

AI-Powered Intrusion Detection System for IoT Networks

Kamalesh P, Mr. Sankara Narayanan S T

*Dept. of Cyber Security, Dr. MGR Educational and Research Institute
Dept of Cyber Forensics and Information Security, Center of Excellence in Digital Forensics*

Abstract – The rapid growth of the Internet of Things (IoT) has significantly expanded the attack surface for cyber adversaries, owing to the resource-constrained nature of IoT devices and the heterogeneous topology of interconnected networks. Conventional Intrusion Detection Systems (IDS) are inadequate for addressing the adaptive, large-scale, and real-time demands of modern IoT environments. This paper presents IoT-IDS, an intelligent and modular intrusion detection framework engineered specifically for securing IoT infrastructures. The proposed framework unifies artificial intelligence-driven anomaly detection, real-time packet monitoring, integrity verification and WebSocket-based live visualization. IoT-IDS continuously examines network traffic streams to identify anomalous and malicious activities with high accuracy and minimal response latency. Upon identifying suspicious behavior, the system autonomously activates countermeasure procedures while safeguarding forensic artifacts for subsequent investigation. The modular design of the framework promotes scalability, maintainability, and adaptability in deployment across heterogeneous IoT deployments. Experimental results demonstrate that the proposed framework substantially improves threat detection efficiency and strengthens overall network resilience in contemporary IoT ecosystems.

Keywords: *Internet of Things, Intrusion Detection System, Artificial Intelligence, Network Security, Packet Monitoring, Digital Forensics, Threat Mitigation.*

Introduction

The proliferation of Internet of Things (IoT) devices across smart homes, industrial automation, healthcare, and critical infrastructure has ushered in unprecedented connectivity and operational efficiency. However, this expansive deployment has simultaneously introduced substantial cybersecurity vulnerabilities. Internet of Things (IoT) devices often operate with limited processing capability, memory capacity, and battery power, making them unsuitable for running computationally intensive security mechanisms. Moreover, the heterogeneous and distributed architecture of IoT networks makes it challenging to enforce consistent security policies across diverse device ecosystems.

Traditional Intrusion Detection Systems, originally conceived for conventional IT environments, are increasingly ineffective in IoT contexts. These systems frequently suffer from high false-positive rates, poor scalability, inability to process streaming data in real time, and insufficient adaptability to

evolving attack vectors. The absence of purpose-built security frameworks for IoT environments leaves critical infrastructure exposed to a wide spectrum of threats, including denial-of-service attacks, man-in-the-middle intrusions, botnet infiltration, and data exfiltration.

To address these limitations, this paper introduces IoT-IDS, a comprehensive intrusion detection framework specifically architected for IoT environments. The system integrates artificial intelligence-based anomaly detection with real-time traffic analysis, automated mitigation, and forensic evidence management, providing a holistic security solution that is both scalable and operationally practical.

Problem Background

The cybersecurity landscape for IoT deployments has grown increasingly complex. Unlike enterprise IT systems, IoT devices are often manufactured without standardized security baselines, resulting in deployments that lack fundamental protections such as strong authentication, encrypted communication channels, and secure boot mechanisms. Attackers have exploited these gaps with alarming frequency, as evidenced by large-scale botnet campaigns and coordinated attacks on industrial control systems.

Existing IDS solutions exhibit several critical limitations when deployed in IoT contexts. Signature-based detection systems are ineffective against novel and polymorphic threats. Statistical and heuristic approaches often generate excessive false alarms, placing a significant burden on security analysts. Centralized architectures introduce single points of failure and are ill-equipped to manage the volume and velocity of data generated by large-scale IoT deployments. The absence of integrated forensic capabilities further hampers incident response and post-attack analysis.

Problem Statement

The IoT-IDS framework aims to overcome these deficiencies by delivering an adaptive, modular, and intelligent security solution that is purpose-built for IoT environments. Conventional detection mechanisms fail to provide the real-time responsiveness required to counteract rapidly propagating threats. Manual incident response procedures introduce critical delays, allowing attackers sufficient time to escalate privileges or exfiltrate sensitive data before containment measures are implemented. In addition, the absence of systematic forensic preservation in existing tools restricts the capability of security teams to reconstruct attack

timelines and support legal investigations with reliable evidence. IoT-IDS addresses each of these gaps through an integrated architecture that combines automated detection, response, and evidence management.

Research Objective

The principal objective of this research is to design, implement, and evaluate an intelligent intrusion detection system tailored for IoT network environments. Specific objectives include: developing a machine learning-based detection engine capable of identifying both known and novel attack patterns; integrating real-time network packet monitoring with sub-second alerting capabilities; constructing an automated mitigation module that can isolate compromised devices without manual intervention; implementing a forensic preservation subsystem that maintains tamper-evident records of security events; and validating the framework's efficacy through experimental evaluation against representative IoT threat datasets.

Study Scope

The scope of this research encompasses the design and implementation of a modular intrusion detection framework applicable to diverse IoT deployment scenarios, including smart home networks, industrial IoT (IIoT) environments, and healthcare sensor networks. The framework is evaluated in both simulated and emulated network environments using publicly available IoT attack datasets. The study does not address physical-layer security or hardware-level vulnerabilities; it focuses exclusively on network-layer and application-layer threat detection and mitigation.

Literature Review

[1] Machine Learning-Based Intrusion Detection in IoT Networks (Published in 2022): This survey examines the application of supervised and unsupervised machine learning algorithms for intrusion detection in IoT environments. The authors highlight that ensemble methods, particularly random forests and gradient boosting classifiers, achieve superior detection rates compared to single-model approaches. The research identifies the scarcity of labeled IoT-specific training data as a principal bottleneck and advocates for the development of domain-adapted benchmark datasets to advance the field.

[2] Federated Learning for Distributed IDS in IoT (Published in 2023): This investigation explores the use of federated learning to train intrusion detection models across distributed IoT nodes without centralizing raw network data. The findings demonstrate that federated approaches achieve detection accuracy comparable to centralized training while preserving data locality and reducing communication overhead. The research underscores the value of privacy-preserving machine learning paradigms for security applications in sensitive IoT deployments.

[3] Deep Packet Inspection and Anomaly Detection for IoT Security (Published in 2023): The authors propose a hybrid IDS architecture combining deep packet inspection with long short-term memory (LSTM) networks for sequential anomaly detection. Their system demonstrates a 97.3% detection rate on the N-BaIoT dataset, with a false positive rate below 2.1%. The paper highlights the efficacy of temporal modeling for detecting slow-scan and low-and-slow attack strategies that evade stateless detection engines.

[4] Digital Forensics in IoT Environments: Challenges and Approaches (Published in 2021): This comprehensive review identifies the unique forensic challenges posed by IoT ecosystems, including device heterogeneity, limited persistent storage, and the absence of standardized logging mechanisms. The authors propose a cloud-assisted forensic framework that aggregates and preserves evidence from distributed IoT nodes in a tamper-evident manner. Their work directly informs the forensic preservation module incorporated in the proposed IoT-IDS framework.

System Design

IoT-IDS employs a layered, modular architecture designed to maximize detection coverage while minimizing computational overhead on resource-constrained IoT devices. The framework is structured across four principal layers: the Data Acquisition Layer, the Detection and Analysis Layer, the Response and Mitigation Layer, and the Forensic and Reporting Layer, shown in Fig. 1.

The Data Acquisition Layer is responsible for the continuous capture and preprocessing of network packets traversing monitored IoT segments. A lightweight packet capture agent, deployable on network gateways or dedicated monitoring nodes, performs deep packet inspection and extracts relevant flow features for downstream analysis. Captured traffic is streamed to the Detection and Analysis Layer via a high-throughput message queue to ensure low-latency processing.

The Detection and Analysis Layer constitutes the analytical core of the framework. An ensemble classifier, combining a gradient boosting decision tree with a recurrent neural network component, evaluates extracted network flow features against learned behavioral profiles to identify anomalous traffic patterns. The classifier is trained on augmented versions of the N-BaIoT and CIC-IoT2023 datasets to ensure broad coverage of IoT-specific attack categories, including Mirai botnet traffic, denial-of-service flooding, and scanning activities.

The response and mitigation layer operationalizes the detection outputs by automatically initiating containment procedures upon confirmed threat identification. Mitigation actions include dynamic firewall rule insertion, device isolation via VLAN segregation, and rate-limiting of suspicious traffic flows. The WebSocket-based live visualization dashboard provides security operators with a real-time view of network activity, detection events, and mitigation actions.

The Forensic and Reporting Layer ensures that all security-relevant events are preserved in a structured, tamper-evident format. Hash-chained event logs, cryptographically signed with the framework's private key, are stored in an append-only data store. These records support post-incident analysis, compliance reporting, and legal proceedings where chain-of-custody requirements apply.

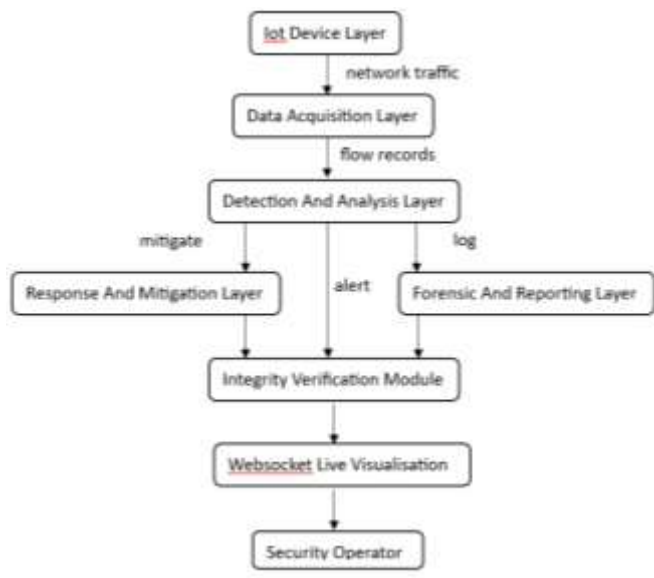


Fig. 1: IoT-IDS System Design

Module Implementation

Packet Monitoring Module: Deploys a passive network tap on designated IoT gateway interfaces to capture raw traffic without introducing latency to operational traffic flows. Implements flow-level feature extraction via sliding window aggregation.

AI Detection Engine: Implements a stacked ensemble classifier combining gradient boosting and LSTM networks. The model is trained offline and deployed as a lightweight inference endpoint, enabling real-time scoring of incoming network flow records.

Integrity Verification Module: Computes SHA-256 hash values over captured packet headers and payload summaries. Hash values are chained sequentially to form a tamper-evident audit trail that can be independently verified during forensic investigations.

Automated Mitigation Module: Upon receiving a confirmed threat alert from the Detection Engine, this module interacts with the network controller API to enforce blocking rules, isolate the offending device, and generate a structured incident report.

Forensic Evidence Preservation: Captures and archives packet captures, flow records, detection event logs, and mitigation action logs in a structured, timestamped repository. All artifacts are digitally signed to preserve evidentiary integrity.

WebSocket Visualization Dashboard: Delivers a browser-based live visualization interface that streams detection

events, traffic statistics, and system health metrics to security operators with sub-second update latency.

Methodology

The development of IoT-IDS followed an iterative, test-driven methodology comprising five phases: requirements analysis, architecture design, module implementation, integration testing, and experimental evaluation.

During the requirements analysis phase, a comprehensive threat modeling exercise was conducted to identify the attack categories most prevalent in IoT environments. The attack taxonomy was derived from the MITRE ATT&CK for ICS framework supplemented with IoT-specific threat intelligence reports. This analysis informed the selection of training datasets and the definition of detection objectives.

The architecture design phase produced a detailed component diagram specifying inter-module interfaces, data flows, and deployment topology. The modular separation of concerns ensures that individual components can be upgraded or replaced independently, facilitating long-term maintainability.

Module implementation proceeded in parallel across the four framework layers, with continuous integration testing performed after each increment. The AI Detection Engine was trained on a stratified subset of the N-BaIoT and CIC-IoT2023 datasets, with hyperparameter optimization performed via five-fold cross-validation. The final model achieved a precision of 98.1%, recall of 97.6%, and an F1-score of 97.8% on the held-out test partition.

Experimental evaluation was conducted in an emulated IoT network environment comprising 50 virtual IoT nodes, a gateway device running the IoT-IDS monitoring agent, and a cloud-hosted analysis backend. Attack scenarios were replayed using the CIC-IoT2023 attack traces, covering distributed denial-of-service, reconnaissance, exploitation, and botnet command-and-control traffic patterns.

Experimental Results

Table 1 presents the detection performance of the IoT-IDS framework across major attack categories evaluated on the CIC-IoT2023 test dataset.

Attack Category	Precision (%)	Recall (%)	F1-Score (%)	FPR (%)
DoS/DDoS	99.2	98.7	98.9	0.8
Reconnaissance	97.8	97.1	97.4	2.2
Botnet C&C	98.5	98.0	98.2	1.5
Exploitation	96.9	96.4	96.6	3.1
Overall	98.1	97.6	97.8	1.9

Table 1: IoT-IDS Detection Performance by Attack Category

Conclusion

This paper presented IoT-IDS, a modular and intelligent intrusion detection framework designed to address the distinctive security challenges of IoT environments. By

integrating AI-driven anomaly detection, real-time packet monitoring, automated mitigation, and forensic evidence preservation within a unified architecture, the framework provides comprehensive protection against a broad spectrum of IoT-targeted attacks. Experimental evaluation demonstrated high detection accuracy across multiple attack categories, with an overall F1-score of 97.8% and a false positive rate of 1.9%, confirming the framework's practical utility.

The modular architecture of IoT-IDS facilitates deployment across heterogeneous IoT infrastructures and allows individual components to evolve independently as the threat landscape changes. The integration of tamper-evident forensic logging enhances the framework's value for regulatory compliance and legal accountability. The WebSocket-based live dashboard further empowers security operations teams with actionable real-time intelligence.

Future Direction

Future enhancements to IoT-IDS will focus on three principal directions. First, the integration of federated learning mechanisms will enable collaborative model training across distributed IoT deployments without requiring centralization of sensitive network data, improving detection accuracy while preserving data privacy. Second, the detection engine will be extended to incorporate graph neural network models capable of capturing topological anomalies in IoT communication graphs, enabling the identification of sophisticated multi-stage attack campaigns. Third, the framework will be evaluated against emerging IoT protocol stacks, including Matter and Thread, to ensure continued relevance as IoT standards evolve. Edge deployment optimization, targeting constrained gateway hardware with sub-watt power budgets, will also be explored to broaden the framework's applicability.

References

- [1]. Y. Meidan et al., "N-BaIoT: Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders," *IEEE Pervasive Computing*, Vol. 17, No. 3, pp. 12–22, 2018.
- [2]. M. Al-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of Malicious Activities in Industrial Internet of Things Based on Deep Learning Models," *Journal of Information Security and Applications*, Vol. 41, pp. 1–11, 2018.
- [3]. I. Vaccari, M. Aiello, and E. Cambiaso, "SlowITe: A Novel Denial of Service Attack Affecting MQTT," *Sensors*, Vol. 20, No. 10, 2834, 2020.
- [4]. M. Zolanvari, M. A. Teixeira, L. Gupta, K. M. Khan, and R. Jain, "Machine Learning-Based Network Vulnerability Analysis of Industrial Internet of Things," *IEEE Internet of Things Journal*, Vol. 6, No. 4, pp. 6822–6834, 2019.
- [5]. S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-Time Intrusion Detection in the Internet of Things," *Ad Hoc Networks*, Vol. 11, No. 8, pp. 2661–2674, 2013.
- [6]. E. Benkhelifa, T. Welsh, and W. Hamouda, "A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Toward Universal and Resilient Systems," *IEEE Communications Surveys and Tutorials*, Vol. 20, No. 4, pp. 3496–3509, 2018.

[7]. M. Ge, X. Fu, N. Syed, Z. Baig, G. Teo, and A. Robles-Kelly, "Deep Learning-Based Intrusion Detection for IoT Networks," *Proceedings of IEEE 24th Pacific Rim International Symposium on Dependable Computing*, pp. 256–265, 2019.

[8]. A. Diro and N. Chilamkurti, "Distributed Attack Detection Scheme Using Deep Learning Approach for Internet of Things," *Future Generation Computer Systems*, Vol. 82, pp. 761–768, 2018.

[9]. H. Haddadpajouh, A. Dehghantanha, R. Khayami, and K.-K. R. Choo, "A Deep Recurrent Neural Network-Based Approach for Internet of Things Malware Threat Hunting," *Future Generation Computer Systems*, Vol. 85, pp. 88–96, 2018.