A Course Based Project Report on

Wi-Fi Network Traffic Prediction System using Machine Learning

Submitted to the

Department of CSE-(CyS, DS) and AI&DS

in partial fulfilment of the requirements for the completion of course
COMPUTER NETWORKS AND ETHICAL HACKING
LABORATORY (22PC2CY201)

BACHELOR OF TECHNOLOGY

IN

Department of CSE-(CyS, DS) and AI&DS

Submitted by

23071A06776 – B. AKSHITHA

23071A6777 – B. MANASWINI

23071A6778– C. SAI CHARITH

23071A6779 – CH. ROHITHA

23071A6780 – CH. KARTHIK

Under the guidance of

Mrs. G. USHA RANI

(Course Instructor)

Assistant Professor, Department of CSE-(CYS,DS) AND AI&DS
VNRVJIET

Department of CSE-(CyS, DS) and AI&DS

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING & TECHNOLOGY

An Autonomous Institute, NAAC Accredited with 'A++' Grade, NBA
Vignana Jyothi Nagar, Pragathi Nagar, Nizampet (S.O), Hyderabad – 500 090, TS, India

November 2025

VALLURUPALLI NAGESWARA RAO VIGNANA JYOTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY

An Autonomous Institute, NAAC Accredited with 'A++' Grade, NBA Accredited for CE, EEE, ME, ECE, CSE, EIE, IT B. Tech Courses, Approved by AICTE, New Delhi, Affiliated to JNTUH, Recognized as "College with Potential for Excellence" by UGC, ISO 9001:2015 Certified, QS I GUAGE Diamond Rated

Vignana Jyothi Nagar, Pragathi Nagar, Nizampet(SO), Hyderabad-500090, TS, India

Department of CSE-(CyS, DS) and AI&DS

CERTIFICATE

This is to certify that the project report entitled **"Wi-Fi Network Traffic Prediction System using Machine Learning"** is a bonafide work done under our supervision and is being submitted by **Ms. B. AKSHITHA(23071A06776), , Ms. B. MANASWINI(23071A6777), Mr. C. SAI CHARITH(23071A6778, Ms. CH. ROHITHA(23071A6779), Mr. CH. KARTHIK(23071A6780)** in partial fulfilment for the award of the degree of **Bachelor of Technology** in **CSE-(CyS, DS) and AI&DS**, of the VNRVJIET, Hyderabadduring the academic year 2025-2026.

Mrs. G. Usha Rani

Assistant Professor

Dept of CSE-(CyS, DS) and AI&DS

Dr. T. Sunil Kumar

Professor & HOD

Dept of CSE-(CyS, DS)and AI&DS

VALLURUPALLI NAGESWARA RAO VIGNANAJYOTHI INSTITUTE OF ENGINEERING & TECHNOLOGY
An Autonomous Institute, NAAC Accredited with 'A++' Grade, NBA
Vignana Jyothi Nagar, Pragathi Nagar, Nizampet (S.O), Hyderabad – 500 090, TS, India

Department of CSE-(CyS, DS) and AI&DS

DECLARATION

We declare that the course based project work entitled **"Wi-Fi Network Traffic Prediction System using Machine Learning"** submitted in the Department of **CSE-(CyS, DS) and AI&DS**, Vallurupalli Nageswara Rao Vignana Jyothi Institute of Engineering and Technology, Hyderabad, in partial fulfilment of the requirement for the award of the degree of **Bachelor of Technology in CSE-(CyS, DS) and AI&DS** is a bonafide record of our own work carried out under the supervision of **Mrs.G.Usha Rani, Assistant Professor, Department of CSE-(CyS, DS) and AI&DS , VNRVJIET.** Also, we declare that the matter embodied in this thesis has not been submitted by us in full or in any part there of for the award of any degree/diploma of any other institution or university previously.

Place: Hyderabad.

23071A06776 – B. AKSHITHA
23071A6777 – B. MANASWINI
23071A6778– C. SAI CHARITH
23071A6779 – CH. ROHITHA
23071A6780 – CH. KARTHIK

ACKNOWLEDGEMENT

We express our deep sense of gratitude to our beloved President, Sri. D. Suresh Babu, VNR Vignana Jyothi Institute of Engineering & Technology for the valuable guidance and for permitting us to carry out this project.

With immense pleasure, we record our deep sense of gratitude to our beloved Principal, Dr. C.D Naidu, for permitting us to carry out this project.

We express our deep sense of gratitude to our beloved Professor Dr.T.SUNIL KUMAR, Professor and Head, Department of CSE-(CyS, DS) and AI&DS , VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad- 500090 for the valuable guidance and suggestions, keen interest and through encouragement extended throughout the period of project work.

We take immense pleasure to express our deep sense of gratitude to our beloved Guide, Mrs. G. USHA RANI, Assistant Professor in CSE-(CyS, DS) and AI&DS, VNR Vignana Jyothi Institute of Engineering & Technology, Hyderabad, for her valuable suggestions and rare insights, for constant source of encouragement and inspiration throughout my project work.

We express our thanks to all those who contributed for the successful completion ofour project work.

23071A06776 – B. AKSHITHA

23071A6777 – B. MANASWINI

23071A6778– C. SAI CHARITH

23071A6779 – CH. ROHITHA

23071A6780 – CH. KARTHIK

INDEX

S.No	Topic	Pg.No.
1.	Abstract	6
2.	Introduction	7
3.	Methodology	8
4.	Implementation and Result	11
5.	Conclusion	13
6.	References	14

ABSTRACT

With the rapid increase in Wi-Fi enabled devices, smart gadgets, and high-bandwidth applications, modern wireless networks experience highly dynamic and unpredictable traffic patterns. Traditional rule-based network monitoring and congestion management techniques are no longer capable of accurately forecasting network behavior or responding effectively to sudden usage fluctuations. As a result, Wi-Fi networks often suffer from congestion, increased latency, reduced throughput, degraded Quality of Service (QoS), and user dissatisfaction.

To overcome these limitations, this project aims to develop an intelligent **Wi-Fi Network Traffic Prediction System using Machine Learning**. The system learns network behavior from historical traffic logs and predicts future network load, enabling proactive resource management and congestion prevention. Along with traffic forecasting, the system is designed to detect anomalies, such as sudden bandwidth spikes, unusual user behavior, or traffic patterns indicative of cyber-attacks (e.g., DDoS-like activity).

The proposed solution uses advanced machine learning models, including **Random Forest and Long Short-Term Memory (LSTM) networks**, along with statistical anomaly detection approaches, to:

- Accurately forecast future Wi-Fi traffic trends
- Identify and flag abnormal traffic behavior in near real-time
- Provide visualization support for traffic pattern monitoring and anomaly insights
- Assist network administrators in making intelligent, proactive decisions for bandwidth allocation and performance optimization

By predicting network congestion before it occurs and identifying anomalies in traffic flow, the system improves network reliability, enhances QoS, and ensures efficient utilization of network resources in dynamic Wi-Fi environments.

INTRODUCTION

In today's hyper-connected digital landscape, computer networks play a pivotal role in enabling seamless communication, data exchange, and resource sharing across devices and platforms. Among these, Wi-Fi networks have emerged as the most widely adopted form of wireless connectivity due to their flexibility, cost-effectiveness, and ease of deployment. From homes and educational campuses to corporate offices and public spaces, Wi-Fi has become the backbone of modern networking infrastructure.

However, the rapid proliferation of Wi-Fi-enabled devices—such as smartphones, laptops, smart TVs, IoT sensors, and wearables—has introduced significant challenges in managing network traffic. These devices generate highly dynamic and non-linear traffic patterns, driven by bandwidth-intensive applications like video streaming, cloud gaming, real-time conferencing, and smart automation. As a result, network administrators face increasing difficulty in maintaining consistent performance, especially during peak usage periods or in environments with fluctuating demand.

Traditional network monitoring and congestion management techniques rely heavily on rule-based systems and static thresholds. While these methods were effective in earlier, more predictable network environments, they fall short in today's complex scenarios. They lack the adaptability to respond to sudden spikes in traffic, cannot anticipate future load conditions, and often fail to detect anomalies such as unusual user behavior or potential security threats. This leads to frequent issues such as:

- **Network congestion**, resulting in slower data transmission and reduced throughput
- **Increased latency**, affecting real-time applications like VoIP and video conferencing
- **Degraded Quality of Service (QoS)**, leading to user dissatisfaction and operational inefficiencies
- **Security vulnerabilities**, as anomalous traffic patterns may go unnoticed

To address these limitations, this project proposes an intelligent Wi-Fi Network Traffic Prediction System powered by machine learning. The system is designed to learn from historical traffic data, forecast future network load, and detect anomalies in near real-time. By leveraging predictive analytics, it enables proactive resource allocation, early congestion mitigation, and enhanced security monitoring.

The solution integrates two powerful machine learning models:

- **Random Forest**, a robust ensemble learning method that serves as a baseline for traffic classification and feature importance analysis
- **Long Short-Term Memory (LSTM)** networks, a type of recurrent neural network (RNN) capable of capturing temporal dependencies in time-series data, making it ideal for forecasting complex traffic patterns

In addition to prediction and anomaly detection, the system includes a real-time visualization dashboard built using Gradio. This interface allows users to interact with the system, observe traffic trends, compare actual versus predicted values, and gain insights into feature influence through explainable AI techniques such as SHAP (Shapley Additive explanations).

METHODOLOGY

The methodology adopted in this project follows a structured pipeline that transforms raw Wi-Fi traffic data into actionable insights through machine learning. Each stage—from preprocessing to simulation—is carefully designed to ensure accuracy, robustness, and real-time applicability.

1. Data Preprocessing

Raw network traffic data often contains inconsistencies, missing entries, and noise due to device variability and logging errors. Preprocessing is a critical step that prepares this data for effective model training. It includes:

- **Handling Missing Values:** Techniques such as forward-fill, backward-fill, and interpolation are used to fill gaps in time-series data without distorting traffic patterns.
- **Normalization and Scaling:** Features like packet size, latency, and throughput are normalized using Min-Max or Standard Scaler to ensure uniformity and improve model convergence.
- **Feature Engineering:** Derived features such as traffic rate changes, session density, and rolling averages are created to enrich the dataset and improve predictive performance.
- **Time-Series Structuring:** For LSTM input, data is reshaped into sequences with fixed window sizes, preserving temporal dependencies.

2. Model Training

Two machine learning models are trained and evaluated to perform traffic prediction:

- **Random Forest:** A decision-tree-based ensemble model used for baseline predictions. It is effective for identifying feature importance and handling non-linear relationships. Its interpretability makes it suitable for initial analysis and comparison.
- **Long Short-Term Memory (LSTM):** A deep learning model tailored for time-series forecasting. LSTM networks use memory cells to retain long-term dependencies, making them ideal for capturing traffic trends and periodic fluctuations. The model architecture includes input layers, hidden LSTM cells, dropout layers for regularization, and dense output layers for traffic estimation.

Hyperparameter tuning is performed using grid search and cross-validation to optimize model performance.

3. Anomaly Detection

Anomaly detection is essential for identifying unusual traffic behavior that may indicate congestion, device overload, or security threats. The system uses:

- **Residual Analysis:** The difference between predicted and actual traffic is monitored. Significant deviations are flagged as anomalies.
- **Statistical Thresholds:** Dynamic thresholds based on standard deviation and percentile ranges are applied to detect outliers.

- **Pattern Recognition:** Sudden spikes, drops, or repetitive patterns resembling DDoS attacks are identified using time-series anomaly detection algorithms.

Anomalies are logged and visualized for further inspection and response.

4. Evaluation Metrics

To assess the accuracy and reliability of the prediction models, the following metrics are used:

- **Mean Absolute Error (MAE):** Measures the average magnitude of errors between predicted and actual values.
- **Root Mean Square Error (RMSE):** Penalizes larger errors more heavily, providing insight into prediction stability.
- **R^2 Score (Coefficient of Determination):** Indicates how well the model explains the variance in the data. A higher R^2 score reflects better model fit.

These metrics are computed for both Random Forest and LSTM models to compare performance across different traffic scenarios.

5. Explainability

Understanding model decisions is crucial for trust and transparency. The system incorporates:

- **SHAP (SHapley Additive exPlanations):** A game-theoretic approach to explain individual predictions by assigning importance scores to each feature. SHAP plots reveal which features—such as latency, packet size, or session count—most influence traffic predictions.
- **Feature Ranking:** Helps network administrators prioritize monitoring of critical parameters and refine data collection strategies.

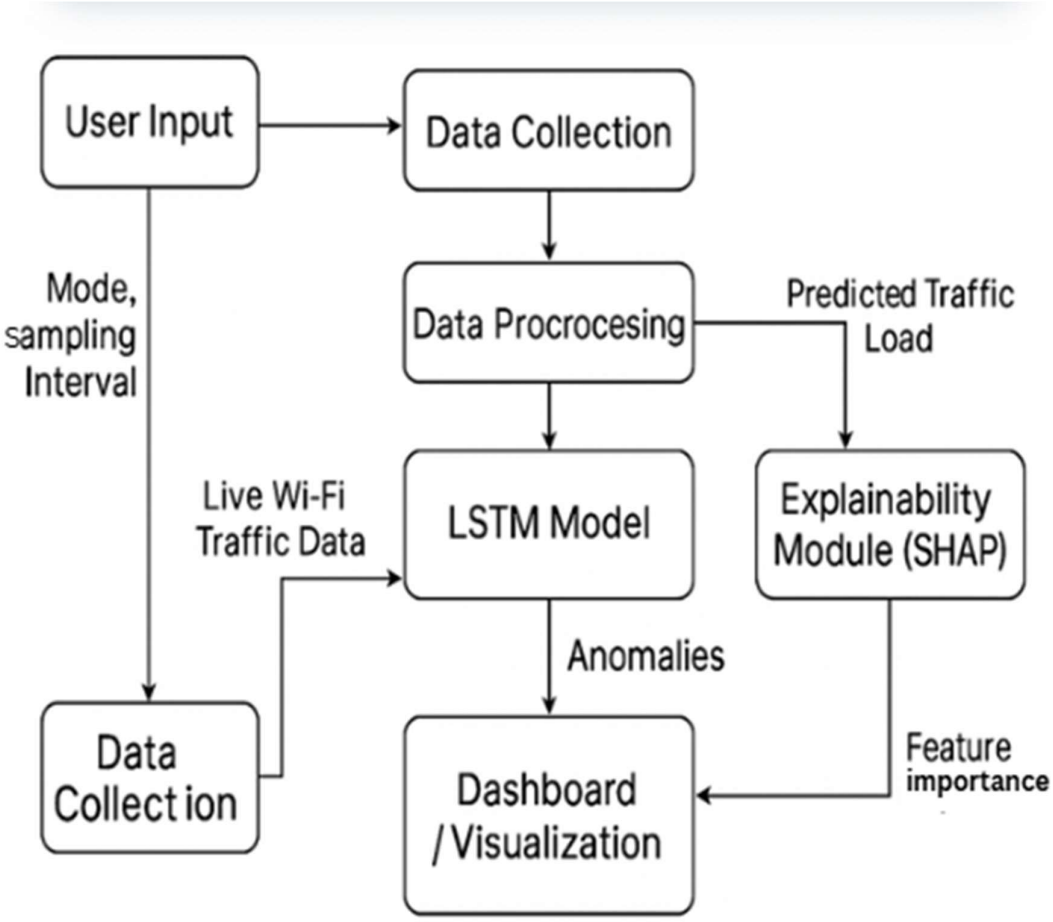
6. Simulation

To test the system under controlled conditions, synthetic data streams are generated that mimic real-time Wi-Fi traffic. This includes:

- **Traffic Spikes and Drops:** Simulated to evaluate anomaly detection sensitivity.
- **Variable Load Patterns:** Created to test model adaptability across different usage scenarios.
- **Noise Injection:** Used to assess model robustness against imperfect data.

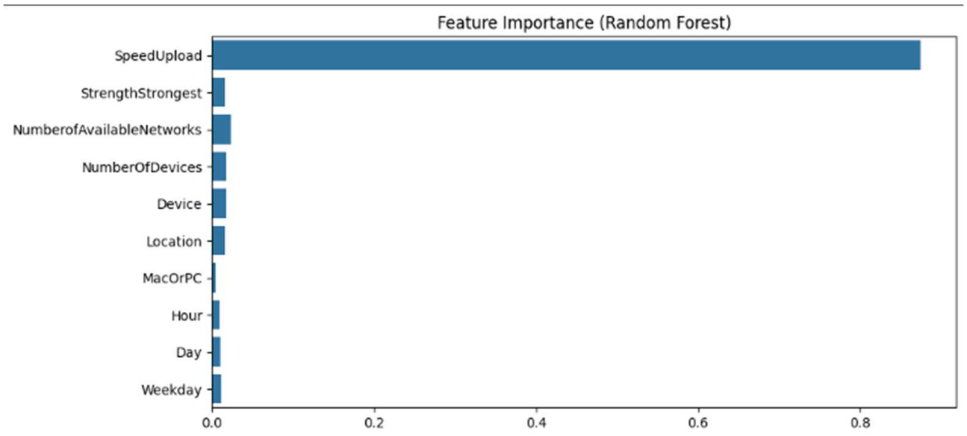
Simulation ensures the system can handle real-world variability and supports iterative testing before deployment.

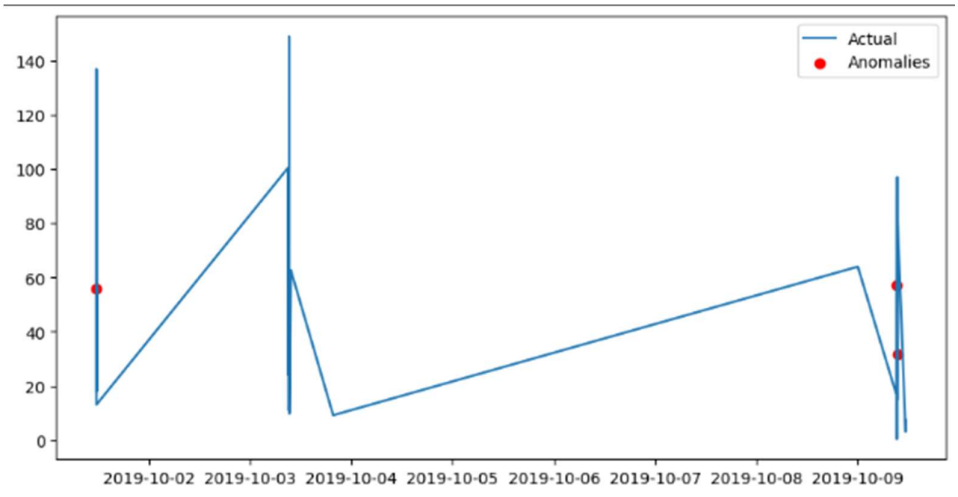
Architecture diagram:



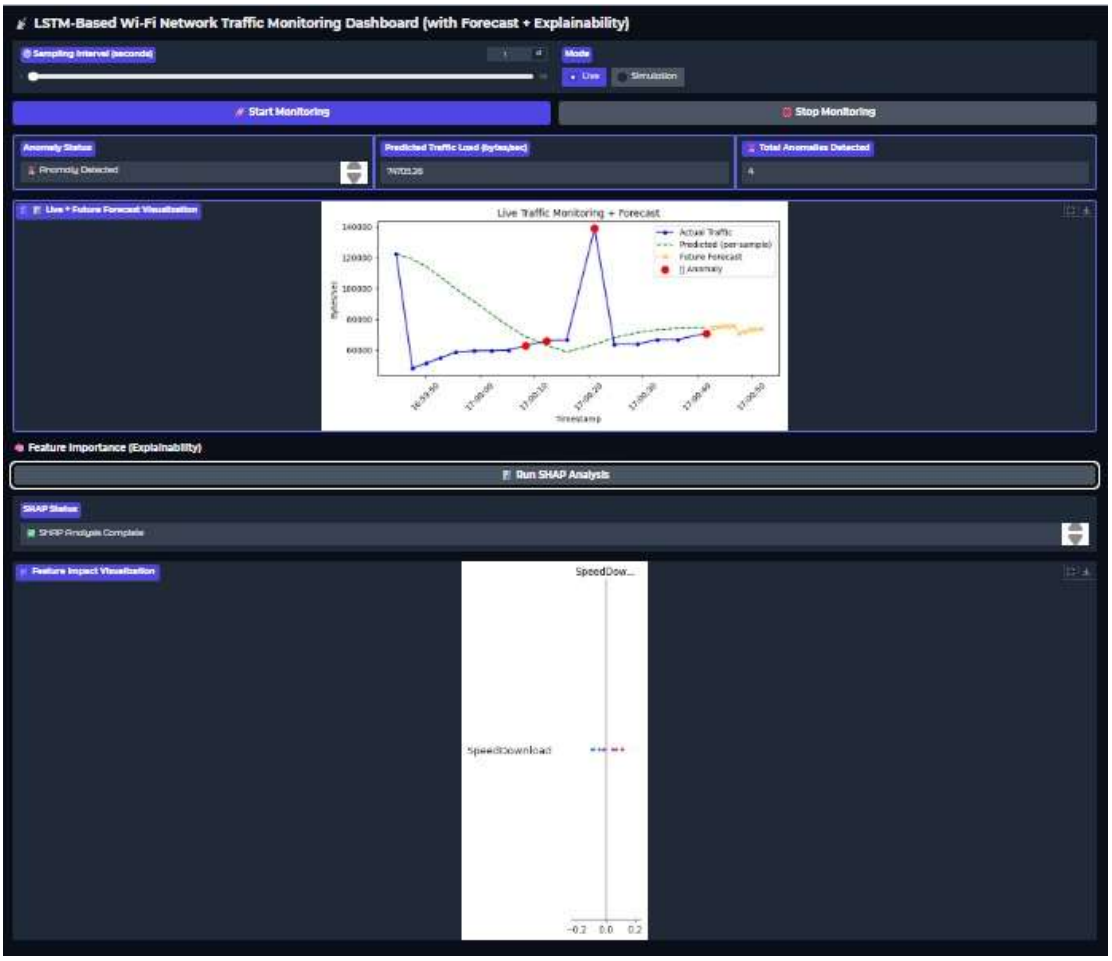
IMPLEMENTATION AND RESULTS

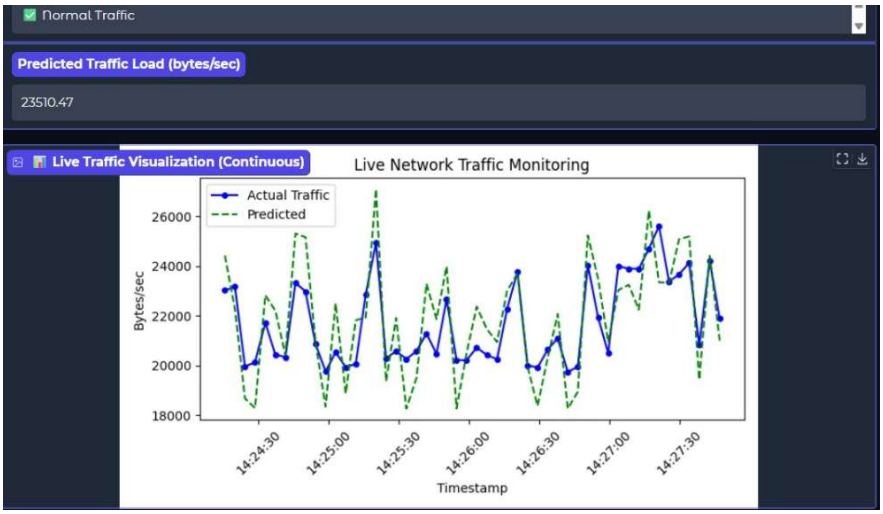
- **Tools Used:** Python, TensorFlow/Keras, Scikit-learn, Pandas, Gradio.
- **Training Results:**
  - LSTM outperformed Random Forest in capturing long-term trends.
  - Real-time monitoring enabled early detection of anomalies like DDoS-like spikes.
- **Visualization:** The dashboard provided intuitive plots for traffic trends and anomalies.
- **Feature Insights:** Key features influencing traffic included packet size, latency, and session count.





Dashboard:


LSTM-Based Wi-Fi Network Traffic Monitoring Dashboard (with Forecast + Explainability)
Start Monitoring
Stop Monitoring
Live Traffic Monitoring + Forecast
Feature Importance (Explainability)
Run SHAP Analysis


Normal Traffic
Predicted Traffic Load (bytes/sec)
23510.47
Live Traffic Visualization (Continuous)
Live Network Traffic Monitoring
Actual Traffic
Predicted
Bytes/sec
Timestamp

CONCLUSION

The implementation of the Wi-Fi Network Traffic Monitoring System with Forecast and Explainability successfully demonstrates the capability of deep learning techniques to accurately predict, analyze, and interpret dynamic network traffic behaviors in real time. Through Long Short-Term Memory (LSTM) neural networks, the system effectively captured temporal dependencies and complex nonlinear patterns within Wi-Fi traffic data, providing valuable insights for proactive network management.

Key Findings from the Implementation:

- **Accurate Forecasting:**
  The LSTM model efficiently predicted future traffic loads based on historical data, outperforming traditional statistical methods. It successfully forecasted short-term fluctuations and long-term trends, aiding in congestion avoidance and capacity planning.
- **Real-Time Monitoring:**
  The system continuously monitored live or simulated network traffic, dynamically visualizing actual versus predicted data. This enabled users to observe performance changes and take corrective actions before bottlenecks occurred.
- **Anomaly Detection:**
  By comparing predicted and actual traffic, the system identified anomalies such as sudden spikes or drops in throughput—often early indicators of congestion, device overload, or security threats (e.g., DDOS attacks).
- **Explainability through Feature Importance:**
  The integration of explainable AI (using SHAP analysis) provided transparency into model decisions, highlighting which features—such as download speed, signal strength, or number of connected devices—most influenced the predictions.
- **Scalability and Adaptability:**
  The architecture can easily be extended to multiple network environments, from small Wi-Fi setups to enterprise-scale infrastructures, supporting both offline forecasting and real-time dynamic adaptation.

This project validates that LSTM-based prediction models can serve as intelligent, proactive tools for network traffic management. They not only enhance the understanding of traffic dynamics but also enable predictive optimization—making Wi-Fi networks more reliable, efficient, and adaptive.

Future Enhancements:
Further improvements can focus on integrating reinforcement learning for adaptive control, optimizing edge deployment for faster real-time analytics, and combining multi-source data (IOT, routers, cloud logs) for even more robust predictions and anomaly detection.

Ultimately, this system marks a step toward self-aware, explainable, and data-driven network management, bridging the gap between traditional monitoring tools and next-generation intelligent network infrastructure.

REFERENCES

1. Kurose, J.F., & Ross, K.W. *Computer Networking: A Top-Down Approach*, Pearson.
2. Cisco Annual Internet Report, 2023.
3. "Machine Learning-Based Network Traffic Prediction", IEEE, 2021.
4. "A Deep Learning Framework for Wi-Fi Traffic Forecasting", ACM, 2022.
5. "Random Forest for Network Traffic Prediction", Springer, 2020.
6. "ML-Based Anomaly Detection in SDN Networks", Elsevier, 2022–2023.
7. SHAP Documentation – Explainable AI for Feature Importance.