Title: Enhancing Cybersecurity in IoT Networks Using Machine Learning

Authors:

Aarush Padha, Priya Mehra, Rahul Singh

Abstract:

This paper explores how machine learning can improve the security of Internet of Things (IoT) networks. With the rapid adoption of IoT in smart homes and industries, security vulnerabilities have become a major concern. We propose a hybrid detection framework combining supervised and unsupervised learning to identify abnormal behaviors in real-time.

1. Introduction:

The Internet of Things (IoT) connects billions of devices worldwide, but these devices often lack strong security. Traditional rule-based systems are ineffective against evolving threats. Machine learning provides a promising alternative by adapting to new attack patterns.

2. Related Work:

Previous studies have used SVMs, decision trees, and neural networks for intrusion detection. However, these approaches lack flexibility and often suffer from false positives. Our approach improves upon this by combining clustering and classification.

3. Proposed Method:

Our framework includes a data preprocessing module, anomaly detector (using K-Means), and a classifier (Random Forest). We collected data from a simulated smart home environment over 3 weeks, including both normal and malicious activities.

4. Results:

The hybrid model achieved 96.4% accuracy and reduced false positives by 18% compared to baseline methods. It was able to detect common attacks like DDoS, packet injection, and spoofing effectively.

5. Conclusion:

Machine learning offers a scalable and adaptive approach to securing IoT environments. Our hybrid framework demonstrates strong potential for real-world deployment. Future work involves integrating deep learning models and edge deployment.

References:

[1] Ahmed et al., "ML for IoT Security", IEEE, 2021

[2] Zhou et al., "Anomaly Detection in IoT", Elsevier, 2020