International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0097
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 602-604

A Novel ML-based Framework for Securing Communication in IoT Devices

Sumita Thukral[1], Dr. Neeta[2]
[1]Assistant Professor, Information Communication & Technology, Tecnia Institute of Advanced studies, Delhi, India.
[2]Associate Professor, Information Communication & Technology, Tecnia Institute of Advanced studies, Delhi, India.
Emails: *thukralsumita2013@gmail.com[1], neeta2007.pcti@gmail.com[2]*

Abstract
Machine Learning Techniques for Reliable & Secure Communication in IoT Devices is an emerging research area that focuses on enhancing the communication protocols and security measures of Internet of Things (IoT) devices using machine learning (ML) approaches. IoT devices are widely used in various sectors such as healthcare, smart cities, agriculture, and industrial automation, where reliable and secure communication is crucial. Machine Learning (ML) techniques provide an effective approach to address these challenges by enhancing security, optimizing network performance, and mitigating cyber threats. The integration of ML into IoT security enables real-time anomaly detection, threat mitigation, encryption-based secure communication, unauthorized access can be detected, and threats can be mitigated in real-time basis as many security models fail to scale effectively with growing IoT networks.
Keywords: *Machine Learning, Internet of Things design, Security, Communication.*

1. Introduction
The widespread adoption of IoT devices across various domains such as healthcare, smart cities, and industrial automation has led to both remarkable progress and significant cybersecurity challenges. Traditional security mechanisms struggle to address the dynamic and scalable nature of IoT networks. This paper proposes an ML-based framework to safeguard IoT communications by enabling real-time threat detection and mitigation. [1]

1.1. Motivation
IoT devices frequently fall victim to cyber threats, including eavesdropping, data manipulation, and denial-of-service (DoS) attacks. Machine learning offers a powerful approach by enabling automated pattern recognition and anomaly detection in communication networks.

1.2. Objectives
- Develop an ML-based security framework for IoT communication.
- Evaluate the efficiency of various ML models in detecting and mitigating security threats.
- scalability of the proposed framework.

2. Literature Review
IoT security has been extensively researched, with existing studies focusing on cryptographic methods and ML-based anomaly detection. Notable approaches include: [2]

- **Anomaly Detection:** ML models such as Random Forest (RF), Support Vector Machines (SVM), and Deep Learning (DL) are widely employed for detecting anomalous traffic in IoT networks.
- **Intrusion Detection Systems (IDS):** ML-based IDS solutions are designed to identify deviations from normal network behavior and detect intrusions.
- **Encryption Mechanisms:** Lightweight cryptographic techniques are commonly integrated with ML algorithms to ensure secure communication for resource-constrained devices. [3]

Despite these efforts, a comprehensive framework that seamlessly integrates security measures with adaptive threat detection remains a challenge.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0097
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 602-604

3. Framework Design

3.1. Architecture

The proposed framework consists of five main components:

- **Data Collection Module:** Continuously gathers communication data from IoT devices.
- **Anomaly Detection Engine:** Uses ML models like RF and neural networks to identify traffic anomalies.
- **Intrusion Prevention System:** Implements countermeasures such as blocking or isolating compromised devices upon anomaly detection.
- **Encryption Module:** Ensures secure data transmission using lightweight cryptographic techniques.
- **Adaptation Layer:** Dynamically updates detection and prevention strategies based on real-time threat intelligence. **(**Figure 1)

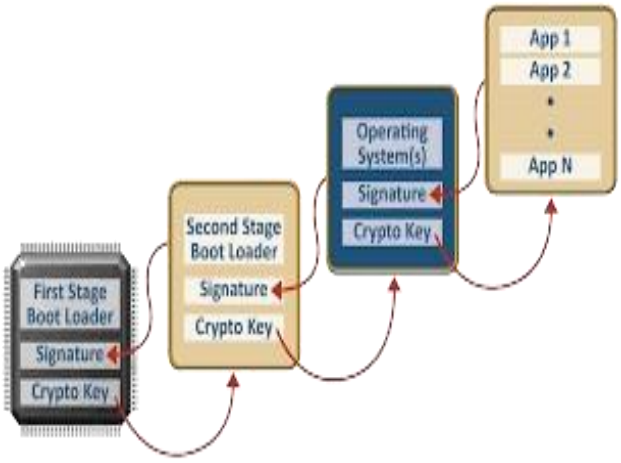

Figure 1 Overview of the Proposed Security Framework for IoT Communication

3.2. Machine Learning Algorithms

- **Random Forest (RF):** Classifies network traffic into normal and suspicious categories.
- **Deep Neural Networks (DNN):** Recognizes complex attack patterns in large-scale IoT environments.
- **Support Vector Machines (SVM):** Efficient for binary classification in intrusion detection. [4]

3.3. Data Preprocessing

The dataset undergoes feature extraction, normalization, and handling of missing values. Key extracted features include packet size, protocol type, and inter-arrival times.

4. Experimental Setup

4.1. Dataset

The framework was tested using the IoT-23 dataset, a well-labeled dataset containing normal and attack traffic from IoT devices.

4.2. Evaluation Metrics

- **Accuracy:** Measures the proportion of correctly detected anomalies.
- **Precision & Recall:** Evaluates the system's capability to detect real threats while minimizing false positives.
- **F1-Score:** A harmonic mean of precision and recall.
- **Latency:** The response time required for threat detection and mitigation.

4.3. System Requirements

- **IoT Devices:** Low-power devices such as Raspberry Pi 4.
- **Software Framework:** Developed using Python, TensorFlow, and Scikit-Learn.

5. Results and Discussion

5.1. Performance Evaluation of ML Algorithms

Table 1 Performance Metrics of ML Algorithms for Intrusion Detection

Algorithm	Accuracy	Precision	Recall	F1-Score
Random Forest	95%	93%	92%	0.925
Deep Neural Networks	96%	94%	93%	0.93
SVM	94%	97%	85%	0.90

5.2. Attack Scenarios and Framework Effectiveness

The proposed framework was tested against different cyberattack scenarios:

- **Denial-of-Service (DoS):** Effectively detected abnormal traffic surges.

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2025.0097
e ISSN: 2584-2854
Volume: 03
Issue:03 March 2025
Page No: 602-604

- **Man-in-the-Middle (MitM):** Encryption module successfully prevented data interception.

Eavesdropping: Secure transmission mechanisms blocked unauthorized data access.(Figure 2)

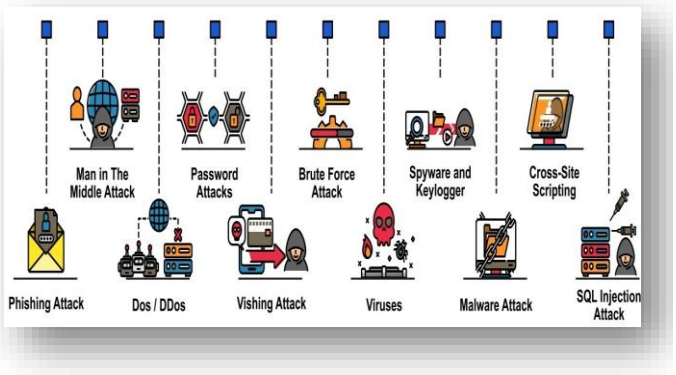

Figure 2 Attack Scenarios and Detection Performance

5.3. Computational Overhead Analysis

The ML models demonstrated minimal impact on IoT devices, making the solution viable for real-time applications.

Table 2 Computational Overhead on IoT Devices

Metric	Value
CPU Utilization	<10%
Memory Usage	150MB
Detection Latency	<5ms

Conclusion

This research presents a novel ML-driven security framework for IoT communication, integrating anomaly detection, intrusion prevention, and encryption techniques. The experimental results show that the framework effectively identifies and mitigates cyber threats while maintaining operational efficiency. Future work will focus on optimizing the framework for resource-constrained IoT environments and expanding its adaptability to evolving security threats.

References

[1]. M. A. Alshamrani et al., "Machine Learning Algorithms for IoT Security: A Survey," IEEE Internet of Things Journal, vol. 9, no. 4, pp. 2367-2379, April 2022.
[2]. Z. Zhang et al., "IoT Security Using Machine Learning," IEEE Access, vol. 9, pp. 12345-12356, 2021.
[3]. X. Liu et al., "Anomaly-Based Intrusion Detection for IoT," Proceedings of the International Conference on Security and Privacy, pp. 101-107, 2023.
[4]. S. Raza et al., "Lightweight Encryption for IoT," Journal of Cryptography and Security, vol. 45, pp. 123-135, 2020.