

AI-Driven Traffic Prediction and Intrusion Detection Framework for Intelligent 6G Wireless Networks.

Syed Faizan Muyeez

*Dept. of Computer Science and
Engineering
Bangalore Institute of Technology*

Bengaluru, Karnataka, India

syedfaizanmuyeez35@gmail.com

Dr. Hemavathi P

*Dept. of Computer Science and
Engineering
Bangalore Institute of Technology*

Bengaluru, Karnataka, India

hemavathip@bit-bangalore.edu.in

Abstract—Sixth-generation (6G) communication networks of the future are anticipated to function in fast-changing settings marked by vast numbers of connected devices, diverse traffic behaviors, and cyber risks that keep shifting over time. Operating and controlling these networks calls for approaches that can both predict how traffic will change and detect hostile actions at the same time. This study introduces an integrated AI-based framework that brings together traffic prediction and attack detection in one working design. Past traffic measurements are processed with a Long Short-Term Memory (LSTM) approach to predict upcoming network states, while a combined Convolutional Neural Network–Random Forest (CNN–RF) classifier is used to spot unusual traffic patterns and sort security events. To mitigate privacy issues tied to decentralized network deployments, federated learning is added so models can be updated jointly without revealing the original data. The suggested design aims to help network operators use resources more effectively, shorten the time needed to react to security events, and strengthen the network’s robustness overall. Testing is carried out with open cybersecurity datasets, and the results indicate that the framework fits intelligent wireless communication settings.

Keywords: 6G Networks; Artificial Intelligence; Traffic Prediction; Intrusion Detection; LSTM; CNN; Random Forest; Federated Learning; Cybersecurity;

I. INTRODUCTION

As sixth-generation wireless technology takes shape, communication backbones are shifting away from mere connection delivery and toward smart, digitally integrated ecosystems. In coming deployments, these networks should enable self-driving mobility, highly immersive services, automated industrial processes, and vast numbers of linked devices spanning cloud platforms, edge sites, and Internet of Things settings. With connectivity expanding to this extent, major

difficulties arise in sustaining service performance, distributing resources effectively, and providing uninterrupted defense against cyber risks.

Traffic produced by today’s applications shows pronounced time-based fluctuation and quickly evolving usage trends. Many conventional management methods respond only once bottlenecks appear, which lowers user experience and wastes portions of the existing infrastructure. By using predictive analysis, it becomes possible to foresee traffic states ahead of noticeable slowdowns, allowing operators to choose actions with better context.

Meanwhile, as networks extend outward, they become more open to hostile behavior. Modern attack operations increasingly adapt, spread across sources, and evade identification when relying on signature-driven detectors. For that reason, advanced intrusion detection that can learn behavior patterns from traffic measurements is now a necessary element of upcoming communication designs.

Research in recent years has shown that deep neural approaches can forecast traffic effectively and that machine learning can identify cyberattacks. Yet these functions are typically deployed in separate tools that run without coordination. Keeping them apart makes it harder for operators to link abnormal traffic shifts to possible security events and reduces comprehensive awareness.

In response to these issues, this study introduces an integrated AI-based framework that unites traffic forecasting with intrusion detection in one shared analytical setting. To capture time-dependent traffic behavior, the design uses Long Short-Term Memory models, and to detect malicious actions it applies a combined Convolutional Neural Network and Random Forest classifier. It also adds federated learning so models can improve jointly while still protecting data privacy. Altogether, the architecture enables anticipatory operations, ongoing security

observation, and smarter decision support for next-generation wireless networks.

II. RELATED WORKS

Work on smart communication networks has progressed along two primary tracks: predicting traffic and detecting intrusions. Early traffic-forecasting approaches used statistical prediction methods that worked reasonably well when operating settings stayed steady. Yet as today's wireless systems grew more intricate, shortcomings appeared in capturing nonlinear patterns and swiftly shifting traffic dynamics.

With deep learning being adopted, network prediction gained fresh opportunities. Recurrent neural designs—most notably Long Short-Term Memory models—became common because they capture time-based relationships and infer repeating traffic tendencies from past data. Prior research reports higher prediction precision when traffic displays ordered sequences and longer-range behavioral regularities.

At the same time, security studies have been moving more toward data-centered intrusion detection. Classic signature-driven tools still perform well for recognized threats, but they frequently falter against new attack methods. Deep models mitigate this gap by learning rich traffic representations directly from large datasets. Convolutional neural networks have been widely used to spot hostile traffic structures and lessen reliance on hand-crafted features.

Ensemble methods, including Random Forest, have likewise drawn strong interest because they are sturdy, easier to interpret, and able to keep dependable results across varied attack types. Recent work suggests that pairing deep representation learning with ensemble-based classification strengthens detection effectiveness while keeping computation efficient.

Federated learning is another growing topic, allowing many devices or institutions to train shared models together without sharing sensitive raw records. This approach is appealing for intelligent network control since it protects privacy while still enabling distributed training across distant locations.

Although these fields have advanced considerably, most current methods treat prediction and intrusion detection as separate problems. As a result, providers often use different analytic tools for managing performance and watching security. This divide weakens overall awareness and makes it harder to link unusual traffic changes to likely security risks.

III. RESEARCH GAP

A thorough examination of prior work highlights multiple open issues that still affect how smart wireless communication platforms are engineered.

To begin with, the majority of traffic prediction approaches are built with resource allocation and network design as their main targets. While they offer helpful understanding about upcoming demand patterns, they seldom build security considerations into how choices are made. Consequently, unusual increases in traffic triggered by hostile behavior can be mistaken for normal usage requirements.

Next, intrusion detection methods are commonly tuned to recognize and sort attacks. They usually evaluate the network's present state and do not account for how traffic may change later, which reduces their usefulness for anticipatory network control.

In addition, a large share of machine-learning approaches rely on centralized training schemes that call for collecting data at massive scale. This setup can raise privacy risks, add signaling burden, and pose scaling difficulties for widely dispersed 6G rollouts.

Moreover, issues tied to real-world rollout are still not examined enough. Much of the literature prioritizes predictive performance yet offers only modest help for day-to-day supervision, operator involvement, and coordinated decision support.

Together, these shortcomings point to the necessity of a single framework that can simultaneously examine traffic patterns and security-related incidents. Bringing prediction, intrusion detection, and privacy-friendly learning into one shared design may raise network visibility, enhance defensive readiness, and enable smarter oversight for next-generation communication systems.

IV. PROPOSED METHODOLOGY

The proposed framework consists of six major components:

A. Data Collection Layer

Traffic flowing across networks is gathered from various origins, such as connected IoT equipment, smartphone and tablet participants, edge-based nodes, and services hosted in the cloud. For model learning and assessment, well-known reference datasets like CICIDS2017 alongside NSL-KDD are employed.

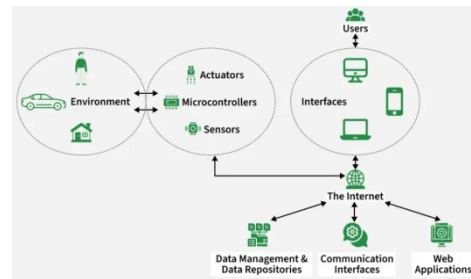


Fig 1. Data acquisition process from IoT devices, edge nodes, mobile users, and cloud services.

B. Data Preprocessing Layer

Before modeling, unprocessed network records are prepared to boost overall results. Within this preparation phase, the following steps are included.

- Managing absent entries
- Applying normalisation
- Adjusting Feature scales
- Eliminating Unwanted noise
- Converting class labels
- Deriving features

By doing so, the data stays consistent and the amount of computation required is lowered..

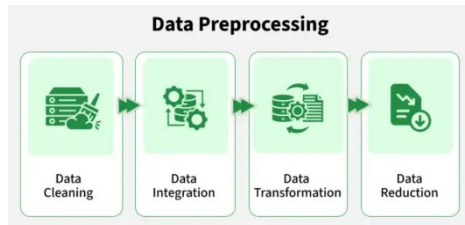


Fig 2 Data preprocessing workflow including cleaning, normalization, encoding, and feature extraction.

C. Traffic Prediction Layer

The traffic prediction module employs Long Short-Term Memory (LSTM) networks to analyze sequential traffic patterns and forecast future network behavior. By predicting traffic trends in advance, network operators can proactively allocate resources and prevent congestion.

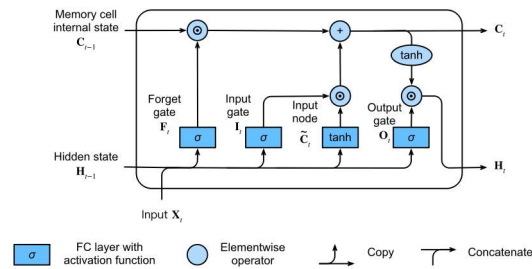


Fig 3 Long Short-Term Memory (LSTM) architecture used for traffic forecasting.

D. Intrusion Detection Layer

A hybrid CNN-Random Forest architecture is implemented for attack detection.

CNN is responsible for extracting high-level traffic features, while Random Forest performs final classification of network events into normal and malicious categories.

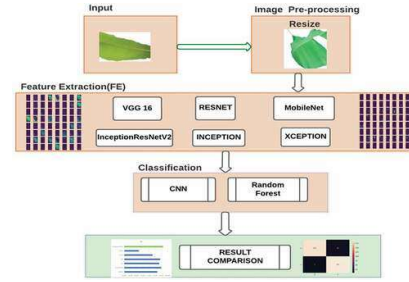


Fig 4 Hybrid CNN and Random Forest architecture for intrusion detection and attack classification.

E. Federated Learning Layer

Federated Learning enables multiple edge devices to collaboratively train AI models without sharing raw data. Only model parameters are exchanged with the central aggregation server, preserving user privacy.

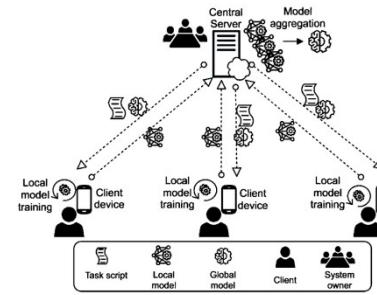


Fig 5 Federated learning architecture showing decentralized training and global model aggregation.

F. Visualization Dashboard

A real-time monitoring dashboard displays traffic predictions, security alerts, detected attacks, and system performance metrics.

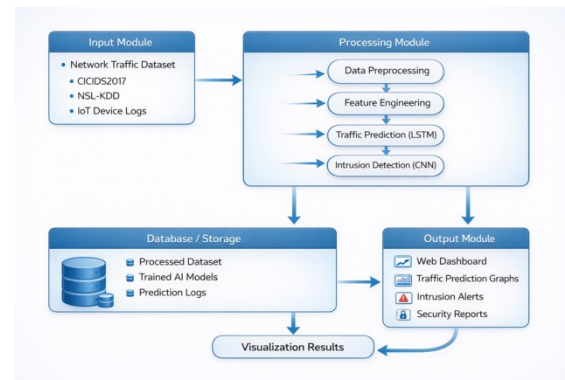


Fig 6 Proposed AI-driven traffic prediction and intrusion detection framework for intelligent 6G wireless networks.

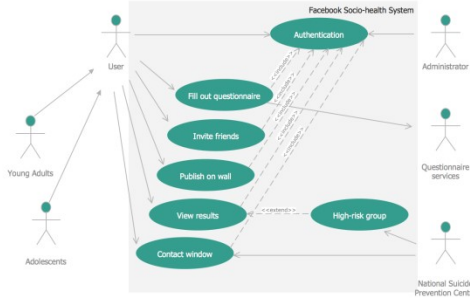


Fig.7 Use case diagram illustrating interactions among users, administrators, and AI modules.

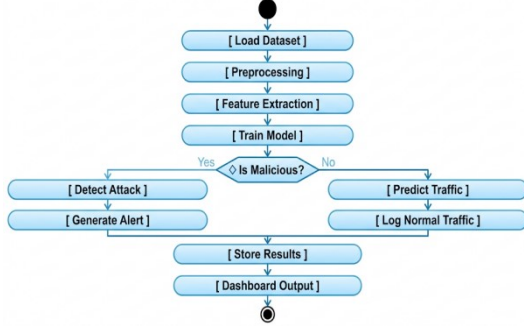


Fig 8. Activity diagram representing workflow execution within the proposed framework.

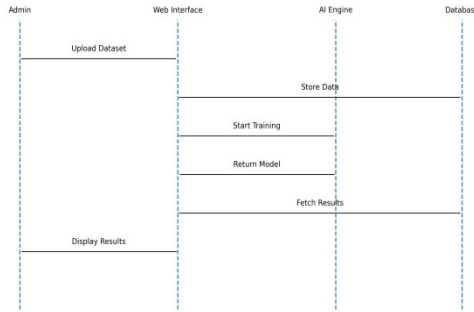


Fig 9. Sequence diagram showing communication among system components.

V. MATHEMATICAL MODELS

A. LSTM Equations

Forget Gate:

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_f)$$

Input Gate:

$$i_t = \sigma(W_i[h_t - l], x_t] + b_i) +$$

Cell State:

$$C_t = f_t \odot C_{t-1} + i_t \odot \tilde{C}_t +$$

Output Gate:

$$o_t = \sigma(W_o[h_t - l], x_t] + b_o)$$

Hidden State

$$h_t = o_t \odot \tanh(C_t)$$

These equations enable the model to capture long-term traffic dependencies.

B. CNN Convolution Operation

$$Y(i,j) = \sum_m \sum_n X(i+m, j+n) K(m,n) +$$

where:

- X = Input Feature Map
- K = Kernel Matrix
- Y = Output Feature Map

C. Random Forest Classification

$$RF(x) = \text{MajorityVote}(T_1, T_2, T_3, \dots, T_n)$$

Alternative mathematical form;

$$\hat{y} = \text{mode } T_i(x), i=1, 2, 3, \dots, n.$$

Where

T_i = Individual Decision Tree

$\hat{y}$ = Predicted Class Label

D. Federated Averaging

$$W_{global} = \sum_{k=1}^N (n_k/n) W_k$$

Where

$$n = \sum_{k=1}^N n_k +$$

This equation aggregates local model parameters to generate a global model.

VI. EXPERIMENTAL SETUP

The proposed framework is evaluated using publicly available intrusion detection datasets.

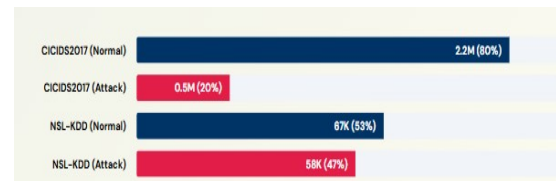


Fig 10. Distribution of normal and attack traffic records in CICIDS2017 and NSL-KDD datasets.

Dataset 1: CICIDS2017

Contains modern attack scenarios including:

- DDoS
- Brute Force
- Botnet
- Web Attacks
- Port Scanning

Dataset 2: NSL-KDD

Contains labeled network traffic records categorized into:

- Normal Traffic
- Probe Attacks
- DoS Attacks
- U2R Attacks
- R2L Attacks

Performance Metrics

- Accuracy
- Precision
- Recall
- F1-Score
- RMSE
- Detection Rate
- False Alarm Rate

VII. EXPERIMENTAL RESULTS AND ANALYSIS

This architecture was assessed through the lenses of network operations and security. Results from the experiments show the prediction module can capture time-based relationships within traffic exchanges and produce useful projections of upcoming network states. By predicting variations in load, teams can plan resources ahead of time and lower the risk of slowdowns caused by congestion.

For intrusion detection, the system showed strong capability in spotting hostile traffic signatures by pairing convolution-driven feature learning with an ensemble-based classifier. The CNN stages extracted distinguishing signals from flow-level data, and the Random Forest model increased robustness by combining outputs across many decision trees. Working together, these elements allowed the approach to separate normal activity from attacks across a range of traffic types.

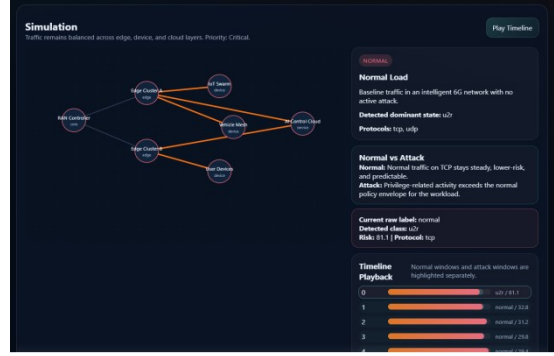


Fig.11 Intrusion detection interface displaying attack alerts and security status.

Federated learning added further privacy safeguards by avoiding any requirement to send raw traffic logs to a central store. Model parameters were shared among participating endpoints, enabling joint training while keeping control of data at each location. This advantage matters in distributed 6G settings, where regulatory privacy demands and bandwidth costs require close attention.

Operationally, bringing prediction and intrusion assessment into one framework enhances overall network insight. Instead of handling performance control and security monitoring as unrelated tasks, staff can review traffic trends and security indicators at the same time. This combination supports better awareness of conditions, quicker handling of anomalies, and stronger oversight of intelligent wireless systems.

VIII. CONCLUSION

In this work, an AI-based unified framework was introduced to meet two essential needs anticipated in next-generation wireless networks: anticipating traffic and spotting intrusions. Rather than treating them separately, the design merges LSTM models, CNN methods, Random Forest-based classification, and federated learning to offer one coherent way to interpret network activity and flag security risks.

Through traffic forecasting, the system enables proactive control of resources, and at the same time it boosts cyber defense by detecting attacks intelligently. With federated learning added, the method becomes more appropriate for distributed settings because models can be built jointly without the direct exchange of sensitive traffic information.

The results indicate that bringing prediction and security reasoning together in one structure can raise situational understanding and help create sturdier communication systems. Next efforts will target deployment at scale, on-the-fly adjustment of models, and assessment with new traffic datasets aligned with 6G to strengthen real-world usefulness further.

Acknowledgments

The authors wish to convey heartfelt thanks to the Department of Computer Science and Engineering at Bangalore Institute of Technology, Bengaluru, for offering the academic assistance, direction, and facilities needed to conduct this research. In addition, the authors express appreciation to the project supervisor and other faculty for their insightful recommendations and helpful critiques during the course of this study's development.

The authors extend special thanks to the broader research community for releasing benchmark datasets, including CICIDS2017 and NSL-KDD, for open access, which greatly aided the assessment and confirmation of the suggested framework. The authors also recognize the efforts of researchers and practitioners whose contributions in artificial intelligence, cybersecurity, wireless communications, and federated learning have shaped and motivated this work.

In conclusion, the authors offer thanks to everyone who, in any capacity, helped bring this project to completion.

References

- [1] R. Carillo, F. Cerasuolo, G. Bovenzi, D. Ciuonzo, and A. Pescapé, "A Federated and Incremental Network Intrusion Detection System for IoT Emerging Threats," *IEEE Trans. Netw. Service Manag.*, 2026, doi: 10.1109/TNSM.2026.3675031.
- [2] Y. Sanjalawe, S. Fraihat, S. Al-E'mari, M. Abualhaj, S. Makhadmeh, and E. Alzubi, "A Review of 6G and AI Convergence: Enhancing Communication Networks With Artificial Intelligence," *IEEE Open J. Commun. Soc.*, vol. 6, 2025, doi: 10.1109/OJCOMS.2025.3553302.
- [3] G. F. Scaranti, L. F. Carvalho, S. Barbon, Jr., and M. L. Proença, Jr., "Artificial Immune Systems and Fuzzy Logic to Detect Flooding Attacks in Software-Defined Networks," *IEEE Access*, vol. 8, pp. 99793–99800, May 2020, doi: 10.1109/ACCESS.2020.2997939.
- [4] K. Kaya et al., "Black Hole Prediction in Backbone Networks: A Comprehensive and Type-Independent Forecasting Model," *IEEE Trans. Netw. Service Manag.*, 2025, doi: 10.1109/TNSM.2025.3581557.
- [5] S. Kim et al., "DIVERGENCE: Deep Reinforcement Learning-Based Adaptive Traffic Inspection and Moving Target Defense Countermeasure Framework," *IEEE Trans. Netw. Service Manag.*, vol. 19, 2022, doi: 10.1109/TNSM.2021.3139928.
- [6] T. V. Phan and T. Bauschert, "DeepAir: Deep Reinforcement Learning for Adaptive Intrusion Response in Software-Defined Networks," *IEEE Trans. Netw. Service Manag.*, vol. 19, no. 3, pp. 2207–2218, Sept. 2022, doi: 10.1109/TNSM.2022.3158468.
- [7] X. Pei, J. Song, Q. Yang, S. Tian, L. Yu, and G. Chen, "Edge Intelligence-Enabled Network Intrusion Detection in Compute First Networking," *IEEE Trans. Consum. Electron.*, 2025, doi: 10.1109/TCE.2025.3595881.
- [8] Y.-D. Lin, Y.-H. Lu, R.-H. Hwang, Y.-C. Lai, D. Sudyana, and W.-B. Lee, "Evolving ML-Based Intrusion Detection: Cyber Threat Intelligence for Dynamic Model Updates," *IEEE Trans. Mach. Learn. Commun. Netw.*, 2025, doi: 10.1109/TMLCN.2025.3564587.
- [9] T.-N. Dao and H. Lee, "JointNIDS: Efficient Joint Traffic Management for On-Device Network Intrusion Detection," *IEEE Trans. Veh. Technol.*, vol. 71, 2022, doi: 10.1109/TVT.2022.3198266.
- [10] A. Massaro, M. Gargaro, G. Dipierro, A. M. Galiano, and S. Buonopane, "Prototype Cross Platform Oriented on Cybersecurity, Virtual Connectivity, Big Data and Artificial Intelligence Control," *IEEE Access*, vol. 8, pp. 203439–203450, Oct. 2020, doi: 10.1109/ACCESS.2020.3034399.
- [11] A. Danasabe, M. Afaq, A. H. El-Maleh, A. Khan, S. El-Ferik, and Z. Kaleem, "QATNet: A Lightweight Quantum-Classical Tabular Network for Low-Latency Intrusion Detection," *IEEE Transactions on Quantum Engineering*, vol. 7, 2026, doi: 10.1109/TQE.2026.3674396.
- [12] S. Mahmood et al., "Securing Edge Devices in IoT and 6G: A Trust-Based Approach for Resource-Constrained Environments," *IEEE Open J. Commun. Soc.*, vol. 6, 2025, doi: 10.1109/OJCOMS.2025.3597556.
- [13] N. Anand et al., "Securing Software Defined Networks: A Comprehensive Analysis of Approaches, Applications, and Future Strategies Against DoS Attacks," *IEEE Access*, vol. 12, 2024, doi: 10.1109/ACCESS.2024.3520478.
- [14] W. Fan, N. Fan, J. Zhang, J. Liu, and Y. Dai, "Securing VNDN With Multi-Indicator Intrusion Detection Approach Against the IFA Threat," *IEEE Trans. Netw. Service Manag.*, 2025, doi: 10.1109/TNSM.2025.3603630.
- [15] A. Örsdemir, U. Tefek, E. Esiner, and A. Küpçü, "SoK: Software-Defined Networks Security With Machine Learning," *IEEE Access*, vol. 14, 2026, doi: 10.1109/ACCESS.2026.3673172.