th round, and $\boldsymbol{g}_k^t$ represents the original model update of the client k in the t th round.

$\text{Clip}(\cdot, C)$ is the gradient clipping function with a clipping threshold of C; C is the cropping threshold; $\text{N}(0, \sigma^2 C^2 \mathbf{I})$ is Gaussian noise with a mean of 0 and a variance of $\sigma^2 C^2$; σ is the noise multiplier and $\mathbf{I}$ is the identity matrix. Ciphertext field aggregation can be based on Formula (7).

$$\text{Enc}(\mathbf{w}^{t+1}) = \sum_{k \in S_t} \alpha_k \, \text{Enc}(\mathbf{w}_k^{t+1}) \qquad (7)$$

In Formula (7), Enc is the homomorphic encryption function, and $\mathbf{w}_k^{t+1}$ is the local model parameter of the client k after adding noise. S_t is the sum of the client sets participating in the aggregation in the t th round.

To meet the regulatory audit requirements, the metadata of each round of training is uploaded to the chain, and the compliance conditions are automatically verified through smart contracts, forming a traceable and verifiable audit closed loop. This mechanism is shown in Figure 5.

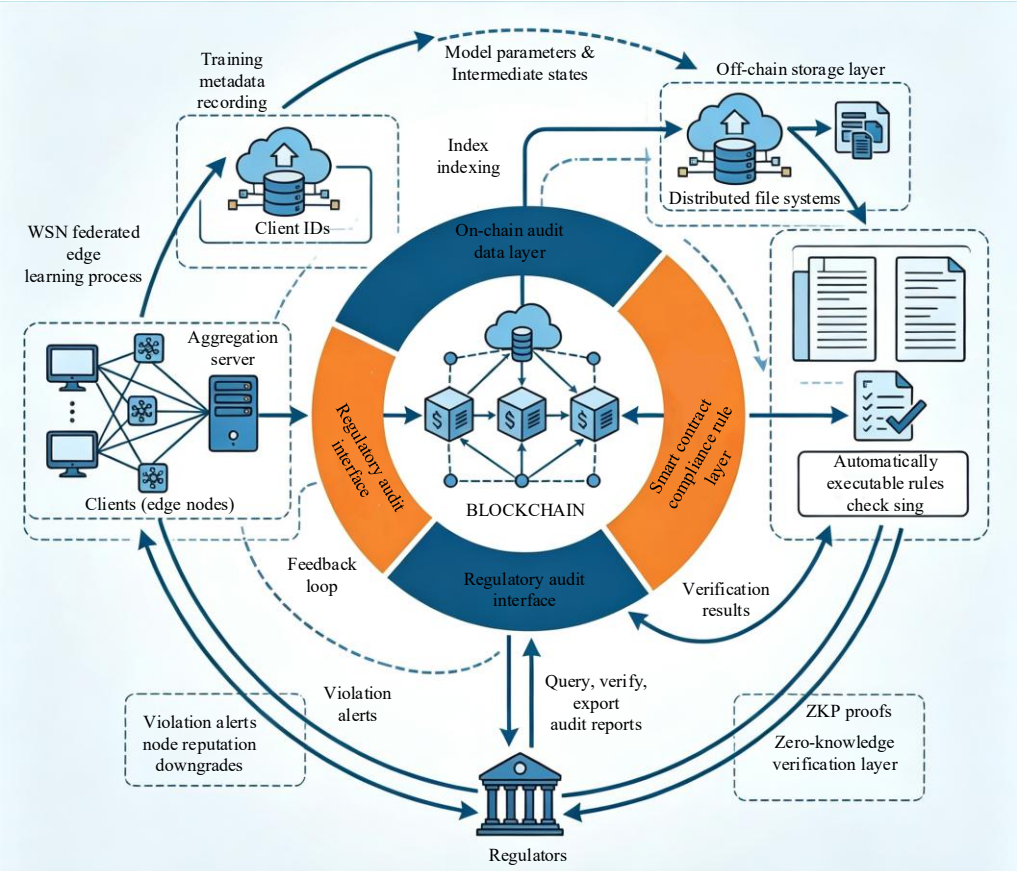


Fig. 5 Blockchain audit and smart contract compliance closed-loop mechanism

In Figure 5, the on-chain audit data layer records the client ID, update hash, timestamp, training rounds, and privacy budget consumption. The off-chain storage layer stores model parameters and intermediate states. The compliance rule layer of smart contracts implements rules such as data minimization, privacy budget caps, and sensitivity constraints. The zero-knowledge proof verification layer proves that the local training complies with the protocol without exposing the model parameters. The regulatory audit interface supports query and verification by regulatory authorities. The feedback loop feeds back violation alerts, node demotion, and policy adjustments

to the federated training process. Compliance determination and privacy budget constraints can be expressed based on Formula (8).

$$\text{Compliance}_t = \prod_{r=1}^{R} \mathbf{1}\left[r(\mathrm{M}_t, \varepsilon_t) = 1\right], \quad \varepsilon_{\text{cum}} = \sum_{t=1}^{T} \varepsilon_t \le \varepsilon_{\max} \qquad (8)$$

In Formula (8), Compliance_t represents the compliance determination result of the t th round, R is the total number of compliance rules, and $\mathbf{1}[\cdot]$ is the indicator function, taking 1 if the condition is met; otherwise, it takes 0. $r(\cdot)$ is the compliance rule r; M_t represents the on-chain audit metadata for the t th round, ε_t represents the privacy budget for the t th round, ε_{cum} represents the cumulative privacy budget, and T represents the total number of training rounds. $\varepsilon_{\max}$ represents the maximum privacy budget allowed. As a result, this framework not only protects the privacy of model updates but also provides verifiable audit evidence for regulators, and forms a closed loop of privacy protection and compliance auditing with the federated edge learning architecture.

3. Results

3.1 Experimental environment and parameter settings

To verify the effectiveness of the proposed WSN federated edge learning architecture, privacy enhancement mechanism and audit compliance framework, the study first provided the experimental environment configuration and key parameter settings, as shown in Table 1.

Table 1 Experimental environment and key parameter settings

Item	Configuration	Parameter	Value
CPU	Intel Core i9-13900K	Number of warehouses / Clients	10
GPU	NVIDIA RTX 4090 24 GB	WSN nodes per warehouse	20
RAM	64 GB DDR5	Total pledge samples	50000
Storage	2 TB NVMe SSD	Feature dimension	32
Operating system	Ubuntu 22.04 LTS	Non-IID degree	0.5
Programming language	Python 3.10	Local epochs	5
Deep learning framework	PyTorch 2.1	Batch size	64
Federated learning framework	Flower 1.6	Learning rate	0.01
WSN simulator	NS-3.38	Optimizer	SGD
DP library	Opacus	FedProx coefficient	0.01
HE library	TenSEAL (CKKS)	Communication rounds	100
ZKP library	libsnark (Groth16)	Client participation rate	0.6
Platform	Hyperledger Fabric 2.5	Trust score threshold	0.7
Smart contract language	Go	Energy threshold	0.2
Communication	100 Mbps LAN, 20 ms latency	Gradient clipping threshold	1

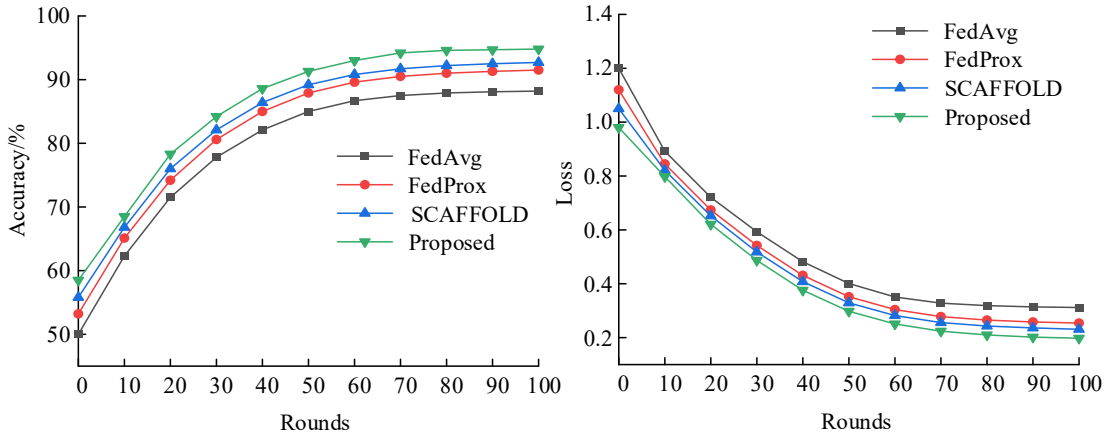
/	/	Noise multiplier	0.8
/	/	Privacy budget per round	0.08

Based on the experimental environment settings and parameters in Table 1, two public and open-source datasets were selected in this study: Industrial Supply Chain (IndustrialSupplyChain-v2) (https://zenodo.org/records/21372906) and Supply Chain Collaborative False Order Recognition Dataset (https://nbsdc.cn/general/dataDetail?id=6933018e195d2658bc1f5419&type=1). Among them, IndustrialSupplyChain-v2 was a programmatically generated multi-domain supply chain risk dataset that explicitly supported benchmark tests for privacy-preserving research such as federated learning and quantum machine learning. This dataset contained 100,000 rows and 110 columns of data, covering nine operational subsystems including supplier management, warehousing, transportation and logistics, macroeconomics and finance, and cybersecurity. The Supply Chain Collaborative False Order Recognition Dataset was directly oriented to federated learning-based supply chain anomaly detection tasks. It realized privacy-preserving false order detection through the cloud-edge collaborative federated learning method, and could be used as effective verification data for the federated edge learning model in the "risk identification" task. The datasets were divided into training set, validation set and test set according to the ratio of 7:2:1.

Meanwhile, controlled experiments were carried out with Federated Averaging (FedAvg), Federated Proximal (FedProx) and Stochastic Controlled Averaging for Federated Learning (SCAFFOLD).

3.2 Performance and ablation analysis of federated edge learning models

Firstly, the accuracy and loss function curves of each method were analyzed, and the results are shown in Figure 6.



(a) Accuracy curve (b) Loss curve

Fig. 6 Curves of test accuracy and loss varying with the number of communication rounds under different aggregation algorithms

In Figure 6, the proposed method yielded higher test accuracy and lower test loss than FedAvg, FedProx and SCAFFOLD across all training rounds. Differences emerged even at the 0-th round of initial evaluation due to distinct initialization strategies and client sampling conditions. As the number of training rounds increased, the proposed method reached a test accuracy of 94.8% and a test loss of 0.198 at the 100-th round. Compared with FedAvg (88.2%, 0.312), the test accuracy improved by 6.6% and the test loss decreased by 36.5%. It also maintained a clear advantage over FedProx (91.5%, 0.254) and SCAFFOLD (92.7%, 0.231).

The influence and robustness of the Non-IID degree on the model performance were further analyzed, and the results are shown in Figure 7.

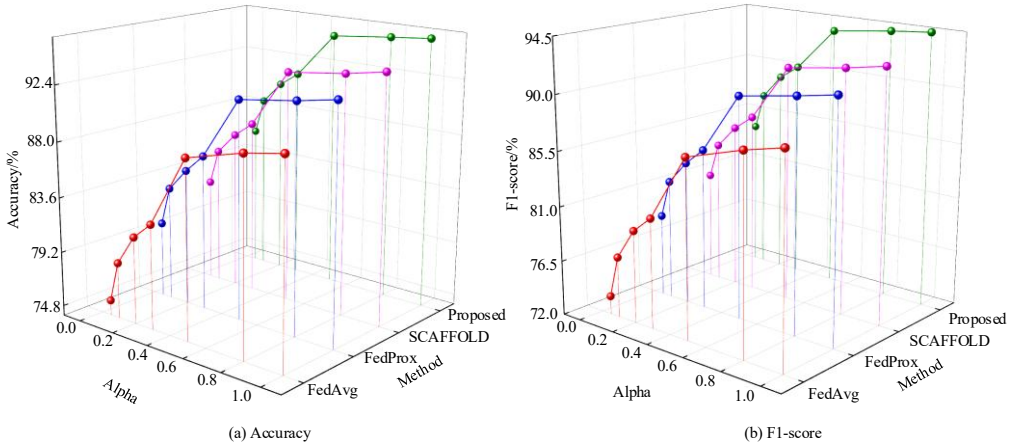


Fig. 7 The impact of non-IID degree on model performance

In Figure 7, as Alpha increased from 0.05 to 1.0 (the Non-IID degree gradually decreased), the test accuracy and F1-score of all four methods continued to rise. The proposed method maintained the optimal performance under all Alpha values. For instance, when Alpha equaled 0.05, the accuracy reached 85.6% and the F1-score reached 84.2%, which were approximately 10.4% and 10.7% higher than those of FedAvg respectively. When Alpha decreased from 1.0 to 0.05, the accuracy and F1-score of the proposed method only decreased by 10.0% and 10.3%, while those of FedAvg decreased by 14.9% and 15.3%. The results indicated that the proposed method had the lowest sensitivity to the intensification of Non-IID.

To verify the independent contribution of each key component in the proposed architecture, ablation experiments were conducted on three components: trust and energy-aware client selection, FedProx proximal term, and communication compression. The performance comparison between the full method (Proposed) and each ablation variant under the Non-IID setting (Alpha=0.5) is presented in Table 2.

Table 2 Ablation study of key components in the federated edge learning architecture

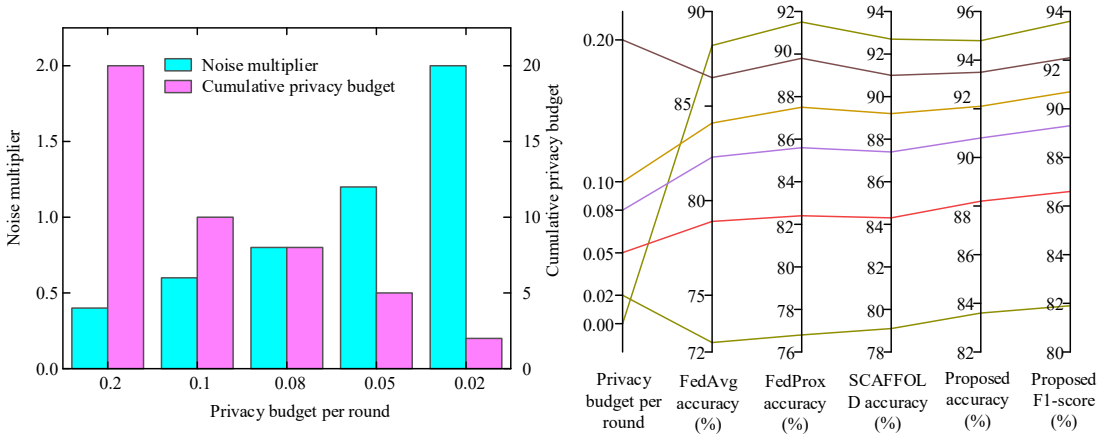
Configuration	Test Accuracy (%)	F1-score (%)	Rounds to 90% Accuracy	Communication Cost (MB)	Energy Consumption (J)	Final Training Loss
Proposed (Full)	94.8	93.6	65	48.5	12.3	0.198
w/o Trust-Energy Selection	91.2	89.8	82	52.1	15.6	0.254
w/o FedProx	90.5	88.9	88	50.3	14.8	0.267
w/o Compression	94.6	93.4	64	156.8	18.2	0.201
w/o All (FedAvg Baseline)	88.2	86.5	92	49	13.5	0.312

In Table 2, the complete method performed the best in terms of test accuracy, F1-score and the number of convergence rounds. After removing the trust and energy-aware client selection, the accuracy rate decreased by 3.6%, the F1-score decreased by 3.8%, the number of convergent rounds increased to 82 rounds, and the energy consumption increased to 15.6 J. This indicated that this component significantly improved the model performance and node sustainability by

suppressing low-quality nodes and balancing energy consumption. After removing the proximal term of FedProx, the accuracy rate decreased by 4.3%, and the number of convergence rounds increased to 88 rounds, indicating that the proximal term played a key role in alleviating the drift of Non-IID clients. After removing communication compression, the accuracy rate only decreased by 0.2%, but the communication overhead soared from 48.5 MB to 156.8 MB, and the energy consumption increased to 18.2 J. This indicated that the compression mechanism significantly reduced the communication and energy overhead of WSN without significantly losing accuracy. Compared with the FedAvg baseline, the accuracy of the complete method increased by 6.6 percentage points, and the number of convergence rounds was shortened by 27 rounds, verifying the effectiveness of the collaborative optimization of each component.

3.3 Privacy enhancement and audit compliance performance assessment

To evaluate the impact of the differential privacy mechanism on the model accuracy, different privacy budgets for each round and corresponding noise coefficients were set. The test accuracy and F1 values of the four methods under the cumulative privacy budget constraint were compared. The results are shown in Figure 8.



(a) Noise multiplier and cumulative privacy budget

(b) Accuracy and F1-score

Fig. 8 Privacy-utility trade-off of different methods under varying privacy budgets

In Figure 8, as the privacy budget decreased, that is, privacy protection was enhanced, the test accuracy rates of the four methods all declined. However, the proposed method maintained the highest accuracy under all privacy budgets. For example, when the privacy budget was 0.08, the accuracy rate reached 90.8%, which was 8.5, 5.2, and 3.4 % higher than that of FedAvg, FedProx, and SCAFFOLD, respectively. When the privacy protection was extremely strong (with a privacy budget of 0.2), the proposed method still achieved 83.6%, while FedAvg only reached 72.5%. The proposed method had less accuracy loss under the same privacy budget, and the F1-score was consistent with the change trend of accuracy, indicating that the trust and energy-aware weighted aggregation and the proximal term of FedProx were helpful to maintain the model utility under the condition of noise addition.

To evaluate the actual overhead of homomorphic encryption security aggregation, the computing and communication performance of the two configurations without homomorphic encryption and with CKKS homomorphic encryption enabled were compared. The results are shown in Figure 9.

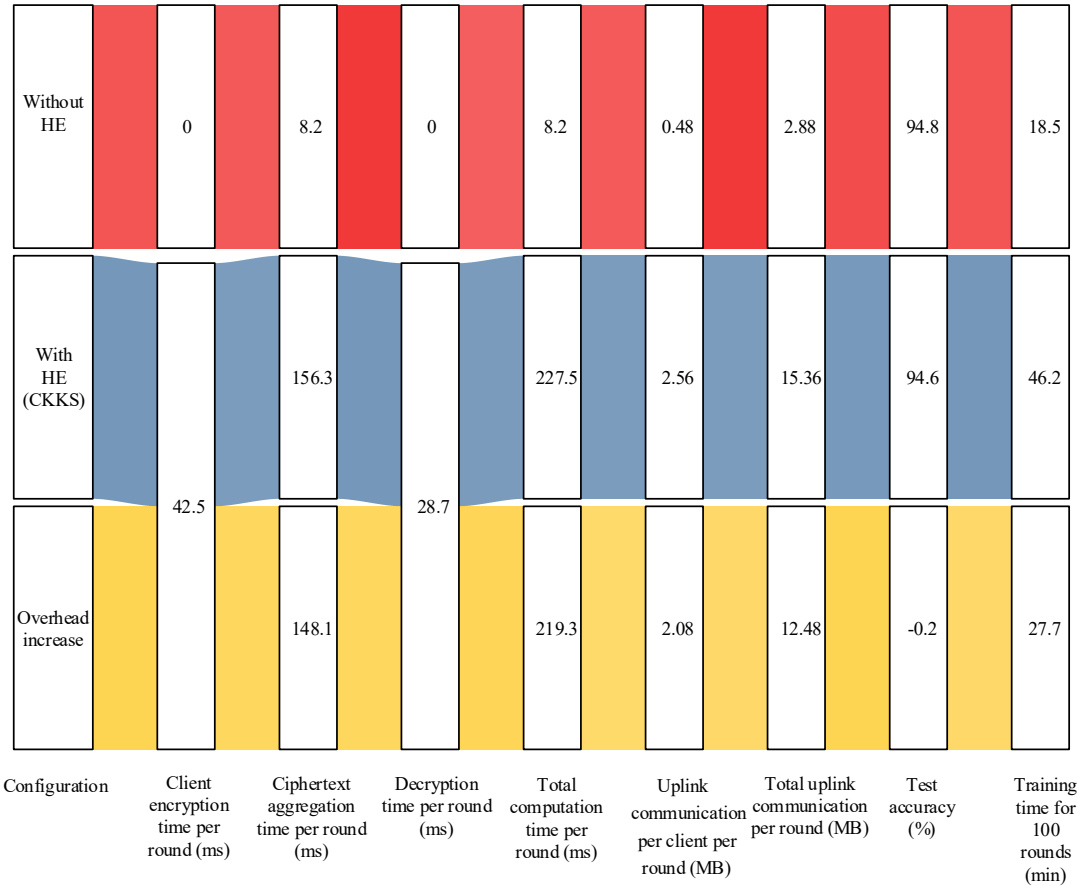


Fig. 9 Computation and communication overhead of homomorphic encryption-based secure aggregation

In Figure 9, after enabling CKKS homomorphic encryption, the time consumption for each round of client encryption was 42.5ms, the time consumption for ciphertext aggregation was 156.3ms, and the time consumption for decryption was 28.7ms. The total computing time increased from 8.2ms to 227.5ms, with the main overhead coming from the aggregation of the ciphertext domain. In terms of communication, the uplink traffic per round for a single client increased from 0.48MB to 2.56MB, and the total uplink traffic rose from 2.88MB to 15.36MB, approximately 5.3 times that of the unencrypted baseline. In terms of accuracy, homomorphic encryption only led to a 0.2% loss in test accuracy (from 94.8% to 94.6%), indicating that ciphertext aggregation had almost no impact on the model's utility.

Finally, the qualitative capabilities of each method in the dimensions of privacy enhancement and audit compliance were analyzed, and the results are shown in Figure 10.



Fig. 10 Qualitative capability comparison of different methods in privacy enhancement and audit compliance

From Figures 10 (a) to (c), FedAvg only supported data not leaving the domain and local model training. FedProx and SCAFFOLD added Non-IID mitigation capabilities on this basis. The three only partially supported communication compression. However, it lacked support capabilities in dimensions such as model update encryption, ciphertext domain aggregation, differential privacy, blockchain audit trail, automatic compliance verification of smart contracts, zero-knowledge proof verification, and regulatory audit interfaces, indicating that it could only meet the basic privacy requirements of federated learning. In Figure 10 (d), the proposed method achieved full support in all 12 dimensions. It not only covered the existing basic capabilities of the three control methods but also further integrated privacy enhancement and audit compliance mechanisms such as ciphertext aggregation, differential privacy, blockchain auditing, smart contract compliance verification, and zero-knowledge proof. In conclusion, the qualitative comparison intuitively showed that the research method was significantly superior to FedAvg, FedProx and SCAFFOLD in terms of privacy protection and audit compliance capabilities, and could better meet the dual requirements of data privacy and regulatory compliance in the scenario of warehouse receipt pledge in supply chain finance.

4. Discussion and conclusion

To address critical issues in the supply chain finance warehouse receipt pledge scenario, including the difficulty in real-time verification of pledged asset status, high risk of financing data privacy leakage, and the lack of verifiable audit trails during the training process, a WSN-based pledged asset perception and digital warehouse receipt generation method was constructed in this study. A WSN federated edge learning architecture integrating trust and energy-aware weighted aggregation, FedProx proximal term and communication compression was designed. Furthermore, a joint secure aggregation mechanism combining differential privacy and homomorphic encryption, as well as an audit compliance framework based on blockchain smart contracts, were proposed.

In terms of federated edge learning model performance, the proposed method achieved a test accuracy of 94.8% and a test loss of 0.198 at the 100-th round. When the Dirichlet parameter Alpha decreased from 1.0 to 0.05, the accuracy of the proposed method only dropped by 10.0%, while that of FedAvg decreased by 14.9%, indicating that the proposed method had the lowest sensitivity to the intensification of Non-IID. Ablation experiments further showed that after removing the trust and energy-aware client selection, the accuracy decreased by 3.6% and the energy consumption increased to 15.6 J; after removing the FedProx proximal term, the accuracy decreased by 4.3% and the number of convergence rounds increased to 88; after removing communication compression, the accuracy only decreased by 0.2%, but the communication overhead surged from 48.5 MB to 156.8 MB. In terms of privacy-utility trade-off, when the per-round privacy budget was 0.08, the accuracy of the proposed method reached 90.8%, and still reached 83.6% under extremely strong privacy protection conditions. For homomorphic encryption, after enabling CKKS, the total per-round computation time increased from 8.2 ms to 227.5 ms, and the uplink traffic of a single client increased from 0.48 MB to 2.56 MB, while the accuracy only lost 0.2%. The numerical results demonstrated that the proposed method outperformed the comparison methods in Non-IID robustness, privacy-utility trade-off and system overhead control. The synergistic effectiveness of the three components (trust and energy-aware weighted aggregation, FedProx proximal term and communication compression) was verified, as well as the capability of the joint mechanism of differential privacy and homomorphic encryption to maintain model utility while protecting the privacy of model updates.

Currently, Zhang L has constructed a digital warehouse receipt management framework integrating the Internet of Things and blockchain in response to the lack of status monitoring of pledged goods and the risk of warehouse receipt fraud. The issuance, transfer and verification of digital warehouse receipts are realized through smart contracts to control the risk of fraud [20]. This report and research share similarities in addressing information asymmetry and fraud risks in warehouse receipt pledge financing by leveraging blockchain and Internet of Things technologies. However, the former focuses on game modeling and operational optimization for financing decisions, without involving multi-warehouse collaborative modeling under the federated learning framework, nor does it take into account privacy-enhancing technologies such as differential privacy and homomorphic encryption. In addition, Yang F proposed a secure credit modeling method combining explainable federated learning and blockchain. This method constructs an explainable federated learning credit scoring system, realizes secure credit data sharing through blockchain, and designs a training mechanism to prevent the leakage of model gradients, ensuring the transparency and traceability of credit decisions while protecting the data privacy of each node [21]. Both this report and research focus on the integrated application of federated learning and

blockchain in credit risk control, and attach importance to privacy protection and decision interpretability. However, this study mainly focused on the interpretability of credit scoring scenarios, and did not involve data collection and digital warehouse receipt generation in the WSN perception layer, nor did it design a trust and energy-aware client selection mechanism oriented to WSN energy constraints. Moreover, its privacy protection scheme mainly relied on the immutability of blockchain and did not introduce the formal privacy guarantee of differential privacy.

In summary, the research deeply integrated the WSN perception layer with the federated edge learning architecture, achieving a full-chain connection from the perception of the physical state of the pledged assets to the generation of digital warehouse receipts, and then to the modeling of multi-warehouse collaborative risk control. Meanwhile, through the collaborative design of trust and energy-aware weighted aggregation, FedProx proximal term and communication compression, high precision, fast convergence and low communication and energy overhead were achieved simultaneously under Non-IID staked data. However, there are still certain deficiencies in the research. The current homomorphic encryption scheme adopted CKKS, which had a large overhead of ciphertext aggregation and might be difficult to run for a long time on resource-constrained WSN edge nodes. Future research will explore more lightweight homomorphic encryption schemes or secure multi-party computation protocols to further reduce the computational and communication overhead of privacy enhancement mechanisms, and study dynamic privacy budget allocation strategies to adapt to staking scenarios of different risk levels.

Funding Statement: No

Declarations：

Ethical approval： Not applicable. This study did not involve human subjects or the collection of personal or sensitive information

Consent to participate： Not applicable, as the annotators were not enrolled as research participants and participated only in expert data annotation.

Consent to publish： Not applicable.

Competing Interest Statement: The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability Statement: Publicly available data

1.Industrial Supply Chain (IndustrialSupplyChain-v2)
（https://zenodo.org/records/21372906）

2. Supply Chain Collaborative False Order Recognition Dataset （https://nbsdc.cn/general/dataDetail?id=6933018e195d2658bc1f5419&type=1）

Reference

[1]Huang J, Liu J, Yang W. Blockchain-based inventory pledge financing: an evolutionary game perspective[J]. Kybernetes, 2026, 55(5): 1801-1827. DOI: 10.1108/k-10-2024-2736.

[2]Alora A, Sasidharan A, Dsouza J. Blockchain integration in supply chain finance: a catalyst for improved cost of capital[J]. Managerial Finance, 2026, 52(4): 720-733. DOI: 10.1108/MF-12-2024-0913.

[3]Vazquez Melendez E I, Bergey P, Smith B. Blockchain technology for supply chain provenance: increasing supply chain efficiency and consumer trust[J]. Supply chain management: An international journal, 2024, 29(4): 706-730. DOI: 10.1108/scm-08-2023-0383.

[4]Tuladhar A, Rogerson M, Engelhart J, et al. Blockchain for compliance: an information processing case study of mandatory supply chain transparency in conflict minerals sourcing[J]. Supply Chain Management: An International Journal, 2024, 29(4): 755-777. DOI: 10.1108/scm-11-2023-0585.

[5]John A, Isnin I F B, Hamid Hussain Madni S, et al. Intrusion detection in cluster‐based wireless sensor networks: Current issues, opportunities and future research directions[J]. IET Wireless Sensor Systems, 2024, 14(6): 293-332. DOI: 10.1049/wss2.12100.

[6]Yoo H J, Kang T, Woo N, et al. LAEC: lightweight authentication protocol for energy-efficient and cost-effective communication in wireless sensor network environments[J]. IEEE Sensors Journal, 2025, 25(16): 31709-31725. DOI: 10.1109/JSEN.2025.3585616.

[7]Zhang J, Cai K, Zhao Q. Warehouse receipt pledge financing using blockchain data asset[J]. International Review of Financial Analysis, 2025, 102: 104104. DOI: 10.1016/j.irfa.2025.104104.

[8]Kong L, Zheng G, Brintrup A. A federated machine learning approach for order-level risk prediction in supply chain financing[J]. International Journal of Production Economics, 2024, 268: 109095. DOI:

[9]Zheng G, Kong L, Brintrup A. Federated machine learning for privacy preserving, collective supply chain risk prediction[J]. International Journal of Production Research, 2023, 61(23): 8115-8132. DOI: 10.1080/00207543.2022.2164628.

[10]Khraisat A, Talukder M A, Uddin M A, et al. RF-FedAvg: Federated learning-based random forest model for intrusion detection in wireless sensor networks[J]. Cluster Computing, 2025, 28(13): 1-21. DOI: 10.1007/s10586-025-05591-8.

[11]Moudoud H, Abou El Houda Z, Brik B. Advancing security and trust in wsns: A federated multi-agent deep reinforcement learning approach[J]. IEEE Transactions on Consumer Electronics, 2024, 70(4): 6909-6918. DOI: 10.1109/TCE.2024.3440178.

[12]Chen J, Yan H, Liu Z, et al. When federated learning meets privacy-preserving computation[J]. ACM Computing Surveys, 2024, 56(12): 1-36. DOI: 10.1145/3679013.

[13]Meese C, Chen H, Li W, et al. Adaptive traffic prediction at the its edge with online models and blockchain-based federated learning[J]. IEEE Transactions on Intelligent Transportation Systems, 2024, 25(9): 10725-10740. DOI: 10.1109/TITS.2024.3391053.

[14]Jagarlamudi G K, Yazdinejad A, Parizi R M, et al. Exploring privacy measurement in federated learning: GK Jagarlamudi et al[J]. The Journal of Supercomputing, 2024, 80(8): 10511-10551. DOI: 10.1007/s11227-023-05846-4.

[15]Namakshenas D, Yazdinejad A, Dehghantanha A, et al. IP2FL: Interpretation-based privacy-preserving federated learning for industrial cyber-physical systems[J]. IEEE Transactions on Industrial Cyber-Physical Systems, 2024, 2(3): 321-330. DOI: 10.1109/TICPS.2024.3435178.

[16]Kioskli K, Grigoriou E, Islam S, et al. A risk and conformity assessment framework to ensure security and resilience of healthcare systems and medical supply chain[J]. International Journal of Information Security, 2025, 24(2): 1-28. DOI: 10.1007/s10207-025-01009-z.
[17]Vlachos I, Reddy P G. Machine learning in supply chain management: systematic literature review and future research agenda[J]. International Journal of Production Research, 2025, 63(16): 5987-6016. DOI: 10.1080/00207543.2025.2466062.
[18]Falcone E C, Fugate B S, Waller M A. Growing, learning, and connecting: Deciphering the complex relationship between government customer concentration and firm performance[J]. Journal of Supply Chain Management, 2024, 60(2): 64-92. DOI: 10.1111/jscm.12319.
[19]Miller J W, Jin Y H, Ortega D L. Shock and awe: a theoretical framework and data sources for studying the impact of 2025 tariffs on global supply chains[J]. Journal of Supply Chain Management, 2025, 61(3): 3-15. DOI: 10.1111/jscm.12350.
[20]Zhang L, Xiong Q, Lan Q. Inventory pledge financing decisions based on a permissioned blockchain by controlling fraudulent risk[J]. RAIRO: Operations Research (2804-7303), 2024, 58(6): 4791-4817. DOI: 10.1051/ro/2024194.
[21]Yang F, Abedin M Z, Hajek P. An explainable federated learning and blockchain-based secure credit modeling method[J]. European Journal of Operational Research, 2024, 317(2): 449-467. DOI: 10.1016/j.ejor.2023.08.040.