AI-Powered Intrusion Detection and Mitigation for Critical Infrastructure in Resource-Constrained Environments

Amohelang Ntjanyana and Dr. Alice Shemi
Department of Computer Science, Copperbelt University, Zambia
Email: amohelangntjanyana@gmail.com

***Abstract*—Cybersecurity threats targeting critical infrastructures are rising globally, with developing nations facing unique challenges due to limited resources, outdated technologies, and inadequate expertise. This paper presents the design and evaluation of an Artificial Intelligence (AI)-powered Intrusion Detection and Mitigation System (IDMS) tailored for such environments. The system integrates multiple machine learning algorithms being Random Forest, Convolutional Neural Networks (CNN), and Recurrent Neural Networks (RNN) trained and tested on benchmark datasets including NSL-KDD, CICIDS2017, and UNSW-NB15. A modular dashboard was developed to support dataset management, model evaluation, real-time alerts, forensic logging, and live packet inspection. Among the tested models, Random Forest achieved the highest detection accuracy of 98.2%, outperforming CNN and RNN while requiring fewer computational resources. The findings demonstrate that AI-driven IDS can provide practical, scalable, and transparent solutions for resource-constrained contexts, thereby strengthening the resilience of critical infrastructure.**

***Index Terms*—Intrusion Detection System, Artificial Intelligence, Cybersecurity, Machine Learning, Critical Infrastructure**

I. Introduction

Critical infrastructures such as telecommunications, finance, and government systems are increasingly exposed to cyberattacks. For nations with limited technical and financial resources, the challenge is even more pressing. Traditional rule-based Intrusion Detection Systems (IDS) are not equipped to deal with the volume and sophistication of modern attacks.

Artificial Intelligence (AI) has emerged as a promising approach to cybersecurity by enabling automated learning of patterns and anomalies in network traffic. By integrating machine learning models into IDS, threats can be identified more accurately and in real time. This research focuses on designing and implementing an AI-powered IDS tailored for Lesotho, a resource-constrained setting where lightweight and adaptable systems are essential.

II. Related Work

Buczak and Guven [1] reviewed data mining and ML techniques for IDS, showing ensemble methods as strong performers. More recently, Khan et al. [2] and Patel and Kumar [3] applied deep learning techniques, demonstrating the ability of CNN and RNN to classify complex traffic patterns.

While effective, deep learning often demands extensive computing power, limiting deployment in developing contexts. Rudin [4] argued for interpretable models in high-stakes domains such as security, underlining the need for trust and transparency.

III. Methodology

A. System Architecture

The IDS was implemented as a modular system with multiple displays, including:

- Admin Dashboard for dataset upload and testing,
- Model Analysis Display for evaluation of Random Forest, CNN, and RNN,
- Alerts Display for real-time anomaly detection,
- Forensic Log Display for storage of incident details,
- System Monitoring for live packet capture and inspection.

B. Datasets

Three benchmark datasets were used:

- NSL-KDD: improved version of KDD'99,
- CICIDS2017: modern dataset capturing DoS, DDoS, brute force, and infiltration attacks,
- UNSW-NB15: hybrid dataset with both normal and malicious traffic.

C. Machine Learning Models

- Random Forest (RF): ensemble classifier known for robustness,
- Convolutional Neural Network (CNN): effective for detecting spatial traffic patterns,
- Recurrent Neural Network (RNN): designed for sequential traffic behavior analysis.

IV. Results and Analysis

Random Forest achieved the best detection accuracy of 98.2%, with precision and recall above 97%. CNN achieved 96.5% accuracy, while RNN followed at 95.8%. Random Forest also produced the lowest false positives, making it more suitable for environments with limited computing resources.

The dashboard interface allowed administrators to manage datasets, monitor traffic, and review forensic logs. Real-time alerts categorized by severity supported timely decision-making.

V. Discussion

The results show that Random Forest remains a strong contender for IDS deployment in low-resource environments, offering high performance with lower computational overhead compared to CNN and RNN. Deep learning models demonstrated promise but required greater resources, making them less practical in this context.

The modular dashboard improved usability by integrating key functions into a single interface. This approach enhanced technical detection capability and institutional trust through transparency.

VI. Conclusion and Future Work

This study demonstrated the feasibility of deploying an AI-powered IDS in a resource-constrained environment such as Lesotho. Random Forest outperformed CNN and RNN in terms of accuracy and efficiency, making it more practical for local infrastructures.

Future work will focus on:

- Integrating Federated Learning for collaborative training,
- Incorporating Explainable AI (XAI) tools such as SHAP and LIME,
- Testing scalability in real-world deployments.

References

[1] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, 2016.

[2] A. Khan, et al., "Deep learning approaches for intrusion detection in IoT networks," *Computers & Security*, 2023.

[3] R. Patel and S. Kumar, "Hybrid CNN-RNN models for anomaly detection in network traffic," *Journal of Information Security*, 2024.

[4] C. Rudin, "Stop explaining black box machine learning models for high stakes decisions and use interpretable models instead," *Nature Machine Intelligence*, 2019.