AI-Powered Secure Network for Intelligent Threat Detection and Automated Mitigation Using Machine Learning

A. Ajina
Department of Artificial Institute and Machine Learning, Ramaiah Institution of Technology, Bengaluru, Karnataka, India

Kota Solomon Raju
CSIR-NAL Campus, Bengaluru, Karnataka, India

Abstract

The rapid escalation of cyber threats has exposed critical limitations in traditional security mechanisms, which frequently fail to address evolving and sophisticated attack vectors. This research presents an AI-powered network security framework utilizing supervised machine learning algorithms specifically Random Forest and XGBoost for real-time vulnerability detection and automated threat mitigation. The architecture consists of three modular components: (i) a real-time traffic monitoring and AI-driven classification engine, (ii) a Node.js backend for automated mitigation and secure logging, and (iii) an interactive React.js dashboard for visualization and system control. Emphasizing scalability, modularity, and secure inter-component communication, the framework enables adaptive threat response via rule-based automation. Extensive experimental evaluation on benchmark intrusion detection datasets demonstrates a detection accuracy of 94.6% and a false positive rate below 6%, with robust performance under heavy network loads. Furthermore, the system establishes a foundation for integrating deep learning based anomaly detection, block chain enabled auditability, and cloud-native deployment. The results underscore the potential of AI-driven architectures to deliver proactive, scalable, and resilient cybersecurity solutions for contemporary digital ecosystems.

Keywords

Artificial Intelligence, Automated Mitigation, Intrusion Detection System (IDS), XGBoost.