IAES International Journal of Artificial Intelligence (IJ-AI)
Vol. 15, No. 1, February 2026, pp. 878~887
ISSN: 2252-8938, DOI: 10.11591/ijai.v15.i1.pp878-887

Gradient descent optimization based weighted federated learning for privacy-preserving framework

Gururaj Prakash Murthy, Chandrashekhar Pomu Chavan
Department of Computer Science and Engineering, PES University, Bangalore, India

Article Info

Article history:

Received Jun 9, 2025
Revised Dec 30, 2025
Accepted Jan 22, 2026

Keywords:

Centralized machine learning
Communication bandwidth
Federated learning
Gradient descent optimization
Internet of things
Privacy preserving
Weighted federated learning

ABSTRACT

Federated learning (FL) is a disseminated machine learning (ML) paradigm that gained significant consideration in modern days, particularly in a domain of the internet of things (IoT). FL saves communication bandwidth when compared to centralized ML processes by eliminating the need to transmit raw client data to a central server, thereby enhancing data privacy. Nevertheless, participant privacy is still compromised through inference attacks and similar threats. Additionally, a data excellence provided through clients can differs significantly, and excessive inclusion of low-quality data during training may degrade the overall performance of the global model. Hence, this research introduces a gradient descent optimization assisted weighted federated learning (GDO-WFL) method for privacy preservation. The proposed GDO-WFL approach is significantly efficient as it strengthens privacy preservation through reducing exposure to inference attacks and optimises gradient updates for secure learning. Through weighting client contributions based on data quality, an undesirable effect of low-quality data can be minimised, helping to maintain a strength as well as accuracy of the global model. The experimental results illustrate a proposed GDO-WFL approach maintains an overall accuracy of 99.3 and 91.5% on MNIST and CIFAR-10 datasets as compared to the existing method of FedlabX method.

Corresponding Author:

Gururaj Prakash Murthy
Department of Computer Science and Engineering, PES University
Bangalore, India
Email: gururajp@pes.edu

1. INTRODUCTION

Through an advancement of artificial intelligence (AI) approaches and techniques, internet of things (IoT) setups are broadly organised in various fields such as wireless networks [1], healthcare, smart cities, and the military [2]. Nevertheless, conventional cloud computing frameworks face challenges in meeting the data processing requirements of real-world applications due to limitations in network bandwidth and growing concerns over data privacy [3]. To tackle the constraints, edge computing [4] is developed within a computation framework of IoT. It develops an edge server for local processing that employs actual information through aggregation, mining, or communication operations [5]. In edge computing, the edge server becomes a significant part as a primary dispensation tool that gives appropriate local services by the entire cloud service architecture [6]. Thus, a blockage of computation as well as communication for conventional cloud-based frameworks has to be addressed. These data are often sourced from edge devices like smartphones, healthcare, global positioning system (GPS) devices, and so on [7]. Nevertheless, this data mostly involves participants' data, medical records, as well as travel antiquity [8]. Unauthorised access to this personal data leads to an important impairment. Moreover, in particular dedicated organisations, data sharing is not allowable [9]. Thus, preserving the privacy of participants' information during performing machine

learning (ML) becomes of supreme significance [10]. The federated learning (FL) is the most important advancement, which becomes a crucial part in the joint learning approach. The FL has been broadly utilised in various areas like blockchain, image processing, computer vision, medical imaging, as well as automatic systems [11], [12]. For conventional centralized learning, it needs to gather a maximum amount of user information for training a network [13]. Nevertheless, user information involves personal data, which results in user information outflow. To ignore privacy outflow and interruption of the data keys, FL is developed [14]. As an evolving distributed learning model, FL has trained model parameters from various users supportively through a lack of perceiving their actual information [15]. The model is a privacy protection method which attained the trust of more participants. Thus, FL has stimulated extensive apprehension in various fields [16]. The FL process also improves the generalization accuracy as each client is equipped to handle the data not exposed to it previously, due to collaborative learning with the other clients, which are exposed to the data [17]. Ultimately, the effectiveness of the global model is enhanced due to the model aggregation at the server. FL architecture should improve the personalization, generalization, and global accuracy [18], [19]. FL architecture saves communication bandwidth when compared to the centralised ML process and is also considered to be privacy-preserving as the raw data at the clients need not be transmitted to the server for the FL learning [20].

The previous works based on the FL-based privacy preserving are discussed here, along with their advantages and limitations limitations. Yan *et al.* [21] introduced the various communication effectiveness mechanisms as well as privacy-preserving cryptographic approaches. A privacy-preserving method integrates the cryptographic approaches and communication networking solutions for securing sensitive data. In that introduced approach, Kafka was introduced for communication distribution, a Diffie-Hellman method for secure server aggregation, as well as gradient discrepancy privacy for intrusion attack anticipation. An introduced method preserved training effectiveness while being capable of solving gradient outflow issues as well as interference attacks. Recently, the development of Kafka-Zookeeper has enabled asynchronous communication and secure, role-based access control, providing anonymous, and reliable data processing capabilities. However, the introduced method did not address robustness to heterogeneous data distributions or Byzantine threats, and Kafka integration added complexity. Chen *et al.* [22] presented a practical and efficient privacy-preserving federated learning (PEPFL) model. Initially, a boosted disseminated ElGamal cryptosystem was developed to address a multi-key issue in FL. Then, the practical partially single instruction multiple data (PSIMD) structure was introduced to encode a plaintext matrix within individual plaintext for encryption, enhancing encryption performance, as well as minimized communication cost in the incompletely homomorphic cryptosystem. Moreover, according to convolutional neural network (CNN) and a developed cryptosystem model, a new privacy-preserving FL structure was introduced through the utilisation of momentum gradient descent (MGD). However, while PEPFL with enhanced ElGamal and PSIMD offered improved security, the model faced challenges in real-time execution due to the computational overhead introduced by homomorphic encryption and matrix-based encoding. Sumitra *et al.* [23] developed a HAFedL, an improved novel Hessian-aware adaptive privacy preserving FL scheme. The architecture introduces specific enhancements to strengthen privacy against gradient leakage attacks (GLA). These modifications ensure that the model's effectiveness is not significantly compromised while improving overall security within the FL framework. The HAFedL is also robust to the data heterogeneity and device heterogeneity (particularly the straggler effect), which may be present in the clients participating in the FL. The performance of HAFedL is tested for two applications-IoT device identification and digit classification. However, the developed HAFedL resisted gradient leakage, but it lacked evaluation under adversarial scenarios and dynamic participant dropout during training. Wang *et al.* [24] implemented a privacy preserving federated learning mechanism through partial low-quality data (PPFL-LQDP). The implemented approach attained better training results by permitting contributors to access partial, low-quality data, thus improving a privacy as well as refuge of FL approach. Particularly, a dispersed Paillier cryptographic scheme was utilized for the protection of privacy and security of members' information at the federated training procedure. However, the implemented scheme did not consider performance degradation due to the frequent inclusion of noisy data.

Zhong *et al.* [25] developed a lightweight privacy-preserving FL scheme based on a dual-server architecture. Our scheme involves only lightweight cryptographic operations, i.e., hash and symmetric encryption operations, and it has low communication overhead. Thus, it is computationally lightweight and round-efficient. Further, it allows users to join/quit an FL task, and it is accuracy-lossless. However, the designed lightweight scheme with dual-server architecture failed to tackle poisoning attacks or incorporate adaptive model update strategies. Wang *et al.* [26] presented a privacy-improved and dependable decentralized federated learning mechanism (PTDFL). Particularly, an efficient gradient encryption algorithm was initially developed for the protection of data privacy, and after invented a concise proof through lack of trapdoors to make sure an effectiveness of inclines. Temporarily, a new local combination mechanism was designed to operate without relying on a trusted third party, ensuring that a combination

outcome remains secure and responsible. Furthermore, PTDFL was also helpful of the data owners for logging in and logging out at an entire DFL operation. However, the introduced PTDFL with decentralized aggregation relied heavily on trustless systems, which increases complexity and risks latency in large-scale systems. Sun *et al*. [27] developed a novel differentially private federated learning (DPFL) scheme named Adap-FedITK, which aimed to achieve low-communication overhead and high-model accuracy while guaranteeing client-level DP. Specifically, this dynamically adjusts the gradient clipping threshold for different clients in each round, based on the heterogeneity of gradients. This approach aims to mitigate the negative impact of DP and achieve a privacy utility tradeoff. To alleviate the high-communication overhead problem in FL, an improved top-k algorithm was introduced, which utilised sparsity and quantisation to compress the model, eliminate communication redundancy, and also integrates coding techniques to further reduce communication. However, Adap-FedITK, despite incorporating dynamic gradient clipping, faced difficulties in balancing privacy and utility due to the use of fixed clipping thresholds, which could lead to potential accuracy degradation. Shan *et al*. [28] presented an FL mechanism through DP protection, which was robust for GLA. The discriminatory updates were utilized for a selection of model parameters through greater effectiveness, thus enhancing a model's utility. Then, designed a deep learning (DL) approach was designed through an automatic clipping and noise attenuation scheme to ensure DP and optimise utility attainment, solving an intrinsic drawback of conventional DL methods through secure DP parameters. The presented approaches exhibited the rapid convergence rates and attained significant performance. However, the presented method ignored model convergence delays and the scalability concerns under large client participation. The reviewed FL literature exhibits key limitations such as vulnerability to gradient leakage, inefficiency with heterogeneous data, high communication overhead, and reliance on trusted third parties. Many models trade off accuracy for privacy and lack support for asynchronous, secure communication. To overcome these, the proposed gradient descent optimization assisted weighted federated learning (GDO-WFL) integrates Kafka-Zookeeper for anonymous communication, applies DP, and uses weighted model updates based on data quality and training effectiveness. This ensures robust, scalable, and privacy-preserving learning without heavy cryptographic overhead.

The key innovations of this research are arranged as follows:

i) An integrated framework of GDO-WFL is introduced in this research to reduce the significant threats in FL.
ii) The practical GDO-WFL approach through Apache Kafka-Zookeeper is developed to attain anonymous authentication through access control list as well as asynchronous model disseminations.
iii) A proposed GDO-WFL approach is compared and estimated through the existing FL approaches based on effectiveness, security as well and accuracy through empirical studies.

This research paper is organised as follows: section 2 demonstrates a proposed methdology. Section 3 outlines the FL for privacy preserving framework. Section 4 demonstrates the results and discussion, and section 5 provides a conclusion.

2. PROPOSED METHODOLOGY

Figure 1 demonstrates a system model of introduced method. Initially, the proposed methodology describes the system model and then defined the model framework of this research. The detailed description and working of the proposed methodology are described in the following section.

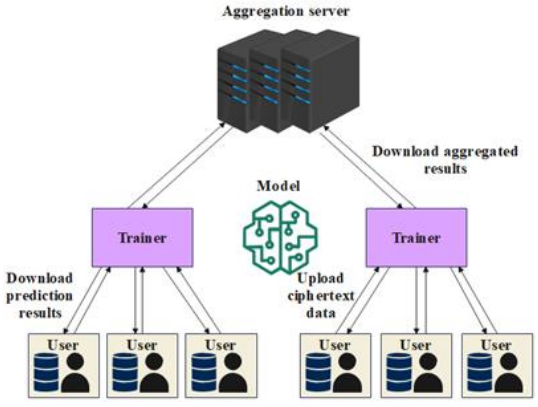

Figure 1. System system model of introduced method

2.1. System model

There are multiple units in the system model such as users, trainers and an aggregation server. This is different from conventional binary units (users and aggregation server) and helps users remain disconnected. A training model influences an approach for comprehending training as well as forecasting. Eventually, an FL approach acquires an optimization training parameter and forecasts outcomes. Each communication line is certain through secure tunnelling protocol (STP).

i) User: in the model framework, a user is an agent who gives ciphertext data for training and forecasting in an FL operation. Initially, each user produces public and private key pairs, and after transmits a key to a server for the model link. After acquiring a link public key, a user encodes and encrypts the data using this key, and then transmits the resulting ciphertext to the trainer for processing. Moreover, a user has to decrypt and decode an information to acquire prediction results.

ii) Trainer: as an ML entity, a trainer involves a DL approach for training model parameters and has to gather encrypted information from users in a local area. Certainly, the trainers work together through a server for training a model through the FL approach. By different iterations, the trainers obtain an efficient trained system used for prediction by users' requests.

iii) Server: as a controller and aggregator, a server has distributed a linked public key and estimated a federated averaging (FedAvg) through aggregated weights from trainers. Furthermore, a server requires various iterations and collaboration to acquire an optimisation model parameter in training procedure. In the proposed framework, even if server conspires through various entities, it does not acquire any information from users.

2.2. Model framework

The model framework involves multiple entities like clients, server and Apache Kafka message queue. Here, a server prepares a framework and transmits an unexperienced approach for requesting a broker in Kafka. Since Kafka operates as a reliable third-party system, when clients request a network from Kafka request broker, they receive this untrained model for their use. After clients request an approach from the Kafka request broker, it depends on an untrained model for the client. The suggested framework enabled a central broker to fix a policy that allows defined clients only according to a 1-out-of-n estimation plan through predefined n features to associate a model. This research considers that there is a recognized protected area between central server and clients. A simple encryption for verification is acquired through a central broker. Every client trains a model according to their local dataset. After a server desires a trained model, clients will reply to a response broker in Kafka through a trained and encrypted approach. Eventually, a response broker will transmit updated approaches to a server, and they perform effective combination method to obtain overall outcome. This structure is perfect for multi-organization FL scenarios for some clients. It is often applied in an actual manufacturing environment through Kafka client-server communication framework, as well as message storage as well as transmission functions. Recently, from a security point-of-view, secure combination as well as DP mechanisms were integrated into the GDO-WFL framework to ensure privacy preservation and effectively mitigate large-scale attacks, assuming the server and clients act as passive adversaries. Figure 2 demonstrates the important structure of the introduced approach. A comprehensive description of this structure is provided in a subsequent section.

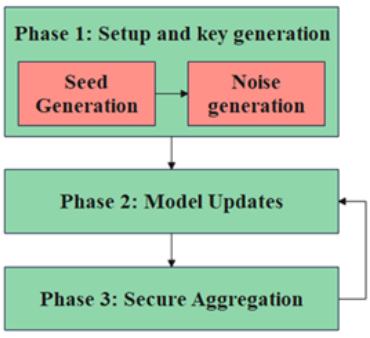

Figure 2. Important structure of the proposed method

2.2.1. Phase 1: setup and key generation

This step involves a generation of key among clients. Assume a group of clients as $C = 1, 2, \ldots, n$. After that, a server selects a suitable group G, while a computational Diffie-Hellman issue is complex. G is a recurring q essential through generator g. The basic constraints are produced using (1).

$$(G,),|G|-q,g\in G:G=<g> \quad (1)$$

Assume $i \neq j \in C$ becomes a static couple of clients. After that a subsequent procedure which involves the seed as well as noise generation has to be implemented for each pair of clients. After the setup and key generation, the seed must be generated.

i) Generation of seed
   - Client i selects a proponent $a_i \in_R Z_q^*$ and transmits to a server through value of g^{a_i}. After that server transmits a pair (i, g^{a_i}) to client j.
   - Client j selects a proposal $a_j \in_R Z_q^*$ and transmits to a server through the value of g^{a_j}. After that server transmits a pair (j, g^{a_j}) to client i.
   - A basic key of the client i and j is $key_{i,j} = g^{a_i a_j}$. At termination of this step, each client $i \in C$ keeps a group of basic keys through different clients, which is in (2).

$$key_i = key_{i,1}, key_{i,2}, \ldots, key_{i,n} \quad (2)$$

ii) Noise generation
   To ignore intrusion attacks, clients have executed DP through increasing noises to weights after model training, which is related to the GDO. In that, a Laplace noise generation strategy of DP is used. A Laplace mechanism conserves (∈,0) DP.

2.2.2. Phase 2: model update

As an outcome of the implementation of primary stage, where a seed and noise are prodiced, each contributing client is prepared to mask the model using the generated noise and key pairs. Simultaneously, clients have updated a system by replying to a request directed from a central server. Systems will reach and stay associated with Kafka brokers associated through Zookeeper. In this condition, even if clients are involved in various surroundings of hardware settings and network bandwidth, this model eventually attains synchronic communication.

2.2.3. Phase 3: secure aggregation

In this stage, a server calculates an aggregated client data for a provided update. Consider $l \in N$ becomes a length of users' information of an unknown update. This distance is varied for each update however static at an individual update. Consider $x_i \in \{0,1\}^l$ becomes the client's data; P_l becomes a pseudorandom generator of output size *l*.

3. FEDERATED LEARNING FOR PRIVACY PRESERVING FRAMEWORK

In the proposed FL model, each k client trains a local model through a similar shared global approach; however, it is trained on different local datasets instead of the central server. Pursuing that, clients securely transmit the updates from their local training to the aggregation server via secure sockets layer/transport layer security (SSL/TLS)-authenticated connections managed by a communication administrator. An aggregation server associates them as well as generates an updated global approach through ideal constraints. A notation w denotes initial weights and *r* demonstrates a count of FL disks, that is continued prior attaining a convergence stage. While every local client's weight is given to an aggregation server at the communication round *t*, a subsequent (3) is acquired from FedAvg algorithm, which is utilized for updating model weights.

$$W_{t+1} = \sum_{k=1}^{k} \frac{n_k}{n} w_{t+1}^k \quad (3)$$

Here, n means a total size of every client dataset, and n_k denotes a size of every client dataset. W_{t+1} demonstrates an updated global approach after an iteration.

A server primarily selects clients who constrain association through active devices, after that the various parts of a system interrelate subsequently to complete an entire procedure:

i) On $t = 0$, a server produced a model was produced from the global data model. In this case, the number of parameters is estimated.
ii) Each k client $(k[1,\ldots,K])$ is required to leverage a global approach to transfer it, nevertheless of if they offer to FL procedure or not. Through individual private data, every k clients re-educate a global approach locally in parallel and designs a new group of local weights w_{t+1}^k.

iii) Chosen clients utilise an information gathered from IoT devices under their access to enhance an approach under estimation whereas keeping a local data's privacy.
iv) To keep client privacy, only the parameters of an updated model are transmitted to a central server.
v) After obtaining the modifications, a server aggregated weights from different node models to generate an unknown model (3). A FedAvg approach is utilised for aggregation. Thus, the parameters are estimated according to a database size at every node.
vi) Update model parameters are returned to clients through a central server.
vii) Every client utilises unknown network parameters and creates modifications according to an unknown data.
viii) For enduring model understanding and enhancement, steps 4 to 7 are repetitive.

3.1. Gradient descent optimization based weighted federated learning

An important limitation in FL is a network bandwidth, which restricts a speed at local updates from multiple establishments are aggregated in a cloud. To tackle this issue, FedAvg utilizes local data for GDO prior performing the weighted average aggregation approach uploaded through every node. An approach profits iteratively, update a global model in every training round according to contributions from contributing organizations. Conventional centralized learning methods integrate data from various organisations into an individual database. This leads to substantial message costs and hazards for data confidentiality. To solve these limitations, the privacy-preserving approach prepared through forecasting approach is proposed for FL. This solution begins through utilzing FedAvg approach for parameter aggregation, gathering incline data from different nodes. After that developed an improved type of FedAvg to reduce communication overhead as well as employ significant combination. This is predominantly advantageous for large-scale and distributed forecasting following:

i) Own supports from clients are weighted according to their data quantity as well as model effectiveness.
ii) An enhanced FL approach through FedAvg is utilized for vigorous aggregation, meets for system dynamic as well as and dawdlers.
iii) Rather than easy averaging, weighted averaging is used, where the weights are identified in terms of every client's data distribution, quality or estimation indices. This approach gives more inspiration to clients through most appropriate or higher-excellence data.
iv) Instead of simple calculation, recent combination approaches have been developed that incorporate statistical characteristics of client updates like variance intervals, to enable a more detailed and robust global update.
v) A purpose of utilizing weighted averaging is to deliberate data's irregular dispersion of data and excellence over clients. Thus, the clients, through less or minimal data from controlling a global approach update, are removed. Rather than evenly averaging an approach update from every client, the weights are applied to every client's update. The weights were estimated according to each client's data dispersal, quality as well as training effectiveness.
vi) Evaluation of a weight: for client *i*, assume d_i denotes the size of a data; q_i denotes a quality score; p_i illustrates an effectiveness of training. The weight w_i for a client is expressed in (4) and (5).

$$w_i = \lambda \times \frac{d_i}{\sum_{j=1}^{N} d_j} + \mu \times q_i + (1 - \lambda - \mu) \times p_i \quad (4)$$

$$w_i = \lambda \times \frac{\sum_{j=1}^{N} d_j}{d_i} + \mu \times q_i + (1 - \lambda - \mu) \times p_i \quad (5)$$

Here, λ and μ demonstrates the hyperparameters identifying the importance of data size as well as quality of a data individually. These assurances provide a most-balanced and accurate depiction of data from each cooperating client. At every communication round, every device estimates local update and then sends it to a central server for aggregation. This iteration continues till an approach meets or a prescribed count of communication rounds is encountered.

4. RESULTS AND DISCUSSION

In the investigation results, a significance of an introduced method of GDO-WFL privacy-preserving is estimated. The experiments of the introduced approach are realized on Python 3.10.12 through Windows 10 OS, 16 GB RAM and Intel i5 processor. A significance of introduced approach is validated through using numerous performance metrics such as accuracy, communication cost, computational cost, and running time.

4.1. Dataset description

This research utilises benchmark MNIST and CIFAR-10 datasets for implementing the significance of the introduced approach. MNIST [29] is a handwritten digital repair dataset involving 60,000 training instances as well as 10,000 testing samples, and 28×28 size grey-level image. MNIST is partitioned into multiple sub-datasets for FL, while a size of every sub-dataset is 100 instances. As associated with MNIST, CIFAR-10 [30] involves the most complex integration, comprising 60,000 32×32 color instances in 10 categories, with 6,000 instances per class. MNIST and CIFAR-10 datasets are broadly utilizing in ML operations like image classification. Whereas these datasets lack involvement of personally identifiable information (PII), they remain vulnerable to specific privacy attacks. A major security threat is involvement implication, where an attacker tries to determine a specific data point is portion of an actual database. Simultaneously, while MNIST and CIFAR-10 datasets lack involvement in PII, it is conceivable to re-classify entities through integrating a dataset with outside data. There is a greater issue that an attacker has tried to re-determine those individuals according to their features.

4.2. Performance evaluation

The significance of the proposed method is estimated with the previous methods by using various performance metrices. The existing methods, such as FL, FedAvg and optimized federate learning (OFL) are estimated and compared with the proposed GDO-WFL. The effectiveness of the proposed method is estimated by using various performance metrices such as number of rounds, number of clients and number of gradients or packets per user.

Table 1 demonstrates the performance evaluation of accuracy based on the number of rounds. The number of rounds such as 5, 10, 15, 20, and 25, is considered to estimate the significance of the introduced approach. In MNIST dataset, the proposed GDO-WFL approach attains the better accuracy of 99.3%, 98.5%, 98.7%, 98.8%, and 98.5% as well as in CIFAR dataset, the proposed GDO-WFL approach attains the better accuracy of 91.5%, 88.7%, 89.1%, 89.5%, and 89.7% based on the different number of rounds of 5, 10, 15, 20, and 25 individually.

Table 2 demonstrates the performance evaluation of accuracy based on the number of clients. The number of rounds such as 2, 4, 6, 8, and 10 is considered to estimate the significance of the introduced approach. In MNIST dataset, the proposed GDO-WFL approach attains the better accuracy of 94.5%, 94.7%, 95.0%, 95.3%, and 95.8% as well as in CIFAR dataset, the proposed GDO-WFL approach attains the better accuracy of 87.3%, 87.5%, 87.9%, 88.1%, and 88.3% based on the different number of rounds of 2, 4, 6, 8, and 10 individually.

Table 1. Performance evaluation of accuracy results (%) based on number of rounds

Dataset	Methods	Number of rounds				
		5	10	15	20	25
MNIST	FL	93.2	93.5	93.8	94.0	94.1
	FedAVg	95.8	95.9	96.3	96.7	96.8
	OFL	96.4	96.5	97.1	97.4	97.5
	GDO-WFL	99.3	98.5	98.7	98.8	98.8
CIFAR-10	FL	83.3	83.4	83.8	84.2	84.3
	FedAVg	84.3	84.5	84.7	84.9	85.0
	OFL	86.1	86.4	86.5	86.9	87.2
	GDO-WFL	91.5	88.7	89.1	89.5	89.7

Table 2. Performance evaluation of accuracy results (%) based on number of clients

Dataset	Methods	Number of clients				
		2	4	6	8	10
MNIST	FL	90.6	90.8	91.2	91.5	91.6
	FedAVg	92.5	92.8	92.9	93.1	93.3
	OFL	93.5	93.6	93.9	94.2	94.4
	GDO-WFL	94.5	94.7	95.0	95.3	95.8
CIFAR-10	FL	80.3	81.6	81.9	82.1	82.5
	FedAVg	83.3	83.7	83.8	84.2	84.5
	OFL	85.3	85.7	85.9	86.0	86.3
	GDO-WFL	87.3	87.5	87.9	88.1	88.3

Table 3 demonstrates the performance evaluation of communication cost based on gradients/packets per user. The number of gradients/packets per user such as 1,000, 2,000, 3,000, 4,000, and 5,000 are considered to estimate a significance of introduced approach. In MNIST dataset, the proposed GDO-WFL

approach attains the better communication cost of 490 KB, 510 KB, 530 KB, 610 KB, and 650 KB as well as in CIFAR dataset, the proposed GDO-WFL approach attains the better communication cost of 450 KB, 490 KB, 520 KB, 640 KB, and 60 KB based on the different number of gradients/packets per user of 1,000, 2,000, 3,000, 4,000, and 5,000 individually.

Table 3. Performance evaluation of communication cost (KB) based on gradients/packets per user

Dataset	Methods	Number of gradients/packets per user				
		1,000	2,000	3,000	4,000	5,000
MNIST	FL	570	600	610	660	700
	FedAVg	540	580	580	640	690
	OFL	520	540	560	630	670
	GDO-WFL	490	510	530	610	650
CIFAR-10	FL	550	590	640	710	740
	FedAVg	520	550	610	690	720
	OFL	490	530	570	660	700
	GDO-WFL	450	490	520	640	670

4.3. Comparative analysis

The comparative analysis of the proposed method based on the existing method is described in this section. Table 4 demonstrates the comparative analysis of the existing method with the proposed method. The effectiveness of the proposed method is validated based on two different datasets like MNIST and CIFAR-10.

Table 4. Comparative analysis of accuracy results (%) of the proposed method with the existing method

Method	Datasets	
	MNIST	CIFAR-10
Centralized learning [21]	98.2	89.3
Proposed GDO-WFL [22]	99.3	91.5

4.4. Discussion

The proposed GDO-WFL approach outperforms existing FL models by ensuring privacy and model performance even under heterogeneous client settings. Unlike previous models, it dynamically accounts for data quality and training effectiveness through weighted averaging, minimizing the effect of stragglers and low-quality contributors. The integration of Kafka-Zookeeper enables asynchronous communication and client anonymity, which is often lacking in traditional FL schemes. Secure aggregation combined with noise injection (DP) significantly reduces privacy leakage risk. The experimental results across MNIST and CIFAR-10 validate the superior accuracy and reduced communication overhead of GDO-WFL. Overall, the model demonstrates an efficient, secure, and scalable solution for FL environments.

5. CONCLUSION

FL is a popular collaborative learning which combinedly to update the weights or gradients for acquiring a global approach. Due to the weights or gradients are sensitive data, it has been investigated under various privacy-preserving approaches. This research proposes a novel privacy-preserving FL approach named GDO-WFL, which solves the problem of extreme contribution of low-quality data in federated training. Through developing a complex estimation value for a data, a non-positive influence of low-quality data on federated training is minimized, while make sure a privacy as well as security of contributor data by secure model. The experimental results illustrates that the proposed GDO-WFL approach attains the overall accuracy of 99.3% and 91.5% on MNIST and CIFAR-10 datasets as compared to the existing method of FedlabX method. In future research, it's important to focus on the impact of malevolent behaviours on both the client and server sides. For instance, a malicious client might manipulate its gradient to influence the accuracy of the global model, while a malicious server could provide users with falsified aggregated results.

FUNDING INFORMATION

Authors state no funding involved.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Gururaj Prakash Murthy	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓	
Chandrashekhar Pomu Chavan		✓				✓	✓	✓	✓	✓	✓	✓		✓

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

– The data that support the findings of this study are openly available in [2012 IEEE Conference on Computer Vision and Pattern Recognition] at http://doi.org/10.1109/CVPR.2012.6248110, reference number [29], upon reasonable request.
– The data that support the findings of this study are openly available in [Technical Report, University of Toronto] at https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf, reference number [30], upon reasonable request.

REFERENCES

[1] J. Zhang, Y. Liu, D. Wu, S. Lou, B. Chen, and S. Yu, "VPFL: a verifiable privacy-preserving federated learning scheme for edge computing systems," *Digital Communications and Networks*, vol. 9, no. 4, pp. 981–989, Aug. 2023, doi: 10.1016/j.dcan.2022.05.010.
[2] Z. Li, H. Bao, H. Pan, M. Guan, C. Huang, and H.-N. Dai, "UEFL: universal and efficient privacy-preserving federated learning," *IEEE Internet of Things Journal*, vol. 12, no. 10, pp. 14333–14347, May 2025, doi: 10.1109/JIOT.2025.3525731.
[3] L. Zhong, L. Zhang, L. Xu, and L. Wang, "MPC-based privacy-preserving serverless federated learning," in *2022 3rd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Jul. 2022, pp. 493–497. doi: 10.1109/ICBAIE56435.2022.9985933.
[4] J. Liu, X. Li, X. Liu, H. Zhang, Y. Miao, and R. H. Deng, "DefendFL: a privacy-preserving federated learning scheme against poisoning attacks," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 36, no. 5, pp. 9098–9111, May 2025, doi: 10.1109/TNNLS.2024.3423397.
[5] F. Wang, Y. He, Y. Guo, P. Li, and X. Wei, "Privacy-preserving robust federated learning with distributed differential privacy," in *2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2022, pp. 598–605. doi: 10.1109/TrustCom56396.2022.00087.
[6] J. Wang, R. Wang, L. Xiong, N. Xiong, and Z. Liu, "SAEV: secure aggregation and efficient verification for privacy-preserving federated learning," *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 39681–39696, Dec. 2024, doi: 10.1109/JIOT.2024.3445964.
[7] Y. Qiao, A. Adhikary, K. T. Kim, C. Zhang, and C. S. Hong, "Knowledge distillation assisted robust federated learning: towards edge intelligence," in *ICC 2024 - IEEE International Conference on Communications*, Jun. 2024, pp. 843–848. doi: 10.1109/ICC51166.2024.10622956.
[8] Z. Liu, J. Guo, W. Yang, J. Fan, K.-Y. Lam, and J. Zhao, "Dynamic user clustering for efficient and privacy-preserving federated learning," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–12, 2024, doi: 10.1109/TDSC.2024.3355458.
[9] Z. Zhang and R. Hu, "Byzantine-robust federated learning with variance reduction and differential privacy," in *2023 IEEE Conference on Communications and Network Security (CNS)*, Oct. 2023, pp. 1–9. doi: 10.1109/CNS59707.2023.10288938.
[10] Z. Lu, S. Lu, X. Tang, and J. Wu, "Robust and verifiable privacy federated learning," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 4, pp. 1895–1908, Apr. 2024, doi: 10.1109/TAI.2023.3309273.
[11] X. Wang, S. Wang, Y. Li, F. Fan, S. Li, and X. Lin, "Differentially private and heterogeneity-robust federated learning with theoretical guarantee," *IEEE Transactions on Artificial Intelligence*, vol. 5, no. 12, pp. 6369–6384, Dec. 2024, doi: 10.1109/TAI.2024.3446759.
[12] S. S. Nagesh, N. Fernando, S. W. Loke, A. G. Neiat, and P. N. Pathirana, "Honeybee-RS: enhancing trust through lightweight result validation in mobile crowd computing," in *2024 IEEE 23rd International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, Dec. 2024, pp. 2553–2558. doi: 10.1109/TrustCom63139.2024.00356.
[13] H. Zeng *et al.*, "BSR-FL: an efficient Byzantine-robust privacy-preserving federated learning framework," *IEEE Transactions on Computers*, vol. 73, no. 8, pp. 2096–2110, Aug. 2024, doi: 10.1109/TC.2024.3404102.

[14] S. Nazir and M. Kaleem, "Federated learning for medical image analysis with deep neural networks," *Diagnostics*, vol. 13, no. 9, Apr. 2023, doi: 10.3390/diagnostics13091532.
[15] L. Zhang, T. Zhu, P. Xiong, W. Zhou, and P. S. Yu, "A robust game-theoretical federated learning framework with joint differential privacy," *IEEE Transactions on Knowledge and Data Engineering*, vol. 35, no. 4, pp. 3333–3346, Apr. 2023, doi: 10.1109/TKDE.2021.3140131.
[16] A.-T. Tran and X.-S. Pham, "A novel privacy-preserving deep learning scheme for the classification of COVID-19 in chest X-ray images," in *2023 15th International Conference on Knowledge and Systems Engineering (KSE)*, Oct. 2023, pp. 1–6. doi: 10.1109/KSE59128.2023.10299433.
[17] M. Shen *et al.*, "Secure decentralized aggregation to prevent membership privacy leakage in edge-based federated learning," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 3, pp. 3105–3119, May 2024, doi: 10.1109/TNSE.2024.3360311.
[18] G. Zheng, L. Kong, and A. Brintrup, "Federated machine learning for privacy preserving, collective supply chain risk prediction," *International Journal of Production Research*, vol. 61, no. 23, pp. 8115–8132, Dec. 2023, doi: 10.1080/00207543.2022.2164628.
[19] K. O.-Agyemeng, Z. Qin, H. Xiong, Y. Liu, T. Zhuang, and Z. Qin, "MSDP: multi-scheme privacy-preserving deep learning via differential privacy," *Personal and Ubiquitous Computing*, vol. 27, no. 2, pp. 221–233, Apr. 2023, doi: 10.1007/s00779-021-01545-0.
[20] T. H. Rafi, F. A. Noor, T. Hussain, and D.-K. Chae, "Fairness and privacy preserving in federated learning: a survey," *Information Fusion*, vol. 105, May 2024, doi: 10.1016/j.inffus.2023.102198.
[21] Y. Yan *et al.*, "Fedlabx: a practical and privacy-preserving framework for federated learning," *Complex & Intelligent Systems*, vol. 10, no. 1, pp. 677–690, Feb. 2024, doi: 10.1007/s40747-023-01184-3.
[22] Y. Chen, B. Wang, H. Jiang, P. Duan, Y. Ping, and Z. Hong, "PEPFL: a framework for a practical and efficient privacy-preserving federated learning," *Digital Communications and Networks*, vol. 10, no. 2, pp. 355–368, Apr. 2024, doi: 10.1016/j.dcan.2022.05.019.
[23] Sumitra, J. Sharma, and M. V. Shenoy, "HAFedL: a Hessian-aware adaptive privacy preserving horizontal federated learning scheme for IoT applications," *IEEE Access*, vol. 12, pp. 126738–126753, 2024, doi: 10.1109/ACCESS.2024.3454074.
[24] H. Wang, Q. Wang, Y. Ding, S. Tang, and Y. Wang, "Privacy-preserving federated learning based on partial low-quality data," *Journal of Cloud Computing*, vol. 13, no. 1, Mar. 2024, doi: 10.1186/s13677-024-00618-8.
[25] L. Zhong *et al.*, "Dual-server-based lightweight privacy-preserving federated learning," *IEEE Transactions on Network and Service Management*, vol. 21, no. 4, pp. 4787–4800, Aug. 2024, doi: 10.1109/TNSM.2024.3399534.
[26] L. Wang, X. Zhao, Z. Lu, L. Wang, and S. Zhang, "Enhancing privacy preservation and trustworthiness for decentralized federated learning," *Information Sciences*, vol. 628, pp. 449–468, May 2023, doi: 10.1016/j.ins.2023.01.130.
[27] X. Sun, Z. Yuan, X. Kong, L. Xue, L. He, and Y. Lin, "Communication-efficient and privacy-preserving aggregation in federated learning with adaptability," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 26430–26443, Aug. 2024, doi: 10.1109/JIOT.2024.3396217.
[28] F. Shan, Y. Lu, S. Li, S. Mao, Y. Li, and X. Wang, "Efficient adaptive defense scheme for differential privacy in federated learning," *Journal of Information Security and Applications*, vol. 89, Mar. 2025, doi: 10.1016/j.jisa.2025.103992.
[29] D. Ciresan, U. Meier, and J. Schmidhuber, "Multi-column deep neural networks for image classification," in *2012 IEEE Conference on Computer Vision and Pattern Recognition*, Jun. 2012, pp. 3642–3649. doi: 10.1109/CVPR.2012.6248110.
[30] A. Krizhevsky, "Learning multiple layers of features from tiny images." *Technical Report*, University of Toronto, Toronto, Ontario, 2009. [Online]. Available: https://www.cs.toronto.edu/~kriz/learning-features-2009-TR.pdf

BIOGRAPHIES OF AUTHORS

Gururaj Prakash Murthy is research scholar at PES University. Completed bachelor of Engineering and master of Engineering in Visveswaraya institute of technology. Worked as software engineer 10 years in IT industry and presently working as an assistant professor from past three years. He can be contacted at email: gururajp@pes.edu.

Chandrashekhar Pomu Chavan received his B.E. degree in Computer Science and Engineering from Guru Nanak Dev Engineering College, Bidar, Karnataka, India, and his M. Tech degree in Network and Internet Engineering from Sri Jayachamarajendra College of Engineering, Mysore, Karnataka, India, where he secured the 3rd rank in the university. He later earned his Ph.D. in the field of Wireless Networking from the Indian Institute of Science (IISc), Bangalore, India. His core research interests include wireless networks, mobile ad-hoc networks (MANETs), IoT, artificial intelligence and machine learning (AIML), cloud computing, ubiquitous networks, network security, pervasive computing, context-aware systems, and post-quantum cryptography. He can be contacted at email: cpchavan@pes.edu.