

Resilient and Privacy Preserving Real-Time Data Offloading Using Federated Game Theory-Optimized MLP-LSTM Framework

Jayaprakash Hampi^{1*}, and Dr.C.B. Vinutha²

¹Department of Electronics and Communications Engineering, Presidency University, Bengaluru, Karnataka, India. jayaprakash.2023ece0003@presidencyuniversity.in, <https://orcid.org/0009-0002-0141-5059>

²Department of Electronics and Communications Engineering, Presidency University, Bengaluru, Karnataka, India. vinutha.cb@presidencyuniversity.in, <https://orcid.org/0000-0001-6720-9077>

Received: September 29, 2025; Revised: November 05, 2025; Accepted: December 29, 2025; Published: February 27, 2026

Abstract

Real-time data offloading is increasingly required in dynamic Internet of Things (IoT) and mobile network environments to reduce latency and enhance computational efficiency. However, this process exposes sensitive information to significant threats, including data leakage, unauthorized access, and adversarial manipulation. To address these challenges, this study proposes a novel Federated Game Theory-Optimized Multi-Layer Perceptron-Long Short-Term Memory (FGO-MLP-LSTM) framework that offers a secure, privacy-preserving, and strategically adaptive solution for real-time data offloading. The core novelty of this work lies in the integration of federated learning, game-theoretic decision modeling, and hybrid deep learning (MLP-LSTM) into a unified security-enhancing architecture. Unlike traditional centralized approaches, the proposed method retains all sensitive data on local edge devices and exchanges only encrypted model updates, substantially mitigating the risk of exposure. Game theory is employed to simulate and analyze interactions among benign agents and adversaries, enabling dynamic optimization of defence strategies under varying threat intensities. Within the framework, the MLP module extracts complex high-dimensional patterns, while the LSTM component captures long-term temporal dependencies essential for detecting real-time anomalies. Preprocessing and min-max normalization further improve data consistency, supporting stable and effective training. Experimental results validate the superiority of the proposed system, achieving 99.3% accuracy, 99.5% precision, 99.4% recall, and 99.4% F1-score—consistently outperforming existing models including Bi-LSTM, LSTM, and Fed-Game. The framework also demonstrates enhanced resilience against poisoning and evasion attacks due to the combined strengths of federated learning and strategic optimization. Overall, the FGO-MLP-LSTM framework provides a scalable and robust solution for secure real-time data offloading, offering clear benefits for next-generation IoT and mobile computing ecosystems.

Keywords: Multi-Layer Perceptron, Long Short-Term Memory, Game Theory, Federated Learning, Data Offloading.

1 Introduction

Offloading of real-time data has been a core need in the contemporary digital ecosystems like mobile networks, IoT, autonomous vehicles, and smart infrastructures (Priya et al., 2025). The disruptive proliferation of data produced by networked devices has surpassed the processing, storage and energy capacity of immediate systems and offloading to edge servers or cloud servers has become imperative to maintain performance, responsiveness and scale (Cappa et al., 2022). Resource optimization made possible by efficient offloading, and the reduction of device-level computational load, as well as the demonstration of latency-sensitive services and applications such as telemedicine, intelligent transportation, and smart cities. Although these advantages exist, real time data offloading has brought about serious security threats because of multi-hop communication, distributed architecture, and heterogeneous devices (Khan et al., 2024). In recent studies, the investigation of intelligent security models based on machine learning (ML), FL, and game theory has become more widespread (Mann et al., 2022). The ML-based models have shown high-detection and mitigation of the cyber threats through continuous learning of the complex pattern using high-dimensional and time data (Jin et al., 2022). Specifically, MLPs are practical when it comes to nonlinear feature representation, whereas LSTM networks are superior at considering temporal variations in sequential information. Hybrid MLP-LSTM models have therefore become interesting alternatives to real-time threat forecasting and dynamic defense (Ikegwu et al., 2022).

Nevertheless, the centralized ML solutions usually demand the transmission of raw data, which poses a severe threat to both privacy and security (Chaudhry et al., 2022). The same limitation is tackled by federated learning which allows decentralized training of models but leaves sensitive information on devices (Alrowais et al., 2022). The model update only technique of FL greatly helps to mitigate the risks of exposure and privacy protection (Goswami et al., 2024; Chen et al., 2023; Ferrag et al., 2022). To fill these gaps, this study proposes hybrid MLPLSTM security framework with federated learning and game-theoretic optimization. The suggested solution to the problem will provide real-time threat detection, privacy-conscious decentralized learning, and adaptive defense solutions with minimal computational and communication overhead. Through the unification of complementary capabilities in a single cohesive architecture, it moves the work forward in secure, scalable, and robust real-time data offloading of next-generation digital architectures.

The major contributions of this article are summarized as follows:

- **Privacy-Preserving Federated Offloading Architecture:** A federated learning-based real-time data offloading architecture is proposed in which sensitive data remains on edge devices, significantly reducing privacy leakage risks while enabling collaborative model learning across distributed nodes.
- **Game-Theoretic Integration within Federated Learning:** A game-theoretic framework is embedded into the federated learning cycle to model strategic interactions among offloading nodes, service providers, and adversaries, enabling proactive and adaptive security decision-making under dynamic threat conditions.
- **Joint Security and Performance Optimization:** The proposed framework jointly optimizes security robustness and computational efficiency, overcoming the limitations of existing approaches that address security and performance in isolation.

- **Hybrid MLP–LSTM Threat Intelligence Model:** A hybrid deep learning core combining multilayer perceptrons for nonlinear feature extraction and LSTM networks for temporal dependency modeling is developed to enhance the accuracy of real-time threat detection and offloading decisions.
- **End-to-End Real-Time Offloading Framework:** An integrated pipeline encompassing data preprocessing, hybrid deep learning inference, federated model aggregation, and game-theoretic strategy optimization is designed for dynamic IoT and mobile computing environments.
- **Improved Resilience to Adversarial Attacks:** By explicitly modeling attacker behaviors and adapting defensive strategies through game-theoretic equilibria, the framework demonstrates enhanced robustness against spoofing, data manipulation, and inference-based attacks.

The organization of the paper includes related works, problem statement and methodology in section 2, 3 and 4. The results and discussion are given in section 5. Section 6 concludes the paper.

2 Related Works

More recent developments in secure and efficient offloading of data have seen an increasing use of ML, FL, and game theory to overcome the difficulties of the large-scale dynamic IoT ecosystems. The ML-based methods, specifically the neural network model, including the MLPs and the LSTM networks, have demonstrated good performances in anomaly behaviors detection and security threats prediction in real-time (Alzaabi & Mehmood, 2024). MLPs can be useful to extract nonlinear features of high-dimensional data, whereas LSTMs can be used to capture time-related information of sequence offloading and network traffic patterns. Nevertheless, the majority of ML-based security tools are based on centralized training, exposing sensitive information to be transferred and reducing scalability and privacy protection (Orabi et al., 2025). Federated learning has become the perspective that can be taken as an alternative to centralized ML because it allows to train models in a decentralized manner, at the same time, retaining raw data at the edge devices. The FL has a major advantage of minimizing the chances of data leakage and unauthorized access because only model updates are shared. A number of studies prove that FL helps improve privacy and robustness of distributed settings; however, the majority of FL-based solutions are considered only in terms of model aggregation and accuracy, yet there is no particular emphasis on adversarial behavior or strategic attack, or joint optimization of security and system performance. Consequently, they are not very flexible to changing threats during real-time offloading situations (Ahlawat & Krishnamurthi, 2023). The approach to the strategic interaction between attackers and defenders in offloading systems has been incorporated as game-theoretic models. These can be used to determine equilibrium strategies that balance between the cost of defense and protection effectiveness by modelling security as a dynamical game (Molokomme et al., 2022). Although game-theoretic solutions are theoretically very robust, many are not connected to learning-based threat prediction and rely on very simple assumptions, making them less realistic in very dynamic IoT settings. A trust-aware task offloading model (TOM) of edge-enabled IoVs in the Internet of Vehicles (IoV) area. The model uses multi-objective optimization (SPEA2), then MCDM and TOPSIS in order to choose the best offloading decisions. The method enhances the service response time, load balancing, and privacy. Nonetheless, the application of evolutionary optimization, decision-making models adds considerable computational complexity, and lack of real-time learning restricts the ability to react to a rapid alteration of the network setting or attack patterns (Ben Hamida et al., 2025).

Mobile edge computing (MEC) is a topic of numerous investigations as a method of minimizing the delay and energy usage in mobile IoT. In a study by (Khattak et al., 2025), secure MEC offloading was studied when an eavesdropper was present and the allocation of tasks, transmission power, CPU frequency, and offloading duration were jointly optimized with the help of convex optimization and Karush-Kuhn-Tucker (KKT) equations. Although the method has significant energy savings and provides certainty of transmission, it presupposes ideal system knowledge and fixed threat models, which do not exist in the practical large-scale IoT applications. Industrial IoT Deep-learning-based security-conscious offloading frameworks have also been considered. Likewise, (Hu et al., 2022) introduced a secure multi-user MEC offloading profile that integrates the resource allocation problem, data compression, and privacy restrictions. Though the solution is scalable and has made a considerable saving on energy, its NP-hard formulation and use of the convex relaxation limits real-time use and dynamic threat response.

Table 1: Comparative analysis of related works on secure and efficient data offloading

References	Application Domain	Method	Key Findings	Limitations
(Ahlawat & Krishnamurthi, 2023)	IoT	RTOS-based delay-aware offloading using multivariable spline linear classification	Reduced latency and rejection rate; improved request execution under varying user densities	Static model design; no adaptive learning or security threat modeling
(Ben Hamida et al., 2025)	IoV	Trust-aware task offloading model (TOM) using SPEA2, MCDM, and TOPSIS	Improved service response time, load balancing, and privacy assurance	High computational overhead; limited real-time adaptability
(Khattak et al., 2025)	MEC	Joint optimization via convex programming and KKT conditions with physical-layer security	Significant energy reduction and secure offloading guarantees	Assumes perfect system knowledge; lacks scalability and learning capability
(Hu et al., 2022)	MEC / Mobile IoT	Secure multi-user compute offloading using compression, resource allocation, and convex optimization	Up to 46% reduction in energy consumption; scalable multi-tasking	NP-hard formulation; limited adaptability to dynamic threat environments

Table 1 shows existing works summary. The current data offloading solutions mainly concentrate on enhancing latency, energy efficiency or trust management without considering the aspects of security, privacy and performance as independent goals. Most techniques are based on centralized learning or control schemes that add overhead to communication and sensitive information to privacy threats. Optimization-based and cryptographic approaches presuppose static systems description and fixed threat behavior, which should restrict the adaptive capability to dynamic and adversarial IoT systems. SDN-enabled and trust-aware frameworks are computationally complex and do not have real-time learning. Deep learning-based approaches enhance the accuracy of decisions, but do not typically focus on privacy-preserving training and strategic model of attackers.

Research Gap: In general, existing literature does not present a unified, dynamic and privacy-conscious framework that could be used to collectively tackle security, scalability and real-time

offloading performance in non-homogenous IoT systems. Based on the above analysis, it is clear that current literature focuses on latency, energy efficiency, privacy, or security individually, centralized learning or control, and fixed threat assumptions. It is evident that there is no unified framework and approach that can offer a balance between privacy-conserving learning and adaptive threat modeling, strategic security optimization, and real-time offloading efficiency to heterogeneous IoT settings. This disparity will encourage the suggested federated, game theory-enhanced hybrid MLP-LSTM framework that will combine these dimensions into a single, scalable, and adaptable offloading framework.

Problem Statement

The current real-time data offloading systems in IoT settings fall short in addressing the cumulative needs of the low latency, high resource usage, high data confidentiality and dynamic security. The majority of existing schemes serve more or less predictable workloads and are thus inefficient in responding to abrupt traffic increases and evolving data distributions leading to bottlenecks, longer latency and worse quality of service - especially when it comes to time-sensitive IoT services. Also, resource allocation algorithms tend to be either non-adaptive or weakly adaptive, causing load imbalance among edge nodes and inefficient energy usage as well as increased operational expenses (Myakala et al., 2024).

Proposed Federated Game Theory-Optimized MLP-LSTM Framework

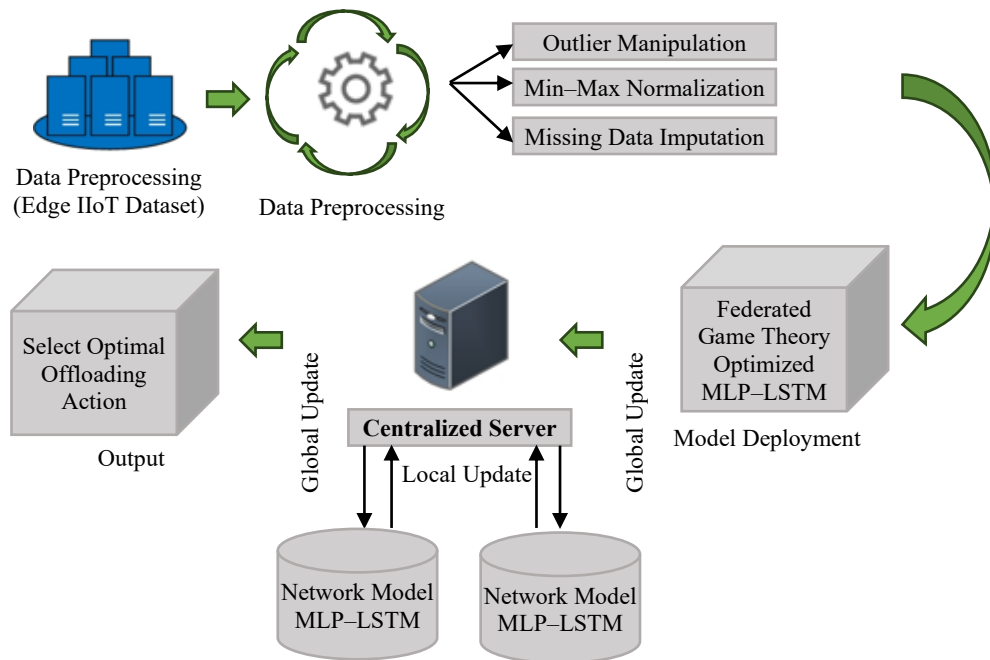


Figure 1: Proposed FGO-MLP-LSTM design

The proposed system design is described in Figure 1 in detail. To create the Edge IoT dataset, edge IoT devices data collection is the first move in the process. To guarantee consistency and quality of data, the raw data undergoes intensive pre-processing such as min-max normalization, missing value imputation and outlier management. The pre-processed data is then entered into the FGO-MLP-LSTM model, which is implemented in a decentralized infrastructure. This model combines the merits of MLP and LSTM networks using several local networks (Network A and Network B). The local networks through

which periodic updates are sent to the centralized server do first training. The server performs the global model update where the local updates are aggregated and this improves the overall learning of the model with privacy of data being preserved. The optimized model helps in the selection of the most appropriate offloading processes upon deployment, where offloading the data is secure and effective, in real-time situations. This unified framework is concerned with resiliency and flexibility of the system in managing and securing the offloading data management processes in an effective manner.

Data Collection

The data acquired is the Edge IIOT data set and is a wide and extensive data of real information that has been collected by the devices set at the network boundaries as the IoT (Edge-IIoTset Cyber Security Dataset, 2022). This data set consists of a wide variety of data used in industrial processes: sensor reading, operational parameters, and environmental condition. In edge-computing environment, the data set reveals the complicated processes of distributed systems, which are on the network edge. Researchers could model the complexity of industrial processes, in real time, with high-resolution and rich data streams to create new machine learning models and optimization algorithms and experiment with them to serve the demands of edge computing environments.

The dataset employed in this research is Edge-IIoTset since it is realistic and multi-layered IoT/IIoT traffic that is essential in testing a resilient and privacy-sensitive real-time data offloading system. Its non-IID distribution and heterogeneous device-specific streams make it the most suitable to federated learning, where it is possible to train without access to raw data. The data naturally exhibits a Non-IID (Non-Independent and Identically Distributed) structure, meaning that each IIoT device or layer generates traffic with different statistical properties. Variations occur due to heterogeneous sensors, uneven data volumes, localized attack patterns, and operational differences across layers such as edge, fog, SDN, NFV, blockchain, and cloud. This Non-IID behavior is crucial for federated learning, where models must train effectively without accessing raw data, despite significant distribution differences across clients. The data is sensor-timed and rich temporal sequences that are capable of supporting the MLP-LSTM architecture of spatial-temporal prediction. Furthermore, it has 14 different types of attacks, which also could be properly modeled and used to include mechanisms of game-theoretic optimization into the offloading procedure. The data set covers seven computing layers, including edge, fog, SDN, NFV, blockchain, and cloud and provides a comprehensive assessment of latency, throughput, and security of the completely offloading pipeline. These characteristics make Edge-IIoTset uniquely suited for validating the proposed Federated Game Theory-Optimized MLP-LSTM framework, ensuring comprehensive assessment of performance, privacy, and resilience.

Pre – Processing Using Min-Max Normalization

The quality and reliability of the ML models have their basis on processing methods like min-max normalization. The data of the dataset are normalized by the min-max normalization to the desired range (in most instances 0 to 1). This step is essential when the data being fed by the edge IoT devices is the data with the potential of explosive scale variation, the original data set. Without normalization, additional range-based attributes can overcome small ranging attributes, which leads to bias in model training and reduces performance. Min-max normalization keeps some equilibrium by normalizing the dimension of all the attributes such that they contribute equally to the learning. This is particularly important to MLP-LSTM models: they require features regions to be stable to learn and predict effectively and rely on the size of the input data in Equation (1).

$$Y_{norm} = \frac{Y - Y_{min}}{Y_{max} - Y_{min}} \quad (1)$$

Min-max normalization can be applied not only to pre-train the data so that it can be trained on a model, but its applications are multiple. Pre-processing data reliability is the most important in federated learning settings whereby several local models are being trained on the distributed data sources and synchronized periodically with a central server. Min-max normalization can be used to more conveniently aggregate updates on a model by making sure that data across a large set of sources have been scaled to similar levels, in addition to making a global model more resilient in general. Consistency improves the modelling capacity of the model to extrapolate to new unobserved data and minimises the probability of overfitting. Furthermore, because optimization procedures can be more efficient at handling features in a fixed range, normalized data helps to make training faster.

Employing FGO-MLP-LSTM for the Selection of Optimal Offloading Security

FGO is the best offloading actions within the FGO-MLP-LSTM model. Through the incorporation of game theory concepts in federated learning, FGO encourages strategic decision-making across decentralized edge devices for optimal offloading strategies in real-time contexts. The process recognizes the competitive environment of networks where various entities compete for available resources, i.e., bandwidth and computational capacity. FGO uses game-theoretic principles, including Nash equilibrium and payoff maximization, to represent the engagement of edge devices and make offloading decisions that optimize overall network utility subject to individual device goals.

In offloading optimization, FGO uses strategic decision-making in order to adaptively choose the best offloading action depending on the prevailing network conditions and device preferences. Edge devices are rational agents and choose offloading strategies strategically in order to maximize their utility and hypothesize the other device behavior. Through the application of ideas in game theory, FGO can be used to consider various offloading scenarios and determine Nash equilibrium solutions in which no device will benefit when another unilaterally deviates off the selected strategy. It is through this strategic decision-making process that FGO-MLP-LSTM can dynamically adapt offloading actions to a changing network condition and thus achieve optimal use of resources and better performance.

Even though FGO entails competition, where game theory optimization is applicable, it can also encourage edge device coordination to meet shared goals, including the reduction of latency and the maximization of throughput. As the natural resource competition progresses, FGO helps to encourage the behavior of cooperation by the way of the synergizing of interests of the individual devices to the common objectives of the network. As the offloading plans are coordinated and the federated learning organizes the activities, FGO allows sharing and collaboration across the edge devices, and so the harmonious benefits are realized to the entire networked ecosystem. This joint optimization technique boosts the total performance and power of offloading decisions that makes FGO-MLP-LSTM to address dynamic network conditions without causing data privacy and ownership breaches.

Federated Learning in Data Privacy and Security

Federated learning enhances privacy of data significantly since with decentralized training and the option of devices different learning a shared model without exchanging raw data, the first can learn together. By maintaining private data on individual edge devices, this method decreases the chances of data breaches and unauthorized access. Data local processing by each device creates model updates, which are then aggregated in a central server. The process under this method preserves the anonymity

of the raw data, that is, the learned parameters are disclosed but not the raw data. Federated learning mitigates privacy issues smoothly and accords data protection regulations including GDPR because the data is shared and data centralization is minimized. This may therefore be applied in the field where sensitivity and privacy of data is a major consideration.

Federated learning allows more than two devices to collaborate in learning, and in a safer and confidential way. The FGO-MLP-LSTM architecture is collaborative in essence that ensures the model is capable of accessing multiple sources of data thereby becoming immune to adversarial attacks. The area of attack is much less than the centralized architectures, as the data stays in the edge devices. In addition, federated learning applies the methods of differential privacy and secure multiparty computation to prevent manipulation and reverse engineering of the model updates. Such security measures render the whole system secure even in the event individual devices are compromised. The decentralized nature of federated learning with no point of failure also makes redundancy and resilience possible. These new security attributes are employed by the federated learning mechanism of FGO-MLP-LSTM to provide an end-to-end solution that improves the overall security of real-time offloading processes, as well as provided enhanced data privacy in the same breath. Figure 2 illustrates the architecture of Federated Learning.

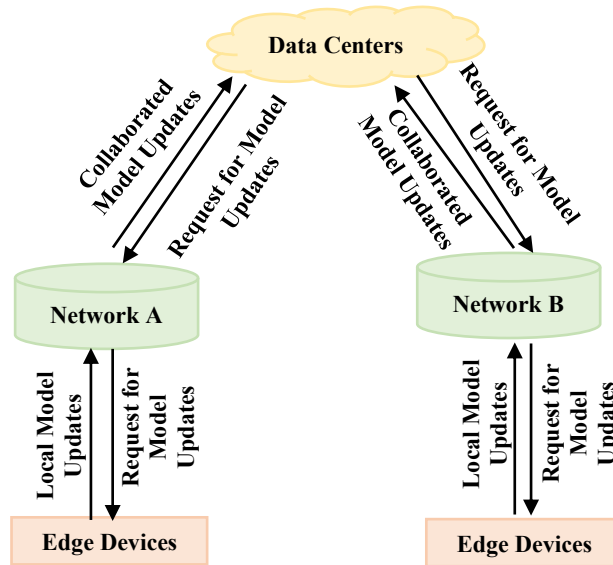


Figure 2: Architecture of federated learning

Game Theory in Strategic Decision Making

Game theory provides a mathematical representation of interactions of entities in a system such as data suppliers, offloading nodes and potential attackers associated with FGO-MLP-LSTM system. Every participant (player) selects strategies to optimize its own reward by taking into account the strategies of the other players. The interaction can be cast as a strategic game in Equation (2).

$$G = (N, S_i, U_i), \quad i \in N \quad (2)$$

Where N is the set of players (e.g., data providers, offloading nodes, attackers), S_i is the strategy set of player i , U_i is the payoff function of player i every node chooses an offloading strategy $s_i \in S_i$, and the payoff function is as in Equation (3):

$$U_i(s) = B_i(s) - C_i(s) \quad (3)$$

Where $B_i(s)$ denotes the advantages (e.g., low latency, high throughput, safe transmission) and $C_i(s)$ denotes the expenses (e.g., computation overhead, bandwidth consumption, or exposure to attack). The system seeks to achieve a Nash Equilibrium, which is given by Equation (4):

$$U_i(s_i^*, s_{-i}^*) \geq U_i(s_i, s_{-i}^*) \quad \forall s_i \in S_i \quad (4)$$

Where s_i^* is player i optimal strategy and s_{-i}^* is the strategy profile of all other players. In equilibrium, no node has an incentive to deviate from its selected strategy unilaterally.

In the FGO-MLP-LSTM model, this balance facilitates optimal offloading decisions in the face of changing environments. Through anticipations of attacker actions and changes in offloading actions correspondingly, the system takes minimum risks of denial-of-service or data exposure while maintaining maximum efficiency. To balance trade-offs in Equation (5), the payoff functions can be extended with security weights α and performance weights β :

$$U_i(s) = \alpha \cdot S_i(s) + \beta \cdot P_i(s) - \alpha \cdot C_i(s) \quad (5)$$

Where $S_i(s)$ signifying security benefits and $P_i(s)$ signifying the performance measurements (e.g. latency reduction, higher throughput). To this end, the game theory allows the FGO-MLP-LSTM model to estimate adversary action, reduce offloading deviation strategy, and achieve security and performance tradeoff in real-time data offloading applications. Figure 3 shows game theory architecture.

The dataset has not explicitly defined data providers, offloading nodes, and attackers as independent variables, but these variables are implicitly described with the help of a multi-layer architecture of the dataset, benign traffic produced by devices, and labeled attack flows. The suggested FGO-MLP-LSTM models devices within the IoT as sources of data, edge/fog/cloud nodes as a data-offloading node, and the fourteen attack categories as attacker behaviors. Game theory is a system level interaction that takes into account strategies of these positions based on the behavioral patterns of the dataset instead of direct columns in the dataset. Therefore, the dataset is appropriate to serve the classification model and the game-theoretic decision-making layer.

Game Theory in Strategic Decision Making

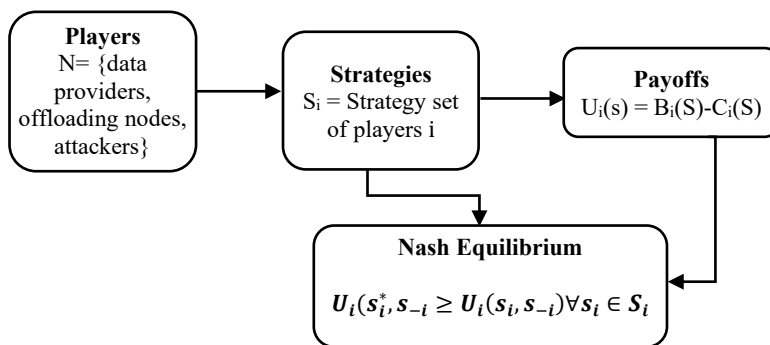


Figure 3: Game theory architecture

MLP-LSTM Models in Pattern Recognition and Prediction

MLP models have performed exceptionally well in job pattern recognition and prediction especially when deployed inside frame works that aim at promoting security in offloading real-time data. MLP is involved in federated game theory optimization precision forecasting and predicting reliability and

capable of effectively detecting complex patterns in any type of stream of data. The need to address nonlinear relationships and to extract intricate mappings in data makes MLPs necessary to support feature extraction and the first steps in data processing in a federated learning system. With the help of MLP and the utilization of LSTM networks that are highly qualified to determine the existing temporal relationships and pattern of sequence not only this structure can enhance the accuracy of predictions, but ensure continuation of effective security control measures throughout the lifetime of distributed data processing process of utmost importance when it comes to safeguarding valuable information in real-time offloading of data cases. Figure 4 shows MLP-LSTM architecture.

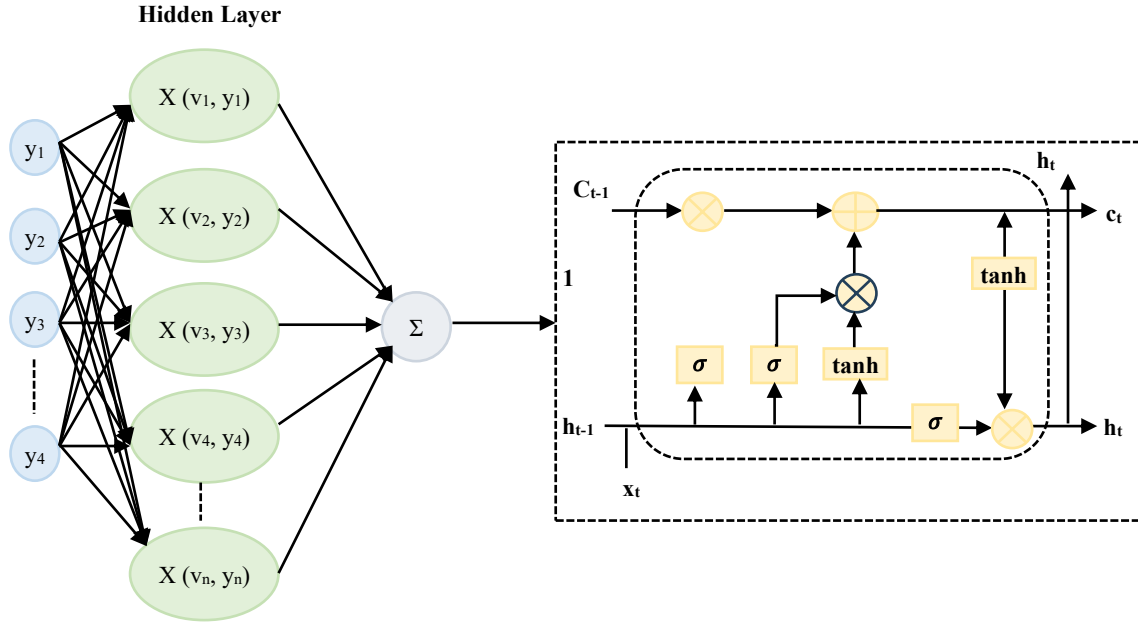


Figure 4: Architecture of MLP-LSTM

The LSTM networks are very valuable in pattern recognition and prediction especially when they supplement the real-time data offloading security with an MLP-LSTM system based on the federated game theory. Applications to time series prediction and natural language processing also need long-term trends and complex temporal dependencies in their sequential data, which LSTMs learn well. The federated learning model depends on the LSTMs to provide a means of decentralized training of models across decentralized edge devices and ensure data privacy and data confidentiality. LSTM architecture can process dynamic and varying data streams that occur in the offloading real-time environment. It possesses especially the memory cells that can store information on a long-term basis. This will provide protection of confidential data throughout the pipeline of data processing and optimal predictive power of models, when combined with LSTMs and MLPs that not only serve effectively in features extraction and nonlinear mapping of input data. The combination of the MLPs and the LSTMs is therefore an effective method of maximizing the performance and reliability of real-time data offloading infrastructures in the distributed computing environment because it does not only resolve the issues of concern in regards to security, but also enhances the precision of the prediction. Input Gate: Controls how much new information is stored in Equation (6):

$$i_t = \sigma(N_i x_t + N_o h_{t-1} + c_i) \quad (6)$$

Forget Gate determines how much previous memory to keep. It is denoted in Equation (7).

$$f_t = \sigma(N_f x_t + N_f h_{t-1} + c_f) \quad (7)$$

Candidate Cell State: Creates new candidate information shown in Equation (8).

$$g_t = \tanh(N_g x_t + N_g h_{t-1} + c_g) \quad (8)$$

Cell state update is shown in Equation (9).

$$p_t = f_t * p_{t-1} + i_t * g_t \quad (9)$$

Hidden State is shown in Equation (10).

$$y_t = h_t = o_t * \tanh(p_t) \quad (10)$$

Output Gate: Controls exposure of the memory in Equation (11).

$$o_t = \sigma(N_o x_t + N_o h_{t-1} + c_o) \quad (11)$$

Where W^*, U^*, W^* : trainable weight matrices, b^* : bias vectors, σ : sigmoid activation and \odot : elementwise multiplication. i_t : Input gate activation controlling how much new information enters the cell. x_t : Input feature vector at time step t . h_{t-1} : Hidden state from the previous time step. f_t means forget gate activation determining how much past information is retained. o_t : Output gate activation governing how much of the internal memory is exposed. g_t Candidate cell state containing new information to be added to memory. p_{t-1} Updated cell state (long-term memory) at time step t . N_i Weight matrix associated with the input gate for the current input x_t . N_o Weight matrix associated with the output gate for both x_t : and h_{t-1} . N_g Weight matrix for generating the candidate cell state. N_f : Weight matrix used in the forget gate computations. c_i refers bias vector for the input gate. c_f means bias vector for the forget gate. c_g means bias vector for the candidate cell state. \tanh : Hyperbolic tangent activation function mapping values to $[-1, 1]$. y_t means final hidden output of the LSTM block at time step t . Both MLP and LSTM networks are vital to use as a robust pattern recognition and forecasting framework to enhance security in real-time offloading data in a federated game theory optimized environment. The MLP module is shown to have high potential in finding nonlinear characteristics in a vast pool of input streams and is able to encrypt extremely complex patterns with minimal effort, or basic pre-processing.

The sequential data analysis and predictability, the possibility to obtain long-term context and time dependencies is particularly well processed by the LSTM networks. In the federated case, where the privacy of the data is the most critical, combining the MLP-LSTM system will guarantee safe sensitive data when the federated model training process is carried out through edge devices. The model establishes data and computational integrity of transaction and incentive and increases model accuracy by the implementation of the game theory of optimization, including strategy of participants and incentive alignment. Integrated approach can not only improve the predictive performance in the evolving environment, but it can also develop strong defense mechanisms against potential attacks on the security, which is the core of applications in machine learning and policy of cybersecurity in distributed computing systems. Pseudocode of proposed FGO-MLP-LSTM framework is shown in algorithm 1.

Algorithm 1: FGO-MLP-LSTM Based Privacy-Preserving Real-Time Offloading

Input:

- IoT data stream D_i from each edge device i
- Learning rate η , number of rounds R , local epochs E

- Game-theoretic parameters: utility functions U_p, U_o, U_a

Output:

- Global optimized model W_{global}
- Real-time secure offloading decision $O_{decision}$

Step 1: Initialization

Initialize global model $global$ (MLP-LSTM parameters)

For each edge device i , initialize local model $W_i = global$

Step 2: Preprocessing

For each incoming batch B_i in D_i :

Apply noise filtering, normalization (min-max), and formatting

Store processed batch PB_i

Step 3: Local Model Training

For round $r=1$ to R do:

For each device i in parallel do:

$W_i^r \leftarrow W_i$

For epoch $e=1$ to E do:

Train MLP layers on PB_i (spatial features)

Train LSTM layers on PB_i (temporal features)

Update local weights W_i^r using gradient descent

Step 4: Federated Aggregation (Privacy-Preserving)

Transmit only W_i^r (no raw data) to server

Server computes:

$W_{global} = \sum(n_i/N_{total})$ // FedAvg

Step 5: Game-Theoretic Optimization

- For each device i do:

Compute utilities:

$U_p(i)$ =provider's privacy utility

$U_o(i)$ =offloading performance utility

$U_a(i)$ =attacker payoff estimation

Determine Nash equilibrium strategy S_i^* :

$S_i^* = \arg \max (U_p, U_o)$

Adjust offloading rules and model parameters using S_i^*

Step 6: Real-Time Offloading

For each new data packet x_i :

Traffic Classification:

$$Class_i = MLP - LSTM(W_{global}, x_i) \in \{Low, Medium, High\}$$

Predict threat score $T_i = Threatscore(W_{global}, x_i)$

If $T_i > \text{threshold}$ OR S_i^* indicates high risk:

$O_{decision} = \text{"Process Locally"}$ // avoid exposure

Else:

$O_{decision} = \text{"Offload Securely"}$ // safe offloading

Step 7: Output

Return $W_{global}, O_{decision}$

Even though the proposed model involves three-class classifications of traffic (Low, Medium, High), the end-offloading outcome in the Algorithm 1 is binary due to the two actionable results of the real-time offloading namely, local processing or secure offloading. The MLP-LSTM gives the traffic class and a threat score (T_i). These are intermediate outputs that are fed to the game-theoretic optimizer that will integrate performance utility, privacy utility, and attacker payoff in order to calculate the equilibrium strategy S_i^* . Depending on S_i^* , the system decides whether the offloading is safe and latency-efficient. Thus, $U_o(i)$, $U_p(i)$, and the process of making resource-conscious decisions to offload are internally computed using the traffic class; however, the final system outputs a binary operational action that is needed in production systems: Process Local when risk is high, or Offload Securely when the conditions are safe and the performance is enhanced. Despite the fact that the MLP-LSTM model attempts to classify traffic into the Low, Medium, and High categories, this classification is an intermediate input into the game-theoretic optimization module. Final offloading decision, $O_{decision} \in \{\text{Process Locally, Offload Securely}\}$, Offload Securely is determined using the traffic class, threat score and Nash equilibrium strategy. This binary output maps edge, fog or cloud nodes in production to process data locally or offload in a secure manner that safeguards privacy, low latency, and high-quality network performance.

Threat Model

The Federated Game Theory-Optimized MLP-LSTM framework proposed is based on a semi-adversarial IoT system where it is reasonable to assume that edge devices, offloading nodes as well as communication channels are vulnerable to internal and external security threats. The adversary model considered comprises both passive adversaries capable of eavesdropping communication links in order to deduce sensitive information during offloading of data or modeling update interactions, and active adversaries that can use malicious traffic, cause denial-of-service (DoS) attacks, or influence the offloading decisions to reduce the system performance. Moreover, individual edge devices can be compromised and perform model poisoning or attempt inference attacks on federated learning rounds. The assumption is that the adversary is unable to attack the federated aggregation server; they do not have access to raw data nor are they able to take control of majority of the participating devices at the same time. The framework combines various security and privacy preservation mechanisms in order to cope with these threats. Federated learning has been used to ensure data confidentiality with only

encrypted model parameters or updates being shared, whilst raw data are kept local to edge devices. The resilience against attacks is enhanced by incorporating game-theoretic optimization into the offloading decision-making process such that the system can predict adversarial strategies and change the offloading policies according to the Nash equilibrium solutions. Decentralized training, optional differential privacy and secure aggregation are other methods used to reduce privacy leakage to avoid reverse engineering of individual data contributions. Additionally, the decentralized system removes the single points of failures, making it stronger and more resistant to failure. Together, this threat-conscious design can allow the proposed framework to attain a reasonable trade-off between security, latency, privacy, and resource efficiency in real-time IoT data offloading conditions.

The proposed Federated Game Theory-Optimized MLP-LSTM model proposes an integrated, robust, and confidential system of real-time data offloading in agile IoT and mobile systems. The major unique feature of it is the way it integrates the concepts of federated learning, game-theoretic optimization, and hybrid deep learning into a single functioning pipeline, which has not been explored on a unified level in the current systems. The conventional federated models pay attention to distributed training but do not have the mechanisms to predict adversarial behavior, whereas the recent game-theoretic offloading methods do not implement deep predictive models and edge privacy. The gaps are met in the proposed framework. The growing volumes of data, applications explain the necessity of this work with high latency, and the growth of security threats to offloading channels. Standardized methods of learning reveal sensitive information, and isolated deep learning frameworks do not guarantee privacy and are not flexible to strategic assaults. The suggested approach will make sure that only local edge devices will hold raw data, eliminating the chances of leakage and unauthorized access largely. The working process includes the preprocessing of the data and training of the local models based on the MLP-LSTM and their use of nonlinear spatial feature and long-time temporal dependencies. Federated learning also gathers model updates without transmitting raw data in such a way that privacy is guaranteed. Game theory is then used to simulate strategic games between data providers, offloading nodes and attackers. The system is able to dynamically optimize the security and performance by calculating equilibrium strategies. Lastly, real-time threat scores are used as a guide to whether the data should be processed locally or safely offloaded. The innovativeness of the framework is indicated by its collaborative privacy protection, attack-sensitive optimization, and excellent predictive performance of the current LSTM, Bi-LSTM, and game-based models, providing a complete, scalable solution to secure real-time offloading.

3 Results and Discussion

The outcomes that are showcased in this part are the consequence of putting the suggested FGO-MLP-LSTM framework into practice using Python. The proposed model, as evidenced by the evaluation of its performance measures, which include accuracy, precision, recall, and F1-score, improves the efficiency and security of real-time data offloading.

Table 2 shows experimental setup details. Proposed model parameters are provided in Table 3. The FGO-MLP-LSTM framework is evaluated in a Non-IID environment to emulate realistic edge IoT scenarios where data distributions vary across devices. This validates the model's ability to maintain performance and privacy under heterogeneous conditions. The game-theoretic module models three types of players—data providers, offloading nodes, and attackers based on the IoT/IIoT traffic and attack annotations in the Edge-IIoT dataset. These roles are abstracted logically to evaluate strategic interactions and optimal offloading decisions. The MLP component consists of two hidden layers with

128 and 64 neurons, while the LSTM component uses two hidden layers with 64 units each to capture long-term temporal dependencies in sequential data. Although the proposed framework targets resource-constrained edge devices, simulations and training of the MLP–LSTM model were performed on a high-performance PC (RTX 3060 GPU, 32 GB RAM) to accelerate experimentation and validate performance. In practical deployment, the model can be pruned or compressed to run efficiently on actual edge nodes. Players are not explicit in the dataset but are modelled logically using device traffic and attack labels. Non-IID environment reflects realistic variations in data distributions across edge devices. Output layer predicts traffic class, which feeds into the game-theoretic optimizer for the final binary offloading decision (Process Locally / Offload Securely). A Non-IID (Non–Independent and Identically Distributed) data environment refers to a scenario where the data generated across different devices or clients does not follow the same statistical distribution. In federated learning settings, each IIoT or edge device produces data with unique sensor types, operational conditions, traffic loads, and attack behaviours. As a result, the overall dataset becomes highly heterogeneous. The Edge-IIoT dataset naturally exhibits Non-IID characteristics because each computing layer (edge, fog, IoT sensors, SDN, NFV, and cloud) generates distinct traffic profiles and anomaly patterns. This Non-IID nature is crucial for evaluating federated models operating in realistic IIoT environments, where uniform or balanced data distribution cannot be assumed.

Table 2: Simulation parameters

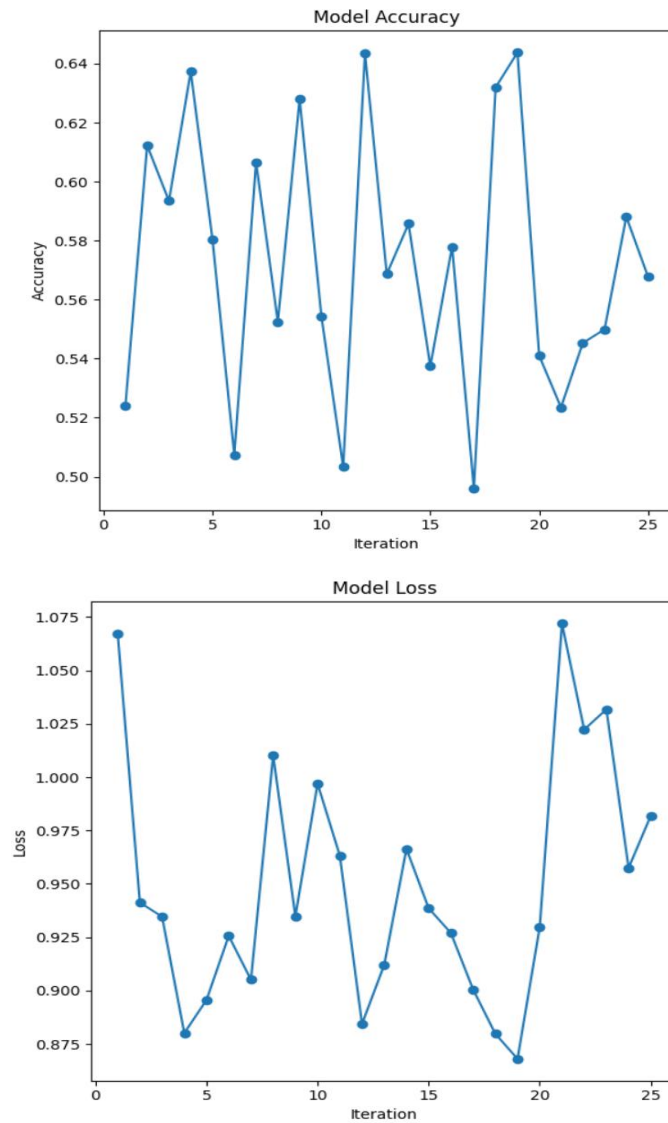
Component	Specification
Programming Language	Python 3.10
Deep Learning Libraries	TensorFlow 2.13 / PyTorch 2.1, Keras 2.13
Federated Learning Framework	TensorFlow Federated (TFF)
Optimization & Game Theory Tools	NumPy 1.25, SciPy 1.11
Preprocessing Libraries	Pandas 2.0, scikit-learn 1.3
Hardware	PC (RTX 3060 GPU, 32 GB RAM)
Operating System	Windows 11

Table 3: Model architecture parameters

Component	Specification
MLP Layers	[128, 64] neurons, ReLU activation
LSTM Layers	2 hidden layer, 64 units, tanh activation
Output Layer	Softmax (3-class traffic: Low, Medium, High)
Loss Function	Cross-entropy
Optimizer	Adam
Learning Rate	0.001
Batch Size	32
Local Epochs per Round	5
Total FL Rounds	50–100
Aggregation Method	FedAvg
Communication Frequency	Once per FL round
Players	Data providers, offloading nodes, attacker
Payoff Function	Weighted utility based on accuracy, latency, and security
Payoff Weights (α, β, γ)	Set empirically: 0.2–0.8 range
Equilibrium Method	Iterative best-response dynamics
Attack Scenarios	Data poisoning, delay-based disruption

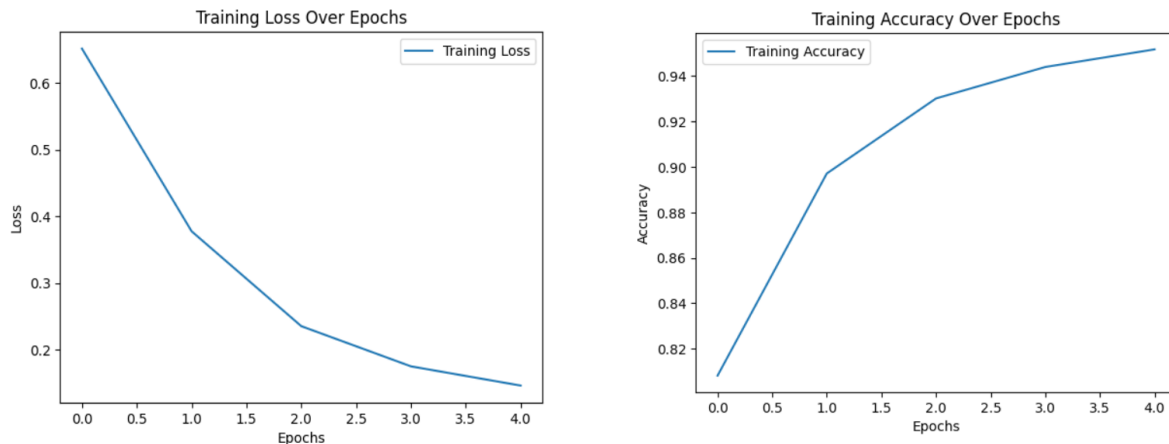
Pattern Recognition MLP-LSTM Performance

The hybrid MLP-LSTM model shows that it has a good pattern recognition capacity because it interacts synergistically with the nonlinear feature interactions and the time information in the IoT and IIoT traffic. The MLP element identifies discriminative features of space, whereas the LSTM identifies time based changing patterns of attacks, which lead to better generalization under time-varying edge scenarios.



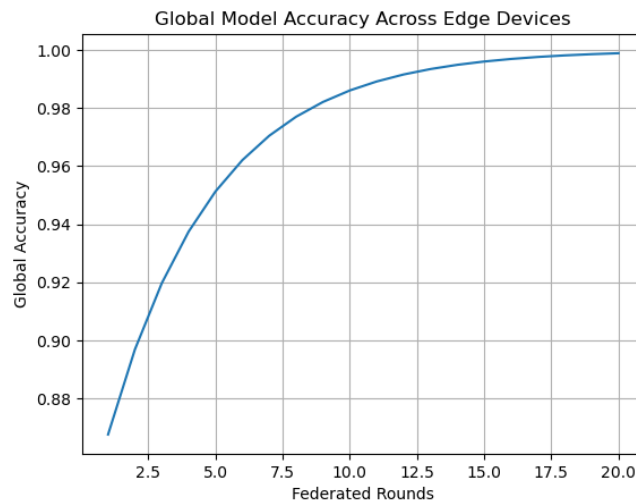
a) Accuracy b) Loss

Figure 5: MLP-LSTM model accuracy and loss



a) Training loss over epochs

b) Training accuracy over epochs



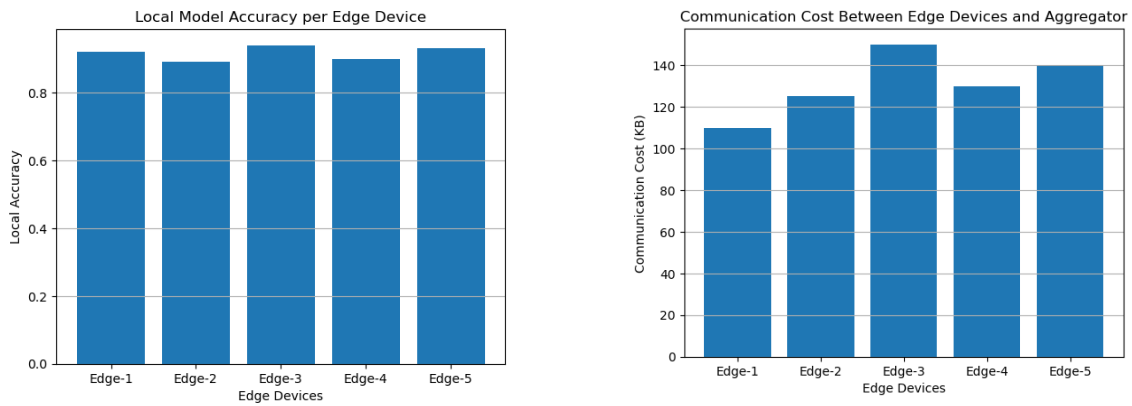
c) Global accuracy across edge devices

Figure 6: FL model performance

The model converges to the correct convergence with steady loss and a steady increase in accuracy with a steady loss, which suggests that learning is taking place and the error of prediction, is minimal Figure 5 as demonstrated by the combined accuracy and loss trends. These findings affirm the fact that the hybrid architecture best fits in real time offloading conditions where the traffic behavior is nonlinear and time varying.

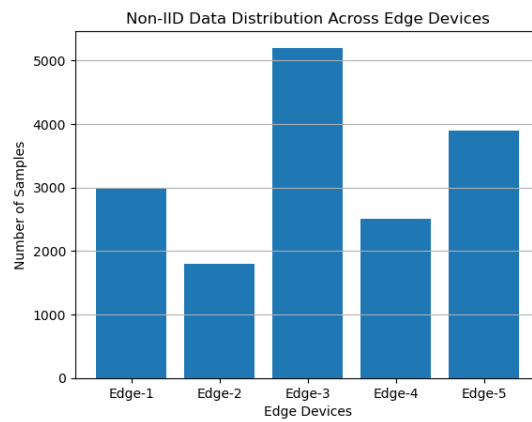
Federated Learning Performance

The Federated Learning performance analysis measures the efficiency of the proposed FGO-MLP-LSTM framework to train models using distributed edge devices without data aggregation in the central storage. The study will discuss global convergence of models, consistency in local accuracy, efficiency in communication and its performance in the aspect of non-IID data in this section. Through frequency of participation, cost of communication and resistance against attack analysis, the evaluation shows that decentralized learning improves privacy, decreases overhead and high predictive accuracy of real-time IoT data offloading environment.



a) Local model accuracy per edge device

b) Cost between edge devices and aggregator



c) Edge device data distribution

Figure 7: FL system characteristics

In Figure 6, the performance and efficiency of the developed federated learning technique are presented. The graphical representations validate the performance and efficiency achieved by the federated learning technique. Figure 6(a) presents the loss achieved by the federated MLP-LSTM model, showing a progressive decline as the number of epochs increases. Figure 6(b) presents the accuracy achieved by the federated MLP-LSTM model, showing an increase as the number of epochs progresses. Figure 6(c) presents the global accuracy achieved by federated devices, ensuring equal performance despite varying Non-IID data distribution.

The distribution of training samples among five edge devices as shown in Figure 7 indicates the Non-IID quality of the dataset. Figure 7a) indicates the accuracy of the local models of each of the edge devices at the classification stage. The accuracy of all the devices is high and relatively similar, which means that on-device learning performance is consistent even in the conditions of decentralized training. The communication overhead of each edge device in transmitting model updates to the central aggregator is shown in figure 7b). The prices will be differentiated among the devices based on the size of the data, the frequency of updates, or the network characteristics. The number of training samples is available on each edge device, which is shown in figure 7c). The skewed data distribution emphasizes a Non-IID case, which involves devices that contain much more information compared to others, which are a realistic federated learning system.

Security and Attack Resilience Evaluation

The effectiveness of the proposed structure against the adversarial behavior is exemplified in Figure 8 that compares the federated and centralized model when subjected to normal, poisoning and evasion attacks. The federated FGO-MLP-LSTM model exhibits high accuracy whereas performance deteriorates drastically when the centralized training is under attack. This is because of decentralized data retention, smaller attack surface and game theory adaptive defense mechanisms.

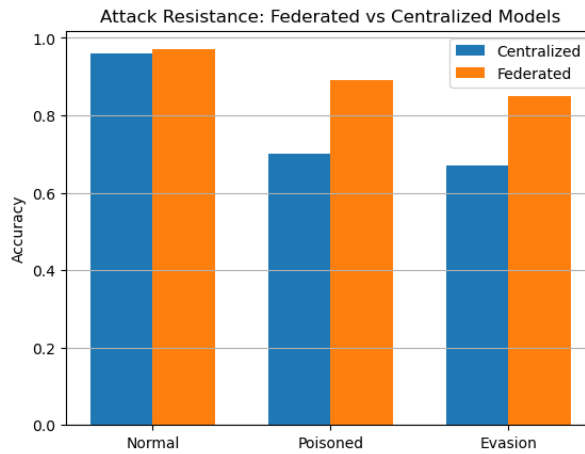


Figure 8: Attack resistance: edge device model vs centralized model

Figure 8 shows the accuracy of the centralized and federated models in three situations, which are the Normal, Poisoned and Evasion attacks. The centralized version is incredibly degraded during the attack case, but the federated version has much greater accuracy. This value proves how the federated FGO-MLP-LSTM architecture is more resilient to adversarial threats with the help of decentralized training, safe aggregation, and game-theoretic optimization. The federated model is advantageous in that it has decentralized data storage, smaller attack surface, and strategic defense using game theory, therefore, loss of accuracy is minimal. The centralized model is however very susceptible to malicious inputs. These results confirm the usefulness of the proposed architecture to protect real-time offloading data settings against various attack vectors.

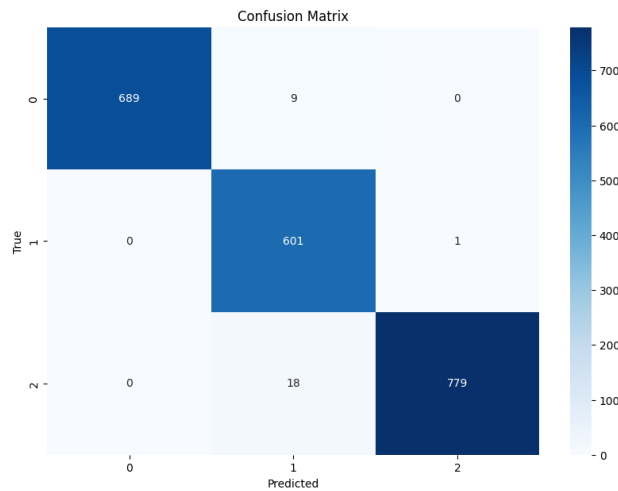


Figure 9: Confusion matrix

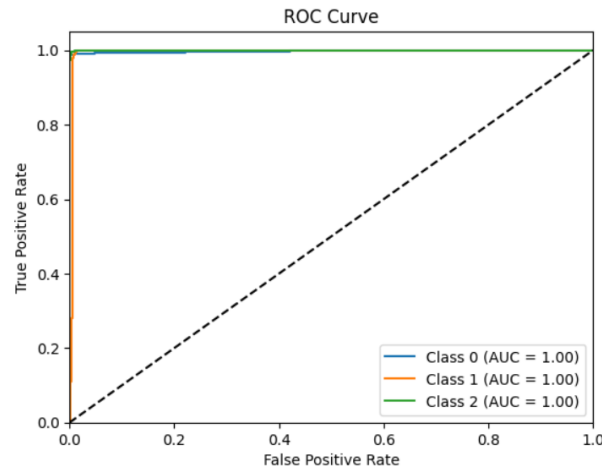


Figure 10: ROC curve

The confusion matrix and ROC curves (Figures 9 and 10) also affirm the high discriminative capability of the model on different types of traffic and show that there is low misclassification and high true positive rates at all times. These findings indicate that the proposed framework has a high degree of reliability in separating between benign and malicious traffic even when there are challenging attack conditions.

Performance Metrics

The performance measures section is the overall evaluation of the proposed framework based on the standard indicators of evaluation accuracy, precision, recall, and F1-score. These measures are a measure of the classification capabilities of a model to normal and malicious IoT traffic. In addition, communication cost, minimum latency, and resistance against attack are measured to evaluate the operational efficiency. The analysis proves that the FGO-MLP-LSTM has better predictive reliability and robustness than the current federated and deep learning methods. The performance metrics of the suggested model are displayed in Figure 11 and include an F1-score of 0.994, recall of 0.94, accuracy of 0.993, and precision of 0.995.

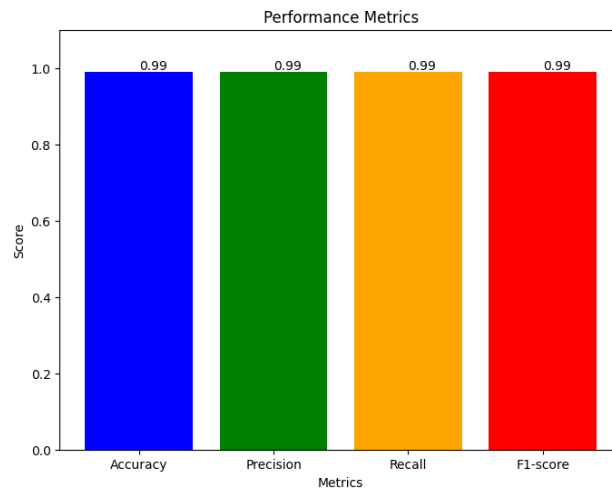


Figure 11: Performance metrics

Table 4: Comparison of performance metrics

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
LSTM (Ashraf et al., 2023)	91	89.10	81.13	88.11
Bi-LSTM (Ashraf et al., 2023)	91.36	90.16	90.11	90.19
Proposed Fed-GT-MLP-LSTM	99.3	99.5	99.4	99.4

Table 4 provides a comparison of the performance metrics of different methodologies utilized in the security of real-time data offloading that incorporate accuracy, precision, recall and F1-score. The proposed Fed-GT-MLP-LSTM framework compares favorably to the existing methods as can be seen in the comparative performance analysis. Although Bi-LSTM had an accuracy of 91% with a relatively lower recall (81.13%), and LSTM had a little better recall (90.11) with the same accuracy rates, both approaches had a problem in the comprehensive balance of accuracy and recall. There was a resultant high improvement in the Fed-Game method with 99% in all measures reflecting the effect of game-theoretic optimization. Nevertheless, the proposed Fed-GT-MLP-LSTM had the best results with a highest accuracy of 99.3, precision of 99.5, recall of 99.4, and F1-score of 99.4. This minor but significant enhancement highlights the efficiency of the integration of federated learning, game theory, and MLP-LSTM architecture in ensuring secure and efficient real-time offloading of data. The findings confirm that the given framework is a more balanced and robust solution as compared to its equivalents. Table 5 shows component-wise performance analysis of proposed study.

Table 5: Ablation study

Method	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
MLP-only Model	92.4	91.8	90.6	91.2
LSTM-only Model	93.1	92.5	91.9	92.2
Centralized MLP-LSTM (No FL)	96.8	96.2	95.9	96.0
Federated MLP-LSTM (No Game Theory)	98.6	98.2	97.9	98.0
Full FGO-MLP-LSTM Framework	99.3	99.5	99.4	99.4

Discussion

The experimental findings show that the Proposed Fed-GT-MLP-LSTM framework performs better in all the most important evaluation measures compared to the base models including Bi-LSTM, LSTM, and Fed-Game. Although the Bi-LSTM and LSTM models are good with about 91 as the accuracy, they are not so good in recall and F1-score, which means that they are not able to learn a network that has complex temporal dependencies and respond to various network traffic settings. Fed-Game provides much better metrics (99% in accuracy, precision, recall, and F1-score) by applying game-theoretic maximization of strategic decision-making, which guarantees equitable contribution of various nodes and strong aggregation. The suggested Fed-GT-MLP-LSTM, however, is more balanced and performs with a higher precision (99.5%), and recall (99.4%).

The minor improvement in performance measures indicates how the framework can enhance the ability of strengthening real-time data offloading security through dynamically setting offloading decisions within the existing network conditions, expected attackers' behaviour, and shared resources. The game theory can also guarantee that there is no dominating node in the decision-making process, which not only minimizes bias, but also makes it more resistant to data imbalance and adversarial manipulations. This results in a worldwide model that performs sensitivity to unknown traffic patterns

and achieves reliability in adverse network conditions. The suggested solution can be a good option to deploy in mission-critical applications where the latency, security, and fairness are all factors to consider as highly scalable, privacy preserving, and secure data offloading is suggested to take place in Edge-IIoT settings. By incorporating Game Theory, make sure that every node including the smaller, noisier, or infrequent traffic patterns gets a good shot in the training process. That is, at model aggregation time, each node's updates are not only weighted by data quantity but also by strategic considerations like data diversity, reliability, and relevance so smaller or less frequent traffic patterns are not overlooked. Consequently, the global model generalizes from a wider range of network behaviours' rather than overfitting on most frequent ones. This results in slightly less aggregate accuracy, but the model is more balanced, fair, and resilient, consistently performing across all classes of network traffic. In actual IIoT applications, this resilience and fairness are frequently more important than optimizing accuracy alone.

4 Conclusion and Future Works

In the rapidly changing IoT and cellular network scenario, real-time data offloading is necessary to improve computing efficiency and minimize latency. Concurrently, security threats such as data leakage and unauthorized access are difficult issues to handle. In this study, a strong model is proposed to improve the security of real-time data offloading based on FGO-MLP-LSTM. This approach, based on federated learning, maintains data secrecy by transmitting model updates and not the sensitive data itself, storing them in local edge devices. The likelihood of data breaches is minimized through this decentralized framework. Game theory simulates the dynamics between data sources, offloading nodes, and possible attackers to make strategic decisions that maximize security and performance. As they can process complex, high-dimensional data and learn long-term associations, the LSTM and MLP modules provide effective pattern detection and predictive analysis. Advanced pre-processing algorithms and min-max normalization ensure consistency and quality of data to allow easy training and quick real-time threat detection. Experimental results indicate the model outperforms its analogues, such as Bi-LSTM, LSTM and Fed-Game with its accuracy of around 99.3 percent. This two-layered solution is scalable, secure and reliable to handle the complicated issues of data security and privacy where real-time data offloading is required. Scalability and flexibility of FGO-MLP-LSTM model are also to be incorporated in future studies to enable more heterogeneity of IoT devices and data. More sophisticated machine learning and game-theoretic models can be improved and investigated further. The second research direction that is of interest is incorporating blockchain technology to verify the authenticity of data exchange and federalization of learning models updates. Lastly, comprehensive bundles of realistic testing and application would be conducted to verify that the frame is effective in a sequence of realistic cases, to ensure that it is sound and viable to withstand real-time data offloading in modern digital settings.

References

- [1] Ahlawat, C., & Krishnamurthi, R. (2023). Towards smart technologies with integration of the internet of things, cloud computing, and fog computing. *International Journal of Networking and Virtual Organisations*, 29(1), 73-124. <https://doi.org/10.1504/IJNVO.2023.134304>
- [2] Alrowais, F., Almasoud, A. S., Marzouk, R., Al-Wesabi, F. N., Hilal, A. M., Rizwanullah, M., ... & Yaseen, I. (2022). Artificial Intelligence Based Data Offloading Technique for Secure MEC Systems. *Computers, Materials & Continua*, 72(2). 10.32604/cmc.2022.025204

- [3] Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, *12*, 30907-30927. <https://doi.org/10.1109/ACCESS.2024.3369906>
- [4] Ashraf, S. N., Manickam, S., Zia, S. S., Abro, A. A., Obaidat, M., Uddin, M., ... & Alsaqour, R. (2023). IoT empowered smart cybersecurity framework for intrusion detection in internet of drones. *Scientific reports*, *13*(1), 18422. <https://doi.org/10.1038/s41598-023-45065-8>
- [5] Ben Hamida, M. B., Basem, A., Varshney, N., & Mostafa, L. (2025). Intelligent design of high-performance fluids for thermal management: integrating response surface methodology, weighted Tchebycheff method, and strength Pareto evolutionary algorithm II. *Scientific Reports*, *15*(1), 21508. <https://doi.org/10.1038/s41598-025-07132-0>
- [6] Cappa, F., Franco, S., & Rosso, F. (2022). Citizens and cities: Leveraging citizen science and big data for sustainable urban development. *Business Strategy and the Environment*, *31*(2), 648-667. <https://doi.org/10.1002/bse.2942>
- [7] Chaudhry, S. R., Liu, P., Wang, X., Cahill, V., & Collier, M. (2022). A measurement study of offloading virtual network functions to the edge. *The Journal of Supercomputing*, *78*(2), 1565-1582. <https://doi.org/10.1007/s11227-021-03907-0>
- [8] Chen, Z., Xiong, X., Wang, W., Xiao, Y., & Alfarraj, O. (2023). A blockchain-based multi-unmanned aerial vehicle task processing system for situation awareness and real-time decision. *Sustainability*, *15*(18), 13790. <https://doi.org/10.3390/su151813790>
- [9] Ferrag, M. A., Friha, O., Hamouda, D., Maglaras, L., & Janicke, H. (2022). Edge-IIoTset: A new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. *IEEE Access*, *10*, 40281–40306. <https://doi.org/10.1109/ACCESS.2022.3165809>
- [10] Goswami, P., Faujdar, N., Debnath, S., Khan, A. K., & Singh, G. (2024). Investigation on storage level data integrity strategies in cloud computing: classification, security obstructions, challenges and vulnerability. *Journal of Cloud Computing*, *13*(1), 45. <https://doi.org/10.1186/s13677-024-00605-z>
- [11] Hu, H., Song, W., Wang, Q., Hu, R. Q., & Zhu, H. (2022). Energy efficiency and delay tradeoff in an MEC-enabled mobile IoT network. *IEEE Internet of Things Journal*, *9*(17), 15942-15956. <https://doi.org/10.1109/JIOT.2022.3153847>
- [12] Ikegwu, A. C., Nweke, H. F., Anikwe, C. V., Alo, U. R., & Okonkwo, O. R. (2022). Big data analytics for data-driven industry: a review of data sources, tools, challenges, solutions, and research directions. *Cluster Computing*, *25*(5), 3343-3387. <https://doi.org/10.1007/s10586-022-03568-5>
- [13] Jin, X., Hua, W., Wang, Z., & Chen, Y. (2022). A survey of research on computation offloading in mobile cloud computing. *Wireless Networks*, *28*(4), 1563-1585. <https://doi.org/10.1007/s11276-022-02920-2>
- [14] Khan, S., Jiangbin, Z., & Ali, H. (2024). Soft computing approaches for dynamic multi-objective evaluation of computational offloading: a literature review. *Cluster Computing*, *27*(9), 12459-12481. <https://doi.org/10.1007/s10586-024-04543-y>
- [15] Khattak, M. I., Yuan, H., Khan, A., Ahmad, A., Ullah, I., & Ahmed, M. (2025). Evolving multi-access edge computing (MEC) for diverse ubiquitous resources utilization: a survey: MI Khattak et al. *Telecommunication Systems*, *88*(2), 71. <https://doi.org/10.1007/s11235-025-01310-1>
- [16] Mann, Z. Á., Metzger, A., Prade, J., Seidl, R., & Pohl, K. (2022). Cost-optimized, data-protection-aware offloading between an edge data center and the cloud. *IEEE transactions on services computing*, *16*(1), 206-220. <https://doi.org/10.1109/TSC.2022.3144645>
- [17] Molokomme, D. N., Onumanyi, A. J., & Abu-Mahfouz, A. M. (2022). Edge intelligence in Smart Grids: A survey on architectures, offloading models, cyber security measures, and challenges. *Journal of Sensor and Actuator Networks*, *11*(3), 47. <https://doi.org/10.3390/jsan11030047>

- [18] Myakala, P. K., Jonnalagadda, A. K., & Bura, C. (2024). Federated learning and data privacy: A review of challenges and opportunities. *International Journal of Research Publication and Reviews*, 5(12), 10-55248. <https://doi.org/10.55248/gengpi.5.1224.3512>
- [19] Orabi, M. M., Emam, O., & Fahmy, H. (2025). Adapting security and decentralized knowledge enhancement in federated learning using blockchain technology: literature review. *Journal of Big Data*, 12(1), 55. <https://doi.org/10.1186/s40537-025-01099-5>
- [20] Priya, S. M., Durga, R., & Nithya, D. (2025, January). A comprehensive survey on data offloading, clustering, resource allocation, and security challenges. In *International Conference on Artificial Intelligence and Smart Energy* (pp. 532-542). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-90482-0_43

Authors Biography



Jayaprakash Hampi Received degree in B. E Electronics and Communications Engineering from Gulbarga University, Karnataka, India in 1998, and M. Tech in VLSI and Embedded Systems from VTU University, Karnataka, India in 2018. 23 years of professional experience in IT industry with extensive experience of leading large complex programs involving cross functional teams, program management, account management, delivery management of multiple programs in the area of Internet of Things (IoT) including both products and Manufacturing. Major research interest is in IoT, Artificial Intelligence, Machine learning, Deep learning and related research areas.



Dr.C.B. Vinutha Presently working as Associate Professor - Selection Grade in the Department of Electronics and Communication Engineering, School of Engineering, Presidency University, Bengaluru, Karnataka, India. She is having more than 22 years of academic experience and 14 years of research experience. Her Bachelor of Engineering in Electronics was completed in the year 1995 from BMS College of Engineering, Bangalore University, Bangalore. Post graduation (MTech) in Digital Communication from MSRIT, VTU, Belagavi in the year 2006. Doctoral Degree in the field of Wireless Sensors Networks was completed in the year 2019 from NMIT, VTU, Belagavi. She has three patents filed of which two have been published as first inventor. She has published various research papers in reputed journals and conferences. The major area of research interest is Wireless Sensor Networks, in particular focuses on the energy saving strategies of cross layer issue in WSN. The other research areas of interest are Image Processing and Edge Computing.