International Journal of Safety and Security Engineering
Vol. 16, No. 6, June, 2026, pp. 1269-1278
Journal homepage: http://iieta.org/journals/ijsse

A Federated Metaheuristic Optimized Deep Learning Framework for Privacy-Preserving Intrusion Detection and Internet of Things Security Analytics

Sowmya T[1], Chandrakala G Raju[1], Sunitha S V[2*], Sujatha T[3], Ananth G S[4], Arpitha K[5], Anusha K S[5], Veena Dhavalgi[6]

[1] Department of Computer Science and Engineering, BMS College of Engineering, Bengaluru 560019, India
[2] Department of Electronics and Communication Engineering, BNM Institute of Technology, Bengaluru 560070, India
[3] Department of Information Science and Engineering, BNM Institute of Technology, Bengaluru 560070, India
[4] Department of Master of Computer Applications, The National Institute of Engineering, Mysuru 570008, India
[5] Department of Computer Science and Engineering, BGS Institute of Technology, Adichunchanagiri University, Mandya 571448, India
[6] Department of Computer Science and Engineering (Cyber-Security), Dayananda Sagar College of Engineering, Bengaluru 560078, India

Corresponding Author Email: sunithasv@bnmit.in

https://doi.org/10.18280/ijsse.160609

Received: 16 April 2026
Revised: 12 June 2026
Accepted: 25 June 2026
Available online: 30 June 2026

Keywords:
differential privacy, edge intelligence, Federated Learning, federated metaheuristic optimization, Grey Wolf Optimization, Particle Swarm Optimization

ABSTRACT

The rapid growth of Internet of Things (IoT) has resulted in significantly greater exposure to cyber threats such as Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), botnet (BoT), and reconnaissance attacks. To overcome these limitations, this study introduces a Federated Metaheuristic Optimized Deep Learning (FMODL) framework to provide privacy-protected IoT intrusion detection and security analytics via Federated Learning (FL), a hybrid Particle Swarm Optimization-Grey Wolf Optimization (PSO-GWO) strategy, and differential privacy. The combination of FL, a hybrid PSO-GWO strategy, and differential privacy allows the framework to achieve secure collaborative learning by not sharing any raw device data while allowing for multiple objectives of maximizing the accuracy of attack detection. It maintains the confidentiality of data while minimizing communication costs associated with each of the two objectives. In this study, the BoT-IoT and Telemetry, Operating Systems, and Network (TON)_IoT datasets are utilized to evaluate the FMODL framework in detecting botnet, DoS/DDoS, and reconnaissance attacks. The experimental results indicate that the FMODL framework achieved 96.4% and 94.8% attack detection accuracies on the respective BoT-IoT and TON_IoT datasets, outperforming established baseline FL techniques. The results support the assertion that the FMODL framework is an effective and scalable alternative to traditional Intrusion Detection System (IDS) systems for providing privacy-assured intrusion detection and security monitoring for IoT and Industrial Internet of Things (IIoT) applications in next-generation environments.

1. INTRODUCTION

The rapid growth of the Internet of Things (IoT) has created a huge number of connected devices which can produce enormous amounts of diverse data within domains such as healthcare, smart cities and industrial automation. The speed at which IoT is growing continues to accelerate and needs new techniques to support intelligent decision-making. Therefore, it is urgent that we apply more sophisticated analytical methods and use Deep Learning (DL) to discover valuable insights in these massive volumes of heterogeneous data across multiple domains. Because traditional centralized learning methods require transferring all raw data from the end-user IoT devices to be stored on cloud servers, there are many risks related to transmitting data; risks include concerns related to privacy and security, as well as large amounts of communication overhead. Federated Learning (FL) is an effective solution to support decentralized training in distributed systems using a federated approach for training models. Instead of sending and transferring raw data to a central location, each of the IoT devices holds its own datasets locally, and then collectively trains a global shared model, keeping data on their devices at all times, thereby preserving privacy and mitigating the risks associated with transmitting data over the network [1].

Many researchers have examined the use of FL in various IoT environments and have reported that FL can effectively improve privacy and security when using distributed systems [2]. While FL helps preserve user privacy and security, it is also vulnerable to privacy loss through updates sent to the shared global model and suffers from issues related to data heterogeneity, communication inefficiencies, and slow model convergence [3]. FL frameworks have widely adopted diffusion privacy in order to help reduce risks associated with

privacy. An IoT system's local differential privacy-based FL model [4] exhibits a high degree of data protection. In addition, an IoT-based FL hybrid-differential privacy method [5] has also enhanced security via IoT systems. These approaches have been continuously researched, and more recently, researchers have successfully combined differential privacy and FL in order to create a framework for cross-platform secure knowledge sharing [5, 6]. Although these approaches mitigate privacy risk, they tend to result in a compromise between privacy and model efficacy in IoT environments that are resource-starved [7].

Some of the challenges identified by several reviews and surveys regarding FL for IoT systems include non-optimized communications, scalability issues, and limited adaptation to waterfall models [8]. Research efforts have recently begun to integrate meta-learning and more advanced privacy-preserving technologies in order to fill these deficiencies via FL [9]. Nonetheless, all of these existing approaches were designed to either enhance privacy or enhance model efficacy but did not simultaneously address multiple conflicting objectives such as model Accuracy, Diversity, Adaptability (ADA), communication costs, and privacy preservation. One important area that current FL frameworks lack is the ability to adaptively optimize their parameters [10]. Most current models use a static hyperparameter setup, which does not work well in dynamic IoT environments where data is non-independent and non-identically distributed.

There is now a much larger attack surface available for bad actors to take advantage of due to the increasing volume of IoT and Industrial Internet of Things (IIoT). Thereby exposing systems to threats such as Denial of Service, Botnet (BoT) attacks and Reconnaissance attacks. Traditional centralized IDS are not able to function well in an IIoT environment due to issues such as lack of privacy, increased communication costs, and the inability of the system to expand its capability. Consequently, there is now a growing demand for FL-IDS as an alternative to traditional IDS. FL-IDS allows for distributed and privacy-preserving security analytics at the edge of the network rather than centralized.

Optimization methods have been developed for use in traditional machine learning, but your research into how those techniques fit into a federated framework, especially with regard to IoT data analytics, is still in its infancy. To address these limitations, we offer a new federated metaheuristic-optimized DL framework for privacy-preserving analytics in IoT environments. This new framework employs a unified approach that integrates FL and an adaptive optimization mechanism to enable dynamic tuning of model parameters, client participation and privacy budgets. The main benefit of our proposed approach is that it is capable of meeting multiple objectives, including maintaining the ADA of the created models, preserving user privacy, and minimizing communications costs at the same time, as well as providing a solution scalable enough for an IoT setting.

IDS currently used in IoT are dependent on centralised data, which leads to insecurity due to the risk of private information being disclosed, the possibility of delayed detection, as well as excessive communication overhead in real-time industrial applications. This study presents a method of providing a secure and effective means of intrusion detection via a framework for security analytics utilizing FL.

This research makes the following major contributions:

- Designed a federated DL framework to enable privacy-preserving analytics in the IoT using a metaheuristic optimization for adapting hyperparameter tuning and selecting clients.
- A multi-objective optimization approach for balancing the trade-offs between ADA, privacy, and communication costs. And the use of differential privacy techniques to protect against data exposure.
- A comprehensive experimental validation demonstrating the advantages of our methodology over many of the existing methods. The remainder of this paper is organized as follows: Section 2 provides a review of the related work with research gaps. Section 3 presents the proposed methodology and mathematical model. Section 4 discusses the experimental setup, dataset details, results and discussions. Finally, Section 5 concludes the paper.

2. RELATED WORK

Research on analytics in the IoT is shifting towards FL technologies to overcome privacy issues and scalability problems.

2.1 Security-focused Federated Learning for Internet of Things intrusion detection

Many studies have been conducted on FL focused on topics such as communication efficiency, optimizations, security, and resource management. An extensive survey evaluated the different techniques utilised in FL for the IoT. This research included an overview of major problems related to FL, including data heterogeneity, communication overhead and security risks. It lacks the specifics regarding the implementation of practical solutions and the development of optimization mechanisms needed to address the challenges presented [11]. As another example of recent developments within the area of FL, an overview of current trends in FL was provided, including an exploration of definition, architectures, and applications to the IoT. Although substantial effort was taken to develop the theory behind FL. It did not explore or identify potential methods to address the issues of performance optimization and real-time deployment for FL [12].

A systematic review analyzed resource optimization in IoT FL and discussed how to use resources, especially in terms of computation and communication, efficiently [13]. A FL framework that used the Lemurs optimizer to minimize communication overhead while still achieving accurate models. This approach was more efficient in terms of bandwidth usage, but it focused solely on optimizing communications rather than considering any privacy-utility trade-offs or multi-objective optimization [14]. The TSFed framework has been proposed to securely and efficiently use FL for industrial IoT networks in three stages: adaptive training, secure aggregation, and optimization. Although the TSFed framework improves system performance and security, it is complex and cannot adapt flexibly or dynamically to heterogeneous IoT environments [15].

An edge framework for federated meta-learning was developed, and a parameter optimization method was proposed to increase a model's ability to adapt to dynamics in the environment. Although the use of meta-learning will assist in generalizing across devices, the model does not consider privacy preservation or communication constraints directly [16]. Malicious node detection in Wireless Sensor Networks

utilizing Network Parameter Mining has been proposed. Their contributions improved network security; however, (i) they devote no attention to FL environments, and (ii) none of the privacy-preserving and distributed learning mechanisms are considered [17]. The authors include a survey on Blockchain-based FL in industrial IoT. In this instance, Blockchain contributes to secure aggregation strategies and trust management; however, it is very computationally intensive, making its use in resource-limited IoT devices impractical [18].

2.2 Privacy-preserving techniques in Federated Learning

A secure FL framework incorporating metaheuristic-based dimensionality reduction and multi-head attention for Distributed Denial-of-Service (DDoS) attack detection achieves improved performance for DDoS attack detection through enhanced detection ADA and robustness compared to more traditional FL techniques. However, these findings are only applicable to a specific application domain, with limited generalization across the broader IoT analytics spectrum [19]. Several optimization techniques were studied for the application of FL in heterogeneous 6G networks, focusing on system design and resource allocation strategies. Their contributions were effective in resolving the challenges associated with heterogeneity; nevertheless, they did not consider the use of privacy-preserving mechanisms or the application of adaptive learning strategies [20]. According to an investigation was conducted on the application of federated machine learning to IoT devices with limited energy resources using a systematic mapping approach. This research identified energy efficiency as an important criterion but did not provide any specific frameworks to measure how energy consumed could be optimized while maintaining the model's ADA or privacy [21].

A comprehensive review of applications, trends and challenges of federated machine learning in IoT-based systems we studied. Despite offering valuable insights that help to shape future research avenues, no concrete solutions are provided to optimise or enhance privacy [22]. The hashing of image datasets to improve dataset quality were used. Although the approach presents a contribution to data preprocessing and quality improvement, the focus is not on federated machine learning or privacy-preserving IoT analytics [23].

2.3 Optimization and resource-efficient Federated Learning

A technology architecture for privacy-preserved IoT with integrated federated machine learning and lightweight natural language processing (NLP) has designed. The architecture aids in enhancing privacy and enabling effective processing of textual IoT data; however, there remains no advanced optimization mechanism deployed or the communication efficient issue is resolved [24]. An energy-aware intrusion prevention system based on deep reinforcement learning for IoT environments has been designed [25]. The system addresses the improvement of both security and energy efficiency in an IoT environment but does not provide support for federated machine learning and therefore cannot guarantee privacy preservation through decentralization of the system.

It is concluded from the above literature that most of the current works are focused on only one type of aspect, privacy, communication or optimization. While there is still few research that combines Metaheuristic Optimization with FL. There is a shortage of works that account for the three metrics of multi-objective optimization. In addition, the currently available frameworks for this type of research have no adaptive, scalable solutions to deal with possible situations in dynamic IoT environments. Therefore, this paper proposes a novel federated metaheuristic-optimized DL framework. It jointly optimizes model performance, the ability to preserve privacy, and the efficiency of communication while providing an analytic solution for IoT systems.

3. PROPOSED MODEL

The Federated Metaheuristic Optimized Deep Learning (FMODL) framework will allow users to do much more than just monitor their networks. With the FMODL framework, users will have the ability to analyze their network traffic for malicious activity such as Denial-of-Service (DoS) attacks, DDoS attacks, and reconnaissance attacks, while still protecting user privacy and personal information. This paper presents an efficient FMODL framework to overcome several IoT analytics challenges, including the issues of data privacy, communication overhead, and model adaptability. FMODL combines several technologies: i.e., FL for decentralized training of a model, metaheuristic optimization for adjusting the trained model's parameters adaptively, and differential privacy to provide a secure communication mechanism. By using a multi-objective optimization strategy, the proposed FMODL model provides a means for balancing and optimizing ADA, privacy, and communication efficiency in the rapidly changing environment of IoT devices. Figure 1 shows the detailed design architecture of the proposed FMODL framework.

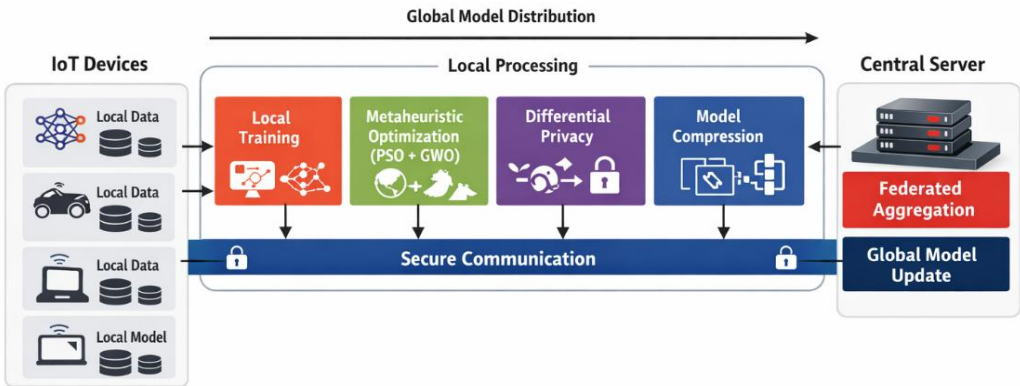

Figure 1. Proposed Federated Metaheuristic Optimized Deep Learning (FMODL) framework design diagram

This depicts an overview of an FL approach within an IoT setting that allows multiple devices to train local models based on their own data without direct sharing of it. To enhance model performance, each device employs metaheuristic strategies including the use of PSO and GWO, followed by implementing differential privacy to ensure privacy of the data.

Before model updates are sent from the devices to a central server for aggregation, the models' size is reduced via model compression to minimize the communication overhead associated with sending the model updates over a secured channel of communication. Once sent to the server, each respective federated aggregated model is then sent back to the devices to allow for continued training and enhancement of the local models based on the performance improvements achieved through FL methods. The data that the *i*-th client has is represented as D_i by the formula presented in Eq. (1).

$$D_i = \{(x_j, y_j)\}_{j=1}^{n_i} \tag{1}$$

where, x_j, y_j are the input feature vector and label of data point j, respectively, and n_i is the number of samples that client i has. The data pre-processing steps done before training using the proposed model include data cleaning. Additionally, before using the raw input data obtained from IoT devices as the raw form of input with respect to the proposed model algorithm, the process of normalizing by Eq. (2) is also completed. The x' will have a mean of 0 and a unit variance which improves convergence during the training phase and stabilizes the entire learning process across the multiple clients by determining how much each feature contributes to the overall model.

$$x' = \frac{x - \mu}{\sigma} \tag{2}$$

where, the output x' is returned when x (the raw input feature vector from the IoT devices) is transformed by normalizing it using the mean μ and standard deviation σ of the dataset.

Eq. (3) defines how the input interacts as it passes through each layer of the DL architecture. The term h^l shows the output of the *l*-th layer, while h^{l-1} indicates the output from the previous layer.

$$h^{(l)} = \sigma\left(W^{(l)} h^{(l-1)} + b^{(l)}\right) \tag{3}$$

where, W^l refers to the weights between layers (l-1) and l, and b^l is the bias vector for layer l. The function $\sigma(\cdot)$ is a nonlinear activation function such as ReLU or sigmoid, which adds non-linearity to the system.

An entirely interconnected DNN is utilized for classification by each IoT client utilizing a local DL model. The network contains an input layer that matches the feature dimension of the dataset, three hidden layers containing 128, 64 and 32 neurons respectively, with ReLU activations applied to all neurons within the hidden layers. The application of the ReLU activation function ensures that there are non-linear features to be learned by the model and allows for a faster rate of convergence. A dropout regularization factor of 0.3 is applied to all hidden layers to mitigate overfitting within a heterogeneous and non-IID IoT environment. A softmax activation function is used within the output layer to perform multi-class classification. The model is trained using the Adam optimizer with categorical cross-entropy as the loss function, with a batch size of 64 (varying from 32–128 depending on resource availability) and 3–5 local epochs per round of federated communication. The learning rate is dynamically adapted to be within the range of [0.0001, 0.01] utilizing the proposed Particle Swarm Optimization-Grey Wolf Optimization (PSO-GWO) optimization strategy, and weight initialization using Xavier initialization improves convergence stability. All clients utilize the same architecture to ensure that all federated nodes and datasets are fair and reproducible. Therefore, the use of this function assists with the development of the model from the IoT data, allowing for identification of complex patterns formed by data during the local training phases. The loss function is given by Eq. (4).

$$\mathcal{L}_i = \frac{1}{n_i} \sum_{j=1}^{n_i} \ell(f(x_j; w), y_j) \tag{4}$$

where, n_i represents the total number of training samples available for client i, which allows the prevalence of loss to be equalized across all local data. Each (x_j, y_j) pair corresponds to the feature vector and label. The function $f(x_j; w)$ gives the output of the DL architecture by applying the parameters w. And, the function $l(\cdot)$ is the loss function to use the DL model is built to learn by minimizing prediction error using IoT data that are readily available to the training clients.

The model update rule defines the new global model parameters after each communication round. The model updating process is given in Eq. (5).

$$w_i^{t+1} = w^t - \eta \nabla \mathcal{L}_i(w^t) \tag{5}$$

where, the new local summary of the model is defined by the local model parameters w^t at client *i* after each communication round. The learning rate is defined as η, which defines the magnitude of the update step. The gradient $\nabla L_i(W^t)$ points in the direction that the loss function is increasing the most. Therefore, subtracting the gradient will move in the direction of the minimum of the loss function. Each client performs this update locally so that the FL framework learns in a decentralized mode.

The proposed framework incorporates a hybrid metaheuristic method for optimization, which combines PSO and the GWO to dynamically tune the hyperparameters of an ML model such as learning rate, batch size, and network configuration. PSO allows exploration of the global search space for solutions, and GWO will allow exploitation of the local search space, thus leading to faster convergence and better ADA. The hybrid optimization strategy has been found especially useful for addressing non-IID and dynamic data distributions from IoT devices.

3.1 Hybrid Particle Swarm Optimization-Grey Wolf Optimization mechanism

The Particle Swarm Optimization equation defines how candidate solutions are updated by Eqs. (6) and (7).

$$v_i^{t+1} = \omega v_i^t + c_1 r_1 (pbest_i - x_i^t) + c_2 r_2 (gbest - x_i^t) \tag{6}$$

$$x_i^{t+1} = x_i^t + v_i^{t+1} \tag{7}$$

where, the particle velocity is given by the equation v_i^t and its current position is defined by the equation x_i^t as potential candidates for solutions. $pbest_i$ denote the local best position and $gbest$ global best position, we use the letters p and r for the control parameters ω, c_1 and c_2 to determine how much exploration and exploitation will occur, and we use the random variables u_1 and u_2 in the range of 0 to 1. The position update generated by the GWO is achieved by means of Eqs. (9) and (10).

$$D = | C \cdot X_p - X | \tag{8}$$

$$X(t+1) = X_p - A \cdot D \tag{9}$$

$$X_{new} = \frac{X_\alpha + X_\beta + X_\delta}{3} \tag{10}$$

where, X_α denotes the first best candidate solution, X_β the second and X_δ the third best candidate solutions. These will be the best candidates to lead the leadership structure in GWO. With respect to the control parameters, A and C will allow for movement to be made towards the optimal solution and provide sufficient exploration and exploitation of the space of solutions.

The hybrid method combines the strengths of each of these optimization methods using Eq. (11).

$$X_{hybrid} = \lambda X_{PSO} + (1-\lambda) X_{GWO} \tag{11}$$

where, λ represents the weighting factor for determining the contribution of the PSO and GWO methods to the overall performance. The hybridization of these two methods allows for improvement in the speed of convergence of the method and the quality of the solution produced.

3.2 Privacy preservation mechanism

In order to protect the confidentiality of the data, the framework employs a differential privacy mechanism by introducing controlled noise to the local model update prior to transmission. This prevents any malicious party from being able to reconstruct sensitive data from the model parameter or gradient. Through the use of a tunable parameter, it is possible to adjust the level of privacy protection while still maintaining the ADA of the model. The addition of noise is represented in Eq. (12).

$$\tilde{g}_i = g_i + \mathcal{N}(0, \sigma^2) \tag{12}$$

where, $N(0, \sigma^2)$ is defined as a Gaussian distribution, μ = 0 and $\sigma = \sigma^2$. Therefore, when generating the noisy gradient $\tilde{g}_i$. It is impossible for adversaries to use any piece of local data to infer sensitive data. The value of the parameter σ will determine the amount of noise added. The privacy budget is defined by Eq. (13).

$$\epsilon = \frac{\Delta f}{\sigma} \tag{13}$$

where, ϵ measures how much privacy has been guaranteed to the user, Δf represents how sensitive the output function is to changes in data, σ is the standard deviation of the added $N(0, \sigma^2)$, and it will correlate with how much an input datapoint impacts performance. Communication cost is defined as Eq. (14).

$$\widehat{w}_i = Q(w_i) \tag{14}$$

where, w_i represents the local model parameters at client i, and $Q(\cdot)$denotes a compression function such as quantization or sparsification. The communication cost is formulated as Eq. (15). This calculation provides a total amount of data sent between clients for every communication round. Reducing this communication cost is critical for effective FL solutions in large-scale IoT systems.

$$C_{comm} = \sum_{i=1}^{K} | w_i | \tag{15}$$

where, C_{comm} denotes the total communication overhead, K denotes the total number of clients participating in the system, and $|w_i|$ represents the size of model parameters being sent by each client.

3.3 Federated aggregation strategy

The global server uses a weighted average aggregation procedure when compiling the weighted private updates it receives from the participatory clients. This process provides clients with larger datasets more benefit to the global model than clients with smaller datasets. Therefore, this weighted average aggregation process is performed repeatedly until the global model converges, as outlined by Eq. (16).

$$w^{t+1} = \sum_{i=1}^{K} \frac{n_i}{\sum_j n_j} \cdot \widehat{w}_i \tag{16}$$

where, the updated global model at round $t+1$ is denoted by w^{t+1}, and the parameters of the compressed and privatized local model are denoted by $\widehat{w}_i$. The number of samples at client i is represented by the term n_i and, the total number of samples across all of the participating clients is indicated by the term $\sum_j n_j$.

Select the most appropriate clients to participate in the training process; as such, it provides efficient and reliable training, while minimizing the consumption of resources. The client score for client *i* is given by Eq. (17).

$$S_i = \alpha_1 Acc_i + \alpha_2 E_i - \alpha_3 L_i \tag{17}$$

where, S_i represents the score for client i based on the suitability for training, while the ADA of the local model for that client is given by the term Acc_i. E_i represents the energy available for the device of client i, L_i indicates the communication latency. The coefficients $\alpha_1, \alpha_2, \alpha_3$ determine the weighting of these three factors for each client. The clients with the highest scores will be selected to participate in the training process, thereby maximizing the efficiency of the network resources and the stability of the training process.

3.4 Multi-objective optimization

The proposed framework for the learning process as a multiple-object optimization problem, rather than solely focusing upon achieving increased prediction performance.

This model offers optimization of ADA, privacy and communication costs simultaneously and therefore provides a practical balanced solution for IoT systems in the real world as a whole. The overall optimization objective will be represented as defined in Eq. (18).

$$\mathcal{F} = \alpha\mathcal{L}_{acc} + \beta\mathcal{L}_{priv} + \gamma\mathcal{L}_{comm} \quad (18)$$

where, F represents the total optimization objectives, $\mathcal{L}_{acc}$ denotes the ADA loss, $\mathcal{L}_{priv}$ denotes the privacy loss, and $\mathcal{L}_{comm}$ denotes the communication cost. The weights α, β, γ represent the balance of competing objectives. This formulation ensures that model optimization can take place on all three objectives at once.

The iterative training process continues until the global model has converged. The convergence will be determined by changes in the model weights between successive rounds. Thus, ensuring that the model's optimization process does not create any unnecessary computations. The condition for convergence will be expressed in Eq. (19).

$$| w^{t+1} - w^t | < \delta \quad (19)$$

where, w^t and $(w^t + 1)$ refer to the global parameters of the model during each of the two communication rounds, while the threshold value δ is a very small number. Once two consecutive model parameters have been updated in such a way that the distance between them is less than δ, then the model has converged. This criterion guarantees that training is stable over time and avoids having to perform unneeded computations later.

The overall process starts from the IoT devices where data is collected to create a local model that trains and optimizes itself before sending an optimized update to the central server. The optimized update has been compressed and completes the privacy process before it is sent to the central server to be aggregated with other updates. After the central server has created an updated global model based on aggregation, the updated global model is sent back to clients for them to continue the process iteratively until the model has converged. The iterative way to build the model continues to allow learning while conserving privacy and minimizing communication cost.

4. RESULTS AND DISCUSSION

4.1 Experimental setup

This section provides a detailed experimental setup, dataset, and results of the FMODL framework. A Python implementation consisting of TensorFlow/PyTorch for the DL backend and the FL simulation environment will allow experimentation over a system consisting of an Intel i7 CPU with 16GB of RAM with GPU acceleration enabled. The simulator consists of a number of IoT edge devices or 'clients' which have a heterogeneous distribution of data respectively.

The network performance evaluation occurs in a controlled environment where communication latency, bandwidth constraints and packet loss are emulated to represent the IOT environment by three different variables. These are latency, defined as the end-to-end delay between the client's transmission of model updates and the global model's return of those updates for each communication round. Throughput, defined as the total amount of correctly transmitted data over time across all clients, is to be determined. Packet delivery ratio is defined as the number of packets received successfully divided by the total number of packets that are sent, and energy consumption is determined using a combined communication and computation cost model for IoT edge devices. To ensure statistical validity, all experiments will be performed 10 times independently using different random seeds.

4.2 Datasets description

The experiments have been carried out to evaluate the effectiveness of FMODL to confirm the performance of it using benchmark IoT datasets. The datasets chosen for this study are the BoT-IoT Dataset [26] and Telemetry, Operating systems, and Network (TON)_IoT Dataset [27]. These are both widely used as data sources for evaluating intrusion and anomaly detection in IoT environments. The BoT-IoT Dataset contains a realistic representation of botnet attack data recorded over its lifespan provides different categories of botnet attacks, including: DDoS, DoS, and reconnaissance attacks. The TON_IoT Dataset provides telemetry data collected from multiple sources like IoT sensors, operating systems, network systems within the Internet of Things. Each dataset provided an example of heterogeneous data collected, consequently, allowing for the evaluation of FMODL as compared to the non-IID distribution of data used within FL.

Preprocessing of each dataset involved removing rows from the datasets with missing values, normalising all features using z-score normalisation, and encoding certain feature types that are categorical in nature. Once these processing steps are completed, simulations are conducted across a number of clients where all clients are provided a set of non-overlapping data to allow for similarities related to data heterogeneity.

The proposed FMODL framework performs under IoT conditions, a thorough analysis of the network performance at the network level has been conducted using two datasets, BoT-IoT, and TON_IoT. This assessment is centered around important metrics such as latency, throughput, packet delivery ratio (PDR), and energy consumption, which are very important to distributed IoT environments.

4.3 Performance analysis across datasets

Table 1 and Figure 2 show a comparison of the network performance of the proposed FMODL model between the two datasets. The performance of the model is shown to be better on the BoT-IoT dataset as it had a lower latency of 120 ms compared to 135 ms for TON_IoT, indicating that data is being processed and responded to more rapidly. The throughput achieved with the BoT-IoT dataset is also better than that seen with the TON_IoT dataset (920 kbps compared to 880 kbps), suggesting that the FMODL model is able to transmit more data over time in real-time. The packet delivery ratio (PDR) shows congestion due to the number of packet losses in the BoT-IoT dataset (98.2%) compared to the TON_IoT dataset (97.5%), providing for better reliability when communicating that there will be fewer packet drops as a result of using the BoT-IoT dataset. Finally, the BoT-IoT dataset showed lower energy consumption results (0.85 J) than with the TON_IoT dataset (0.92 J), indicating that the FMODL model is more energy-efficient when used on the BoT-IoT dataset. Overall, the proposed FMODL model demonstrates good network performance and resource efficiency when operating with the

BoT-IoT dataset.

Table 1. Proposed model network performance comparison using different datasets

Metric	BoT-IoT (FMODL)	TON_IoT (FMODL)
Latency (ms)	120	135
Throughput (kbps)	920	880
Packet Delivery Ratio (%)	98.2	97.5
Energy Consumption (J)	0.85	0.92

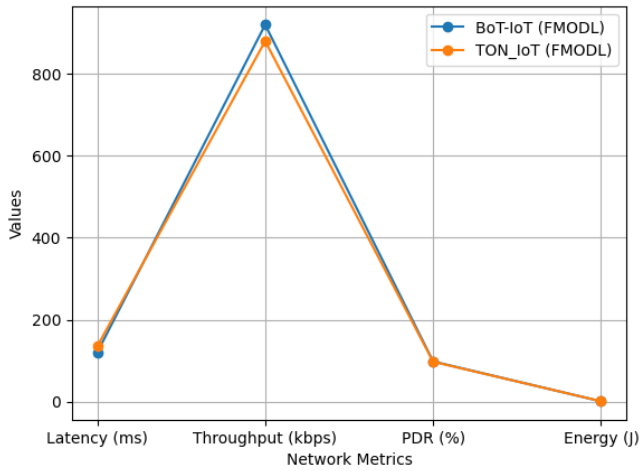

Figure 2. Network performance comparison of Federated Metaheuristic Optimized Deep Learning (FMODL) model

The performance of the proposed model based on BoT-IoT and TON_IoT datasets is shown in Table 2 and Figure 3 under several classification metrics. The metrics include ADA, Malicious Traffic Detection Efficiency (MTDE), False Alarm Reduction Capability (FARC) and Intrusion Classification Performance (ICP). The proposed model achieved better performance on the BoT-IoT dataset with the following classification metrics; ADA (96.4%), FARC (95.8%), DE(95.1%), and ICP (95.4%) compared to the TON_IoT dataset that recorded slightly lower classification metrics than the BoT-IoT dataset; ADA (94.8%), FARC (94.1%), MTDE (93.5%), and ICP (93.8%). From these results, we can say that the proposed model can more accurately identify and classify patterns from the BoT-IoT dataset; however, the proposed model maintains high-quality performance on both datasets.

To evaluate the contribution of each component in the proposed FMODL framework, an ablation study is conducted on both BoT-IoT Dataset and TON_IoT Dataset. The study systematically removes or modifies key modules namely metaheuristic optimization, differential privacy, and communication optimization to analyze their individual impact on overall model performance.

The additional ablation analysis incorporates the same four separate base models tested using independent optimization techniques (only using PSO and only using GWO) in addition to using FL without optimization models. The results of the experiment indicate that both PSO and GWO alone perform better than traditional FL-based algorithms; however, the proposed hybrid algorithm (PSO + GWO) demonstrates higher averages on each independent trial than either algorithm alone while exhibiting reduced standard deviations on each trial. This validates the use of both forms of exploration (PSO) and exploitation (GWO) together within an FMODL model.

Table 2. Performance of the proposed model on both datasets

Metric	BoT-IoT Dataset (%)	TON_IoT Dataset (%)
ADA	96.4	94.8
FARC	95.8	94.1
DE	95.1	93.5
ICP	95.4	93.8

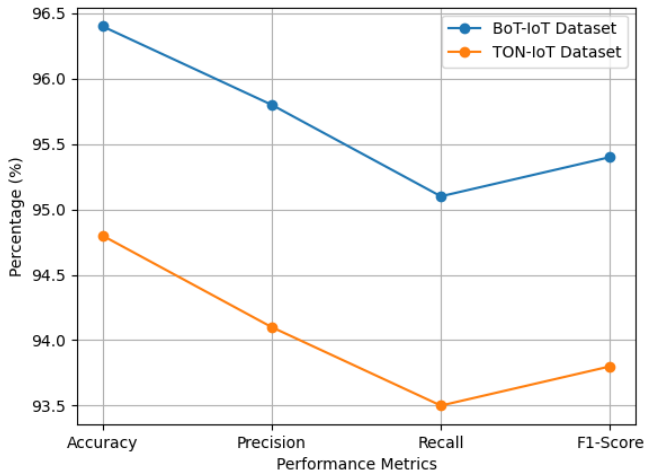

Figure 3. Performance comparison of proposed Federated Metaheuristic Optimized Deep Learning (FMODL) model

Table 3 shows the results of an ablation study that evaluates the impact of every element that makes up the new FMODL framework on the BoT-IoT and TON_IoT datasets. The full FMODL model has the most considerable values for all five metrics at ADA, with everyone receiving a score of 96.4% and 94.8%, respectively. This signifies that all elements integrated together can produce a very efficient model for classification. When the meta-heuristic optimization is excluded, there is a large decline in performance, indicating that meta-heuristics are very important for improving the efficiency of learning. Likewise, removing differential privacy resulted in a slight drop in output values, which indicates there is a small trade-off between privacy and ADA. Therefore, those who are concerned with privacy could see a decrease in performance. Also, removing the communication optimization resulted in a significant decrease in output value. This shows communication optimization has a significant effect on ensuring the efficient transfer of data through a given communication medium. Therefore, all modifications made to improve the FMODL framework contribute collectively to improving ADA, FARC, MTDE, and ICP for the models on both data sets.

Baseline models like Centralized DL, FL, and FL with Differential Privacy are all re-implemented in the same experimental environment using the BoT-IoT and TON_IoT data sets. To allow for comparison to existing literature qualitatively, but not quantitatively, given that there are differences between the datasets used in this research and elsewhere, as well as with preprocessing methods and evaluation protocols employed in various studies.

Table 4 shows that the new FMODL framework greatly surpasses the performance of the baseline methods for all evaluation metrics. The centralized deep-learning approach yields reasonable performance, though it does not have

privacy protection. The federated-learning strategy offers some added protection against illegal access to your data, but the performance degrades significantly with non-IID data-distributing concerns. Adding differential privacy to the FL model provides additional protection, but because you must add noise to the data before you analyze it, this also leads to decreased ADA by a small amount. In comparison, the new FMODL approach integrates the federated-learning model, protects the privacy of the data, and employs hybrid optimisation to achieve good results with an ADA of 96.4%, FARC 95.8%, MTDE 95.1%, and ICP 95.4%. This illustrates the effectiveness and capability of the FMODL framework to operate successfully with IoT data.

Results from Table 5 clearly indicate that there is a trade-off between preserving privacy and improving model performance through differential privacy in the FMODL framework. A low privacy budget ($\varepsilon = 0.5$) contributes to heavier additions of noise into the gradients for greater privacy, though the ADA is significantly lower (91.2% and 89.7% on BoT-IoT and TON_IoT respectively). As the privacy budget increases ($\varepsilon = 1.0$ and $\varepsilon = 2.0$), the amount of additional noise decreases, which allows the model to learn more representative patterns from the data resulting in improved ADA. At $\varepsilon = 5.0$, the model experiences a minimal effect from noise, providing the highest level of performance (96.4% and 94.8%). Overall, the results obtained conform to what has been expected relative to differential privacy, whereby FMODL achieves a consistent balance of privacy preservation versus predictive ADA across varying budgets of privacy.

The results of the experiments showed that the proposed FMODL framework has achieved a better and higher level of performance than the baseline models for both the BoT-IoT and the TON_IoT datasets. The overall results confirm that the FMODL framework is able to achieve a very good balance between ADA, privacy, and efficiency for IoT analytic applications.

Table 3. Ablation study results on both datasets

Configuration	BoT-IoT Dataset				TON_IoT Dataset			
	ADA (%)	FARC (%)	MTDE (%)	ICP (%)	ADA (%)	FARC (%)	MTDE (%)	ICP (%)
Full FMODL (Proposed)	**96.4**	**95.8**	**95.1**	**95.4**	**94.8**	**94.1**	**93.5**	**93.8**
Without Metaheuristic Optimization	93.2	92.4	91.6	92.0	91.5	90.8	90.2	90.5
Without Differential Privacy	95.1	94.5	94.0	94.2	93.6	92.9	92.3	92.6
Without Communication Optimization	94.3	93.7	93.1	93.4	92.7	92.0	91.4	91.7
Federated Learning (FL) only	93.2	92.4	91.6	92.0	91.5	90.8	90.2	90.5
FL+ Particle Swarm Optimization (PSO)	94.6	93.2	93.4	93.1	92.8	92.1	92.4	91.5
FL+ Grey Wolf Optimization (GWO)	94.3	93.1	93.7	92.9	92.5	91.5	91.6	91.8

Table 4. Performance comparison on Internet of Things (IoT) datasets

Method	ADA (%)	FARC (%)	MTDE (%)	ICP (%)
Centralized Deep Learning (DL)	91.8	90.5	89.7	90.1
Federated Learning (FL)	93.2	92.4	91.6	92.0
FL + Differential Privacy	92.5	91.2	90.8	91.0
Proposed FMODL	96.4	95.8	95.1	95.4

Table 5. Trade-off between privacy and model performance

E Value	ADA (BoT-IoT)	ADA (TON_IoT)
0.5 (high privacy)	91.2%	89.7%
1.0	93.8%	92.4%
2.0	95.6%	94.1%
5.0 (low privacy)	96.4%	94.8%

5. CONCLUSION

This paper describes a novel FMODL framework for conducting IoT data analysis that ensures both user privacy and security. The FMODL Framework incorporates FL, a hybrid metaheuristic optimization methodology, and differential privacy to overcome common obstacles encountered in privacy-sensitive environments. In terms of performance metrics, the general outputs of the FMODL Framework are evaluated against benchmarked datasets provided an ADA rating of 96.4% and 94.8% with high FARC, DE, and ICP ratings. Similarly, the MMODL framework demonstrated good levels of communication efficiency compared to traditional benchmarked methods producing high levels of performance compared to those traditional benchmarked methods.

Future research will be concentrated on expanding the FMODL Framework to support large-scale, dynamic IoT systems, accommodating adaptable methods for maintaining data privacy, and evaluating lightweight approaches to implementing analytics on resource- limited edge devices. Further exploration of deploying the FMODL Framework in real time and validating performance results across varying domains will provide an opportunity to improve the overall scalability and generalization of performance outputs when deploying practical IoT solutions.

REFERENCES

[1] Kuppili, Y.K., B., J.J. (2023). Federated learning for IoT: Ensuring privacy and security in distributed networks. International Journal of Intelligent Systems and

Applications in Engineering, 12(1s): 171-179. https://www.ijisae.org/index.php/IJISAE/article/view/3404.

[2] Sharma, S., Guleria, K. (2023). A comprehensive review on federated learning based models for healthcare applications. Artificial Intelligence in Medicine, 146: 102691. https://doi.org/10.1016/j.artmed.2023.102691

[3] Elzemity, A., Arief, B. (2024). Privacy threats and countermeasures in federated learning for Internet of Things: A systematic review. In 2024 IEEE International Conferences on Internet of Things (iThings) and IEEE Green Computing & Communications (GreenCom) and IEEE Cyber, Physical & Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics, Copenhagen, Denmark, pp. 331-338. https://doi.org/10.1109/iThings-GreenCom-CPSCom-SmartData-Cybermatics62450.2024.00072

[4] Zhao, Y., Zhao, J., Yang, M.M., Wang, T., Wang, N., Lyu, L. (2021). Local differential privacy-based federated learning for Internet of Things. IEEE Internet of Things Journal, 8(11): 8836-8853. https://doi.org/10.1109/JIOT.2020.3037194

[5] Liu, W.Y., Cheng, J.H., Wang, X.L., Lu, X.J., Yin, J.W. (2022). Hybrid differential privacy based federated learning for Internet of Things. Journal of Systems Architecture, 124: 102418. https://doi.org/10.1016/j.sysarc.2022.102418

[6] Khalaf, O.I., Ashokkumar, S.R., Algburi, S., Anupallavi, S., Selvaraj, D., Sharif, M.S., Elmedany, W. (2024). Federated learning with hybrid differential privacy for secure and reliable cross-IoT platform knowledge sharing. Security and Privacy, 7(3): e374. https://doi.org/10.1002/spy2.374

[7] Shaik, S.B., Tadikonda, S. (2023). Federated learning with differential privacy for secure and scalable edge computing in IoT systems. SSRN. http://doi.org/10.2139/ssrn.5270348

[8] Hu, R., Guo, Y.X., Ratazzi, E.P., Gong, Y.M. (2020). Differentially private federated learning for resource-constrained Internet of Things. arXiv preprint arXiv:2003.12705. https://doi.org/10.48550/arXiv.2003.12705

[9] Li, H., Ge, L., Tian, L. (2024). Survey: Federated learning data security and privacy-preserving in edge-Internet of Things. Artificial Intelligence Review, 57(5): 130. https://doi.org/10.1007/s10462-024-10774-7

[10] Telkar, S.S., Yogi, M.K. (2025). A comprehensive review of differential privacy with federated meta-learning for privacy-preserving medical IoT. ICCK Transactions on Wireless Networks, 1(1): 16-31. https://doi.org/10.62762/TWN.2025.327420

[11] Dritsas, E., Trigka, M. (2025). Federated learning for IoT: A survey of techniques, challenges, and applications. Journal of Sensor and Actuator Networks, 14(1): 9. https://doi.org/10.3390/jsan14010009

[12] Papadopoulos, C., Kollias, K.F., Fragulis, G.F. (2024). Recent advancements in federated learning: State of the art, fundamentals, principles, IoT applications and future trends. Future Internet, 16(11): 415. https://doi.org/10.3390/fi16110415

[13] Silva, L.G.F., Sadok, D.F.H., Endo, P.T. (2023). Resource optimizing federated learning for use with IoT: A systematic review. Journal of Parallel and Distributed Computing, 175: 92-108. https://doi.org/10.1016/j.jpdc.2023.01.006

[14] Al-Betar, M.A., Abasi, A.K., Alyasseri, Z.A.A., Fraihat, S., Mohammed, R.F. (2024). A communication-efficient federated learning framework for sustainable development using lemurs optimizer. Algorithms, 17(4): 160. https://doi.org/10.3390/a17040160

[15] Putra, M.A.P., Karna, N.B.A., Zainudin, A., Kim, D.S., Lee, J.M. (2024). TSFed: A three-stage optimization mechanism for secure and efficient federated learning in industrial IoT networks. Internet of Things, 27: 101287. https://doi.org/10.1016/j.iot.2024.101287

[16] Zhu, X.F., Fan, Q.S., Peng, J.Q., Qian, Y.W. (2025). A federated meta-learning aided intelligent edge framework by using the parameter optimization approach. Journal of Wireless Communications and Networking, 2025: 84. https://doi.org/10.1186/s13638-025-02511-7

[17] Sunitha, R., Chandrika, J. (2021). Malevolent node detection based on network parameters mining in wireless sensor networks. International Journal of Digital Crime and Forensics (IJDCF), 13(5): 130-144. https://doi.org/10.4018/IJDCF.20210901.oa8

[18] Shawkat, M., El-desoky, A., Ali, Z.H., Salem, M. (2025). Blockchain and federated learning based on aggregation techniques for industrial IoT: A contemporary survey. Peer-to-Peer Networking and Applications, 18: 192. https://doi.org/10.1007/s12083-025-01991-0

[19] Alanazi, A.A., Althbiti, A., Ghorashi, S.A., Birkea, F.M.O., Soto-Diaz, R., Escorcia-Gutierrez, J. (2025). Secure federated learning with metaheuristic optimized dimensionality reduction and multi-head attention for DDoS attack mitigation. Scientific Reports, 15: 33291. https://doi.org/10.1038/s41598-025-15052-2

[20] Luo, B., Han, P.C., Sun, P., Ouyang, X.M., Huang, J.W., Ding, N.N. (2023). Optimization design for federated learning in heterogeneous 6G networks. IEEE Network, 37(2): 38-43. https://doi.org/10.1109/MNET.006.2200437

[21] El Mokadem, R., Ben Maissa, Y., El Akkaoui, Z. (2023). Federated learning for energy constrained devices: A systematic mapping study. Cluster Computing, 26: 1685-1708. https://doi.org/10.1007/s10586-022-03763-4

[22] Adam, M., Baroudi, U. (2024). Federated learning for IoT: Applications, trends, taxonomy, challenges, current solutions, and future directions. IEEE Open Journal of the Communications Society, 5: 7842-7877. https://doi.org/10.1109/OJCOMS.2024.3506214

[23] Joshi, A., Shet, A.V., Thambi, A.S., R, S. (2023). Quality improvement of image datasets using hashing techniques. In 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, pp. 18-23. https://doi.org/10.1109/IITCEE57236.2023.10091044

[24] H D, K., G K, S., M, C., Dhananjaya, S., K P, S., Jairam, B.G., R, S. (2025). Privacy-preserving IoT framework with Federated Learning and lightweight NLP integration. Journal Europeen des Systemes Automatises, 58(5): 953-961. https://doi.org/10.18280/jesa.580509

[25] Rekha, K.S., Jainapur, P., Manjushree, K., Dhananjaya, S., Nandini, S.R., Nandini, G., Sunitha, R. (2025). Deep reinforcement learning-based energy-aware intrusion prevention in IoT environment. International Journal of

Safety & Security Engineering, 15(8): 1745-1754. https://doi.org/10.18280/ijsse.150819

[26] Koroniotis, N., Moustafa, N., Sitnikova, E., Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. Future Generation Computer Systems, 100: 779-796. https://doi.org/10.1016/j.future.2019.05.041

[27] Alsaedi, A., Moustafa, N., Tari, Z., Mahmood, A., Anwar, A. (2020). ToN_IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems. IEEE Access, 8: 165130-165147. https://doi.org/10.1109/ACCESS.2020.3022862

NOMENCLATURE

D_i	Dataset held by client (i)
x_j, y_j	Input feature vector and label of sample (j)
n_i	Number of samples at client (i)
w^t	Global model parameters at communication round (t)
w_i^t	Local model parameters of client (i)
$\widehat{w_i}$	Compressed and privatized local model update
η	Learning rate
L_i	Local loss function at client (i)
∇L_i	Gradient of loss function
v_i^t	Velocity of particle in PSO
x_i^t	Position of particle in PSO
$pbest_i$	Personal best solution in PSO
$gbest$	Global best solution in PSO
$X_\alpha, X_\beta, X_\delta$	Best solutions in Grey Wolf Optimizer
A, C	Control parameters in GWO
λ	Hybrid weighting factor (PSO vs GWO)
g_i	Local gradient update
$\widetilde{g_i}$	Noise-added gradient (Differential Privacy)
σ	Standard deviation of Gaussian noise
ϵ	Privacy budget
$Q(\cdot)$	Compression function
$C_{\{comm\}}$	Communication cost
S_i	Client selection score
$\alpha_1, \alpha_2, \alpha_3$	Weights for client selection
F	Multi-objective optimization function
α, β, γ	Objective weights
δ	Convergence threshold