Toward AI-driven Monitoring And Malware Detection Framework For IoT And Edge Systems

Ehsan Saeedizade[i], Jake Lyon[ii], Shamik Sengupta[i]
University of Nevada, Reno[i], The College of Wooster [ii]

Introduction and Motivation

IoT and edge environments are increasingly critical to public services and industry, yet they remain highly vulnerable due to scale, heterogeneity, and limited resources.

- **65–80% of cloud security incidents originate from misconfigurations**, not zero-day exploits
- A major **August 2025 ransomware attack on Nevada state systems** caused service disruption in DMV and other agencies
- Industry reports show:
  - **188% increase in cloud-based incidents (2024–2025)**
  - **300% daily attack increase in SOC operations**
  - Average **breach cost exceeds $2.4M**

These trends show that **security failures are no longer exceptional events** but recurring operational risks.

Problem Statement

Despite extensive investment in security tools, they face fundamental limitations:

- **Fragmented monitoring** across hosts, networks, and cloud layers
- **High-overhead data collection** is unsuitable for resource-constrained devices
- **Rule-based detection** systems that:
  - Do not adapt to **evolving threats**
  - Generate **excessive alerts** and noise
  - Require **significant manual SOC effort**

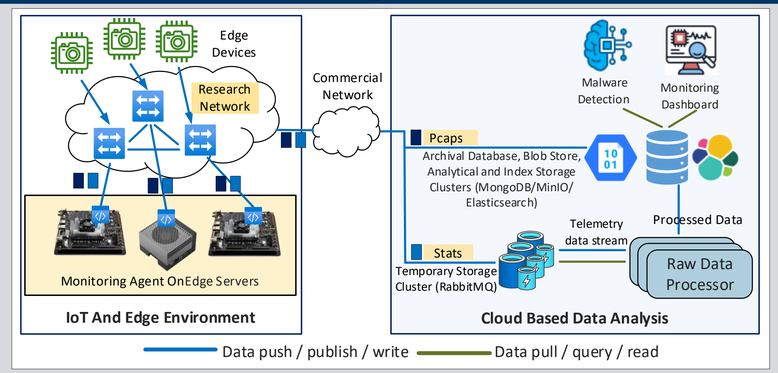
Industry reports indicate that **41% of organizations rely on more than 10 security vendors**, requiring analysts to **correlate alerts across multiple dashboards** and tools, often **spending up to one hour per alert**.

Proposed Solution

We propose an **AI-driven monitoring and anomaly detection framework** that integrates:

- ✓ **Lightweight, continuous monitoring** at the edge
- ✓ **Scalable data ingestion and visualization** in the cloud
- ✓ **Machine learning–based malware** detection and evaluation under data scarcity and temporal drift

Monitoring Framework

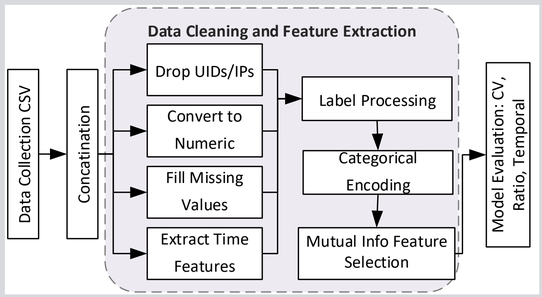


Lightweight monitoring agents are deployed on edge servers to capture system and network behavior with minimal overhead.

- ✓ **Host-level** telemetry (CPU, memory, and disk usage)
- ✓ **Network-level** monitoring (TCP/UDP statistics)
- ✓ Continuous **PCAP collection** from network interfaces

Agents publish **Stats** and **PCAPs** to a scalable **ELK pipeline** and **blob store** for further analytics

AI-driven Malware Detection Workflow

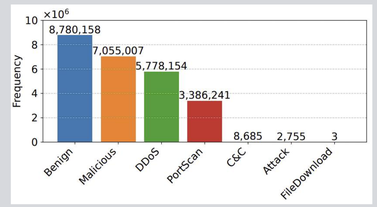


Flow-level **features extracted** from PCAP files are stored in CSV files containing packet statistics, timing information, and protocol metadata. All **CSV files are concatenated** into a unified dataset, **session-specific identifiers** (e.g., IPs and UIDs) and **missing values are removed**, and **features are converted** to numeric form. **Temporal features** (e.g., hour-of-day and day-of-week) are derived from timestamps. **Labels are encoded** to support both binary and multiclass classification tasks. **Mutual information gain analysis is applied for feature selection**, and all numerical **features are normalized using Min–Max scaling**. The resulting dataset is evaluated using multiple **machine learning models under different evaluation settings**.

Results

The framework is evaluated on the sampled **IoT-23 dataset**, a labeled collection of benign and malicious IoT network traffic, under three scenarios to assess the **accuracy**, **dataset size efficiency**, and **robustness** of ML models to evolving threats.

A. Label Distribution

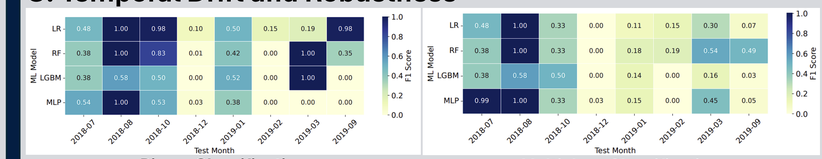


B. Performance and Sensitivity to Training Data Size

Train Ratio	Binary F1-score				Multiclass F1-score			
	LR	RF	LGBM	MLP	LR	RF	LGBM	MLP
0.3	0.9853	0.9987	0.9987	0.9977	0.6125	0.8372	0.5648	0.7227
0.4	0.9853	0.9989	0.9987	0.9977	0.6087	0.8380	0.5439	0.7934
0.5	0.9852	0.9990	0.9987	0.9977	0.6111	0.9797	0.4143	0.7865
0.6	0.9854	0.9991	0.9987	0.9977	0.6064	0.8364	0.4111	0.7942
0.7	0.9853	0.9991	0.9987	0.9977	0.6129	0.9792	0.5169	0.8032
0.8	0.9854	0.9992	0.9987	0.9968	0.6052	0.9769	0.5723	0.8005

Tree-based models provide consistently **strong performance**. **MLP** is a viable alternative when **capturing complex patterns** is essential. **RF consistently leads** across tasks and training sizes. **MLP**'s performance **improves with more data.**

C. Temporal Drift and Robustness



As **malware behavior** and traffic patterns **change over time**, to address temporal drift, it is crucial to **continuously monitor** and **implement adaptive learning strategies**, such as model **fine-tuning**, **online learning**, based on **newly observed data**.

References

[1] J. Vitorino, R. Andrade, I. Prac¸a, O. Sousa, and E. Maia, "A comparative analysis of machine learning techniques for iot intrusion detection," in International Symposium on Foundations and Practice of Security. Springer, 2021, pp. 191–207.
[2] S. Garcia, A. Parmisano, and M. J. Erquiaga, "Iot-23: A labeled dataset with malicious and benign iot network traffic (version 1.0.0) [data set]. zenodo," Jan. 2020. [Online]. Available: https://doi.org/10.5281/zenodo.4743746
[3] J. Ferdous, R. Islam, A. Mahboubi, and M. Z. Islam, "A survey on ML techniques for multi-platform malware detection: Securing pc, mobile devices, iot, and cloud environments," Sensors (Basel, Switzerland), vol. 25, no. 4, p. 1153, 2025.

The work in this study was supported by the NSF under grant numbers #2346755 and #2349092.