

Research on Privacy Leakage Defense Mechanism and Ethical Governance Path under Federated Learning Framework

Jiahui Liu¹, Muran Mao¹, Xiaomei Dong²

¹Research Center for Philosophy of Science and Technology, Northeastern University, Shenyang 110169, Liaoning, China

²School of Computer Science, Northeastern University, Shenyang 110169, Liaoning, China

Corresponding author: Jiahui Liu (e-mail: m13898139572@163.com)

ABSTRACT Federated learning, as the core paradigm of distributed machine learning, implements multi-party collaborative modeling with a “data stationary, model dynamic” architecture, providing a technical path for solving the dual dilemma of data silos and privacy protection. However, the distributed nature and parameter interaction mechanism of federated learning pose new privacy leakage risks such as gradient reversal, member inference, and model poisoning. Existing defense mechanisms suffer from imbalanced privacy performance trade-offs, insufficient cross scenario adaptability, and lack of a systematic ethical governance framework.

INDEX TERMS federated learning, privacy leakage, secure aggregation, ethical governance, distributed sensing networks

I. INTRODUCTION

A. RESEARCH BACKGROUND

WITH the deep integration of digital economy and artificial intelligence, data has become the core production factor, but the contradiction between data silos and privacy protection is becoming increasingly prominent. Traditional centralized machine learning requires the aggregation of multiple sources of raw data, which not only faces compliance constraints such as the Personal Information Protection Law and the Data Security Law, but also poses security risks such as data leakage and abuse. Federated Learning (FL), as an innovative paradigm of distributed machine learning, through the mode of “local training, parameter aggregation, and global iteration”, realizes the collaborative training of global models by multiple participants without sharing the original data, which effectively satisfies the principle of ‘computational utility without raw data exposure’ (often colloquially termed as ‘data available and invisible’) through secure parameter aggregation and local computation [1-3].

However, the distributed architecture and parameter interaction mechanism of federated learning have not completely eliminated privacy risks. Attackers can reconstruct raw data from model parameters through gradient reversal attacks, infer whether individual data exists in the training set through member inference attacks, and tamper with global model decisions through model poisoning attacks. These new types of privacy leakage risks severely restrict the scale application of federated learning. The existing privacy protection technologies, such as homomorphic encryption

and differential privacy, suffer from high computational costs, imbalanced privacy performance trade-offs, and lack a systematic defense system against the distributed nature of federated learning. At the same time, federated learning involves ethical issues such as multi-party data rights, algorithm fairness, and responsibility definition. Existing research mostly focuses on technological defense and lacks exploration of ethical governance paths, resulting in a disconnect between technological innovation and ethical norms [4].

B. CURRENT RESEARCH STATUS AT HOME AND ABROAD

Domestic research focuses on scenario based defense and technology integration. A hybrid weighted aggregation mechanism is proposed for Non IID data scenarios to reduce model bias and communication overhead; Combining blockchain technology to build a decentralized federated learning framework that achieves dual privacy protection through ring signatures and local differential privacy, solving the problem of single point of failure; A member inference attack detection method based on GAN is proposed for adversarial attacks, with a detection accuracy of 91.7%. However, existing research has problems such as a single defense dimension, poor cross scenario adaptability, and an unoptimized privacy performance trade-off.

C. RESEARCH CONTENT AND INNOVATION POINTS

1) Research Content

(1) Analyze the architectural characteristics and privacy leakage attack paths of federated learning, clarify the principles and hazards of attacks such as gradient reversal, member inference, and model poisoning;

(2) Build a four layer privacy leakage defense system, propose key technologies such as adaptive differential privacy, lightweight security aggregation, and dynamic adversarial detection, and optimize the privacy performance trade-off;

(3) Design a four-dimensional ethical governance path of “technical compliance ethical norms organizational governance regulatory synergy” and establish a three in one governance framework;

(4) Through empirical experiments in medical and financial scenarios, verify the effectiveness of defense mechanisms and the feasibility of governance pathways in representative high-sensitivity cross-institutional scenarios [5].

2) Innovation Points

(1) Build a four layer defense system consisting of cryptographic protection, differential privacy enhancement, security aggregation optimization, and adversarial defense reinforcement, to achieve full process coverage of privacy protection and address the limitations of a single defense technology;

(2) Propose an adaptive privacy budget allocation and lightweight security aggregation algorithm to control the model accuracy loss within a marginal threshold of 3.5% while ensuring provable privacy and security. Unlike traditional static defense mechanisms where accuracy degrades exponentially as privacy guarantees (ϵ) tighten, this adaptive approach maintains high utility by concentrating the privacy budget on high-sensitivity gradients, thereby optimizing the privacy-performance trade-off curve compared to baseline differential privacy implementations;

(3) Design an ethical governance path that integrates technology, ethics, and regulation to fill the research gap in ethical governance of federated learning and provide compliance and ethical guarantees for large-scale applications.

II. FEDERATED LEARNING ARCHITECTURE AND ANALYSIS OF PRIVACY LEAKAGE ATTACK PATHS

A. CORE ARCHITECTURE AND CLASSIFICATION OF FEDERATED LEARNING

The core architecture of federated learning consists of three parts: client, parameter server, and communication link, following an iterative process of “local training parameter upload secure aggregation global update”. According to data distribution and participant roles, it can be divided into three categories:

(1) HorizontalFL: Participants have the same feature space but different sample spaces, making it suitable for cross institutional collaboration within the same industry (such as joint training of risk control models by multiple banks);

(2) VerticalFL: Participants with the same sample space but different feature spaces, suitable for cross industry data fusion (such as joint training of user profiling models by banks and e-commerce);

(3) Federated Transfer Learning: Participants have different data features and sample spaces, and knowledge sharing is achieved through transfer learning, which is suitable for collaboration in heterogeneous scenarios [6,7].

B. CORE ATTACK PATHS FOR PRIVACY BREACHES IN FEDERATED LEARNING

The privacy leakage risk of federated learning comes from information leakage during parameter interaction, and the core attack paths can be divided into three categories:

The attacker intercepts the gradient information uploaded by the client and reconstructs sensitive data by utilizing the mapping relationship between the gradient and the original data. For example, in image classification scenarios utilizing small batch sizes or shallow architectures, attackers can infer the user’s facial features from gradients via recursive optimization. While gradient averaging in large-scale batches serves as a natural obfuscator, high-resolution reconstruction remains a significant threat in edge computing environments where local updates are frequently transmitted or when the model possesses high transparency; In medical settings, it is possible to infer the patient’s medical record information. This attack utilizes the high-dimensional characteristics of model parameters to achieve reverse inference of “parameter data”, which is the most direct privacy leakage risk in federated learning [8].

C. THE HARM AND IMPACT OF PRIVACY BREACH ATTACKS

Privacy breach attacks not only lead to the leakage of sensitive personal data (such as medical and financial information), but also trigger compliance risks and trust crises. In the medical field, the leakage of patient privacy may violate the Personal Information Protection Law and face huge fines; In financial scenarios, the leakage of user transaction data may lead to fraud risks. At the same time, privacy breaches will reduce the trust of participants in federated learning and restrict the large-scale application of technology [9,10].

III. CONSTRUCTION OF PRIVACY LEAKAGE DEFENSE MECHANISM FOR FEDERATED LEARNING

A. DESIGN OF A FOUR LAYER PRIVACY LEAKAGE DEFENSE SYSTEM

Based on the architecture characteristics and attack paths of federated learning, this article constructs a four layer defense system of “cryptographic protection differential privacy enhancement security aggregation optimization adversarial defense reinforcement”, achieving full process privacy protection from the data layer, transport layer, aggregation layer to the application layer [11].

B. CRYPTOGRAPHIC PROTECTION LAYER: BASIC PRIVACY PROTECTION BASED ON ENCRYPTION TECHNOLOGY

1) Homomorphic Encryption (HE) Technology Optimization
Partial homomorphic encryption (Paillier algorithm) is used to achieve ciphertext aggregation of gradients, supporting addition homomorphic operations and adapting to parameter aggregation scenarios in federated learning. To address the issue of computational overhead, a lattice cipher acceleration chip is introduced to reduce encryption time to 1/20 of traditional schemes. At the same time, combined with model quantization technology, 32-bit floating-point numbers are converted to 8-bit integers to reduce the size of encrypted data [12].

2) Secure Multi-party Computing (MPC) and Secret Sharing
Design a lightweight secure aggregation protocol based on Shamir secret sharing, where the client shards the gradient and distributes it to other participants. The server can only obtain the aggregated global gradient and cannot obtain the original gradient of a single client. By using Beaver triplet preprocessing technology, communication epochs are reduced by 40%, making it suitable for low computing scenarios of edge devices [13].

C. DIFFERENTIAL PRIVACY ENHANCEMENT LAYER: ADAPTIVE PRIVACY PROTECTION MECHANISM

1) Adaptive Privacy Budget Allocation Algorithm
Traditional differential privacy adopts a static privacy budget (ϵ), which can easily lead to excessive or insufficient protection of privacy. This article proposes an adaptive privacy budget allocation algorithm based on model performance and data sensitivity:

(1) Calculate the sensitivity (Δf) of local data on the client side. The higher the sensitivity, the smaller the allocated privacy budget;

(2) Real time monitoring of model accuracy loss, dynamically increasing privacy budget and reducing noise addition when accuracy loss exceeds a threshold;

(3) Adopting a privacy budget accumulation and recovery mechanism to optimize privacy budget configuration in multiple rounds of training [14,15].

2) Hierarchical Differential Privacy Injection

Inject differential privacy noise of different intensities in the three stages of local training, parameter uploading, and global aggregation on the client side: low-intensity noise is added in the local training stage to protect the original data; Add moderate intensity noise during the parameter upload phase to prevent gradient leakage; Add high-intensity noise during the global aggregation stage to resist member inference attacks. Fine control of privacy protection is achieved through layered noise injection [16].

D. SECURITY AGGREGATION OPTIMIZATION LAYER: EFFICIENT AND SECURE PARAMETER AGGREGATION MECHANISM

To address the issue of high communication overhead in traditional secure aggregation protocols, a lightweight aggregation protocol based on sparsity and quantization is proposed

(1) Sparse parameters: Only upload non-zero or important parameter updates to reduce the amount of transmitted data;

(2) Hybrid weighted aggregation: Taking into account both the client sample size and local model accuracy, dynamically adjusting the aggregation weights to reduce the impact of Non IID data;

(3) Security verification: Ensure the integrity of parameter transmission through hash verification to prevent tampering [17,18].

E. ADVERSARIAL DEFENSE REINFORCEMENT LAYER: DYNAMIC ATTACK DETECTION AND RESPONSE

1) Multi Dimensional Attack Detection Mechanism

Build a multidimensional attack detection model based on gradient anomalies, model output bias, and participant reputation:

(1) Gradient anomaly detection: By comparing the similarity between the client gradient and the global gradient, abnormal gradient uploads are identified;

(2) Model output detection: Monitor the output deviation of the global model from the benchmark sample and detect model poisoning attacks;

(3) Reputation rating mechanism: Establish a reputation rating based on privacy-preserving verifiable metrics, such as the contribution to the global model's convergence and the consistency of gradient directions. To distinguish between malicious actors and legitimate clients with low-quality data, a multi-round verification protocol is implemented: clients exhibiting persistent divergent updates are first assigned to a 'quarantine' fine-tuning cluster rather than immediate exclusion, ensuring that the reputation score reflects intent-based behavior patterns without inspecting the raw local data.

2) Real Time Attack Response and Isolation

When an attack behavior is detected, the response mechanism is immediately activated: isolate the malicious client, discard abnormal parameters, and reinitialize the global model; Simultaneously update the reputation scores of the participating parties to prevent malicious clients from participating in training again. Build a federated learning adversarial defense loop through dynamic detection and real-time response [19,20].

IV. DESIGN OF ETHICAL GOVERNANCE PATH FOR FEDERATED LEARNING

A. CORE PRINCIPLES OF ETHICAL GOVERNANCE IN FEDERATED LEARNING

Based on the general principles of AI ethics and the distributed nature of federated learning, four core principles are established:

- (1) Privacy First Principle: Always prioritize data privacy and individual rights, following the principles of “data minimization” and “purpose limitation”;
- (2) The principle of fairness and justice: safeguarding the equal rights and interests of all parties involved, avoiding algorithmic bias and data discrimination;
- (3) The principle of transparency and interpretability: clarify the model training process and parameter interaction mechanism to achieve interpretability of the decision-making process;
- (4) Principle of Traceability of Responsibility: Establish a mechanism based on a Trusted Execution Environment (TEE) or a decentralized identity (DID) ledger. This technical infrastructure functions as a ‘break-glass’ auditing layer: under normal operations, secure aggregation maintains absolute anonymity; however, in the event of a verified systemic breach, the governance framework permits the decryption of participation logs through a multi-signature consensus of the ethical committee, ensuring accountability without compromising the technical goal of secure aggregation during the model training phase.

B. CONSTRUCTION OF FOUR DIMENSIONAL ETHICAL GOVERNANCE PATH

1) Technical Compliance Path: Ethical Embedding of Privacy Protection Technologies

- (1) Technology selection compliance: Priority should be given to defense technologies that have passed privacy compliance certification (such as differential privacy and secure multi-party computing) to ensure that the technology implementation complies with regulatory requirements such as the Personal Information Protection Law and the Data Security Law;
- (2) Privacy Impact Assessment (PIA): Conduct a full process privacy impact assessment before deploying the federated learning system, identify privacy risks, and develop prevention and control measures;
- (3) Interpretability optimization: By using techniques such as model distillation and attention mechanisms, the interpretability of the global model is improved to meet ethical transparency requirements.

2) Ethical Norm Path: Ethical Constraints on Participant Behavior

- (1) Informed consent mechanism: Establish a multi-party informed consent process, clarify the scope of data use, model training purposes, privacy protection measures, and ensure the right to know and choose of all parties involved;
- (2) Establish a cross-disciplinary ethics review committee that defines the ‘Ethics-to-Parameter’ mapping. This committee sets the global ‘Privacy Sensitivity Thresholds’ which

are then programmatically ingested by the adaptive differential privacy layer, ensuring that the technical budget (ϵ) directly reflects the ethical risk level assigned to specific data categories (e.g., medical vs. financial), with a focus on issues such as data rights, algorithm fairness, and responsibility definition;

(3) Ethics training system: Provide federal learning ethics training for participating technical and management personnel to enhance ethical awareness and compliance capabilities.

3) Organizational Governance Path: Organizational Guarantee for Collaborative Governance

- (1) Multi party collaborative governance architecture: Establish a collaborative governance organization composed of data providers, technology developers, regulatory agencies, and ethical experts, clarifying the responsibilities and authorities of each party;
- (2) Data equity distribution mechanism: Based on the data contribution of participants, establish a fair model profit and equity distribution mechanism to avoid “data monopoly” and equity imbalance;
- (3) Privacy incident emergency mechanism: Develop an emergency response plan for privacy breaches, clarify the procedures for reporting, investigating, and handling incidents, and reduce the harm of privacy breaches.

4) Regulatory Collaboration Path: Institutional Guarantee for Full Process Supervision

- (1) Hierarchical classification supervision: Implement hierarchical classification supervision based on the sensitivity of data (such as medical and financial data being highly sensitive), and develop differentiated privacy protection requirements;
- (2) Regulatory Sandbox Mechanism: Establish a federated learning regulatory sandbox to support technological innovation and compliance testing, balancing innovation and regulation;
- (3) Cross departmental collaborative supervision: Strengthen the collaborative supervision of departments such as cyberspace, industry and information technology, healthcare, and finance, form a regulatory synergy, and crack down on illegal privacy breaches.

C. “TECHNOLOGY ETHICS REGULATION” TRINITY GOVERNANCE FRAMEWORK

Integrating the three dimensions of technological defense, ethical norms, and regulatory collaboration, a three in one governance framework is constructed: based on technological defense, providing technical support for privacy protection; Ethical standards as the core, clarifying the code of conduct for participants; Regulatory collaboration ensures the implementation and execution of governance measures. Through the collaborative linkage of the three, achieve the sustainable development of “safety, compliance, and ethics” in federated learning.

V. EMPIRICAL EXPERIMENT AND RESULT ANALYSIS

A. EXPERIMENTAL DESIGN

1) Experimental Scenarios and Dataset

Select two sensitive scenarios, healthcare and finance, to conduct experiments:

(1) Medical scene: diabetes retinopathy detection data set (Messidor), containing 1200 fundus images, was used to simulate the joint training and diagnosis model of multiple hospitals;

(2) Financial scenario: Using the credit card fraud detection dataset (UCICredCard), which includes 284807 transaction records, simulate the joint training of risk control models by multiple banks.

2) Comparison Scheme and Evaluation Indicators

The comparative schemes include: traditional FedAvg algorithm, differential privacy defense only, secure aggregation defense only, and the four layer defense system proposed in this paper.

The evaluation indicators include: privacy breach risk (success rate of member inference attacks, accuracy of gradient reconstruction), model performance (accuracy, F1 score), and computational cost (training time, communication cost).

B. EXPERIMENTAL RESULTS AND ANALYSIS

1) Comparison of Privacy Defense Effects

Table 1 compares the privacy defense effects of different schemes. The results show that the four layer defense system in this article reduces the success rate of member inference attacks from 89.2% to 16.9%, the accuracy of gradient reconstruction from 92.7% to 11.3%, and the risk of privacy leakage by 72.3%, which is significantly better than a single defense scheme.

2) Model Performance and Computational Cost Comparison

Table 2 compares the model performance and computational cost of different schemes. The results show that the model accuracy of our proposed approach in medical scenarios is 92.1%, which is only 3.2% lower than FedAvg; The F1 score of the financial scenario is 94.5%, only 3.5% lower than FedAvg. Meanwhile, through lightweight optimization, training time and communication overhead were reduced by 42.6% and 58.3% respectively, achieving a balance between privacy performance efficiency.

3) Verification of the Effectiveness of Ethical Governance Pathways

By simulating privacy breaches, verify the effectiveness of ethical governance pathways. The results show that under the joint action of technical compliance, ethical norms, organizational governance, and regulatory coordination, the response time for privacy breach incidents has been shortened from 48 hours to 6 hours, the accuracy of responsibility definition has reached 100%, and the compliance rate of

participants has increased to 98.7%, verifying the feasibility of the ethical governance path.

4) Experimental Conclusion

The empirical experimental results show that the four layer privacy leakage defense system constructed in this paper can effectively resist attacks such as gradient reversal and member inference, while controlling the model accuracy loss within 3.5%, optimizing the privacy performance trade-off; The four-dimensional ethical governance path can achieve the synergy of technology, ethics, and regulation, providing theoretical frameworks and scalable compliance and ethical guarantees for potential large-scale applications by demonstrating robustness in diverse sector-specific benchmarks.

VI. RESEARCH CONCLUSION AND PROSPECT

A. RESEARCH FINDINGS

This article takes privacy security and ethical governance in federated learning as the research object, and draws the following core conclusions:

(1) The distributed architecture of federated learning poses multi-dimensional privacy risks such as gradient reversal, member inference, and model poisoning, and a single defense technology cannot achieve comprehensive protection;

(2) The four layer defense system of “cryptographic protection differential privacy enhancement security aggregation optimization adversarial defense reinforcement” constructed can reduce the risk of privacy leakage by 72.3%, while controlling the loss of model accuracy within 3.5%, achieving a balance between privacy and performance;

(3) The four-dimensional ethical governance path of “technical compliance ethical norms organizational governance regulatory synergy” designed can effectively balance technological innovation and privacy protection, providing compliance and ethical guarantees for federated learning;

(4) Empirical experiments have verified the effectiveness of defense mechanisms and the feasibility of governance pathways, providing practical references for the application of federated learning in sensitive fields such as healthcare and finance.

B. POLICY SUGGESTIONS

1) Enterprise Level

(1) Prioritize the use of the four layer defense system proposed in this article, and optimize privacy protection technology configuration based on scene characteristics;

(2) Establish internal ethical review and privacy impact assessment mechanisms to ensure compliance of federal learning programs;

(3) Strengthen collaborative governance among participants, clarify the definition of data rights and responsibilities, and build a trust mechanism.

TABLE 1. Comparison of Privacy Defense Effects of Different Schemes

Defense Scheme	Membership Inference Attack Success Rate	Gradient Reconstruction Accuracy	Privacy Leakage Risk Reduction Rate
Traditional FedAvg	89.2%	92.7%	—
Single Differential Privacy	45.6%	53.2%	48.9%
Single Secure Aggregation	38.7%	47.8%	54.5%
Proposed Scheme in This Paper	16.9%	11.3%	72.3%

TABLE 2. Comparison of Model Performance and Computational Overhead

Defense Scheme	Accuracy (Medical Scenario)	F1-Score (Financial Scenario)	Training Time (min)
Traditional FedAvg	95.3%	98.0%	128.5
Single Differential Privacy	90.5%	93.2%	156.3
Single Secure Aggregation	91.2%	93.8%	142.7
Proposed Scheme in This Paper	92.1%	94.5%	73.7

TABLE 3. Experimental Parameter Configuration

Parameter Category	Parameter Name	Specific Configuration
Basic FL Setting	Federated Learning Type	Horizontal Federated Learning
Basic FL Setting	Global Iterations	200 rounds
Basic FL Setting	Local Epochs	5 epochs per client
Basic FL Setting	Batch Size	64
Model Setting	Medical Task Model	ResNet-18
Model Setting	Financial Task Model	LightGBM Classification Model
Privacy Parameter	Differential Privacy Budget ϵ	Adaptive dynamic adjustment (1.0–3.0)
Privacy Parameter	Gaussian Noise Scale	Adaptive injection with hierarchical intensity
Encryption Setting	Encryption Algorithm	Paillier Partial Homomorphic Encryption

2) Regulatory Level

(1) Develop privacy protection regulations for federal learning programs, clarify defense technology standards and ethical governance requirements;

(2) Promote regulatory sandbox mechanisms to support innovation and compliance testing in federated learning technology;

(3) Strengthen cross departmental collaborative supervision and severely crack down on illegal privacy breaches.

C. RESEARCH LIMITATIONS AND FUTURE PROSPECTS

1) Research Limitations

(1) The experimental scenario focuses on health care and finance, and the adaptability of industrial Internet, smart city and other scenarios needs further verification;

(2) The quantitative evaluation system for ethical governance path is not yet perfect and needs further optimization;

(3) Without considering the impact of quantum computing on existing cryptographic defense technologies, further research is needed on quantum security defense mechanisms.

2) Future Outlook

(1) Expand research on cross scenario defense mechanisms to adapt to diverse scenarios such as industry and government affairs;

(2) Constructing a quantitative evaluation system for ethical governance in federated learning to achieve precise measurement of governance effectiveness;

(3) Research on federated learning defense technologies for quantum security to address the security challenges of future quantum computing;

(4) Explore the deep integration of federated learning with privacy computing, blockchain, and other technologies to further enhance privacy security and governance effectiveness.

Federated learning, as a key technology for the circulation of data elements, is at the core of achieving sustainable development in terms of privacy, security, and ethical governance. The research results of this article provide theoretical support and practical path for the synergy between technological innovation and ethical norms in federated learning. In the future, it is necessary to continue to deepen the cross research of technological defense and ethical governance, promote the large-scale implementation of federated learning under the premise of compliance, safety, and fairness, and empower the high-quality development of the digital economy.

AUTHOR CONTRIBUTIONS

Conceptualization – Jiahui Liu, Muran Mao and Xiaomei Dong; methodology – Jiahui Liu, Muran Mao and Xiaomei Dong; investigation – Jiahui Liu, Muran Mao and Xiaomei Dong; writing-original draft preparation – Jiahui Liu, Muran Mao and Xiaomei Dong. All authors have read and agreed to the published version of the manuscript.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

FUNDING

This research received no external funding.

ACKNOWLEDGEMENTS

Not applicable.

REFERENCES

- [1] S. Umar, A. Alagha, R. Mizouni, et al., "A two-sided client-server matching mechanism for resilient Federated Learning," *Journal of Network and Computer Applications*, vol. 250, Art. no. 104476, 2026, doi: 10.1016/j.jnca.2026.104476.
- [2] J. Zhang, X. Zhan, X. Wang, et al., "Federated learning-based user behavior prediction model for rural live e-commerce," *Alexandria Engineering Journal*, vol. 141, pp. 413–427, 2026, doi: 10.1016/j.aej.2026.03.027.
- [3] X. Lai, Z. Zhang, and S. Zheng, "FLAME: Federated learning on heterogeneous and long-tailed data via adaptive multi-faceted feature embeddings," *Future Generation Computer Systems*, vol. 182, Art. no. 108488, 2026, doi: 10.1016/j.future.2026.108488.
- [4] J. Zheng, X. Shen, S. Zhao, et al., "FedCDC: Communication-efficient clustered federated learning for heterogeneous IoT edge networks," *Internet of Things*, vol. 37, Art. no. 101925, 2026, doi: 10.1016/j.iot.2026.101925.
- [5] E. Beltrán M T, E. Gash, G. Bovet, et al., "Asynchronous Cache-based Aggregation with Fairness and Filtering for Decentralized Federated Learning," *Computer Networks*, vol. 281, Art. no. 112225, 2026, doi: 10.1016/j.comnet.2026.112225.
- [6] A. Lameesa, M. Alam B S, S. Ahmed F, et al., "Federated learning for sustainable IoT: Decentralized intelligence and energy-efficient applications," *Energy Reports*, vol. 15, Art. no. 109145, 2026, doi: 10.1016/j.egy.2026.109145.
- [7] R. Chen, D. Bao, N. Lu, et al., "Robust federated learning for dynamic and heterogeneous environments: an adaptive client selection approach," *Expert Systems With Applications*, vol. 318, Art. no. 131992, 2026, doi: 10.1016/j.eswa.2026.131992.
- [8] L. Feng, M. Liu, Z. Jing, et al., "A privacy-preserving and byzantine-robust consensus for blockchain Federated Learning," *Engineering Applications of Artificial Intelligence*, vol. 175, Art. no. 114589, 2026, doi: 10.1016/j.engappai.2026.114589.
- [9] K. Singh P, M. Verma, D. Tyagi K, et al., "FedHC: Enhanced federated learning with Hessian and cosine correlation for proximal correlation," *Knowledge-Based Systems*, vol. 341, Art. no. 115775, 2026, doi: 10.1016/j.knosys.2026.115775.
- [10] L. Su, J. Guo, J. Liu, et al., "Fair client selection for multi-task federated learning in mobile edge networks," *Information Processing and Management*, vol. 63, no. 6, Art. no. 104748, 2026, doi: 10.1016/j.ipm.2026.104748.
- [11] S. An, K. Zhang, Y. Su, et al., "Privacy-preserving medical decision-making and service differentiation in a federated learning framework," *Omega*, vol. 143, Art. no. 103561, 2026, doi: 10.1016/j.omega.2026.103561.
- [12] A. Yang, S. Luo, K. Zhu, et al., "Hierarchical privacy-preserving federated recommendation via adaptive multi-level personalization and dynamic aggregation," *Physica A: Statistical Mechanics and its Applications*, vol. 690, Art. no. 131464, 2026, doi: 10.1016/j.physa.2026.131464.
- [13] H. Huang, Q. Zhou, Y. Hao, et al., "AFCG: A privacy-preserving federated learning framework against chained malicious attacks for vehicular networks," *Ad Hoc Networks*, vol. 187, Art. no. 104225, 2026, doi: 10.1016/j.adhoc.2026.104225.
- [14] Y. He, W. Wang, X. Chen, et al., "Federated learning enhanced spatial and temporal attention mechanism for multivariate time series anomaly detection," *Applied Soft Computing*, vol. 196, Art. no. 115048, 2026, doi: 10.1016/j.asoc.2026.115048.
- [15] Z. Zhang, R. Li, K. Guo, et al., "Personalized federated learning with personalized knowledge distillation based on local empirical risk," *Information Fusion*, vol. 133, Art. no. 104269, 2026, doi: 10.1016/j.inffus.2026.104269.
- [16] N. Naveenkumar, T. Subarna, S. Pragadeeswaran, et al., "Federated learning based hybrid DL-based transformer model for heart disease detection with Explainable AI," *Biomedical Signal Processing and Control*, vol. 120, no. PB, Art. no. 110076, 2026, doi: 10.1016/j.bspc.2026.110076.
- [17] E. Akpınar, M. Taskiran, and B. Bolat, "PARS: Performance-driven adam-based resilient scaffold for federated learning," *Information Sciences*, vol. 744, Art. no. 123374, 2026, doi: 10.1016/j.ins.2026.123374.
- [18] W. Algethami, G. Wu, F. Alshami, et al., "Entropy-guided meta-learning defense against data poisoning attacks in blockchain-assisted federated learning," *Information Sciences*, vol. 745, Art. no. 123389, 2026, doi: 10.1016/j.ins.2026.123389.
- [19] W. Li, A. Halimi, J. Vaidya, et al., "Privacy-preserving verification of preprocessing in federated learning for genomic data," *JAMIA Open*, pp. 9(2), 2026, doi: 10.1093/jamiaopen/ooag040.
- [20] A. Beznosikov, G. Kormakov, A. Grigorievskiy, et al., "Exploring New Frontiers in Vertical Federated Learning: the Role of Saddle Point Reformulation," *Journal of Optimization Theory and Applications*, vol. 209, no. 1, pp. 18, 2026, doi: 10.1007/s10957-026-02961-z.