

Ahood Alshahrani

Machine Learning-Based Intrusion Detection for IoT Networks: A Literature Review

Introduction

The Internet of Things (IoT) connects billions of devices worldwide, enabling automation, data sharing, and intelligent control. However, as IoT networks grow, they become vulnerable to cyberattacks due to their distributed nature and limited computational resources. Traditional security systems are not efficient enough to detect complex or novel attacks in such environments. Machine Learning (ML) offers a promising solution for intrusion detection systems (IDS) that can analyze patterns, detect anomalies, and identify malicious activities in IoT networks.

A Deep Learning-Based Intrusion Detection System for IoT Networks (Khan et al., 2020)

Summary: This study proposed a Convolutional Neural Network (CNN)-based IDS that detects both known and unknown attacks in IoT environments. The model was trained on the NSL-KDD dataset and achieved an accuracy of 98.2%. It demonstrated superior detection of Denial-of-Service (DoS) and probing attacks compared to traditional classifiers.

Critical Analysis: The study is innovative due to its deep learning approach; however, its dependence on an older dataset limits its applicability to modern IoT traffic. The lack of testing on real IoT devices is another limitation.

Lightweight Intrusion Detection for IoT Using Random Forest and Feature Selection (Ahmed et al., 2021)

Summary: The authors introduced a lightweight IDS using Random Forest with optimized feature selection to reduce computational cost. The system achieved 96.4% accuracy on the CICIDS2017 dataset while maintaining low processing overhead.

Critical Analysis: The study's strength lies in balancing detection accuracy and efficiency, making it suitable for resource-constrained IoT devices. However, it does not handle evolving attack types dynamically.

Federated Learning for Privacy-Preserving Intrusion Detection in IoT (Zhang et al., ٢٠٢٢)

Summary: This research implemented a federated learning-based IDS, enabling multiple IoT devices to collaboratively train a global model without sharing raw data. The approach improved privacy and scalability while maintaining ٩٤% detection accuracy.

Critical Analysis: The main advantage is data privacy and scalability. However, communication overhead and model synchronization present challenges in large IoT deployments.

Hybrid Intrusion Detection Model Using CNN and LSTM for IoT (Rao et al., ٢٠٢٣)

Summary: The study proposed a hybrid deep learning model combining CNN for spatial feature extraction and LSTM for temporal sequence analysis. The hybrid model achieved ٩٩% accuracy in detecting attacks on the BoT-IoT dataset.

Critical Analysis: Combining CNN and LSTM enhanced both accuracy and adaptability. However, training such hybrid models requires high computational power, limiting deployment on edge devices.

بدقة عالية جدًا، لكنه يحتاج طاقة معالجة كبيرة LSTM و CNN) العربية: (نموذج هجين يجمع بين

Transfer Learning-Based IDS for IoT (Hussein et al., ٢٠٢١)

Summary: This research utilized transfer learning to adapt pre-trained models to new IoT attack datasets, minimizing training time and data requirements. The proposed system achieved competitive accuracy with significantly reduced computational effort.

Critical Analysis: Efficient in adapting to new environments but relies on similarity between source and target datasets, which may not always exist.

Explainable AI for IoT Intrusion Detection (Wang et al., ٢٠٢٤)

Summary: This study incorporated explainable AI (XAI) techniques to interpret ML-based intrusion decisions, increasing transparency and trust. The model used SHAP values to explain predictions and achieved ٩٥,٧% accuracy.

Critical Analysis: Provides transparency and accountability in IDS, but slightly compromises performance due to additional computation for explainability.

Connections and Conflicts

All papers emphasize using ML to improve IoT security through anomaly detection, achieving high accuracy. Most focus on balancing detection performance with computational efficiency. Conflicts appear in the choice of methods: deep learning provides better accuracy, while lightweight or federated models focus on efficiency and privacy.

Synthesis Table

Author (Year)	Method	Dataset	Accuracy	Strengths	Limitations
Khan et al. (٢٠٢٠)	CNN	NSL-KDD	٩٨,٢%	High detection rate	Outdated dataset
Ahmed et al. (٢٠٢١)	Random Forest	CICIDS٢٠١٧	٩٦,٤%	Lightweight	Not adaptive
Zhang et al. (٢٠٢٢)	Federated Learning	Custom IoT Data	٩٤%	Privacy & scalability	Comm. overhead
Rao et al. (٢٠٢٣)	CNN + LSTM	BoT-IoT	٩٩%	High accuracy	High computation
Hussein et al. (٢٠٢١)	Transfer Learning	UNSW-NB١٥	٩٧%	Fast training	Data similarity needed
Wang et al. (٢٠٢٤)	XAI + ML	IoT-٢٣	٩٥,٧%	Explainability	Performance cost

Discussion

The reviewed literature reveals a significant evolution in ML-based IoT intrusion detection. Early studies relied on traditional algorithms, while recent ones leverage deep and hybrid learning models.

The trade-off between accuracy, explainability, and computational cost remains a key research challenge.

Future work should explore adaptive models that can learn in real-time while preserving device efficiency and data privacy.

References

Khan, M. et al. (۲۰۲۰). Deep Learning-Based IDS for IoT Networks. IEEE Access.

Ahmed, A. et al. (۲۰۲۱). Lightweight IDS Using Random Forest. Elsevier Computers & Security.

Zhang, L. et al. (۲۰۲۲). Federated Learning for Privacy-Preserving IDS. IEEE Internet of Things Journal.

Rao, S. et al. (۲۰۲۳). Hybrid CNN-LSTM IDS for IoT. Springer Journal of Network Security.

Hussein, R. et al. (۲۰۲۱). Transfer Learning for IoT Security. Journal of Information Security and Applications.

Wang, X. et al. (۲۰۲۴). Explainable AI for IoT IDS. IEEE Transactions on Dependable and Secure Computing.