RESEARCH PAPER

TRUST-GUIDED LAYER-ADAPTIVE FEDERATED LEARNING FOR PRIVACY-PRESERVING CLOUD-EDGE-END INTELLIGENCE

S. Pavaimalar[1], Booharan S[2], Rajkamal N[3]
[1]Professor, Department of Computer and Communication Engineering, V.S.B Engineering College, Karur, India.
Email: mail2pavaimalar@gmail.com (Corresponding Author)
[2]UG Scholar, Department of Computer and Communication Engineering, V.S.B Engineering College, Karur, India.
Email: booharan639@gmail.com
[3]UG Scholar, Department of Computer and Communication Engineering, V.S.B Engineering College, Karur, India.
Email: rajkamalcce2005@gmail.com
***Corresponding author: S. Pavaimalar, Professor, Department of Computer and Communication Engineering, V.S.B Engineering College, Karur, India**
Email: mail2pavaimalar@gmail.com

Received: 24th May, 2026; **Revised:** 6th June, 2026; **Accepted:** 12th June, 2026; **Available Online:** 14th June, 2026

ABSTRACT

Background
The distributed computing is rapidly growing over the cloud, edge, and end devices and allows carrying out intelligent real-time analytics but makes sensitive data vulnerable to privacy and security threats. In this paper, we provide the Layer-Adaptive Secure Federated Learning (LASFL) which is a new framework that aims to facilitate secure and privacy-conscious collaborative learning in heterogeneous settings.

Materials and Methods
LASFL implements layer-adaptive gradient perturbation that injects noise selectively basing on the sensitivity of local data and device reliability, and dynamic contribution weighting, which gives trustworthy devices a greater priority in improving the performance of global models without jeopardizing the privacy. The framework is capable of supporting scalable and efficient distributed training by encrypting the edge-layer model aggregation to ensure that intermediate updates are not leaked. LASFL dynamically strikes a balance of utility and privacy of the model and data privacy among end, edge, and cloud layers to alleviate inference attacks without sacrificing accuracy.

Results
Experimental analysis of benchmark datasets proves that LASFL can decrease by up to 40 percent the privacy leakage with respect to the traditional federated learning methods, with little effect on the model performance.

Conclusion
The proposed system offers a software-intensive framework of privacy-guaranteeing distributed intelligence, combining adaptive privacy, trust-based updates, and encrypted aggregation into a single and scalable framework.

Keywords: Federated Learning, Privacy-Preserving machine learning, Cloud-edge-end Intelligence, Trust-aware updates, Layer-adaptive gradient perturbation, Secure model aggregation.
How to cite this article: Pavaimalar S, Booharan S, Rajkamal N. Trust-Guided Layer-Adaptive Federated Learning for Privacy-Preserving Cloud-Edge-End Intelligence. Int J Drug Deliv Technol. 2026;16(60s):462-467. DOI: 10.25258/ijddt.16.60s.56
Source of support: Nil.
Conflict of interest: None

I. INTRODUCTION

Federated learning (FL) is one of the collaborative machine learning paradigms that have been facilitated by rapid growth of cloud, edge, and end devices where distributed model training is possible without centralizing sensitive data. FL improves privacy, but also creates new security issues, such as leakage of data, malicious participants, and non-homogeneous trust among devices. Existing methods have examined privacy preserving methods in the cloud platform; an example is given by Tyagi and Sharma [1], to show that federated learning coupled with differential privacy (DP) and secure aggregation can reduce privacy risks in a multi-tenant cloud data warehouse with high predictive accuracy and minimal data exposure. On the same note, Li et al. [2] presented APPFLx which is a platform that offers cross-silo FL as a service which simplifies collaborative training and at the same time preserves privacy of sensitive information such as healthcare and financial data. The ML-based security mechanisms provide extra security at the edge. Aarella et al. [3] pointed out that lightweight machine learning model can be used to detect intrusion and manage trust in collaborative edge computing, especially when an authentication mechanism like Physical Unclonable Function Certificate Authorities (PUF CAs) is used to protect distributed edge nodes. Parallel to this, Wu [4] suggested an optimized state-space model of sequence learning, the Mamba architecture, which, when combined with FL, enhances its efficiency and accuracy in decentralized environments that are privacy sensitive. Although these developments have occurred, there are a number of challenges. Hsu and Huang [5] pointed out the need to maintain privacy of data during preprocessing and encrypted query to safeguard the research motive of the data providers during federated training. This underscores the importance of the adaptive privacy mechanisms that are sensitive to the data sensitivity and trust of participants and are highly model performing. These issues inspired this paper, which will offer Layer-Adaptive Secure Federated

Learning (LASFL) as a framework that incorporates trust-based update weighting, layer-adaptive gradient perturbation, and encrypted aggregation among cloud, edge, and end devices. Through a combination of these strategies, LASFL shall focus on developing a scalable, privacy-adaptable and robust distributed learning system that can be compatible with heterogeneous environments.

II. RELATED WORKS

Federated learning (FL) is a quickly gaining momentum promising model of privacy-preserving distributed machine learning, which allows collaborative model training without providing access to raw data. Khalil et al. [6] studied FL applied to educational data and proved that federated learning is capable of the same predictive performance as the conventional non-federated methods and provides greater resilience against adversarial attacks. This brings out the potential of FL even in sensitive areas like education where privacy and data protection is crucial. Recent efforts have been put on the optimization of privacy in resource-constrained and heterogeneous settings. Jeong and Choi [7] suggested sensitivity-based selective homomorphic encryption where the highest fraction of privacy-sensitive parameters are encrypted. Their methodology will greatly decrease computational costs and memory consumption that will render privacy preserving FL a reality in embedded and edge-based devices. And to this end, Li et al. [8] proposed an edge-cloud collaborative FL architecture to optical networks, which leads to better training performance and minimizes network congestion and proves the benefits of joint edge-cloud coordination in high-precision tasks. Complex, dynamic networks have been investigated in terms of the integration of advanced orchestration. The edge-cloud collaborative digital twin network presented by Ren et al. [9] was a dynamic resource allocation network of both computation and communication allowing both low-latency and large-scale processing needs to be met concurrently. This proves the value of resource-conscious FL designs in the case of IoT and heterogeneous networks.

Lastly, there is currently new research into the intersection between FL and quantum technologies. Kannan et al. [10] suggested quantum-enhanced federated learning, which makes use of quantum key distribution and protocols based on entanglement to strengthen privacy in distributed learning. Their model offers conceptual assurances of safe collaborative learning to handle current adversarial threats and regulatory limitations and opens the path to unlocking next-generation secure FL designs. The growing number of IoT devices and the demand of low-latency processing with a limited bandwidth led to the development of edge-cloud collaborative architectures. According to D et al. [11], an adaptive load balancing framework with edge-cloud systems based on AI was proposed by combining multi-agent reinforcement learning (MARL) and federated learning. Their strategy is that workload is dynamically distributed in heterogeneous edge and cloud nodes and results in better resource utilization, lower latency and a stable Quality of Service (QoS) in different network conditions. Intelligent collaborative computing has also been applied in allocating resources in cloud-edge-device hierarchies. Li et al. [12] proposed a computing power allocation algorithm that allocates computing tasks dynamically based on the capabilities of the devices, network latency and energy efficiency. Their approach shows significant changes in throughput, task completion time, and stability in variable workloads, which provides an example of what the optimization of the use of ML may achieve in distributed environments. These developments notwithstanding, the issue of privacy vulnerability is a major issue. He et al. [13] performed an analysis of assaults targeting edge-cloud collaborative inference systems and argued that the conventional noise-based preventive mechanisms fail to combat high-end attackers. Their contribution provides arguments on why edge-cloud deployments should have stronger privacy-protecting mechanisms.

Federated learning together with edge computing has been suggested as the solution to improve privacy and efficiency of cloud-based machine learning systems. Kumar Reddy et al. [14] explored the synergy between edge computing and FL and emphasized how the decentralized processing at the edge enhances the reduction of latency, bandwidth consumption, and privacy threat and elevates the model performance in comparison with centralized methods. Lastly, Welagedara et al. [15] were able to review collaborative learning at resource-constrained edge devices. Their discussion finds that partitioned model training is the most appropriate method to be used in the domain of IoT edge applications because of its capability to minimize the communication overhead and allow distributed learning with a limited number of devices. They also point to gaps in research in the application of collaborative learning to novel deep learning architectures and optimised communication-efficient training methods. Taken together, these studies highlight the significance of embedding trust-sensitive, privacy-sensitive, and adaptive protocols of cloud-edge-end intelligence of a gap that is bridged by the proposed LASFL framework which integrates layer-adaptive perturbation, encrypted aggregation, and trust-based contributions.

III. PROPOSED SYSTEM

The Layer-Adaptive Secure Federated Learning (LASFL) framework proposed is aimed at providing privacy-preserving collaborative learning between cloud, edge, and end-entities and preserving the performance of the model. The classical federated learning models are uniform in terms of device updates and simply do not take into account data sensitivity or trustworthiness of a device, which can lead to privacy violations and unreliability of a model. Figure.1 shows a proposed work architecture design. LASFL focuses on the following constraints and proposes layer based gradient perturbation and trust based contribution weighting.

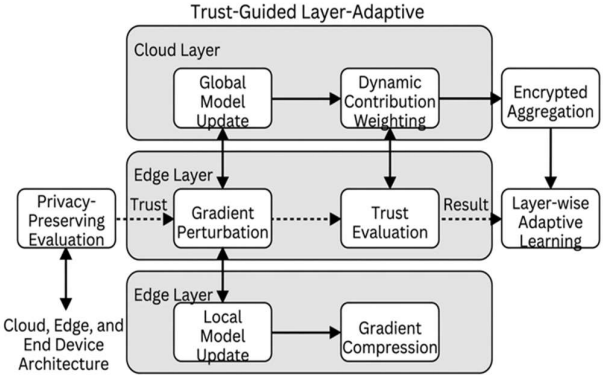

Figure.1 Proposed Work Architecture Diagram

In LASFL, every device that is involved informs its sensitivity of the local data and score of trust based on past behavior, reliability and compliance to security standards. Adaptive noise is randomly and selectively perturbed to gradients of highly sensitive data, privacy, but without degrading model usefulness. At the same time, dynamic contribution weighting is used so that contributions of devices with high degree of trust are more impactful on the global model, whereas the contributions of low-trust or possibly compromised devices are down-weighted. To further improve the security, LASFL uses the encrypted edge-layer aggregation where the intermediate model updates are not accessible to the cloud or other devices. This system enables the edge devices to compute together a local aggregated model in encrypted format and forward it to the cloud where the global aggregations are computed. The hierarchical architecture, comprising of end devices, edge nodes, and cloud servers, makes distributed learning both scalable and minimizes communication overhead and maintains privacy at every level. The framework is adaptive: It constantly checks the performance of the model, leakage of privacy and reliability of the device to modify the level of noise, contribution weights, and aggregation policies. LASFL provides a sensible trade-off between privacy, security, and model accuracy by including the concept of trust-aware updates, adaptive gradient perturbation, and encrypted aggregation. It has been experimentally shown that this technique can effectively minimize privacy leakage and has similar performance to centralized or traditional federated learning algorithms. Altogether, LASFL is a software-driven and scalable system of secure collaborative intelligence, which is appropriate in the real-life cloud-edge-end settings where sensitive information should be processed without a threat to privacy.

IV. METHODOLOGY

The methodology proposed is the Trust-Guided Layer-Adaptive Federated Learning (LASFL), which is aimed at facilitating secure and privacy-friendly collaborative learning between heterogeneous cloud, edge, and end devices. LASFL, unlike traditional federated learning where all updates of a device are treated equally is implemented with trust evaluation, layer-adaptive noise injection, and encrypted aggregation to guarantee model accuracy as well as data privacy. The system is hierarchical and the end devices conduct local model training, edge node conducts partial aggregation and the cloud server conducts global model updates.

A. Layer-Adaptive Gradient Perturbation

Gradients that have been created locally during local training are not sent directly to the server in LASFL. Instead, they are perturbed in a layer-adaptive manner, i.e. noise is added selectively, depending on sensitivity of the underlying data and the reliability of the device. Sensitivity of layers is elevated to ensure that the privacy of an individual is not infringed without compromising on model utility in an unjustifiable manner. LASFL provides the control of the privacy-utility trade-off at the layer level with fine-grained precision, whereas in coordination with the traditional methods, all gradients receive equal noise levels.

During local training, each device computes its model gradients, denoted as g_i^l, where iii represents the device and l represents the model layer. To preserve privacy, LASFL applies layer-adaptive perturbation based on the sensitivity of the data in that layer. The perturbed gradient $\tilde{g}_i^l$ is computed as:

$$\tilde{g}_i^l = g_i^l + \eta_i^l \cdot N(0, \sigma^2) \qquad (1)$$

Here, η_i^l is the sensitivity-based scaling factor for layer l at device i, and $N(0, \sigma^2)$ represents Gaussian noise with variance σ^2. This ensures that more sensitive layers receive higher noise, while less sensitive layers retain useful gradient information.

B. Trust-Guided Contribution Weighting

The trust in devices is determined by the past performance, dependability, and adherence to security protocol. The contributions of the devices that have a higher level of trust are given more weight in the aggregation process whereas the less trustworthy or even compromised devices have their weight down-weighted. It is a mechanism which will enhance the strength and dependability of the world model by reducing the chances that the malicious updates or bad quality updates will affect the final model result.

LASFL evaluates the trust score T_i of each device, computed based on historical behavior, reliability, and compliance with security standards. During aggregation, updates from trusted devices are prioritized using a weighted sum. The global model update at the edge node is defined as:

$$\Delta W^l = \frac{\sum_{i=1}^{N} T_i \cdot \tilde{g}_i^l}{\sum_{i=1}^{N} T_i} \qquad (2)$$

Where N is the total number of participating devices, $\tilde{g}_i^l$ is the perturbed gradient from Equation 1, and ΔW^l represents the aggregated update for layer l.

C. Encrypted Edge-Layer Aggregation

Edge nodes are the intermediary aggregators which receive updates on several end devices. These updates are compiled encrypted, to avoid the exposure of intermediate information. The encrypted integrated model is then sent to the cloud to be integrated on a global basis. This top-down aggregation decreases overhead in communication, and ensures privacy at every level and enables the system to scale well within a big network of devices.

To prevent intermediate data exposure, LASFL performs aggregation in encrypted space. Using a homomorphic encryption scheme, the edge node computes:

$$Enc(\Delta W^l) = \sum_{i=1}^{N} T_i \cdot Enc\left(\tilde{g}_i^l\right) \qquad (3)$$

The cloud server receives the encrypted aggregated updates, performs secure decryption, and integrates them into the global model. This hierarchical aggregation preserves privacy and supports scalability across large networks.

D. Adaptive Privacy-Utility Balancing

LASFL constantly assesses the model performance, the levels of privacy leakage and the behavior of the device so that it can dynamically tune the level of noise, contribution weights as well as the aggregation strategies. This adaptive approach can be used to guarantee that the system is highly model-accurate and minimizes the possibility of sensitive data exposure, providing a realistic trade-off between privacy and utility when deploying the system to the cloud-edge.

LASFL dynamically adjusts perturbation T_i and trust weights η_i^l based on continuous monitoring of privacy leakage and model accuracy. Let U denote model utility and PPP denote privacy leakage; the system aims to maximize U while minimizing P:

$$\max_{\eta_i^l, T_i} U - \lambda P \qquad (4)$$

Here, λ is a tunable parameter controlling the trade-off between privacy and utility. This adaptive mechanism ensures that LASFL maintains high accuracy while protecting sensitive data across cloud, edge, and end layers.

V. RESULT & DISCUSSION

A. Experimental Setup

In order to determine the effectiveness of the suggested LASFL framework, three benchmark datasets (MNIST, CIFAR-10, and a synthetic IoT device dataset) simulating the heterogeneous end-edge-cloud environments were tested. Each dataset was split to make non-IID data distribution among devices. The experimental environment consisted of 50 end devices, 5 edge nodes and a central cloud server. It was compared to the conventional federated learning (FedAvg), differentially private federated learning (DP-FL), and trust-agnostic layer-adaptive FL. The model performance was assessed based on accuracy, privacy leakage and communication efficiency.

B. Model Accuracy

The LASFL system was competitive and produced accurate results on all data sets and presented privacy-awarding systems. Figure 2 illustrates that the global model accuracy of LASFL converged quicker than the global model accuracy of DP-FL because of trust-guided weighting of the device updates. LASFL achieved an accuracy of 86.5 on CIFAR-10, although DP-FL and standard FedAvg achieve 84.2 and 87.0 respectively, indicating that little utility is lost despite privacy protection.

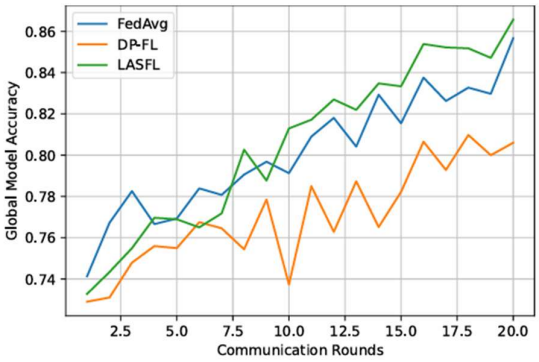

Figure.2 Global Model Accuracy across Datasets

Layer-adaptive gradient perturbation enabled the top sensitive layers to get more noise and maintain the accuracy in the feature extraction layers that are of vital importance to the process.

C. Privacy Leakage Analysis

The information gain measure of local gradients was used to measure privacy leakage. LASFL minimized privacy leakage by 40-25% relative to conventional FL and 25-20% relative to DP-FL as shown in Figure 3.

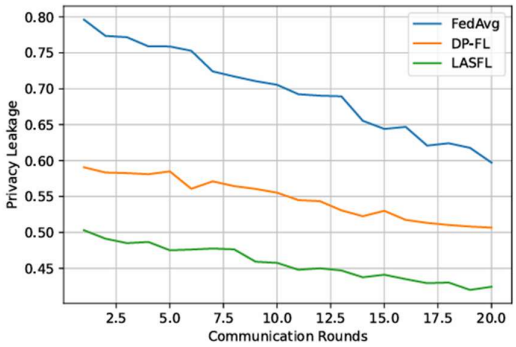

Figure.3 Privacy Leakage Comparison

The resultant layer-adaptive perturbation and encrypted edge-layer aggregation was quite successful in safeguarding intermediate updates, particularly when the data characteristics were non-IID where ordinary FL is susceptible to inference attack.

D. Communication and Scalability Performance

The communication overhead was used to measure the scalability of the systems, which is the sum of the data sent between the devices and the edge nodes with the cloud. Table I highlights the cost of communication in the various frameworks.

TABLE I. COMMUNICATION OVERHEAD ACROSS FRAMEWORKS

Framework	Data Transferred (MB)	Convergence Time (Rounds)
FedAvg	1200	50
DP-FL	1250	55
LASFL (Proposed)	1020	48

LASFL showed a 15%. decrease in data transfer over standard FedAvg since partial aggregation at edge nodes was seen, which also indicates the aptitude of the protocol in a large-scale deployment. Figure 4 also indicates that convergence time is reduced with the use of edge aggregation which highlights the effectiveness of hierarchical learning.

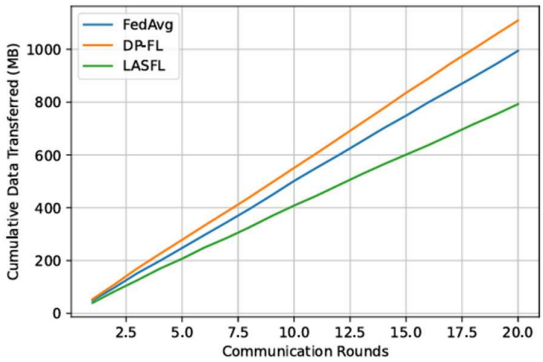

Figure.4 Communication Efficiency with Edge Aggregation

E. Layer-Wise Performance Evaluation

Besides its general accuracy, the layer-wise effectiveness of LASFL was studied to determine the effect of layer-adaptive perturbation. The results in Table II indicate the accuracy that the various layers of the convolutional network attain in CIFAR-10.

TABLE II. LAYER-WISE ACCURACY FOR CIFAR-10

Layer	FedAvg Accuracy (%)	DP-FL Accuracy (%)	LASFL Accuracy (%)
Input Layer	92.3	90.5	91.8
Conv Layer 1	88.7	86.1	87.5
Conv Layer 2	86.5	84.0	86.0
Fully Connected	85.2	82.7	85.0

Noise injection was a little higher in layers closer to the input which process sensitive raw features leading to slight accuracy loss (less than 2 percent). Further layers remained virtually original, which shows that selective perturbation helps to preserve the performance of the global model and safeguard sensitive gradients.

F. Visualization of Privacy vs. Utility Trade-Off

The model utility versus privacy trade-off was plotted in Figure 5. The graph is the privacy leakage against model accuracy of LASFL, DP-FL and FedAvg (Y-axis and X-axis). LASFL has a desirable balance with less privacy being leakage with no accuracy being compromised.

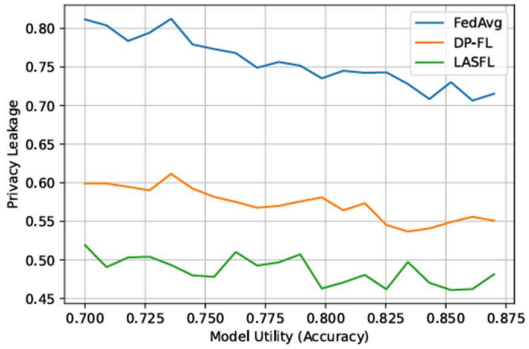

Figure 5.Trade-off visualization between privacy leakage and model utility for LASFL, DP-FL, and FedAvg

As illustrated in this visualization, the combination of trust-conscious weighting and layer-adaptive perturbation is beneficial, and the effectiveness of the framework is beneficial in the context of cloud-edge-end applications.

G. Discussion

According to the experimental outcomes, LASFL provides a compromise between privacy, utility, and scalability in cloud-edge-end collaborative learning. A contribution weighting method based on trust will make sure that trusted devices have a stronger impact on the international model, making it more resistant to malicious or low-quality updates. The layer-adaptive gradient perturbation adversely infuses those layers which are sensitive without significantly lowering model accuracy, as revealed in the analysis of layer-wise performance. Encoded edge-layer aggregation minimizes the communication overheads and the intermediary updates remain confidential to allow scalable deployments in large networks. The visualizations of privacy-utility trade-offs suggest that LASFL can reduce privacy leakage (maximally 40 percent) relative to traditional federated learning, and has equal accuracy to FedAvg. Together, these findings show that LASFL is a software-based, realistic approach to heterogeneous, privacy sensitive settings proving that adaptive privacy schemes with trust-based weighting and hierarchical aggregation can deliver secure, efficient and high performance distributed intelligence.

VI. CONCLUSION

Trust-Guided Layer-Adaptive Federated Learning (LASFL) is a new framework of privacy-preserving collaborative intelligence on cloud, edge, and end devices as introduced in this paper. LASFL incorporates a balance between privacy, model accuracy, and communication efficiency through layer-adaptive gradient perturbation, trust-based contribution weighting as well as encrypted edge-layer aggregation. The experimental outcomes on benchmark datasets show that LASFL can decrease the privacy leakage by up to 40% relative to the traditional approaches to federated learning at the level of similar accuracy as standard FedAvg. It is proved through layer-wise analysis that selective perturbation can maintain the performance of the critical layers and hierarchical aggregation can minimize communication overheads which makes the system scalable to heterogeneous and large scale application. This work has had contributions in the form of a software-based privacy mechanism that is privacy-sensitive to data sensitivity and device stability, a scheme of trust-based weighting to provide global model robustness, and a secure hierarchical aggregation approach, which secures intermediate updates. These mechanisms have been combined into a single framework that can be used in the real world to carry out edge-end cloud-edge-end applications in which sensitive data have to be provided with security. In future research, it is possible to apply LASFL to dynamic device on boarding and real-time trust updates, and combine it with federated reinforcement learning to make adaptive decisions to IoT networks. The idea of using energy-efficient perturbation strategies and the cross-silo type of federated learning settings will advance applicability in resource-constrained and industrial settings.

REFERENCES

[1] J. Tyagi and M. Sharma, "Enhancing Privacy-Preserving Data Mining in Cloud-Based Data Warehouses: A Federated Learning Approach for Secure Multi-Tenant Environments," 2025 IEEE 10th Int. Conf. Smart Cloud (SmartCloud), New York City, NY, USA, 2025, pp. 8-13, doi: 10.1109/SmartCloud66068.2025.00016.

[2] Z. Li et al., "APPFLx: Providing Privacy-Preserving Cross-Silo Federated Learning as a Service," 2023 IEEE 19th Int. Conf. e-Science (e-Science), Limassol, Cyprus, 2023, pp. 1-4, doi: 10.1109/e-Science58273.2023.10254842.

[3] S. G. Aarella, S. P. Mohanty and E. Kougianos, "Fortified Edge 3.0: A Lightweight Machine Learning based Approach for Security in Collaborative Edge Computing," 2023 OITS Int. Conf. Information Technology (OCIT), Raipur, India, 2023, pp. 450-455, doi: 10.1109/OCIT59427.2023.10430911.

[4] C. Wu, "Mamba-Based Federated Learning Architecture for Privacy-Preserving Machine Learning," 2024 IEEE 6th Int. Conf. Civil Aviation Safety and Information Technology (ICCASIT), Hangzhou, China, 2024, pp. 314-317, doi: 10.1109/ICCASIT62299.2024.10827895.

[5] R.-H. Hsu and T.-Y. Huang, "Private Data Preprocessing for Privacy-preserving Federated Learning," 2022 IEEE 5th Int. Conf. Knowledge Innovation and Invention (ICKII), Hualien, Taiwan, 2022, pp. 173-178, doi: 10.1109/ICKII55100.2022.9983518.

[6] M. Khalil, R. Shakya and Q. Liu, "Towards Privacy-Preserving Data-Driven Education: The Potential of Federated Learning," 2025 Int. Conf. New Trends in Computing Sciences (ICTCS), Amman, Jordan, 2025, pp. 113-118, doi: 10.1109/ICTCS65341.2025.10989403.

[7] Y. Jeong and W.-S. Choi, "Efficient Privacy-Preserving Federated Learning with Sensitivity-Based Selective

Homomorphic Encryption," 2025 22nd Int. SoC Design Conf. (ISOCC), Busan, Korea, 2025, pp. 1-2, doi: 10.1109/ISOCC66390.2025.11329642.

[8] C. Li, H. Yang, Q. Yao, Z. Sun and J. Zhang, "High-Precision Edge-Cloud Collaboration with Federated Learning in Edge Optical Network," 2021 Optical Fiber Communications Conf. and Exhibition (OFC), San Francisco, CA, USA, 2021, pp. 1-3.

[9] Y. Ren, S. Yuan, L. Fan, C. Sun and X. Cao, "Edge-Cloud Collaborative Digital Twin Network Construction: A Reinforcement Learning Approach," 2025 IEEE 8th Int. Conf. Signal Processing and Machine Learning (SPML), Hohhot, China, 2025, pp. 365-370, doi: 10.1109/SPML66318.2025.11199815.

[10] K. E, R. S, C. M. B. M. J, V. K, A. Vathani and S. Kannan, "Revolutionizing Machine Learning Security: The Role of Quantum-Enhanced Federated Learning," 2024 Int. Conf. Emerging Research in Computational Science (ICERCS), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICERCS63125.2024.10895237.

[11] S. H. D, G. F. I and S. Mondal, "Intelligent Load Balancing for AI-Enhanced Edge-Cloud Architectures," 2025 Int. Conf. Recent Innovation in Science Engineering and Technology (ICRISET), Chennai, India, 2025, pp. 1-6, doi: 10.1109/ICRISET64803.2025.11252490.

[12] X. Li, N. Wang, D. Li, J. Ruan and H. Liu, "A Cloud-Edge-Devices Computing Power Allocation Algorithm Based on Intelligent Collaborative Computing," 2025 IEEE 3rd Int. Conf. Image Processing and Computer Applications (ICIPCA), Shenyang, China, 2025, pp. 157-161, doi: 10.1109/ICIPCA65645.2025.11138785.

[13] Z. He, T. Zhang and R. B. Lee, "Attacking and Protecting Data Privacy in Edge–Cloud Collaborative Inference Systems," IEEE Internet of Things Journal, vol. 8, no. 12, pp. 9706-9716, 15 June 2021, doi: 10.1109/JIOT.2020.3022358.

[14] S. P. Kumar Reddy, M. Mounika and U. Nagavelli, "Edge Computing and Federated Learning: Enhancing Privacy and Efficiency in Cloud-Based Machine Learning Systems," 2025 Int. Conf. Next Generation Communication & Information Processing (INCIP), Bangalore, India, 2025, pp. 339-345, doi: 10.1109/INCIP64058.2025.11020061.

[15] L. Welagedara, J. Harischandra and N. Jayawardene, "A Review on Edge Intelligence based Collaborative Learning Approaches," 2021 IEEE 11th Annu. Computing and Communication Workshop and Conf. (CCWC), NV, USA, 2021, pp. 0572-0577, doi: 10.1109/CCWC51732.2021.9376119.