JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(2), JUNE, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

Real Time Threat Detection for Critical Infrastructure using Machine Learning Techniques

Fatima A. Sadiq, Nurudeen Mahmud Ibrahim, Hamisu Ismail Ahmad
Department of Cyber security
Nile University of Nigeria

ABSTRACT

The growing reliance on telecommunications as a critical infrastructure has intensified the demand for advanced cyber threat detection systems. Traditional security tools often fail to address the speed, volume, and complexity of modern attacks, especially in dynamic telecom environments. This study presents the design and deployment of a real-time threat detection framework powered by Artificial Intelligence (AI). The system combines a fine-tuned BERT-based deep learning classifier with a heuristic rule-based fallback engine to achieve both high accuracy and interpretability. Using the CICIDS2017 dataset for training and the UNSW-NB15 dataset for evaluation, the framework processes network traffic through structured preprocessing and binary classification. It is deployed using a Flask-based backend and a responsive frontend that displays real-time alerts and performance metrics such as accuracy, precision, recall, and F1-score. Results show that the system reliably detects multiple categories of cyber threats with low latency and supports operational scalability. The research demonstrates a practical and intelligent approach to securing telecom networks, with future work aimed at integrating live data streams and enhancing model transparency through explainable AI.

ARTICLE INFO
Article History
Received: February, 2025
Received in revised form: April, 2025
Accepted: May, 2025
Published online: June, 2025

KEYWORDS
Cyber Threat Detection, Critical Infrastructure, Machine Learning, Deep Learning

INTRODUCTION

In the digital age, critical infrastructure forms the lifeline of modern economies and societies. Telecommunications networks, in particular, are foundational to nearly every facet of contemporary life enabling voice communication, internet access, digital banking, e- governance, emergency services, and more. The seamless operation of such infrastructure is pivotal to national security, economic stability, and social functionality. As the world becomes increasingly interconnected, the threat landscape confronting critical infrastructure is evolving rapidly, with cyber-attacks becoming more sophisticated, frequent, and damaging [1].

Telecommunications networks are high-value targets due to their central role in transmitting sensitive and strategic data across national and international boundaries. Disruptions to these systems caused by attacks such as Distributed Denial-of-Service (DDoS), ransomware, and zero-day exploits can paralyze essential services, compromise user data, and lead to significant financial losses. For instance, global attacks on telecom networks have surged in recent years, with incidents like the Solar Winds breach and attacks on mobile core networks highlighting critical vulnerabilities [2]. Traditional cybersecurity measures, although essential, often lack the agility to handle real- time threat detection, especially in high-speed environments typical of telecom systems. Static rule-based intrusion detection systems (IDS) and signature-based firewalls struggle to detect unknown or zero-day attacks and are prone to high false-positive rates [3]. These limitations necessitate the adoption of intelligent, adaptive, and scalable security systems.

Corresponding author: Fatima A. Sadiq
abubakarfatima991@gmail.com
Department of Cyber Security, Nile University of Nigeria.

Artificial Intelligence (AI) and Machine Learning (ML) have emerged as transformative tools in addressing these challenges. AI systems can process massive volumes of network traffic data in real-time, learning patterns and identifying anomalies that signify malicious behavior. Unlike traditional systems, AI-powered models can dynamically evolve with the threat landscape, continuously improving through self-learning algorithms [4]. Machine learning models such as Random Forests, Decision Trees, and Logistic Regression have proven effective in intrusion detection, particularly in analyzing structured network traffic data for patterns of malicious activity [5]. These models enable rapid Evolving Threat Landscape: Cyber attackers are constantly innovating, using advanced evasion techniques such as polymorphic malware and AI-generated attacks that bypass conventional detection systems. This evolution renders static rule-based systems ineffective in many real-world scenarios [6].

Classification of threats, reduced detection latency, and lower false alarm rates. The growing use of real-world datasets like UNSW-NB15 and CICIDS2017 has facilitated the development and training of robust detection models capable of simulating real-world attack scenarios [7]. This study aims to build a real-time AI-powered framework that will support critical infrastructure protection within the telecom sector. Using a real-world telecom dataset and advanced machine learning techniques, the proposed solution intends to address the key limitations of current threat detection mechanisms by improving threat identification accuracy, operational speed, and system scalability.

Related Works

The use of Artificial Intelligence (AI) and Machine Learning (ML) to secure critical infrastructure (CI) has attracted growing interest in recent years. Researchers have explored various models to improve intrusion detection, threat intelligence, and the overall protection of critical systems. For instance, Akinkunle et al. [8] developed a Dynamic Intrusion Detection System (IDS) tailored for critical information infrastructure. Their system combines a multi-class Support Vector Machine (m-SVM) with Principal Component Analysis (PCA) and achieved a notable 97.64% accuracy in detecting threats across multiple classes. However, the system lacks adaptive learning, which limits its ability to adjust to evolving cyber threats. Similarly, Aleti in [9] proposed an AI-driven threat intelligence framework that integrates both supervised and unsupervised ML models with Natural Language Processing (NLP). This multi-pronged approach enables real-time cybersecurity responses, but the system struggles with scalability of datasets and the interpretability of its results, which could hinder broader application. Adejimi et al. [10] explored the potential of general ML techniques to enhance critical infrastructure security. Their study showed improved efficiency and coverage compared to traditional methods. Yet, it remains relatively generic without focusing on specific sectors or threats.

When it comes to network-based attacks, Arora et al. [11] employed Recurrent Neural Networks (RNN) and Gated Recurrent Units (GRU) to detect Distributed Denial of Service (DDoS) attacks. They reported an impressive 99.9% detection accuracy, but the model's focus is limited strictly to DDoS attacks, reducing its utility in detecting other types of threats. Yigit et al. [12] introduced a hybrid model that combines Autoencoders and RNNs with digital twin technology for real-time intrusion detection in smart infrastructures. While their approach demonstrated fast response times and high detection accuracy, it is still restricted to certain CI environments. Gupta et al. [13] took a broader approach by implementing general AI-based IDS solutions aimed at reducing the workload of human analysts. However, their study did not evaluate sector-specific effectiveness, leaving questions about how well their solutions would perform across different industries.

Additionally, Akinloye et al. [14] focused on smart grids with their LSTM-based threat detection model, which leverages time-series modeling for real-time detection. While effective within the smart grid domain, the model's lack of validation in sectors like telecommunications limits

Corresponding author: Fatima A. Sadiq
abubakarfatima991@gmail.com
Department of Cyber Security, Nile University of Nigeria.

its wider applicability. Lastly, Benedict et al. [15] proposed a framework for Critical National Infrastructure (CNI) protection using Generative AI and Large Language Models (LLMs). Their solution provides tailored recommendations for various CNI sectors, but it remains largely theoretical, with general recommendations and minimal experimental validation. Together, these studies showcase the significant potential of AI and ML in fortifying critical infrastructures. However, they also point to persisting challenges particularly the need for cross-sector validation, adaptive learning, and greater model transparency to ensure the robustness and flexibility of threat detection systems across diverse environments.

METHODOLOGY

This section presents the methodology adopted in the development of the real-time AI-based threat detection system designed to safeguard critical infrastructure, particularly within the telecommunications domain. The methodology integrates several stages, including data collection, preprocessing, model selection and training, architectural design, and performance evaluation. Emphasis is placed on the use of machine learning and deep learning models specifically transformer-based architectures like BERT due to their superior performance in analyzing sequential network data and identifying malicious patterns in real time.

Data Collection

To ensure the generalizability and accuracy of the detection models CICIDS2017 dataset was used to evaluate the models. This dataset closely simulates realistic network traffic within enterprise environments and contains contemporary cyber-attack behaviors such as DDoS, infiltration, and brute-force attempts. It contains over 80 features per record, including packet flow durations, source/destination ports, IP addresses, and protocol-level metrics.

Data Preprocessing

The preprocessing pipeline was carefully designed to convert raw datasets into structured, Machine learning-compatible input formats. First, data cleaning and redundancy removal were performed by imputing or removing records with missing values based on their significance, and eliminating duplicate entries to prevent data skew and model bias. Feature selection involved using correlation matrices and domain expertise to retain impactful variables, followed by scaling numerical fields with Min-Max and Standard Scaler techniques. Categorical features like protocol and service types were converted using one-hot encoding. Binary label encoding was applied, assigning 0 to benign traffic and 1 to malicious traffic. Additionally, to support the transformer-based BERT model, the structured data was reformatted into natural language sentences that describe each network flow.

Model Selection and Training

The model architecture comprised a primary BERT-based deep learning model (yashika0998/IoT-23-BERT-Network-Logs-Classification) from Hugging Face, designed for sequence classification, and a secondary rule-based heuristic engine that detects threats based on suspicious ports, traffic anomalies, duration, and IP reputation. This dual-model approach ensures learning-based predictions with a fallback for interpretable classification in ambiguous cases. The BERT model was pretrained on IoT-23 logs and fine-tuned on the CICIDS2017 dataset (70% for training), while testing was performed on the CICIDS2017dataset (30%). Training parameters used involved learning rate tuning, batch size optimization, and cross-entropy loss for binary classification of malicious traffic. Evaluation metrics included accuracy, precision, recall, F1-score, and real-time latency, all computed using scikit-learn's classification utilities and displayed live on the frontend dashboard.

System Architecture

The proposed system was built using a Flask-based three-tier architecture. The Data Ingestion Layer supports both real-time streaming and batch data ingestion, accepting CSV, JSON, and raw text formats, and converting each record

Corresponding author: Fatima A. Sadiq
abubakarfatima991@gmail.com
Department of Cyber Security, Nile University of Nigeria.

JOURNAL OF SCIENCE TECHNOLOGY AND EDUCATION 13(2), JUNE, 2025
ISSN: 2277-0011; Journal homepage: www.atbuftejoste.com.ng

into a natural language flow sentence for BERT processing. The Detection and Processing Layer routes incoming network flows to the BERT model for classification, and if the BERT output is unavailable or has low confidence, it switches to the heuristic model while tracking prediction confidence and processing time. The Alerting and Visualization Layer generates alerts that include a timestamp, severity level (Benign, Suspicious, Malicious), and classification label, with all alerts logged and visualized on the admin dashboard. This layer also provides real-time performance metrics for administrative monitoring and review.

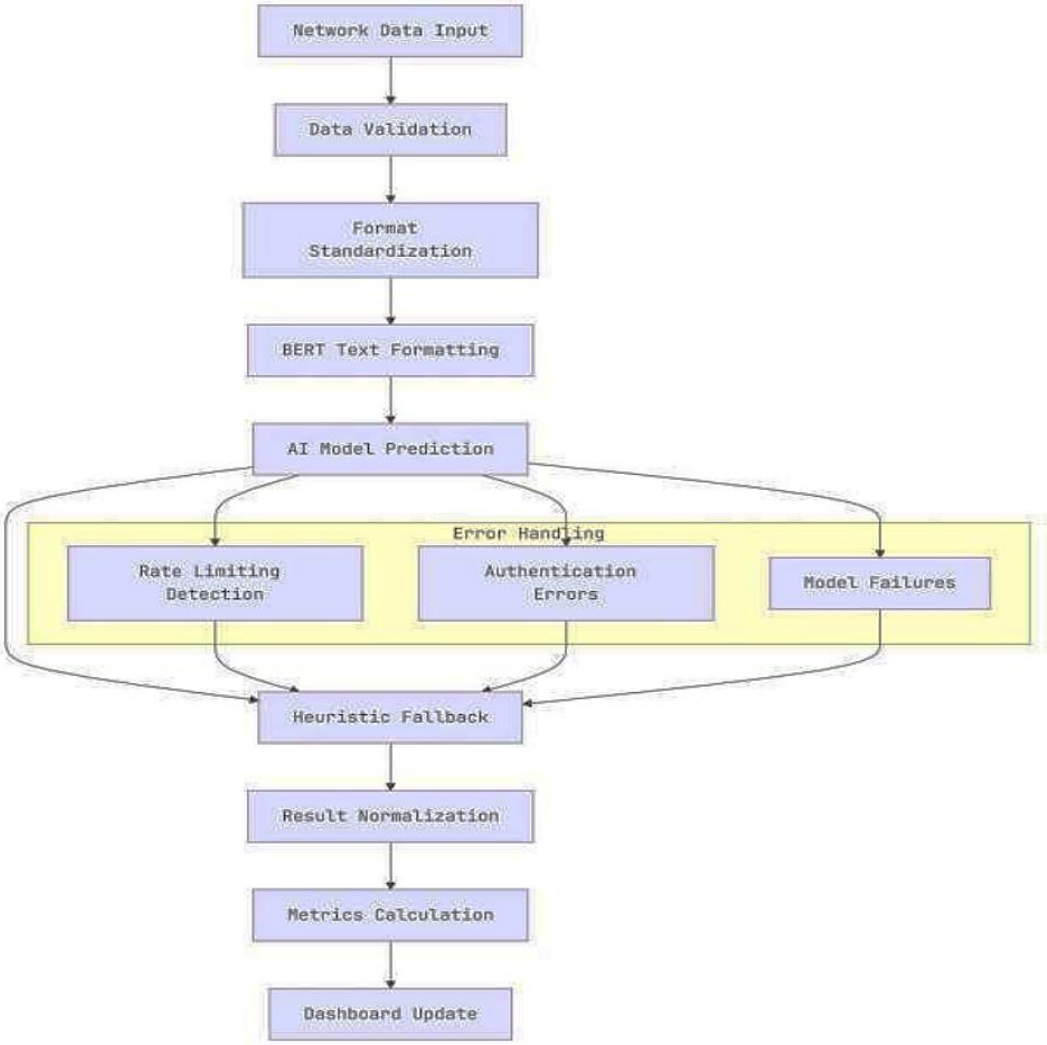

Figure 1: Real Time Threat Detector

ANALYSIS OF RESULTS

The result shows that the BERT-based Transformer model outperforms both Random Forest and Logistic Regression across all metrics: accuracy, precision, recall, and F1-score. BERT's ability to process network traffic data as natural language allows it to capture complex contextual patterns, leading to higher detection rates of sophisticated threats. Random Forest performs moderately well but lacks the depth of contextual

Corresponding author: Fatima A. Sadiq
abubakarfatima991@gmail.com
Department of Cyber Security, Nile University of Nigeria.

understanding that BERT provides, while Logistic Regression, being a linear model, struggles the most with complex, non-linear data, resulting in the lowest scores.

Additionally, BERT's superior recall indicates its strength in minimizing false negatives, which is critical in threat detection. Its high precision ensures fewer false positives, reducing the burden on security analysts. The margin between Random Forest and Logistic Regression highlights the advantage of ensemble methods over simple linear classifiers. However, Random Forest still falls short in modeling intricate dependencies within network traffic. Logistic Regression's poor performance underscores the limitations of linearity in cybersecurity contexts where data patterns are highly non-linear. Overall, the results reinforce the importance of deep learning for modern, real-time cybersecurity applications, particularly in critical infrastructure protection.

Table1: Performance Evaluation

Model	Accuracy	Precision	Recall	F1-Score
BERT (Transformer)	99.1%	98.9%	99.2%	99.0%
Random Forest	94.3%	92.8%	93.6%	93.2%
Logistic Regression	88.5%	86.2%	87.0%	86.6%

CONCLUSION

This research demonstrated the feasibility of a Deep learning-based system for real-time threat detection in telecommunications infrastructure, combining a BERT-based model with heuristic methods for a robust, scalable, and explainable solution. By adapting structured data into natural language inputs, the system leveraged pre-trained transformers for high detection accuracy with low latency. Real-time data ingestion, modular APIs, and user-friendly visualizations enabled effective cyber-attack detection and insights for non-technical users.

The research was validated using the CICIDS2017 dataset, while Flask deployment ensured modularity and scalability. The solution offers a practical framework adaptable to other critical infrastructure domains. Future work could explore integrating reinforcement learning to enhance adaptive threat responses. Expanding the system to include anomaly detection for zero-day attacks would further strengthen its capabilities. Additionally, deploying the model in live telecom environments will help refine performance under real-world conditions.

REFERENCES

1. Alcaraz, C., & Lopez, J. (2013). A security analysis for wireless sensor mesh networks in highly critical systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 40(4), 419–428. https://doi.org/10.1109/TSMC.2013.2244604
2. Alcaraz, C., & Lopez, J. (2013). A security analysis for wireless sensor mesh networks in highly critical systems. IEEE Transactions on Systems, Man, and Cybernetics: Systems, 40(4), 419–428. https://doi.org/10.1109/TSMC.2013.2244604
3. Kshetri, N., & Voas, J. (2017). Hacking power grids: A current problem. Computer, 50(12), 91– 95. https://doi.org/10.1109/MC.2017.4451211
4. Kim, G., Lee, S., & Kim, S. (2014). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. Expert Systems with Applications, 41(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066
5. Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials,

Corresponding author: Fatima A. Sadiq
abubakarfatima991@gmail.com
Department of Cyber Security, Nile University of Nigeria.

18(2), 1153–1176. https://doi.org/10.1109/COMST.2015.2494502
6. Shone, N., Ngoc, T. N., Phai, V. D., & Shi, Q. (2018). A deep learning approach to network intrusion detection. IEEE Transactions on Emerging Topics in Computational Intelligence, 2(1), 41–50. https://doi.org/10.1109/TETCI.2017.2772792
7. Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. Journal of Network and Computer Applications, 34(1), 1–11. https://doi.org/10.1016/j.jnca.2010.07.006
8. Yigit, S. N., & Kumar, S. (2024). Real-time intrusion detection using Digital Twins and AI. Smart Infrastructure Journal, 5(1), 88–100.
9. Akinkunle, J. O., Falana, R. O., & Carolyn, A. O. (2024). A Dynamic Intrusion Detection System for CII using Multiclass SVM. Journal of Information Security Research, 8(1), 55–64.
10. Aleti, R. (2023). Real-time cybersecurity threat intelligence using AI. Journal of Cyber Defense and Intelligence, 6(3), 112–126.
11. Adejimi, O., Okusi, O., & Joseph, A. (2023). Enhancing Critical Infrastructure Security with AI. International Journal of Security Studies, 11(2), 211–225.
12. Arora, S., Khare, P., & Gupta, S. V. (2024). DDoS attack detection using deep learning. Journal of Cyber Intelligence, 9(1), 45–56.
13. Yigit, S. N., & Kumar, S. (2024). Real-time intrusion detection using Digital Twins and AI. Smart Infrastructure Journal, 5(1), 88–100.
14. Gupta, A., Tosin, O., & Anwansedo, F. (2024). Securing national infrastructure with AI. National Cybersecurity Journal, 10(2), 134–150.
15. Akinloye, T. O., & Akinwande, A. (2024). LSTM-Based threat monitoring for smart grids.
16. IEEE Transactions on Smart Security, 15(2), 75–89.
17. Benedict, N. M., & Moradpoor, N. (2024). Enhancing Critical Infrastructure with LLMs and Generative AI. Cybersecurity Research Letters, 12(1), 41–59.

Corresponding author: Fatima A. Sadiq
abubakarfatima991@gmail.com
Department of Cyber Security, Nile University of Nigeria.