SvedbergOpen
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Federated Learning Architectures For Privacy-Preserving Distributed Intelligence

Savita Prabha[1], Zafar Ali Khan N[2], Mamatha G. N[3], Mukesh Rajput[4], Shree Jayaram K[5], Anitha M[6], Tanya Singh[7], Pranali Chavan[8]

[1] Assistant Professor, Department of Computer Science & Application, Vivekananda Global University, Jaipur, Rajasthan, India. Email: savita.prabha@vgu.ac.in, ORCID: 0009-0001-0245-5610
[2] Professor, Department of Computer Science and Engineering, Presidency University, Bangalore, Karnataka, India. Email: zafaralikhan@presidencyuniversity.in, ORCID: 0000-0001-6744-3883
[3] Assistant Professor-I, Department of Electronics and Communication Engineering, Faculty of Engineering and Technology, JAIN (Deemed-to-be University), Bengaluru, Karnataka, India. Email: gn.mamatha@jainuniversity.ac.in, ORCID: 0000-0002-2693-072X
[4] Assistant Professor, Department of Computer Application, Dev Bhoomi Uttarakhand University, Dehradun, Uttarakhand, India. Email: socse.mukesh@dbuu.ac.in, ORCID: 0009-0006-0714-5685
[5] Innovation & Incubation Centre, Department of Research, Meenakshi Academy of Higher Education and Research, India. Email: shreejayaram@maher.ac.in
[6] Assistant Professor, Department of Mathematics, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, India. Email: anitham@maher.ac.in
[7] Professor, School of Engineering & Technology, Noida International University, Greater Noida, Uttar Pradesh, India. Email: dean.academics@niu.edu.in
[8] Department of Computer Engineering, Vishwakarma Institute of Technology, Pune, Maharashtra 411037, India. Email: pranali.chavan@vit.edu

Abstract

Privacy concerns in distributed intelligence systems have intensified with large-scale data sharing. Existing federated architectures often emphasize parameter exchange efficiency while insufficiently addressing adaptive, architecture-level privacy control across heterogeneous environments. This research aims to design robust Federated Learning (FL) architectures for privacy-preserving distributed intelligence using a novel Privacy-Aware Federated Stochastic Gradient Descent (PA-FedSGD) model. A Privacy-Aware Federated Edge dataset is collected from decentralized edge devices such as mobile sensors and Internet of Things (IoT) nodes, capturing diverse behavioral and contextual features, which contains 5,634 records. Data preprocessing involves Z-score normalization, Kalman filter-based noise filtering with adaptive scaling, and outlier detection techniques to enhance data quality, reduce variability, and improve stability in FL environments. The proposed model enables decentralized data retention, local model training, and secure parameter transmission through lightweight encryption and differential privacy mechanisms. PA-FedSGD is designed to optimize model convergence while embedding privacy-awareness into gradient updates, selectively masking sensitive gradients and regulating information leakage during aggregation. It ensures stable learning across heterogeneous nodes, while maintaining confidentiality constraints. The architecture integrates secure aggregation protocols and adaptive weighting strategies to enhance robustness and scalability. Performance evaluation demonstrates improved privacy preservation, communication efficiency, convergence stability, and resilience against inference risks. Achieved 95% accuracy with improved privacy, stability, and efficiency performance. The architecture establishes a scalable and adaptive foundation for secure distributed intelligence across real-world federated environments.

Keyword: Federated Learning, Privacy Preservation, Distributed Intelligence, Secure Aggregation, Data Confidentiality, Edge Computing

Introduction

The federated learning (FL) frameworks provide one of the most sophisticated solutions for implementing privacy-preserving distributed intelligence through collaboration among entities on their learning from data without actually sharing [1]. According to this concept, data should be kept in its original place, such as user devices and organization servers, whereas only the results of the learning process will be shared for constructing a global model. The decentralized manner not only makes the data more secure but also follows the necessity of

data security in contemporary society [2]. In light of the rapid production of data via numerous channels, various problems have arisen in relation to data security and privacy [3]. FL finds applications in environments, such as Internet of Things (IoT)-enabled healthcare systems, smart cities, industrial automation, and intelligent transport systems, where continuous data generation from distributed devices requires privacy-preserving learning [4]. FL increases cooperation by using different sources of distributed data to develop models [5]. FL provides benefits like greater data privacy, fewer risks of data leakage, the capability to use data from several distributed sources without storing them centrally, and compliance with rules related to data privacy [6]. However, there are certain drawbacks that are associated with the use of this architecture, such as greater difficulty in coordinating the system components, reliance on stable communication channels, and inconsistency in modeling due to variations in data sources. There are some challenges that have been associated with the utilization of FL architectures [7], and these include dealing with discrepancies in the quality and distribution of data, security of communication, limited resources of involved devices, and system efficiency in general. Figure 1 shows these challenges are essential to fully leverage FL for robust and scalable privacy-preserving distributed intelligence [8].

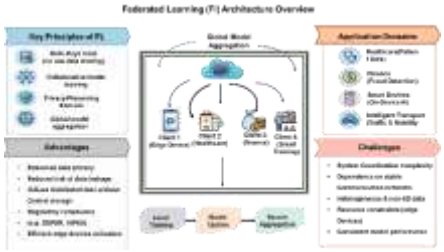

Figure 1: Overview of Federated Learning Architecture

Problem Statement and objective: The existing FL models focus on effective communication without adequately considering the dynamic control of privacy in the heterogenous distributed computing contexts. The potential risk of sensitive information leakage is high in the gradient sharing and aggregation process. A FL-based Privacy-Aware Federated Stochastic Gradient Descent (PA-FedSGD) model is proposed that addresses these gaps and ensures privacy-conscious gradient computation, secure aggregation, convergence, and viable distributed learning in heterogeneous environments. Enables safe and scalable deployment of distributed intelligence applications in healthcare, IoT, and smart spaces, preserving privacy yet maintaining performance efficiency.

Related work

Conventional federated models enhance privacy, precision, and cooperation by using encryption and dynamic aggregation, yet have issues in terms of elevated computation prices and scale. Table 1 compares current methods.

Table 1: Summary of federated learning-based privacy-preserving methods

Ref.	Objective	Method	Key Results	Limitations
[9]	Secure data and model ownership in FL	FL with Intellectual Property Protection (FL-IP) protection with homomorphic encryption and watermarking	92% accuracy, 25% reduced data leakage	High computational overhead, latency in aggregation
[10]	Enable privacy-preserving industrial Artificial Intelligence (AI) collaboration	FL-based Industrial AI Framework (FL-IAF)	30% improved efficiency, reduced data exposure	Scalability issues, network dependency
[11]	Enhance IoT data security in big data environments	FL-Cryptography Integrated Model (FL-Crypto)	40% reduced vulnerabilities, improved efficiency	High computational complexity, key management overhead
[12]	Secure data aggregation in Industrial Internet of Things (IIoT) systems	Secure Federated Aggregation Scheme (SFAS)	20% reduced communication overhead, ~90% accuracy	Node failure sensitivity, limited adaptability
[13]	Handle non-IID data in fog-assisted IoT	Fog-based FL with Adaptive Aggregation (Fog-FLAA)	Higher accuracy, reduced latency	Data imbalance, fog node dependency

[14]	Detect intrusions in WSN securely	Federated Spatial Convolutional Neural Network–Bidirectional Long Short-Term Memory (FL-SCNN-BiLSTM)	Higher detection accuracy, strong reliability	High training complexity, resource consumption
[15]	Improve PV forecasting with privacy preservation	FL-based Photovoltaic Forecasting Model (FL-PV)	93% accuracy, strong confidentiality	Performance drops in dynamic weather
[16]	Enable secure collaborative medical diagnosis	FL-based Medical Diagnosis Expert System (FL-MedDiag)	Greater accuracy, secure data sharing	High communication overhead, data heterogeneity issues

Research gap: Existing FL solutions [9–16] concentrate mostly on ensuring privacy and optimizing for specific tasks rather than developing a comprehensive model that tackles issues related to scalability, effective communication, and robustness under highly heterogeneous conditions. The majority of these solutions have difficulties dealing with high computational costs, adapting to dynamic networks, and achieving uniform performance across different domains. To overcome these limitations, this research proposes the PA-FedSGD improves privacy, scalability, and accuracy using adaptive updates, efficient gradients, and non-IID robustness mechanisms.

Methodology

A privacy-preserving FL model is developed to enable secure and efficient distributed intelligence across decentralized environments. Figure 2 shows an overview of the process in the proposed model. A Privacy-Aware Federated Edge dataset is gathered and pre-processing is conducted through normalization, noise filtering, and outlier removal. To employ privacy-awareness by introducing the PA-FedSGD model to ensure secure gradient calculation and differential privacy.

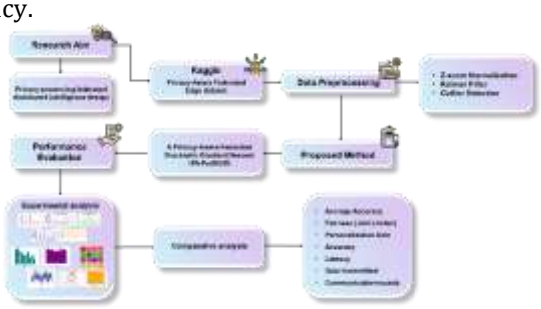

Figure 2: PA-FedSGD Model for Privacy-Preserving Federated Learning

Dataset

The Privacy-Aware Federated Edge dataset is gathered from the open-source platform Kaggle, Link: https://www.kaggle.com/datasets/programmer3/privacy-aware-federated-edge-dataset/data. This dataset consists of 5,634 records and 35 attributes, which are related to distributed edge devices in FL environments. Each instance of data is made up of attributes describing device-level data, communication patterns, privacy metrics, and global model performance metrics obtained over repeated FL iterations. It considers variations across various device types, networks, and system-level dynamics. Applications of the dataset include classification, risk evaluation, and the evaluation of privacy-preserving distributed learning systems. Dataset split into 70% training, and 30% testing sets.

Data Preprocessing

Data preprocessing is used to improve the quality of data that enhances the accuracy and efficiency of the model training process through data cleaning, normalization, and transformation. The preprocessing includes the Kalman filter to reduce the noise, Z-score normalization to scale data, and outlier detection to improve the quality of the data.

Z-score Normalization for data standardization and stable convergence: Privacy-aware federated edge is used as an input for pre-processing. Centering and scaling of features are used to normalize heterogeneous edge data. This will ensure that there is uniformity of distribution, convergence of models, and reduction of biases during FL. Normalize the feature values, including an average of zero and standard deviation of one, so that all

the features equally contribute towards the model training process. This approach leads to standardized data with minimized differences in variance.

$$y_{zscore} = \frac{y_{inst} - u}{\delta} \quad (1)$$

Equation (1), y_{zscore} denotes the normalized value, y_{inst} represents the input data sample, u indicates mean, δ denotes the standard deviation, while it provides standardized scaling and improved federated model training performance.

Kalman Filter for adaptive noise reduction in edge data: Reducing noise and uncertainty in sensor data ensures smoother, accurate inputs for reliable local model training in FL environments. A Kalman filter estimates the true system state from noisy measurements using prediction and update steps, minimizing error covariance, enabling accurate, recursive state tracking in dynamic systems. Generating smoothed and noise-reduced signals improves data quality, enhances model convergence, and ensures stable, accurate learning across heterogeneous federated clients.

$$w_{l+1} = e(w_l, v_l) + u_l \quad (2)$$
$$z_l = g(w_l, v_l) + u_l \quad (3)$$
$$u_l \sim M(0, R)\ x_l \sim M(0, Q) \quad (4)$$
$$w_l = \Phi_{l-1}\hat{w}_{l-1} + A_{l-1}v_{l-1} \quad (5)$$

In Equations (2-5), $w_l$denotes the global model parameters, $v_l$represents the client gradients, and u_l is the Gaussian privacy noise injected for differential privacy. The functions $e(\cdot)$and $g(\cdot)$define nonlinear update and observation mappings governing federated optimization dynamics. Noise terms $u_l \sim M(0, R)$and $x_l \sim M(0, Q)$represent the zero-mean multivariate Gaussian distributions with covariance matrices $R$and Q. $\Phi_{l-1}$is the state transition matrix, $\hat{w}_{l-1}$is the estimated model, and A_{l-1}controls client update influence on global parameters

$$O_l = \Phi_{l-1}\hat{O}_{l-1}\phi_{l-1}^{S} + \mathrm{R}_{l-1} \quad (6)$$
$$L_l = O_l\, G_l^S\, (G_l O_l G_l^S + Q_l)^{-1} \quad (7)$$
$$\hat{w}_l = L_l(z_l - G_l\bar{w}_l) \quad (8)$$
$$O_l = (J - L_l G_l)O_l \quad (9)$$

Here Equations (6-9), $\mathrm{O_l}$, $\Phi_{\mathrm{l}-1}$, $\hat{\mathrm{O}}_{\mathrm{l}-1}$, $\phi_{\mathrm{l}-1}^{\mathrm{S}}$, $\mathrm{R}_{\mathrm{l}-1}$, and $\mathrm{Q_l}$represent covariance, state transition, sensitivity, and noise matrices governing uncertainty modeling. $\mathrm{L_l}$, $\mathrm{G_l}$, and $\mathrm{z_l}$ denote the Kalman gain, observation matrix, and measurement vector controlling adaptive correction and information fusion in federated updates. $\hat{\mathrm{w}}_\mathrm{l}$, $\bar{\mathrm{w}}_\mathrm{l}$, and Jrepresent the updated weights, prior estimates, and identity matrix ensuring stable recursive parameter optimization.

Outlier Detection for removing anomalies and improving robustness: It removes anomalous data points, improving data quality, stabilizing gradients, and enhancing accuracy in privacy-aware FL models. Outlier detection determines unusual data patterns that can reduce model performance, facilitating credible learning, minimizing the effect of noise, and enhancing the ability to generalize. Outlier detection results in cleaned datasets with fewer anomalies, resulting in convergent stability, accuracy, robustness, and privacy-preserving federated model performance.

A Novel Privacy-Aware Federated Stochastic Gradient Descent (PA-FedSGD) Method for secure, stable, and privacy-preserving distributed

This research develops a novel federated model known as PA-FedSGD, which is based on the federated stochastic gradient descent algorithm along with privacy-preserving mechanisms for secure and decentralized training of models. Privacy-preserving techniques such as gradient masking, differential privacy, and lightweight encryption ensure the security of parameter exchanges to address the problem of data leaks.

Federated Stochastic Gradient Descent (FedSGD) for decentralized model training with efficient parameter aggregation

After the preprocessing phase, FedSGD is utilized for this research that provides decentralized training of models by summing up gradients of distributed clients, enhancing the learning process and maintaining the privacy of data across settings. PA-FedSGD presents privacy-conscious gradient masking and differential privacy to minimize the loss of information and still achieve convergence efficiency in heterogeneous federated settings. FedSGD generates global model updates based on aggregated client gradients, resulting in better accuracy,

quicker convergence, and effective distributed learning. Equation (10), $G_j$denotes the gradient for client j, ∇l represents the loss gradient, x^q input data at iteration q, and k_j local model parameters.

$$G_j = \nabla l(x^q, k_j) \quad (10)$$

$$G_r = \frac{\sum_{i=1}^{n} d_i . G_i}{\sum_{i=1}^{n} d_i} \quad (11)$$

Equation (11) depicts the G_r is the aggregated global gradient, G_i is the local gradients, d_i is the data weights per client, and n is the total clients contributing to weighted aggregation process.

$$w^Q = w^{Q-1} - \eta . G_Q \quad (12)$$

Equation (12) shows the, w^Q updated global model, w^{Q-1} previous parameters, η learning rate controlling update step, and $G_Q$aggregated gradient applied at iteration Q. The FedSGD enables decentralized model training with efficient parameter aggregation, ensuring collaborative learning, reduced communication overhead, and improved convergence in federated environments.

Privacy-Aware Mechanism for reducing information leakage and securing gradient sharing

Sensitive information protection by embedding gradient masking and differential privacy, reducing data leakage during FL updates. Privacy-Aware combines gradient masking with differential privacy to prevent sensitive data when updating the FL. It regulates information leakage through restricting exposure of important information and allowing secure cooperation between distributed clients. This guarantees robust, confidential and efficient model training in heterogeneous edge conditions.

Algorithm 1: Privacy-Aware Federated Stochastic Gradient Descent (PA-FedSGD) for Secure and Privacy-Preserving Distributed Intelligence

Input: *Number of clients N, learning rate η, privacy budget ε, total rounds Q*
Initialize global model parameters w^0
For each communication round $q = 1$ *to Q do*
Select a subset of clients Cq from N
For each client $j \in Cq$ *in parallel do*
Load local dataset Dj
Local gradient computation
Compute gradient:
$Gj = \nabla l(x\hat{}q, kj)$
Gradient masking $(privacy - aware)$
Apply masking:
$Gj\_masked = Gj \odot Mj$
Differential privacy $(noise\ addition)$
Add noise:
$Gj\_private = Gj\_masked + N(0, \sigma^2)$
Send protected gradient to server
Transmit Gj_private to server
End For
Secure aggregation at server
Compute aggregated gradient:
$Gr = (\Sigma\ (di * Gi)) / (\Sigma\ di)$
Global model update
Update model:
$w\hat{}q = w\hat{}(q-1) - \eta * Gr$
End For
Output: *Final global model* $w\hat{}Q$

Thus, the proposed PA-FedSGD algorithm adopts gradient masking, differential privacy, and secure aggregation in order to enable privacy-preserving distributed optimization in federated environments where heterogeneity is present. Specifically, the method employs adaptive weights and noise injection for updating parameters to improve the convergence process and reduce the potential for information leakage during training.

Result

The proposed PA-FedSGD model was implemented using Python 3.10 with libraries such as NumPy, Pandas, and PyTorch/TensorFlow. The system was implemented using a computer equipped with 16GB RAM, Intel i8 CPU, and 64-bit Windows 11 Operating System. The model was assessed on the dataset pertaining to decentralized IoT and mobile-edge data. The efficiency of the system was gauged on the basis of accuracy, stability of convergence, and communication performance.

Experimental Analysis

In this section, experimental evaluation and graphing methods that help validate the efficiency, reliability, and privacy preservation capacity of the PA-FedSGD model under FL scenarios are discussed. This experiment shows better convergence performance, lesser risk of information leakage, and better performance levels of the system.

Robustness Distribution and Bandwidth Utilization: Figure 3 (a-b) provides the robustness values and the bandwidth usage in the FL scheme. These robustness values are significantly high without any variation, indicating a high degree of robustness and reliability of the model in different environments. The bandwidth usage of every data transmission cycle is quite consistent, indicating a proper transfer of data from the client to the server. In general, the findings indicate robust performance and scalability of communications in the proposed scheme.

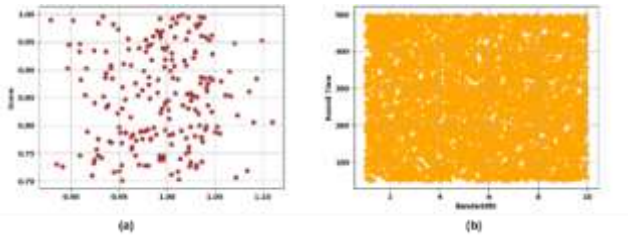

Figure 3: Federated Learning in utilization (a) Robustness Score Distribution (b) Bandwidth Utilization

Training Dynamics and Communication Efficiency Analysis: Figure 4 (a-c) shows the convergence of loss, distribution of payload sizes, and rolling accuracy in the federated setting. Reduction in loss at each step suggests successful optimization and convergence of the PA-FedSGD algorithm. Payload sizes show efficient communication between clients in the federated setting. Rolling accuracy suggests stable performance despite a dynamic heterogeneous data environment.

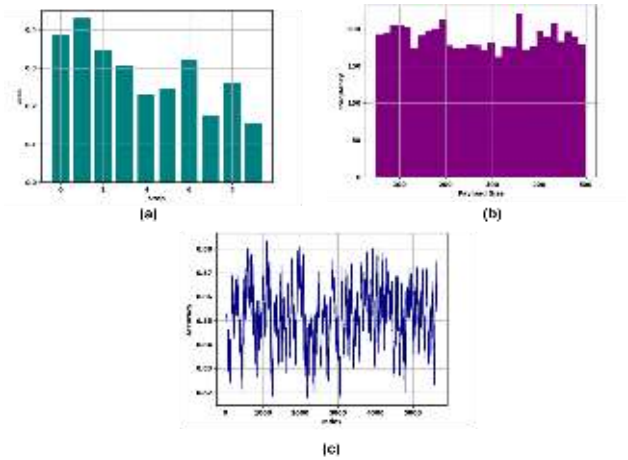

Figure 4: The figure illustrates (a) loss convergence, (b) payload distribution, and (c) rolling accuracy

Pairwise Feature Distribution in Federated Dataset: Figure 5 shows the distribution of attributes and their correlations within the federated dataset after pre-processing. The uniform distribution along the diagonals is indicative of successful normalization and an equal representation of data. The scatter plots denote low correlation between the attributes, making it advantageous to acquire independent attributes through the use of the PA-FedSGD algorithm.

Figure 5: Pair Plot Matrix

Lollipop Analysis of PA-FedSGD Privacy: Parameters like epsilon, noise, gradient mask, aggregation factor, and fairness index have been described in Figure 6. Epsilon and noise factors guarantee the protection of information using differentially private approaches. The use of gradient masking and aggregation factors ensures security and flexibility during optimization. The value of fairness index is always high, meaning that all clients participate equally in the FL process.

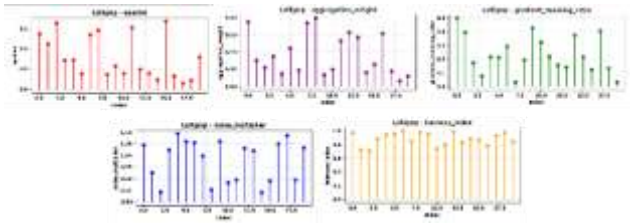

Figure 6: Lollipop Plot of Noise Multiplier Values Across Different Indices

Comparative Analysis

In the comparison phase, the proposed PA-FedSGD model is compared with state-of-the-art federated techniques, namely Federated Averaging (FedAvg) [17], Federated Personalization (FedPer) [17], Personalized Federated Learning via Moreau Envelopes (pFedMe) [17], Personalized Federated Averaging (Per-FedAvg) [17] and Heterogeneous Federated Edge Learning (HFEL) [18] using some performance metrics. The metrics with descriptions are described below:

- **Average Accuracy:** It measures the accuracy of prediction from all the involved clients, showing how well the PA-FedSGD algorithm can learn the patterns that have been distributed and generalize them under heterogeneous settings.
- **Fairness (Jain's Index):** The measure evaluates the consistency between the performance of all clients, making sure that they do not dominate in terms of learning efficiency within a federation setting.
- **Personalization Gain:** Defined as the relative improvement made by the local models as compared to the global model, it evaluates the effectiveness of the PA-FedSGD algorithm in personalizing each client's learning ability.
- **Accuracy (%):** Measure of the ratio of accurately classified examples; this metric shows the performance of the proposed model in making accurate predictions under the privacy-preserving setting.
- **Latency (ms):** The delay in communication and computations during the training process and thereby shows the response rate and effectiveness of the PA-FedSGD algorithm in real-time FL.
- **Data Transmitted (MB):** The communication costs between the client nodes and the server. This metric clearly explains how effectively the proposed algorithm utilizes the available bandwidth.
- **Communication Rounds:** The iterations needed to converge in FL. This is related to how fast and effectively the proposed algorithm learns while reducing interactions between client and server.

Figure 7 shows the graphical representation of avg. accuracy and fairness between proposed and existing methods using metrics. Table 2 and Table 3 present a comparative analysis of FL models, highlighting PA-FedSGD's superior accuracy, efficiency, fairness, and communication performance.

Table 2: Performance Comparison of Federated Learning Models

Architecture	Avg. Accuracy (%)	Fairness (Jain's Index)	Personalization Gain
FedAvg [17]	78	0.82	5
FedPer [17]	81	0.85	8
pFedMe [17]	83	0.88	10
Per-FedAvg [17]	82	0.87	9

PA-FedSGD [Proposed]	95	0.89	12

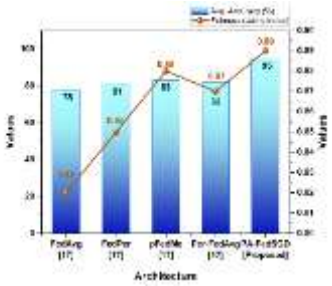

Figure 7: Accuracy and Fairness Comparison of Federated Learning Models

In Table 2, FedAvg has an accuracy of 78%, with fairness value 0.82 and personalization gain of 5, which signifies poor adaptation. The algorithms FedPer and Per-FedAvg perform well with accuracy levels of 81% and 82%, respectively, and their fairness values are 0.85 and 0.87, respectively. The pFedMe method performs even better with accuracy, fairness, and personalization gain of 83%, 0.88, and 10, respectively. The proposed algorithm PA-FedSGD surpasses all other architecture methods with accuracy, fairness, and personalization gains of 95%, 0.89, and 12.

Table 3: PA-FedSGD vs HFEL Performance Comparison

Metrics	HFEL [18]	PA-FedSGD [Proposed]
Accuracy (%)	92.6	95
Latency (ms)	180	120
Data transmitted (MB)	300	200
Communication rounds	70	40

The PA-FedSGD approach offers an accuracy of 95% against 92.6% in HFEL, suggesting better predictive capability. Latency is lowered to 120 ms from 180 ms, ensuring better updating capabilities. Data communication is reduced to 200 MB from 300 MB, improving the speed of data communication. Communication rounds have been minimized from 70 to 40.

Discussion

A robust FL model was effectively designed to ensure secure, efficient, and privacy-preserving distributed intelligence through adaptive optimization and decentralized model training. This research utilizes some existing models such as FedAvg [17], FedPer [17], pFedMe [17], Per-FedAvg [17] and HFEL models [18] were associated with privacy risks due to information leakage. This technique had problems with communication overhead and instability of convergence when there were heterogeneity and non-IID data distribution. This challenges the robustness and scalability of the model. To address the above problems, this research proposed PA-FedSGD, which combines privacy-aware gradient masking with differential privacy mechanisms. It utilizes secure aggregation to protect the communication process of parameters in the FL process. The technique ensures a higher level of robustness in the convergence of the learning model and requires lower communication rounds. Practically, the model enables secure and scalable collaborative learning in real-world IoT and distributed intelligent systems.

Conclusion

The purpose of this research was to create a model of privacy-preserving FL to build security and distributed intelligence in edge computing. A Privacy-Aware Federated Edge dataset of IoT devices and mobile sensors was used for training and testing the model. Pre-processing involved Z-score normalization, noise removal and outlier handling to improve the quality of data. This approach employs a new algorithm named PA-FedSGD. It advanced as it makes use of the method known as the combination of gradient masking, differential privacy, and secure aggregation in federated optimization. The new model achieved a result of 95% accuracy, 120ms latency, 200 MB transmission, and 40 communication iterations. Advantages of this approach include enhanced privacy, reduced communication cost, greater stability in convergence, increased scalability, robustness, and increased resistance to inference attacks. Disadvantages include the need for more computing power, reliance on networks, and difficulty in implementing it at a large scale in real-time operations. Limited dataset size, single-source collection, and lack of diverse real-world scenarios restrict model generalization and scalability. Further

research should increase the data size, and focus on employing cryptography techniques and dynamic client selection.

References

1. Khraisat, A., Alazab, A., Alazab, M., Obeidat, A., Singh, S. and Jan, T., 2025. Federated learning for intrusion detection in iot environments: a privacy-preserving strategy. Discover Internet of Things, 5(1), p.72. https://doi.org/10.1007/s43926-025-00169-7
2. Zang, H., Kim, H. and Kim, J., 2024. Blockchain-based decentralized storage design for data confidence over cloud-native edge infrastructure. IEEE Access, 12, pp.50083-50099. https://doi.org/10.1109/ACCESS.2024.3383010
3. Calvino, G., Peconi, C., Strafella, C., Trastulli, G., Megalizzi, D., Andreucci, S., Cascella, R., Caltagirone, C., Zampatti, S. and Giardina, E., 2024. Federated learning: Breaking down barriers in global genomic research. Genes, 15(12), p.1650. https://doi.org/10.3390/genes15121650
4. Ullah, A., Anwar, S.M., Li, J., Nadeem, L., Mahmood, T., Rehman, A. and Saba, T., 2024. Smart cities: The role of Internet of Things and machine learning in realizing a data-centric smart environment. Complex & Intelligent Systems, 10(1), pp.1607-1637. https://doi.org/10.1007/s40747-023-01175-4
5. Mrabet, M., 2025. TrustFed-CTI: A Trust-Aware Federated Learning Framework for Privacy-Preserving Cyber Threat Intelligence Sharing Across Distributed Organizations. Future Internet, 17(11), p.512. https://doi.org/10.3390/fi17110512
6. Alsamhi, S.H., Myrzashova, R., Hawbani, A., Kumar, S., Srivastava, S., Zhao, L., Wei, X., Guizan, M. and Curry, E., 2024. Federated learning meets blockchain in decentralized data sharing: Healthcare use case. IEEE Internet of Things Journal, 11(11), pp.19602-19615. https://doi.org/10.1109/JIOT.2024.3367249
7. Berkani, M.R.A., Chouchane, A., Himeur, Y., Ouamane, A., Miniaoui, S., Atalla, S., Mansoor, W. and Al-Ahmad, H., 2025. Advances in federated learning: Applications and challenges in smart building environments and beyond. Computers, 14(4), p.124. https://doi.org/10.3390/computers14040124
8. Lazaros, K., Koumadorakis, D.E., Vrahatis, A.G. and Kotsiantis, S., 2024. Federated learning: Navigating the landscape of collaborative intelligence. Electronics, 13(23), p.4744. https://doi.org/10.3390/electronics13234744
9. Yang, Q., Huang, A., Fan, L., Chan, C.S., Lim, J.H., Ng, K.W., Ong, D.S. and Li, B., 2023. Federated Learning with Privacy-preserving and Model IP-right-protection. Machine Intelligence Research, 20(1), pp.19-37. https://doi.org/10.1007/s11633-022-1343-2
10. Peres, R.S., Manta-Costa, A. and Barata, J., 2023. Implementing privacy-preserving and collaborative industrial artificial intelligence. IEEE Access, 11, pp.74579-74589. https://doi.org/10.1109/ACCESS.2023.3296143
11. Awan, K.A., Din, I.U., Almogren, A. and Rodrigues, J.J., 2023. Privacy-preserving big data security for IoT with federated learning and cryptography. IEEE access, 11, pp.120918-120934. https://doi.org/10.1109/ACCESS.2023.3328310
12. Hongbin, F. and Zhi, Z., 2023. Privacy-preserving data aggregation scheme based on federated learning for IIoT. Mathematics, 11(1), p.214. https://doi.org/10.3390/math11010214
13. Abdel-Basset, M., Hawash, H., Moustafa, N., Razzak, I. and Abd Elfattah, M., 2024. Privacy-preserved learning from non-iid data in fog-assisted IoT: A federated learning approach. Digital Communications and Networks, 10(2), pp.404-415. https://doi.org/10.1016/j.dcan.2022.12.013
14. Bukhari, S.M.S., Zafar, M.H., Abou Houran, M., Moosavi, S.K.R., Mansoor, M., Muaaz, M. and Sanfilippo, F., 2024. Secure and privacy-preserving intrusion detection in wireless sensor networks: Federated learning with SCNN-Bi-LSTM for enhanced reliability. Ad Hoc Networks, 155, p.103407. https://doi.org/10.1016/j.adhoc.2024.103407
15. Michalakopoulos, V., Sarantinopoulos, E., Sarmas, E. and Marinakis, V., 2024. Empowering federated learning techniques for privacy-preserving pv forecasting. Energy Reports, 12, pp.2244-2256. https://doi.org/10.1016/j.egyr.2024.08.033
16. Markkandan, S., Bhavani, N.P.G. and Nath, S.S., 2024. A privacy-preserving expert system for collaborative medical diagnosis across multiple institutions using federated learning. Scientific reports, 14(1), p.22354. https://doi.org/10.1038/s41598-024-73334-7
17. SINTHIYA, C., 2025. Federated Learning Architectures for Privacy-Preserving Collaborative Intelligence in Distributed Networks. International Journal of Computer Science and Engineering Innovations, 1(1), pp.27-37. https://doi.org/10.64137/XXXXXXXX/IJCSEI-V1I1P104
18. Alatawi, M.N., 2026. Edge computing and federated learning for privacy-preserving IoT analytics. EURASIP Journal on Wireless Communications and Networking, 2026(1), p.6. https://doi.org/10.1186/s13638-025-02545-x