# Evaluating Machine Learning Models for Network Anomaly Detection in IoT Environments

Bilal Abdulhadi
Computer Engineering
Biruni University

DR. MHD RAJA ABOU HARB
mharb@biruni.edu.tr

## 1 Introduction

The rapid development of the Internet of Things (IoT) has significantly transformed modern communication and computing systems. IoT devices are now widely used in various applications such as smart homes, healthcare, transportation, and industrial automation. These devices continuously collect and exchange large amounts of data over networks, making them an essential part of everyday life. However, this rapid growth has also introduced serious security challenges [5].

One of the main issues in IoT environments is that many devices are resource-constrained, meaning they have limited processing power, memory, and energy. As a result, they often lack strong built-in security mechanisms. This makes IoT networks highly vulnerable to different types of cyberattacks, including Distributed Denial of Service (DDoS), malware infections, data breaches, and unauthorized access [2]. Traditional security solutions, such as rule-based intrusion detection systems, are often not sufficient to handle the dynamic and complex nature of IoT environments.

To address these challenges, machine learning (ML) techniques have been widely adopted in recent years for intrusion detection. Unlike traditional methods, ML-based systems can learn patterns from network traffic data and automatically detect abnormal behavior. This allows them to identify both known and unknown attacks more effectively [1]. Supervised learning methods, such as Decision Trees and Random Forest, are commonly used due to their high accuracy, while unsupervised and semi-supervised approaches are gaining attention for their ability to work with limited labeled data.

In addition, deep learning models such as Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) have shown promising results in capturing complex patterns in IoT network traffic. These models are capable of analyzing both spatial and temporal features, leading to improved detection performance [3]. However, they often require large datasets and high computational resources, which may limit their practical use in real-world IoT systems.

This literature review focuses on recent research works that apply machine learning techniques for intrusion detection in IoT networks. The selected studies are analyzed based on their methodologies, strengths, limitations, and performance metrics. A comparative analysis is provided to highlight the differences between these approaches, followed by a discussion of the existing research gaps and potential directions for future work.

# 2 Literature Review

Several recent studies have explored the use of machine learning techniques for intrusion detection in IoT networks. These works focus on improving detection accuracy, reducing false positives, and handling the unique challenges of IoT environments such as limited resources and dynamic network behavior.

In [1], a machine learning-based network intrusion detection system was proposed that focuses on both anomaly detection and attack classification. The approach uses feature selection techniques such as ANOVA and Chi-square to improve model performance. Multiple machine learning algorithms were evaluated, and the results showed that Random Forest and XGBoost achieved the highest accuracy. This study highlights the importance of proper feature selection and dataset balancing in improving detection performance.

In [2], the application of supervised machine learning algorithms for intrusion detection in IoT networks was investigated. Different models, including Decision Trees, Random Forest, and K-Nearest Neighbors, were compared using the BoTNeTIoT dataset. The results indicated that Random Forest provided high accuracy and strong generalization. However, the study also identified challenges related to data imbalance and the need for effective preprocessing techniques.

A hybrid deep learning model combining Convolutional Neural Networks (CNN) and Recurrent Neural Networks (RNN) was introduced in [3]. The CNN component extracts spatial features from network traffic, while the RNN component captures temporal patterns. The model achieved high detection accuracy and low false positive rates, demonstrating the effectiveness of combining multiple deep learning techniques. However, the model requires significant computational resources, which may limit its applicability in resource-constrained IoT environments.

In [4], a self-supervised learning approach for anomaly detection in IoT networks was proposed. Unlike traditional supervised methods, this approach does not rely heavily on labeled data. Instead, it uses techniques such as contrastive learning, autoencoders, and transformers to learn useful representations from unlabeled data. The results showed strong performance in detecting anomalies, making this approach suitable for dynamic environments where labeled data is limited.

Finally, a review of machine learning techniques for IoT attack detection was presented in [5]. The study discussed both supervised and unsupervised learning methods, including Support Vector Machines, Random Forest, and neural networks. It also highlighted the strengths and weaknesses of each approach, providing a broad understanding of current trends in IoT security research.

Overall, these studies demonstrate that machine learning and deep learning techniques are effective tools for intrusion detection in IoT networks. However, each approach has its own limitations, particularly in terms of computational cost, data requirements, and adaptability to new attack patterns.

# 3 Comparative Analysis

Table 1: Comparison of Machine Learning Approaches for IoT Intrusion Detection

| **Reference** | **Methodology / Approach** | **Strengths** | **Limitations** | **Performance Metrics** |
|---|---|---|---|---|
| Lee and Majd (2023) | Machine learning models (Random Forest, XGBoost) with ANOVA and Chi-square feature selection | High detection accuracy, effective feature selection, handles multiple attack types | Requires careful feature engineering, dataset preprocessing needed | Accuracy, classification performance |
| Zhang (2025) | Supervised learning (Decision Tree, Random Forest, KNN) using BoTNeTIoT dataset | Good generalization, simple implementation, strong performance with Random Forest | Dataset imbalance affects results, requires preprocessing | Accuracy, prediction time |
| Ramdan et al. (2025) | Hybrid deep learning model (CNN + RNN) combining spatial and temporal features | High accuracy, low false positives, captures complex patterns | High computational cost, not suitable for low-resource IoT devices | Accuracy, Recall, F1-score, inference time |
| Kour et al. (2025) | Self-supervised learning using contrastive learning, autoencoders, and transformers | Works with unlabeled data, adaptable to new attacks, reduces manual labeling | Complex model design, higher training complexity | Accuracy, Precision, AUC-ROC |
| Srivastava et al. (2025) | Review of ML techniques (SVM, RF, KNN, Neural Networks) | Provides broad overview, compares multiple algorithms | No experimental validation, lacks performance testing | Not applicable |

# 4 Research Gap Analysis

Although recent studies have shown significant progress in using machine learning techniques for intrusion detection in IoT networks, several important limitations still exist. One major issue is the strong dependency on labeled datasets in many supervised learning approaches. Models such as Decision Trees and Random Forest require large amounts of labeled data for training, which is often difficult and time-consuming to obtain. In real-world IoT environments, attack patterns continuously evolve, making it challenging to maintain updated labeled datasets [2, 4].

Another limitation is related to the computational complexity of advanced models, especially deep learning techniques. Hybrid models such as CNN-RNN achieve high detection accuracy by capturing both spatial and temporal features, but they require high processing power and memory. This makes them difficult to deploy on IoT devices, which are usually resource-constrained. As a result, there is a gap between high-performance models and their practical applicability in real-world IoT systems [3].

In addition, while newer approaches such as self-supervised learning reduce the need for labeled data, they introduce other challenges, including increased model complexity and longer training times. Furthermore, many existing studies focus mainly on improving accuracy, without considering important factors such as real-time detection, energy efficiency, and scalability. Therefore, future research should focus on developing lightweight and adaptive intrusion detection models that can operate efficiently in dynamic IoT environments while maintaining high detection performance.

# References


[1] K. Lee and N. E. Majd, "Anomaly Detection and Attack Classification in IoT Networks Using Machine Learning," in *Proc. IEEE 42nd Int. Performance Computing and Communications Conf. (IPCCC)*, 2023.

[2] Y. Zhang, "A Machine Learning-Based Intrusion Detection System for Securing Internet of Things Networks," in *Proc. 7th Int. Conf. Information Science, Electrical and Automation Engineering (ISEAE)*, 2025.

[3] L. Ramdan, U. Aditiawarman, and J. Asian, "Enhancing IoT Network Intrusion Detection with Integrated CNN-RNN Model," in *Proc. IEEE 11th Int. Conf. Computing, Engineering and Design (ICCED)*, 2025.

[4] H. Kour, P. Bavadiya, and S. Kumar, "Self-Supervised Learning for Anomaly Detection in IoT Networks," in *Proc. 3rd Int. Conf. Advancement in Computation and Computer Technologies (InCACCT)*, 2025.

[5] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," *IEEE Communications Surveys & Tutorials*, 2021.