

Research Methodology in Computer Science (AI800)

Student Name: Mohammed Alhawshabi

Student ID: 261002622

Title: Machine Learning for Network Intrusion Detection in IoT Networks

Literature Review

Paper 1

Summary: Studies explore ML/DL models (e.g., SVM, Random Forest, Deep Learning) for detecting intrusions in network traffic.

Key Findings: High detection accuracy reported in controlled datasets.

Limitations: Reliance on outdated datasets, limited real-world validation, high computational cost.

Paper 2

Summary: Studies explore ML/DL models (e.g., SVM, Random Forest, Deep Learning) for detecting intrusions in network traffic.

Key Findings: High detection accuracy reported in controlled datasets.

Limitations: Reliance on outdated datasets, limited real-world validation, high computational cost.

Paper 3

Summary: Studies explore ML/DL models (e.g., SVM, Random Forest, Deep Learning) for detecting intrusions in network traffic.

Key Findings: High detection accuracy reported in controlled datasets.

Limitations: Reliance on outdated datasets, limited real-world validation, high computational cost.

Paper 4

Summary: Studies explore ML/DL models (e.g., SVM, Random Forest, Deep Learning) for detecting intrusions in network traffic.

Key Findings: High detection accuracy reported in controlled datasets.

Limitations: Reliance on outdated datasets, limited real-world validation, high computational cost.

Paper 5

Summary: Studies explore ML/DL models (e.g., SVM, Random Forest, Deep Learning) for detecting intrusions in network traffic.

Key Findings: High detection accuracy reported in controlled datasets.

Limitations: Reliance on outdated datasets, limited real-world validation, high computational cost.

Paper 6

Summary: Studies explore ML/DL models (e.g., SVM, Random Forest, Deep Learning) for detecting intrusions in network traffic.

Key Findings: High detection accuracy reported in controlled datasets.

Limitations: Reliance on outdated datasets, limited real-world validation, high computational cost.

Critical Analysis

Most studies demonstrate strong performance; however, they rely heavily on simulated or outdated datasets and lack adaptability to real-world IoT environments.

Connections

All papers focus on ML-based intrusion detection and aim to improve accuracy and efficiency.

Conflicts

Differences exist between traditional ML and deep learning approaches, as well as centralized vs distributed systems.

Year	Method	Finding	Limitation
2020	SVM	High accuracy	Old data
2021	RF	Low false positives	Scalability
2022	DL	Better detection	High cost

Problem Statement

Based on the literature review, existing machine learning-based intrusion detection systems show high accuracy but depend heavily on outdated datasets and controlled environments.

IoT networks introduce new challenges such as dynamic traffic patterns, limited resources, and real-time requirements, which current models fail to handle effectively.

Although ML and DL approaches have been proposed, they often suffer from high false positive rates and lack generalization.

This highlights the need for a more adaptive and efficient intrusion detection model tailored for IoT environments.

Research Objectives

To analyze existing machine learning and deep learning techniques for intrusion detection.

To identify limitations in current IDS models based on the literature review.

To design an efficient ML-based intrusion detection model for IoT networks.

To evaluate the model using accuracy, precision, recall, and F1-score.

To improve detection accuracy and reduce false positives.