FEDERATED LEARNING BASED TRAFFIC INTELLIGENCE FOR PRIVACY PRESERVING DISTRIBUTED OPTIMIZATION OF WIRELESS NETWORK PERFORMANCE

J. RAVINDRA BABU[1], K. PRASUNA[2], Y. V. K. D. BHAVANI[3], PRASAD DEVARASETTY[4], R. SUDHA KISHORE[5], S. SINDHURA[6]

[1]Associate Professor, Department of ECE, PVP Siddhartha Institute of Technology, Vijayawada, A.P, India.
[2]Associate Professor, Department of Electronics and Communication Engineering, Vijaya Institute of Technology for Women, Vijayawada-521108, AP, India.
[3]Assistant Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram - 522302, Guntur, AP, India.
[4]Professor, Department of Computer Science and Engineering, DVR & Dr. HS MIC College of Technology, Andhra Pradesh, India.
[5]Professor, Department of Computer Science & Engineering, VVIT University, Nambur, Guntur, A.P, India.
[6]Assistant Professor, Department of Computer Science and Engineering, Dr.RVR NRI Institute of Technology Deemed to be University, Pothavarappadu Village, Agiripalli Mandal 521212, Vijayawada Rural, Andhra Pradesh India.
Email: ssindhurapraveen@gmail.com

ABSTRACT

The intensive development of wireless communication systems and data-intensive applications has created a very dynamic and unpredictable network traffic patterns, which are very much challenging to maintain Quality of Service (QoS). The classic network optimization methods that are based on the traditional and centralized methodologies tend to be inefficient to adapt to the real-time changes in traffic and brings forth the concern of scalability, privacy, and communication overhead. In solving these challenges, the present study suggests a federated learning-based traffic intelligence to privacy-preserving distributed optimization of wireless network performance. Various distributed nodes can cooperatively learn a global model in the proposed approach without providing raw data, thus preserving data privacy and minimizing communication cost. The framework combines the traffic prediction with adaptive network optimization techniques such as dynamically allocating bandwidth, load balancing, and congestion control. Experimental findings indicate that the proposed model can greatly enhance the performance of a network in comparison to traditional and centralized machine learning methods. Significant increases in accuracy of prediction, throughput, latency, packet loss ratio, and spectral efficiency have been noted. In addition, the framework ensures high utilization of the network to different traffic conditions, which underscores its scalability and flexibility. Generally, the suggested federated learning-based solution offers a scalable and efficient privacy-conscious solution to next-generation wireless networks, such as 5G and IoT networks.

Keywords: *Federated Learning, Wireless Networks, Traffic Prediction, Network Optimization, Privacy Preservation*

1. INTRODUCTION

The wireless communication technologies transformed contemporary digital infrastructure with the ability to provide seamless connectivity to various areas: Internet of Things (IoT), smart cities, healthcare, industrial automation, and real-time communication systems [1]. The high rate of mobile device proliferation, cloud computing and applications that consume a lot of bandwidth has greatly augmented the pressure on the wireless network resources. As a result, contemporary wireless networks are marked by extremely dynamic, heterogeneous and unpredictable traffic patterns that present serious challenges of ensuring a consistent Quality of Service (QoS)[24,25].

The extreme rise in the amount of data traffic has resulted in serious problems such as network congestion, higher latency, loss of packets, and poor use of the limited spectral resources. Such difficulties are exacerbated by next-generation networks (5G and beyond) where networking requirements like ultra-reliable low-latency communication (URLLC) and massive machine-type communication (mMTC) require highly adaptive and intelligent management of the network [2]. Thus, effective traffic forecasting and dynamic resource optimization is now critical when it comes to guaranteeing a stable network performance [3].

Traditional network optimization methods are mostly based on fixed settings and control reactions [4,29]. Although these methods are easy and commonly used, they are not effective in responding to the dynamism of traffic conditions. Consequently, they tend to result in a slow reaction to traffic jams and inefficient use of the network resources [26]. Machine learning (ML)-based traffic prediction is one of the solutions to these shortcomings, allowing networks to forecast traffic demand and take an active optimization move [5,30].

Nevertheless, the majority of existing ML-based solutions use a centralized paradigm, where massive amounts of data are gathered and run in a central server [6]. This method presents some serious issues such as privacy of data, higher overhead of communication, and reduced scalability of distributed network systems. Raw data never stops in a large scale wireless system not only wasting bandwidth but also increasing the security risks [7].

In order to address these shortcomings, this research paper presents a federated learning (FL)-driven distributed traffic intelligence system. Federated learning enables multiple distributed nodes, such as base stations and edge devices, to collaboratively train a global model without sharing raw data. Rather, the exchange of model parameters only is guaranteed, which guarantees privacy protection and minimizes communication expenses. This decentralized model facilitates scalable, efficient and intelligent network optimization that is appropriate in next-generation wireless networks.

1.1. Background and Problem Context

As wireless communication systems evolve, networks have grown more complex with the introduction of heterogeneous devices, dissimilar types of traffic, and dynamic user behavior. The complexities of this nature cannot be dealt with using the conventional optimization techniques, which cannot be flexible and predictive [27,28]

Offering traffic patterns and being able to optimize proactively, machine learning-based solutions have displayed encouraging results. Nevertheless, they are not applicable to distributed scenarios in the real world because they are dependent on centralized data processing [8]. The problems of data ownership, privacy rules, and network latency complicate the use of centralized learning with large-scale deployments. These issues raise the necessity of a decentralized and privacy-conscious learning system that will be able to work effectively among distributed network nodes.

1.2. Motivation for Federated Learning in Wireless Networks

Federated learning in wireless networks is inspired by a number of practical and technological reasons. First, it has brought about data privacy as a huge issue particularly where sensitive user information is involved. Federated learning attempts to resolve this problem by making sure that raw data is localized to the node [9].

Second, communication overhead required to send large-scale traffic information to a central server is also greatly minimized, since only model updates are exchanged. This results in efficiency in bandwidth and latency.

Moreover, federated learning provides scalable and distributed intelligence, which is critical to the contemporary wireless networks like 5G and IoT ecosystems. By allowing local model training and global collaboration, FL enhances adaptability and real-time decision-making capabilities in dynamic network environments.

1.3. Key Contributions of the Study

The present study presents a new federated learning-based model in traffic prediction and wireless network optimization. Its most significant contribution is that it allows training models in a distributed way without losing the privacy of data, which is one of the biggest shortcomings of the centralized machine learning methods.

The framework proposed combines federated traffic prediction and intelligent network optimization strategies that enable proactive and adaptive allocation of resources. This integration has a great enhancement in network performance parameters which include throughput, latency, packet loss, as well as spectral efficiency.

Also, the research gives a detailed comparative study between the traditional techniques, centralized ML strategies, and the upcoming federated learning model. The findings show the efficiency, scalability, and applicability of the presented strategy in the next-generation wireless networks.

1.4. Research Objectives

These aims of the research are established to direct the formation and assessment of a federated learning-based framework to optimize intelligent wireless networks.

The specific research objectives are as follows:

- To create a federated learning-based traffic prediction model that can be used to make the right prediction on network traffic patterns without compromising on privacy of the data across distributed network nodes.
- To conceive and realize a distributed optimization system that considers predicted-traffic data in adaptive plans like dynamic allocation of bandwidth, load balancing, and congestion control.
- To compare and contrast the performance of the proposed federated learning solution with traditional and centralized machine learning solutions with the use of key performance metrics such as throughput, latency, packet loss ratio, and spectral efficiency.

2. RELATED WORK

Recent development in wireless communication networks has accentuated the severe necessity of the intelligent predictive traffic and the efficient system of resources optimization mechanisms. The use of machine learning (ML) methods has become popular to overcome the shortcomings of conventional reactive network management techniques. These methods allow proper predicting of traffic and allow making proactive decisions, which enhances the overall performance of the network. However, most ML-based approaches rely on centralized architectures, which introduce significant challenges related to scalability, communication overhead, and data privacy.

Federated learning (FL) is a decentralized learning model that has been proposed to address these problems, allowing joint training of models without exchanging raw data. Mahdi Rahmati and Neda Rahmati (2025) suggested a privacy friendly federated multi-sensor fusion system coupled with edge computing to manage traffic at real time in connected vehicle networks [10]. They have shown that FL with edge intelligence can be used to improve real-time decision-making without compromising data privacy. But their treatment is mostly restricted to vehicle networks and fails to extend to more general wireless communication systems.

In a similar direction, Feng Gao et al. (2024) constructed a communication-efficient federated learning framework to predict wireless traffic [11]. Their effort is directed towards the minimization of communication overheads through optimization of parameter exchange in training. Though the model is better in predicting and efficiency, it is not coupled with adaptive network optimization mechanisms like resource allocation and congestion management.

Further extending federated learning applications, Jian Wei et al. (2025) introduced a three-level FL architecture of privacy-sensitive traffic prediction in IIoT settings [13]. The hierarchical architecture that is proposed improves scalability and sparse traffic data. The study is however, domain specific and is not testing of overall wireless network performance metrics like throughput and latency.

More recently, A. Aalavanthar et al. (2025) presented a federated learning model with multi-objectives to predict traffic in vehicular networks. They combine a variety of parameters, including accuracy of prediction and efficiency of communication, which is why they are suitable in case of intelligent transportation systems [14]. The framework has limitations of being limited to vehicular environments and lacks generalization of wireless network optimization problems.

Similarly, Y. Du and H. Sun (2025) presented a federated learning-based dynamic traffic control system in the context of smart cities through IoT. Their work shows that FL can be used to allow real-time traffic control and management of the network in large cities. Nevertheless, it is more of a study on traffic flow control and not on the optimization of performance in wireless communication networks.

In another related study, S. R. Jeyakumar et al. (2024) presented a federated learning-based hybrid deep learning model of intrusion detection in wireless sensor networks that is secure and privacy preserving [15]. Their solution is based on the significance of security and privacy in distributed learning systems. Although the research centers on network security, but not traffic optimization, it supports the usefulness of federated learning in a wireless setting.

Overall, the current body of literature affirms that machine learning is a strong tool to enhance the accuracy of traffic predictions and the performance of a network. Nevertheless, the centralized ML solutions are associated with privacy issues, expensive communication, and lack of scalability. Even though federated learning [16] solves these problems, the majority of existing literature is either domain-specific (vehicular networks, IoT, or IIoT) or do not implement any optimization technique along with prediction accuracy.

Therefore, there is a distinct research gap in creating a generalized federated learning-based framework that integrates traffic forecasting with real-time optimization of wireless network whilst maintaining privacy, scalability, and efficiency. This paper combats this gap by coming up with a distributed traffic intelligence model that incorporates federated learning and adaptive resource allocation algorithms to improve the overall network performance.

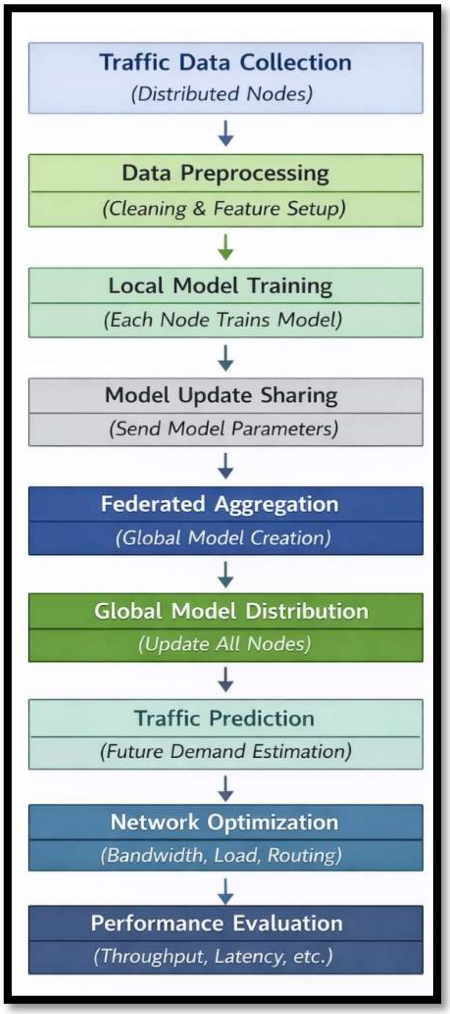

Figure 1: Workflow of the proposed federated learning-based traffic intelligence framework for wireless network optimization.

3. PROPOSED METHODOLOGY

This paper suggests a federated learning-based traffic intelligence system to perform distributed optimization of wireless networks. In contrast to centralized machine learning models [17], the suggested methodology can allow several distributed nodes to learn about traffic patterns and maintain the privacy of data. The framework incorporates the traffic prediction and adaptive optimization strategies to increase the overall effectiveness of the network.

The fig 1 shows the general flow of the proposed federated learning-based framework in which distributed nodes autonomously process traffic data and cooperatively train a global model. Aggregated model is employed to forecast demand of traffic and it allows optimization of networks dynamically, which results in better performance.

3.1. System Architecture

The suggested system uses the paradigm of federated learning whereby several distributed network nodes including base stations and edge devices engage in joint model training. All nodes, without revealing raw data, process their own local traffic data and contribute to a common global model [18].

It is based on five main components: local nodes, local training modules, federated aggregation server, global model distribution and network optimization module. The local nodes are tasked with the responsibility of collecting and pre-processing traffic data and the local training node produces updates to the model using this data. They are sent to the central aggregation server [19], which adds these updates together with a federated averaging mechanism to update the global model. The revised model is thereafter re-distributed to all nodes and the learning and adaptation continues.

Table 1: Components of the Proposed Federated Learning Architecture

Component	Function
Local Nodes	Collect and store traffic data locally
Local Training Module	Train models using local datasets
Aggregation Server	Combine local model updates
Global Model Distribution	Share updated model with nodes
Optimization Module	Apply resource allocation strategies

3.2. Working Mechanism

The workflow of the proposed system is based on the iterative federated learning cycles. To begin with, each node collects real time traffic data and some of the parameters considered in this data are packet flow, delay and throughput [20]. This information is pretreated, and it is utilized to teach local machine learning model.

The nodes transfer model parameters or gradients to the aggregation server and not raw data. These updates are then merged with a weighted averaging technique by the server to generate a global model. The new model is re-shuffled to the whole participating nodes, such that they can optimize their predictions.

It is able to dynamically allocate network resources based on the estimated demand of the network [21] by intelligently allocating network resources through intelligent optimization methods. This is the decentralized mechanism that ensures the effective learning, reduced communication overhead and privacy.

3.3. Algorithm: Federated Traffic Intelligence Framework

The process map of the suggested methodology is as follows:

The algorithm runs a series of federated learning in which local models [22] are trained on distributed nodes and pooled together to form a global model. Traffic prediction is done with the updated model and then dynamic network optimization is done to enhance performance.

```
# Input: Distributed datasets D_i at each node
# Output: Optimized network performance

Initialize global model M

for each round r = 1 to R:

    for each node i:
        Train local model M_i using D_i
        Send M_i to server

    # Federated Aggregation (FedAvg)
    M = Σ (n_i / n) * M_i

    # Traffic Prediction and Optimization
    traffic = predict(M)
    optimize_network(traffic)

# Evaluate performance
return throughput, latency, packet_loss, spectral_efficiency
```

3.4. Mathematical Modeling

The distributed optimization principles [23] are used to mathematically model the proposed federated learning framework. The basic aggregation principle is the Federated Averaging (FedAvg) algorithm that uses local model updates to create a global model.

Global Model Aggregation

$$M = \sum_{i=1}^{N} \frac{n_i}{n} M_i \qquad [1]$$

where $M_i$represents the local model at node i, $n_i$represents the local dataset size and n is the overall number of samples in all the nodes. Such a weighted aggregation is important so that nodes that have more data contribute more to the global model.

Local Model Training Objective

Local loss function is minimized at each node depending on its dataset:

$$\min_{M_i} \ \mathcal{L}_i(M_i) = \frac{1}{n_i} \sum_{j=1}^{n_i} \ell(x_j, y_j; M_i) \qquad (2)$$

where $\ell(x_j, y_j; M_i)$is the loss function (e.g., Mean Squared Error) for sample j.

Global Optimization Objective

The world model seeks to reduce the weighted loss of local losses:

$$\min_{M} n \ \mathcal{L}(M) = \sum_{i=1}^{N} \frac{n_i}{n} \mathcal{L}_i(M) \qquad (3)$$

This formulation will be used to guarantee uniformity between the local and global learning objectives.

Traffic Prediction Function

The trained global model predicts future traffic demand as:

$$\hat{T}(t+1) = f(M, X_t) \qquad [4]$$

where $\hat{T}(t+1)$is the predicted traffic at time $t+1$, and $X_t$represents current network features.

Network Performance Metrics

In order to determine the efficiency of the proposed framework, the mathematical expressions below are used:

Throughput (T):

$$T = \frac{\text{Total Successfully Transmitted Data}}{\text{Time}} \qquad [5]$$

Latency (L):

$$L = \frac{\sum_{k=1}^{P} d_k}{P} \qquad [6]$$

Packet Loss Ratio (PLR):

$$PLR = \frac{\text{Packets Lost}}{\text{Packets Sent}} \qquad [7]$$

Spectral Efficiency (SE):

$$SE = \frac{\text{Data Rate}}{\text{Bandwidth}} \qquad [8]$$

The mathematical formulations above are all a description of the federated learning-based optimization process. The aggregation equation makes sure that the global learning is effective whereas the loss functions direct the local and global model convergence. The prediction function allows proactive traffic estimation and the performance metrics measures the improvements in the network efficiency.

3.5. Network Optimization Strategies

The system uses dynamic optimization strategies to improve network performance based on the predicted traffic demand acquired through the federated model. Such strategies allow making decisions in advance and using resources effectively.

Table 2: Network Optimization Strategies and Objectives

Strategy	Objective
Dynamic Bandwidth Allocation	Minimize congestion and improve throughput
Load Balancing	Distribute traffic evenly across nodes
Adaptive Scheduling	Reduce latency and packet delays
Congestion Control	Prevent packet loss and buffer overflow

All these strategies make sure that the network can adjust to the changing traffic in real time resulting in enhanced Quality of Service (QoS).

3.6. Performance Metrics

The usefulness of the suggested framework is measured with the standard wireless network performance metrics. These metrics will give a quantitative context against which the proposed approach can be compared to conventional and centralized machine learning models.

- Throughput (T): Measures the proportion of successful data transmission throughout the network.
- Latency (L): Measures the overall delay of data packets.
- Packet Loss Ratio (PLR): Represents the loss rate of packet transmissions.
- Spectral Efficiency (SE): Indicates the effective use of the bandwidth.

These performance metrics are vital in gauging network reliability, performance and scalability at different levels of traffic.

4. RESULTS AND DISCUSSION

In this section, a detailed assessment of the suggested federated learning-based traffic intelligence framework will be provided. The results of the proposed model are contrasted with traditional methods of network management and centralized machine learning. The performance measurements are on accuracy of prediction, throughput, latency, packet loss ratio, spectral efficiency and network utilization during different traffic conditions.

4.1. Traffic Prediction Accuracy

Proper traffic forecasting is a critical aspect of network optimization and optimal management of resources in wireless communications. The proposed federated learning (FL)-based model in this study is evaluated and compared to conventional (non-ML) and centralized machine learning methods. These comparisons are made on the basis of the main evaluation measures, which include Mean Absolute Error (MAE) and prediction accuracy.

Table 3: Traffic Prediction Accuracy Comparison

Model	Mean Absolute Error	Prediction Accuracy (%)
Conventional (No ML)	18.6	72.4
Centralized ML	7.9	91.2
Proposed FL Model	6.1	93.8

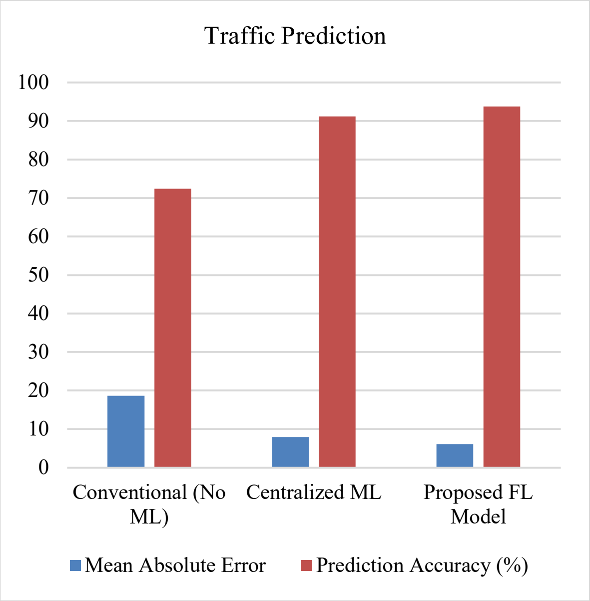

Figure 2: Graphical Representation of Traffic Prediction Accuracy Comparison

The findings of Table 3 clearly show that the proposed federated learning model is superior to the conventional and centralized machine learning models. The FL-based model has the lowest Mean Absolute Error of 6.1, which proves a better precision of prediction, and less deviation of actual values of traffic. Also, it achieves the maximum prediction accuracy of 93.8, which demonstrates its capability to be able to capture complicated and moving traffic patterns.

However, the traditional method performs much worse because of the lack of predictive intelligence, whereas the centralized ML model, despite its efficiency, has limitations since it relies on the aggregation of data and is less adaptable to the distributed environment.

The federated learning model has a better performance owing to the decentralized training process, which involves several nodes jointly learning using different and local traffickers. This helps the model to generalize more when subjected to different network conditions without affecting data privacy. The graphical comparison, as shown in Fig. 2, also helps to note the evident accuracy improvement and decrease of the prediction error that the suggested method offers.

4.2. Throughput Performance Analysis

Throughput is a key performance measure that indicates the efficiency of data transfer in a network that is wireless. It reflects how well data is being delivered through the communication medium and is a direct measure of the ability of the network to support traffic load. Increased throughput means a more efficient use of available resources and enhancing Quality of Service (QoS) to end users.

Table 4: Average Network Throughput

Method	Throughput (Mbps)
Conventional	22.5
Centralized ML	31.8
Proposed FL Model	34.6

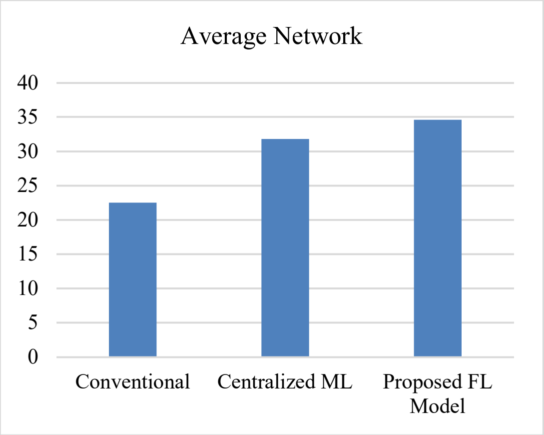

Figure 3: Graphical Representation of Average Network Throughput

The proposed federated learning (FL)-based framework is also compared to traditional network management and centralized machine learning in this study in terms of throughput performance.

Table 4 shows that the proposed federated learning model has significantly enhanced throughput. The traditional method has the lowest throughput of 22.5 Mbps because it is reactive and cannot adjust to the changing traffic characteristics. The centralized ML model increases throughput up to 31.8 Mbps by predicting resource allocation; it is however, limited by scalability and slow adaptability.

The FL-based model proposed has the maximum throughput of 34.6 Mbps, which means that it performs better when dealing with network traffic. This is due to its decentralized learning process that allows real-time prediction of traffic at the distributed nodes. The model can be used to enable proactive allocation of bandwidth, effective load distribution, and minimize congestion by using local data information.

As shown in Fig. 3, the graphical representation unmistakably shows the steady growth in throughput of the traditional methods to centralized ML and to the proposed federated learning method. The findings validate that federated learning coupled with network optimization has a significant impact on increasing the efficiency of data transmission and network performance.

4.3. End-to-End Latency Analysis

The end-to-end latency is a key performance indicator in wireless networks especially with real-time and delay-sensitive applications like video conferencing, online gaming and voice communication. It is the sum of time spent by a data packet on its way to the destination. Reduced latency is critical in responsiveness and high Quality of Service (QoS).

The latency performance of the proposed federated learning (FL)-based framework is evaluated and compared to the traditional and centralized machine learning methods in this study.

Table 5: Average End-to-End Latency

Method	Latency (ms)
Conventional	145
Centralized ML	92
Proposed FL Model	80

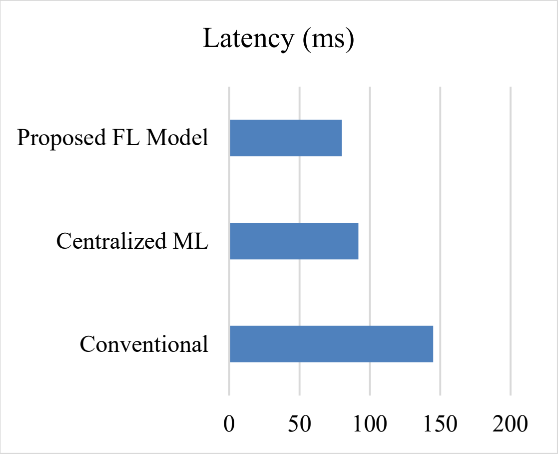

Figure 4: Graphical Representation of Average End-to-End Latency

Table 5 clearly shows that the proposed federated learning model has the lowest latency of all the compared methods. The traditional method has the greatest latency of 145 ms because it is reactive and cannot predict congestion. The predictive capabilities of the centralized ML model also result in a substantial reduction of latency to 92 ms, but there is still a cost in terms of delays in the processing and transmission of data centrally.

The FL-based model also decreases the latency to 80 ms, which means a better responsiveness and efficiency. This enhancement can be largely explained by the fact that decentralized learning mechanism allows identifying the traffic congestion at the earliest stage and promotes adaptive scheduling decisions made at the local node level. The model reduces the processing delays and improves real-time decision-making by reducing reliance on centralized data exchange.

The graphical representation as shown in Fig. 4 shows a steady decrease in latency between standard techniques and centralized ML and on to the federated learning technique. Such findings validate that federated learning with network optimization strategies is much more responsive and is extremely adaptable to delay-sensitive wireless networks.

4.4. Packet Loss Ratio

Packet Loss Ratio (PLR) is one of the most important performance indicators that directly indicate the reliability and stability of a wireless network. It is a ratio of the number of data packets that are lost on their way to a destination. Large packet loss causes retransmission, high delays and poor Quality of Service (QoS), particularly in real-time applications. Hence, it is important to reduce packet loss in order to achieve effective and credible communication.

In this paper, the packet loss performance of the federated learning (FL)-based framework is evaluated against the traditional and centralized machine learning methods.

Table 6: Packet Loss Ratio Comparison

Method	Packet Loss (%)
Conventional	6.8
Centralized ML	2.3
Proposed FL Model	1.7

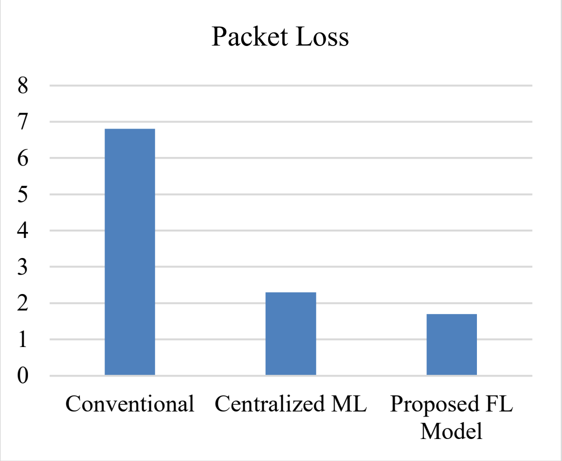

Figure 5: Graphical Representation of Packet Loss Ratio Comparison

The findings in Table 6 suggest that the number of packet losses significantly decreases when applying the suggested federated learning model. The traditional method has the most serious ratio of 6.8% of packet losses because of poor congestion management and prediction facilities. The centralized ML model significantly improves performance by reducing packet loss to 2.3%, owing to its ability to anticipate traffic conditions.

The FL-based model also minimizes packet loss to 1.7% and this illustrates the model as having better network reliability. This can be improved by the decentralized learning mechanism that facilitates the early detection of congestion and the management of the buffer at the local node level. The model efficiently averts network congestion and reduces the number of packets dropped by exploiting real-time traffic information of a network using multiple distributed nodes.

As illustrated in Fig. 5, the graphical representation clearly shows the progressive reduction in packet loss from conventional methods to centralized ML and further to the federated learning approach. Such results prove that the suggested framework increases stability in a network and makes the transmission of data more consistent in different conditions of traffic.

4.5. Spectral Efficiency Analysis

Spectral efficiency is an important performance parameter in wireless communication systems, because it quantifies the efficiency with which the given frequency spectrum is used to transmit data. It is determined as the data rate transmitted using a unit bandwidth and is crucial in solving the increasing demand of high data rates using limited spectrum. Increased spectral efficiency means that network resources are being utilized more efficiently and the overall system capacity is higher.

In this study, the spectral efficiency of the offered federated learning (FL)-based framework is tested and compared to the traditional and centralized machine learning methods.

Table 7: Spectral Efficiency Comparison

Method	Spectral Efficiency (bps/Hz)
Conventional	2.1
Centralized ML	3.4
Proposed FL Model	3.9

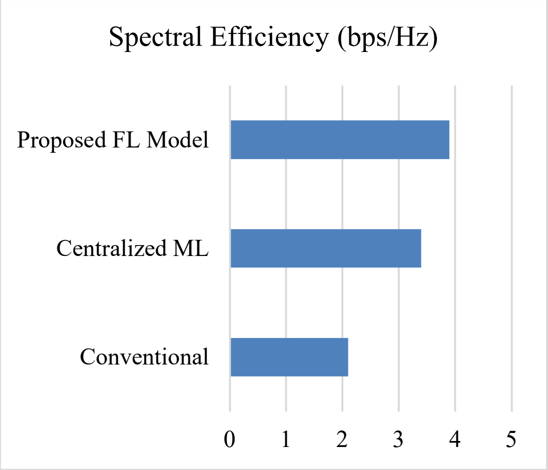

Figure 6: Graphical Representation of Spectral Efficiency Comparison

As shown in Table 7, the proposed federated learning model has the highest spectral efficiency of the compared strategies. The traditional approach is the least efficient with the value of 2.1 bps/Hz because it is associated with the fixed allocation of resources and poor usage of the spectrum. Centralized ML model enhances spectral efficiency to 3.4 bps/Hz by using predictive capabilities that can optimize the management of resources.

The proposed FL-based model also achieves better spectral efficiency of 3.9 bps/Hz, which implies a better performance in terms of spectrum use. The given improvement can be explained mainly by the decentralized learning mechanism allowing the adaptation to the different states of traffic in real time. Through the use of distributed data insights, the model adjusts dynamically transmission parameters (bandwidth allocation and scheduling) and results in a more efficient utilization of spectrum available.

As shown in Fig. 6, the graphical analysis indicates that the spectral efficiency of the conventional approaches is steadily growing to centralized ML and then to the federated learning method. These findings affirm that federated learning combined with network optimization strategies is very effective in enhancing the use of the spectrum and is therefore very appropriate in next generation wireless networks where there is a constraint on the spectrum resources.

4.6. Network Utilization Under Different Traffic Loads

Network utilization efficiency is a significant performance measure that indicates the utilization efficiency of available network resources across different traffic conditions. It is especially applicable in determining the scalability and adaptability of a wireless network as it reflects the capability of the system to sustain its performance under varying load conditions.

This paper evaluates the efficiency of the proposed federated learning (FL)-based framework in terms of low, medium, and high traffic loads and compares it with traditional and centralized machine learning methods.

Table 8: Network Utilization Efficiency

Traffic Load	**Conventional (%)**	**ML-Based (%)**	**FL-Based (%)**
Low	62	78	85
Medium	68	85	91
High	71	89	95

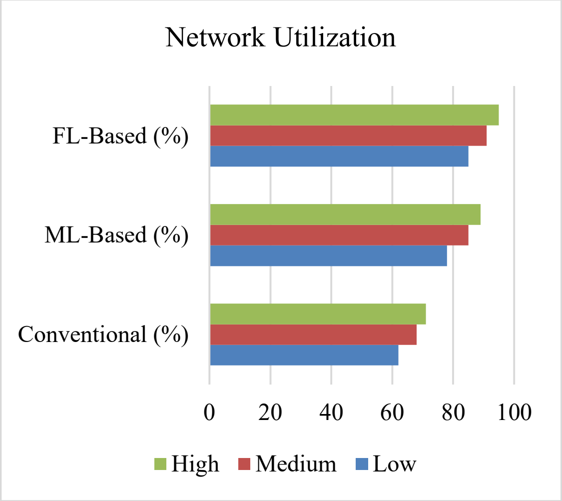

Figure 7: Graphical Representation of Network Utilization Efficiency

Table 8 shows that the proposed federated learning framework has a greater utilization efficiency in every traffic condition. The FL-based model has 85% utilization under low traffic load, which is 62% and 78% in the conventional and centralized ML model, respectively. This shows more efficient utilization of the available resources even in the cases of relatively low demand by the network.

The performance gap is even more noticeable as the load on the traffic grows. The FL-based model has a higher utilization rate of 91% compared to the conventional and ML-based models at medium load of 68% and 85% utilization respectively. In high traffic scenarios, the proposed model has the highest utilization at 95 which implies that the model is very effective in supporting the heavy network demand without much performance degradation.

The high performance of the FL-based model could be explained by the decentralized learning and the ability to be adapted in real-time. The model uses distributed traffic information to dynamically optimize resource allocation and load balancing policies, guaranteeing efficient utilization of all nodes. The federated structure allows optimization to be more local and fast as compared to centralized methods, which can have sluggish decision-making and bottlenecks in communication.

As shown in Fig. 7, in the graphical representation, it is clear that there is a steady increase in utilization efficiency using traditional approaches to centralized ML and then to the federated learning approach. These results substantiate that the suggested structure can be scaled to an impressive degree and can ensure the best performance even under different and high-traffic loads.

4.7. Communication Overhead Analysis

Wireless networks serve as an important concern in terms of communication overhead, especially in large scale distributed applications. It is the volume of information between network nodes and central servers in the process of model training and optimization. The high communication overhead may cause excessive bandwidth usage, network congestions, and latencies, which eventually reduce the overall system performance.

In this research, the communication overhead of the suggested federated learning (FL)-based system is juxtaposed with the traditional centralized machine learning methodology.

Table 9: Communication Overhead Comparison

Method	Data Transmission Requirement
Centralized ML	High
Federated Learning	Low

The findings given in Table 9 clearly demonstrate that the federated learning model significantly decreases the communication overhead in contrast to the centralized machine learning models. Large amounts of raw traffic data have to be sent continuously in a centralized ML, where distributed nodes transmit data to a central server to be processed and trained. This means it consumes a lot of bandwidth and loads the network.

Conversely, federated learning model does not require raw data transmission, as the local nodes can train models on their own. The aggregation server receives only model parameters or weight updates and this drastically reduces the amount of data sent. This reduces the cost of communication as well as increasing the scalability and efficiency of the system.

Moreover, the decrease in the communication overhead is added to the faster model updates and responds better, and the proposed framework is more appropriate to the real-time wireless network environment. One of the main features of federated learning is the capability of distributed learning with a minimum amount of data communication, which is particularly valuable in privacy-sensitive and resource-constrained networks.

4.8. Overall Performance Improvement

In order to give a summarized assessment of the suggested framework, the percentage change of all main performance metrics is generalized in Table 10. This discussion emphasizes the compounding effects of combining federated learning with smart network optimization solutions.

Table 10: Overall Performance Gain

Metric	Improvement (%)
Throughput	+41.3
Latency	-36.6
Packet Loss	-66.2
Spectral Efficiency	+61.9

The findings in Table 10 show conclusively that the proposed federated learning-based framework significantly improves all the performance measures considered. Its throughput improvement of 41.3% is a sign of better efficiency in data transmission and the reduction in latency by a massive 36.6% is a sign of better responsiveness to the network and especially to real-time applications. Additionally, the greatest improvement is seen in the packet loss that is minimized by 66.2% meaning that network reliability and stability are significantly improved. The fact that the spectral efficiency has increased by 61.9% also supports the efficient usage of limited wireless spectrum resources.

Such improvements in performance justify the efficiency of the introduced approach in overcoming the shortcomings of traditional and centralized machine learning solutions. In contrast to centralized models, which rely on the large-scale transmission of data and are prone to scalability challenges, the federated learning architecture allows training distributed models at low communication costs and with high privacy rates. The proposed system can be more adaptive to changing traffic conditions, is more scalable to distributed networks, and can be optimized in real-time in a better way through the use of localized data and collaborative learning. The steady gains in all the measures are a strong indication that the federated learning combined with network optimization strategies can be a powerful and scalable solution to the next-generation wireless communication systems.

5. CONCLUSION AND FUTURE SCOPE

This paper demonstrated a federated learning-based traffic intelligence architecture of distributed optimization of wireless network performance. The proposed solution can overcome the major drawbacks of the traditional and centralized machine learning techniques especially the problem of data privacy, scalability, and communication overhead. The framework allows decentralized model training between distributed nodes and thus performs efficient learning without the need to exchange raw data.

The combination of traffic prediction and adaptive network optimization strategies enables the system to proactively control network resources. The experimental outcomes show that all significant performance indicators, such as increased throughput, decreased latency, minimized packet loss, and improved spectral efficiency are most likely to improve. Moreover, the framework ensures high network utilization with varying loads of traffic, emphasizing its scalability and flexibility to dynamic wireless conditions.

Overall, the results validate that federated learning is a highly secure, effective, and privacy-assuring solution to the next generation of wireless communication systems, especially in 5G and IoT-based networks where distributed intelligence is required.

- Future research can explore the integration of advanced deep learning architectures, such as LSTM and transformer-based models, to further enhance the accuracy of traffic prediction and address intricate temporal relationships.
- To test the performance of the proposed framework in real-life scenarios, it can be scaled to real-time implementation in realistic wireless

systems, such as 5G, edge computing, and large-scale IoT infrastructures.

- Further research is possible on improving the security and resilience of the federated learning system, such as adding secure aggregation methods, blockchain-based systems or adversarial defenses to the federated learning system.

REFERENCES

[1] Y. Liu, J. Q. James, J. Kang, D. Niyato, and S. Zhang, “Privacy-preserving traffic flow prediction: A federated learning approach,” IEEE Internet of Things Journal, vol. 7, no. 8, pp. 7751–7763, 2020.

[2] T. Alqubaysi, A. F. A. Asmari, F. Alanazi, A. Almutairi, and A. Armghan, “Federated learning-based predictive traffic management using a contained privacy-preserving scheme for autonomous vehicles,” Sensors, vol. 25, no. 4, p. 1116, 2025.

[3] W. Ali, I. U. Din, A. Almogren, and J. J. Rodrigues, “Federated learning-based privacy-aware location prediction model for internet of vehicular things,” IEEE Transactions on Vehicular Technology, vol. 74, no. 2, pp. 1968–1978, 2024.

[4] Praveen, S. P., Kamalrudin, M., Musa, M., Harita, U., Ayyappa, Y., & Nagamani, T. (2025). A Unified AI Framework for Confidentiality Preserving Cyberattack Detection in Healthcare Cyber Physical Networks. International Journal of Innovative Technology and Interdisciplinary Sciences, 8(3), 818-841

[5] Praveen, S. P., Lalitha, S., Sarala, P., Satyanarayana, K., & Karras, D. A. (2025). Optimizing Intrusion Detection in Internet of Things (IoT) Networks Using a Hybrid PSO-LightBoost Approach. International Journal of Intelligent Engineering & Systems, 18(3).

[6] I. S. Nwokoro et al., “Federated learning with memory-based cognitive engine to optimize multi-service 5G QoS in a privacy-preserving framework,” Journal of Networking and Communication Systems, vol. 8, no. 4, pp. 1–14, 2025.

[7] Y. Qi, M. S. Hossain, J. Nie, and X. Li, “Privacy-preserving blockchain-based federated learning for traffic flow prediction,” Future Generation Computer Systems, vol. 117, pp. 328–337, 2021.

[8] Y. Qi, M. S. Hossain, J. Nie, and X. Li, “Privacy-preserving blockchain-based federated learning for traffic flow prediction,” Future Generation Computer Systems, vol. 117, pp. 328–337, 2021.

[9] H. A. Tahir, W. Alayed, and W. U. Hassan, “Privacy-preserving federated learning with adaptive model aggregation for efficient vehicle-to-vehicle (V2V) communication in intelligent transportation systems,” IEEE Access, 2025.

[10] M. Rahmati and N. Rahmati, “Privacy-preserving federated multi-sensor fusion with edge computing optimization for real-time traffic management in connected vehicle networks,” International Journal of Intelligent Transportation Systems Research, pp. 1–27, 2025.

[11] F. Gao, C. Zhang, J. Qiao, K. Li, and Y. Cao, “Communication-efficient wireless traffic prediction with federated learning,” Mathematics, vol. 12, no. 16, p. 2539, 2024.

[12] J. Wei et al., “Privacy-preserving sparse traffic flow prediction in IIoT: A three-tier federated learning framework,” IEEE Internet of Things Journal, 2025.

[13] A. Aalavanthar et al., “Multi-objective federated learning traffic prediction in vehicular network for intelligent transportation system,” PeerJ Computer Science, vol. 11, p. e2922, 2025.

[14] Y. Du and H. Sun, “Federated learning-based dynamic traffic management for IoT-enabled smart cities,” IEEE Transactions on Consumer Electronics, 2025.

[15] S. R. Jeyakumar et al., “An innovative secure and privacy-preserving federated learning-based hybrid deep learning model for intrusion detection in internet-enabled wireless sensor networks,” IEEE Transactions on Consumer Electronics, vol. 71, no. 1, pp. 273–280, 2024.

[16] Shariff, V., Paritala, C., & Ankala, K. M. (2025). Federated tree-based ensembles with SHAP explainability and integrated feature selection for secure lung cancer health analytics. Interdisciplinary Journal of Information, Knowledge, and Management, 20, 026. https://doi.org/10.28945/5613

[17] N S Koti Mani Kumar Tirumanadham et al., (2025) "Boosting Student Performance Prediction In E-Learning: A Hybrid Feature Selection And Multi-Tier Ensemble Modelling Framework With Federated Learning", Journal of Theoretical and Applied Information Technology, vol. 103, no. 5, March 2025

[18] N. S. K. M. K. Tirumanadham, T. S and G. V, "Accurate and Explainable AI in Student Performance Prediction Using E-Learning Classification," 2025 International Conference on Next Generation Information System Engineering (NGISE), Ghaziabad, Delhi (NCR), India, 2025, pp. 1-7, doi: 10.1109/NGISE64126.2025.11085384.

[19] M. Padmapriya, S. M, V. T. R. P. K. M, B. R. K, K. K. Reddy Penubaka and R. Shaik, "Energy-

Efficient Task Offloading and Scheduling in Ultra-Dense MEC for 5G Networks," 2025 International Conference on Machine Learning and Autonomous Systems (ICMLAS), Prawet, Thailand, 2025, pp. 1626-1631, doi: 10.1109/ICMLAS64557.2025.10968642.

[20] R. Shaik, S. K. Mandala, Y. K. Aluri, V. P. Kumar, P. L. Supriya and N. Gurrapu, "Wireless Energy Harvesting (WEH) and Specrtum Sharing in Cognitive Radio Networks," 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Goathgaun, Nepal, 2025, pp. 67-72, doi: 10.1109/ICMCSI64620.2025.10883498.

[21] V. Shariff, N. V. S. Pavan Kumar, N. Ashokkumar, S. K. Mandala, M. Ajmeera, N. S. K. M. Kumar Tirumanadham, and P. Chiranjeevi, "SGB-IDS: A Swarm Gradient Boosting Intrusion Detection System Using Hybrid Feature Selection for Enhanced Network Security," Journal of Theoretical and Applied Information Technology., vol. 103, no. 11, pp. 4519–4532, Jun. 2025.

[22] Praveen, S.P., Sharma, K., Parashar, D. et al. Design of an iterative method for adaptive federated intrusion detection for energy-constrained edge-centric 6G IoT cyber-physical systems. Sci Rep 15, 41387 (2025). https://doi.org/10.1038/s41598-025-25293-w

[23] Phani Praveen, S., Ali, M.H., Jarwar, M.A. et al. 6G assisted federated learning for continuous monitoring in wireless sensor network using game theory. Wireless Netw 30, 5211–5237 (2024). https://doi.org/10.1007/s11276-023-03249-0

[24] Kumar Tirumanadham, N. K. M., Phani Praveen, S., Esther Jyothi, V., Thati, B., Swamy, B. N., & Arrora Dewi, D. (2026). CrossMF: A Memory-Augmented Transformer for Fast and Generalizable Emotion Recognition. International Journal of Pattern Recognition and Artificial Intelligence, 2650007.

[25] Islam, S., Praveen, S. P., Ponnaganti, N. D., Kocharla, S., & Safie, N. (2025, November). Enhancing Network Security: Hybrid XGMB Model for Intrusion Detection with Intelligent Feature Engineering. In 2025 International Conference on Electrical Engineering and Informatics (ICEEI) (pp. 1-6). IEEE.

[26] Praveen, S. P., Panguluri, P., Sirisha, U., Dewi, D. A., Kurniawan, T. B., & Efrizoni, L. (2026). Stacked LSTM with Multi Head Attention Based Model for Intrusion Detection. Journal of Applied Data Sciences, 7(1), 475-488.

[27] Reddy, A. S., Praveen, S. P., Ramudu, G. B., Anish, A. B., Mahadev, A., & Swapna, D. (2023, January). A network monitoring model based on convolutional neural networks for unbalanced network activity. In 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) (pp. 1267-1274). IEEE.

[28] Sindhura, S., Phani Praveen, S., Madhuri, A., & Swapna, D. (2022, May). Different feature selection methods performance analysis for intrusion detection. In Smart Intelligent Computing and Applications, Volume 2: Proceedings of Fifth International Conference on Smart Computing and Informatics (SCI 2021) (pp. 523-531). Singapore: Springer Nature Singapore.

[29] S. Y. P. D. Udayakumar, "User activity analysis via network traffic using DNN and optimized federated learning based privacy preserving method in mobile wireless networks," 2023.

[30] C. Zhang, H. Zhang, S. Dang, B. Shihada, and M. S. Alouini, "Gradient compression and correlation driven federated learning for wireless traffic prediction," IEEE Transactions on Cognitive Communications and Networking, vol. 11, no. 4, pp. 2246–2258, 2024.