AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
E-ISSN:3069-0102
VOL.6, NO. 2 (2026)

Data-Driven Framework for IT and Mobile Network Attack Detection

Dr K. BHARGAVI[1], A. GANESH BABU[2]

1Professor, Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences
Anantapur – 515721

2PG Scholar, Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences
Anantapur- 515721

Abstract: The rapid proliferation of Internet of Things (IoT) devices and mobile communication networks has increased the vulnerability of interconnected systems to various cyberattacks, including Distributed Denial of Service (DDoS), malware, spoofing, phishing, and unauthorized access. Traditional security mechanisms often fail to detect sophisticated and evolving threats in real time. This paper presents an intelligent attack detection system for IoT and mobile networks using machine learning techniques. The proposed framework performs data pre-processing, feature extraction, and classification to distinguish normal network behaviour from malicious activities. Supervised learning algorithms are employed to identify attack patterns with high accuracy while minimizing false-positive rates. The system continuously monitors network traffic and generates real-time alerts upon detecting suspicious activities. Experimental results demonstrate significant improvements in detection accuracy, precision, recall, and response time compared with conventional security approaches. The proposed model effectively detects multiple categories of network attacks and enhances the overall security and reliability of IoT and mobile communication environments. The findings indicate that the system improves network resilience, protects sensitive information, and supports secure communication among interconnected devices. Consequently, the proposed framework provides a scalable and efficient cybersecurity solution for next-generation IoT ecosystems and mobile network infrastructures.

Keywords— Internet of Things (IoT), Mobile Networks, Cybersecurity, Attack Detection, Machine Learning, Intrusion Detection System (IDS), Network Security, Anomaly Detection.

1.Introduction

The rapid growth of Internet of Things (IoT) devices and mobile communication networks has enabled seamless connectivity and data exchange across various applications, including smart homes, healthcare, transportation, industrial automation, and smart cities. The widespread adoption of IoT technologies and advanced mobile networks such as 4G and 5G has significantly improved communication efficiency and service delivery. However, the increasing number of interconnected devices has also expanded the attack surface, making these environments vulnerable to numerous cybersecurity threats.

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026

IoT and mobile networks are frequently targeted by attacks such as Distributed Denial of Service (DDoS), malware, phishing, spoofing, botnets, man-in-the-middle attacks, and unauthorized access. Traditional security mechanisms, including firewalls and signature-based intrusion detection systems, often struggle to identify sophisticated and evolving attack patterns. As cyber threats continue to become more complex, there is a growing need for intelligent and adaptive security solutions capable of detecting both known and unknown attacks in real time.

This paper proposes an intelligent attack detection system for IoT and mobile networks using machine learning techniques. The framework collects and analyzes network traffic data, performs and feature extraction, and applies classification algorithms to identify malicious activities accurately. By providing real-time monitoring and alert generation, the proposed system enhances network security, reduces false-positive rates, and improves the reliability and resilience of IoT and mobile communication infrastructures against emerging cyber threats.

2.Literature Survey

Recent studies have demonstrated that machine learning and deep learning techniques can effectively detect IoT and mobile network attacks with high accuracy and reduced false-positive rates. These intelligent approaches enhance network security by identifying both known and emerging cyber threats in real time.

[1] Yogendra Kumar et al : This study reviewed intrusion detection systems for wireless and mobile networks, covering signature-based, anomaly-based, and hybrid detection approaches. The authors found that hybrid IDS techniques provide better detection performance and security. Machine learning methods were shown to improve attack detection accuracy and support real-time monitoring. The study also highlighted challenges related to mobility, energy efficiency, and evolving cyber threats.

[2] Brunel Rolack Kikissagbe et al. : This review analyzed machine learning-based intrusion detection techniques for IoT environments. The authors reported that ensemble learning algorithms achieve high detection accuracy and outperform traditional methods. The study examined various IoT datasets, evaluation metrics, and deployment challenges. It also identified explainable AI and federated learning as promising directions for future IoT security research.

3.Proposed system

The proposed system utilizes the XGBoost machine learning algorithm to detect cyberattacks in IoT and mobile networks. Network traffic data is collected and pre-processed by removing missing values, eliminating duplicates, and normalizing features. Important network attributes are extracted and used to train the XG Boost model for classifying normal and malicious activities. The system can effectively identify attacks such as DoS, DDoS, spoofing, intrusion, and unauthorized access. XG Boost provides high detection accuracy, fast processing speed, and strong scalability for large-scale environments. Experimental results demonstrate improved performance compared to traditional machine learning methods, enhancing the overall security and reliability of IoT and mobile networks.

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026

4.System architecture

The architecture consists of several interconnected modules designed to monitor and analyse network traffic. Initially, network data is collected from IT and mobile communication environments through packet capture and traffic monitoring mechanisms. The collected data undergoes pre-processing, including data cleaning, normalization, and feature extraction, to improve data quality.

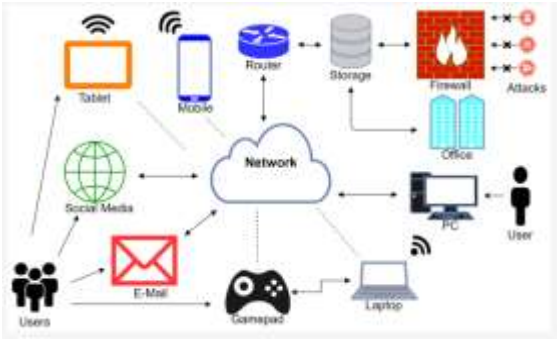

Fig 1: System Architecture

Relevant features are then selected and fed into the machine learning classifier for attack detection and classification. The model identifies various cyber threats such as DoS, DDoS, spoofing, intrusion, and unauthorized access attempts. Finally, the system generates alerts and visual reports, enabling network administrators to take timely actions and enhance overall network security.

5.Methodology

The proposed methodology employs the XG Boost machine learning algorithm to detect cyberattacks in IoT and mobile networks by analysing network traffic data. The collected data undergoes pre-processing, feature extraction, and feature selection to improve classification performance. XG Boost is trained to distinguish between normal and malicious activities, enabling the detection of attacks such as DoS, DDoS, spoofing, and intrusion attempts. The system provides accurate, scalable, and real-time attack detection, enhancing the security and reliability of IoT and mobile network infrastructures.

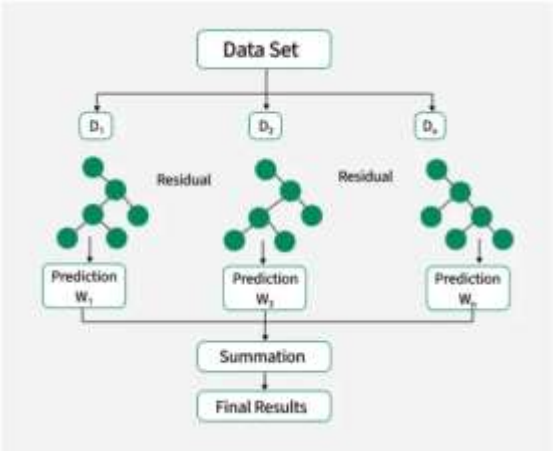

Fig 2: XG Boost Architecture

The XG Boost model is trained using pre-processed network traffic data to classify activities as normal or malicious. It builds multiple decision trees iteratively, where each tree corrects the errors of the previous one. During prediction, the model analyses network features and combines the outputs of all trees to generate the final classification result. This process improves detection accuracy, reduces overfitting, and effectively identifies complex cyberattacks.

6.Design and Construction

The proposed attack detection system is designed to continuously monitor and analyse network traffic generated by IoT devices and mobile networks. It incorporates data pre-processing, feature extraction, and the XG Boost classification model to identify malicious activities with high accuracy. The system processes network traffic in real time and classifies it as normal or attack-related based on learned behavioural patterns. This architecture ensures efficient threat detection, improved network security, and

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026

reliable communication in dynamic network environments.

i) Data Collection: This module gathers network traffic data from IoT devices, mobile networks, and IT infrastructures. The collected dataset contains both normal and attack traffic for model training and testing.

ii) Data Pre-processing: The collected data is cleaned by removing missing values, duplicates, and inconsistencies. Normalization and encoding techniques are applied to prepare the data for machine learning analysis.

iii) Feature Extraction and Selection: Important network features such as packet size, protocol type, and connection duration are extracted from the dataset. Feature selection removes irrelevant attributes to improve model accuracy and efficiency.

iv) Model Training: The selected features are used to train the XG Boost classifier to learn patterns of normal and malicious traffic. Multiple decision trees are built to improve prediction accuracy and reduce errors.

v) Attack Detection and Classification: The trained XG Boost model analyses incoming network traffic and classifies it as normal or malicious. It can detect various attacks such as DoS, DDoS, spoofing, intrusion, and unauthorized access attempts.

Vi) Performance Evaluation and Alert Generation: The system evaluates performance using metrics such as accuracy, precision, recall, and F1-score. When an attack is detected, real-time alerts are generated to notify network administrators for immediate action.

The system achieves high attack detection accuracy and provides efficient real-time threat detection, enhancing the security of IoT and mobile communication networks.

7. Results and Discussion

Experimental results show that the XG Boost classifier achieved high accuracy in detecting various network attacks, including DoS, DDoS, spoofing, and intrusion attempts, with excellent precision and recall. The model outperformed traditional machine learning methods by providing faster execution, improved classification performance, and reliable real-time attack detection.

Fig 3: Deployment of The Project

The fig 3 is deployed and executed within the Py Charm development environment, where the virtual environment is activated and the application files are organized in a structured directory hierarchy. The terminal confirms successful navigation to the Web App module, indicating that the system is ready for application execution and testing.

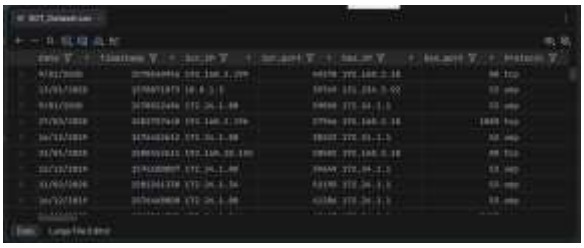

Fig 4: Dataset

The IIoT Dataset contains the Industrial Internet of Things (IIoT) network traffic data used for training and evaluating the proposed attack detection model.

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026

Fig 5: Home Page

The fig 5 Home Page of the IIOT Detection System provides a dashboard for monitoring attack detection performance. It displays key details such as the best model, dataset, user information, and algorithm statistics.

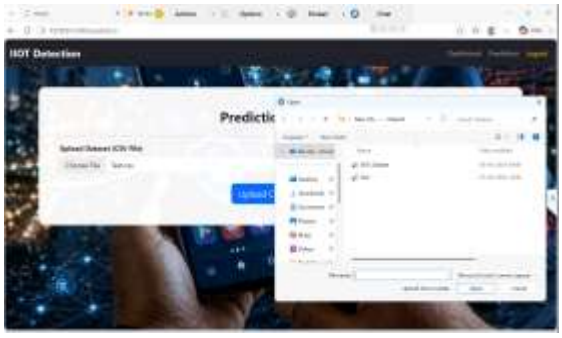

Fig 6: Upload Dataset

The fig 6 Upload Dataset page allows users to import IIoT network traffic data into the system for pre-processing, training, and attack detection analysis.

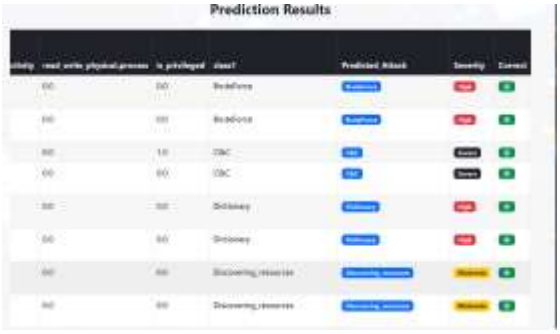

Fig 7: Output Prediction Results

The Output Prediction Results page displays the detected IIoT attacks along with their predicted attack type, severity level, and prediction status. It helps users analyze and verify the classification results generated by the XGBoost-based attack detection system.

Fig 8: Performance Comparison of Machine Learning Models

The proposed XG Boost model achieved the highest accuracy of 98 percent outperforming the Random Forest and SVM classifiers in detecting IIoT network attacks. The results demonstrate that the proposed system provides superior precision, recall, and F-score, making it highly effective for accurate attack detection and classification.

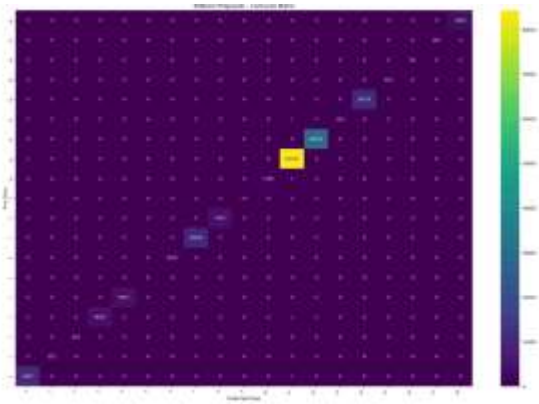

Fig 9: Confusion Matrix Base on XG Boost Classifiers

The confusion matrix illustrates the classification performance of the XG Boost classifier by comparing actual and predicted attack classes. The dominant diagonal values indicate very high prediction accuracy with minimal misclassification of IIoT network attacks.

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026

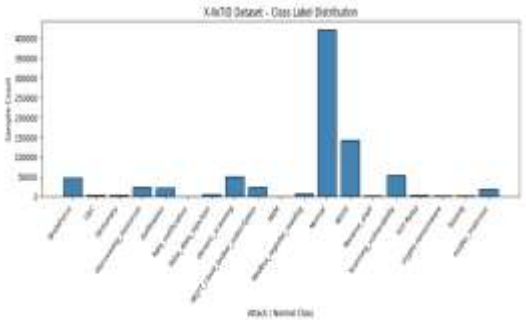

Fig 10: X-IIoTID Dataset Class Label Distribution

The fig 10 illustrates the distribution of different attack categories and normal traffic in the X-IIoTID dataset. It shows that some classes, such as *Normal* and *DDOS*, contain a significantly higher number of samples than others, highlighting the class imbalance present in the dataset used for IIoT attack detection.

Fig 11: Accuracy Comparison Graph

The Accuracy Comparison Graph illustrates the performance of different machine learning algorithms, namely SVM, Random Forest, and XG Boost. The graph shows that XG Boost achieves the highest accuracy, followed by Random Forest and SVM. This comparison helps in identifying the most effective model for the cybersecurity prediction/classification task, with XG Boost demonstrating superior performance.

8.Conclusion and Future Scope

This paper presented an intelligent IT and Mobile Network Attack Detection System using the XGBoost machine learning algorithm. The proposed framework analyses network traffic data and accurately classifies network activities as normal or malicious. Data pre-processing and feature selection techniques improved the quality of the dataset and enhanced model performance. Experimental results demonstrated that the system effectively detects various cyberattacks, including DoS, DDoS, spoofing, intrusion, and unauthorized access attempts. The XG Boost model achieved high accuracy, precision, recall, and F1-score while maintaining low false-positive rates. Its fast processing capability and scalability make it suitable for large-scale IoT and mobile network environments. The system provides real-time threat detection and supports proactive cybersecurity measures. Overall, the proposed framework offers a reliable, efficient, and robust solution for strengthening the security of modern IT and mobile communication networks.

Future Scope: The system can be further enhanced by integrating deep learning and artificial intelligence techniques to improve the detection of sophisticated and zero-day attacks. Future work may also focus on deployment in large-scale IoT and 5G/6G environments for real-time security monitoring. Additionally, incorporating edge and cloud computing technologies can improve scalability, response time, and overall detection performance.

Reference

[1] A. A. Cárdenas, S. Amin, and S. Sastry, “Research challenges for the security of control systems,” *IEEE Security & Privacy*, vol. 6, no. 1, pp. 30–39, 2014.

[2] A. Patcha and J. M. Park, “An overview of anomaly detection techniques: Existing solutions and latest technological

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026

trends," *IEEE Commun. Surveys Tuts.*, vol. 7, no. 1, pp. 3448–3470, 2014.

[3] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2661–2674, 2014.

[4] J. Granjal, E. Monteiro, and J. S. Silva, "Security for the Internet of Things: A survey of existing protocols and open research issues," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 3, pp. 1294–1312, 2015.

[5] A. K. Jain and B. B. Gupta, "Machine learning based intrusion detection system: A comprehensive survey," *IEEE Access*, vol. 3, pp. 1192–1212, 2015.

[6] H. Sedjelmaci and S. M. Senouci, "Intrusion detection and ejection framework against mobile sink attacks in wireless sensor networks," *IEEE Trans. Consumer Electronics*, vol. 61, no. 1, pp. 44–52, 2015.

[7] M. H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita, "Network anomaly detection: Methods, systems and tools," *IEEE Commun. Surveys Tuts.*, vol. 16, no. 1, pp. 303–336, 2014.

[8] Y. Meidan, M. Bohadana, A. Shabtai, et al., "Detection of unauthorized IoT devices using machine learning techniques," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 1–10, 2015.

[9] R. Mitchell and I. R. Chen, "A survey of intrusion detection techniques for cyber-physical systems," *ACM Comput. Surveys*, vol. 46, no. 4, pp. 1–29, 2014.

[10] M. Sarhan, S. Layeghy, and M. Portmann, "Feature Analysis for Machine Learning-Based IoT Intrusion Detection," 2021.

[11] J. Rose, M. Swann, G. Bendiab, S. Shiaeles, and N. Kolokotronis, "Intrusion Detection Using Network Traffic Profiling and Machine Learning for IoT," 2021.

[12] B. R. Kikissagbe and M. Adda, "Machine Learning-Based Intrusion Detection Methods in IoT Systems: A Comprehensive Review," *Electronics*, vol. 13, no. 18, 2024.

[13] P. Turaka and S. K. Panigrahy, "Dynamic Attack Detection in IoT Networks: An Ensemble Learning Approach With Q-Learning and Explainable AI," *IEEE Access*, vol. 12, pp. 161925–161940, 2024.

[14] Q. A. Al-Haija and A. Droos, "A Comprehensive Survey on Deep Learning-Based Intrusion Detection Systems in Internet of Things (IoT)," *Expert Systems*, vol. 42, no. 2, 2025.

Received: 28-04-2026 | Accepted: 02-06-2026 | Published: 12-06-2026