The 13th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications
4-6 September, 2025, Gliwice, Poland

A SIEM-Based Framework for Multi-Layer Data Collection and Anomaly Detection in OT-Networks

Jaafer Rahmani[1] , Salva Daneshgadeh Çakmakçı[2] , Kai Oliver Detken[3] , Axel Sikora[4]
[1, 4] ivESK, Offenburg University, Offenburg, Germany, jaafer.rahmani@hs-offenburg.de, axel.sikora@hs-offenburg.de
[2, 3] DECOIT GmbH & Co. KG, Bremen, Germany, daneshgadeh@decoit.de, detken@decoit.de

***Abstract* — The increasing convergence of Information Technology and Operational Technology networks in Industrial Control Systems has introduced new cybersecurity challenges, necessitating robust anomaly detection mechanisms. Despite progress, a significant gap exists in the literature regarding benchmark datasets that comprehensively incorporate data from both OT and IT networks. Existing datasets often focus on isolated network segments and fail to capture the full spectrum of network, host, and protocol activities, thereby lacking the holistic visibility required to detect sophisticated, multi-stage cyberattacks. To address this gap, this paper proposes a SIEM-based framework for generating a comprehensive dataset by integrating data from two fundamental levels of an ICS architecture: the OT field network and the IT monitoring system. By leveraging a SIEM solution as the core of the framework, data from heterogeneous industrial devices are captured using NetFlow, Auditd, and Zeek integrations to extract network, host, and protocol features, respectively. The collected data, including sensor telemetry, host logs, and protocol events, are systematically aggregated and correlated to provide a global view of normal and anomalous behaviors. This dataset not only facilitates the development and evaluation of a hybrid anomaly detection framework, combining rule-based SIEM alerts with autoencoder-based machine learning at the edge, but also lays the foundation for more effective, SIEM-driven defenses. Federated learning is discussed as a future prospect to further enhance privacy and scalability.**

Keywords* — *IIoT security, hybrid anomaly detection, SIEM, dataset generation, multi-layer telemetry, Operational Technology, Information Technology

I. Introduction

Traditional Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) solutions struggle with the effectiveness in Industrial Internet of Things (IIoT) due to device distribution, resource constraints, and heterogeneity. Most IIoT anomaly detection research relies on IT network traffic, neglecting its OT counterpart as well as application-layer interactions which are critical for identifying sophisticated attacks (e.g., lateral movement, persistent threats).

Centralized security solutions raise scalability and performance issues when handling large IIoT telemetry volumes, increasing computational costs and latency. Cyber threats targeting IIoT, like the LogicLocker ransomware [1] and Mirai botnet [2], highlight these vulnerabilities.

To address these challenges, we propose a hybrid anomaly detection framework that integrates rule-based SIEM techniques with machine learning–driven anomaly detection. A centralized SIEM aggregates logs from IT and OT components and applies predefined detection rules, mapped to the MITRE ATT&CK framework, to rapidly identify known threats. Concurrently, lightweight unsupervised models, specifically autoencoders, run at the edge, learning normal behavior from IIoT traffic and telemetry, and flagging deviations in real time. This dual approach leverages the precision of signature-based detection and the adaptability of behavioral analytics, delivering comprehensive, low-latency threat identification tailored for distributed, resource-constrained IIoT environments. Federated learning is considered as a future extension to enable collaborative model improvements without sharing raw data.

A. Main Contributions

This paper presents key contributions centered on a SIEM-based framework:

1) **Multi-Layer Dataset Generation** We consolidate host-based logs (process metrics, file activity, authentication events, and security alerts) captured by auditd, with protocol data captured by Zeek and network flows captured by NetFlow, addressing fragmented telemetry for improved anomaly detection.
2) **Hybrid Anomaly Detection:** We propose a hybrid approach combining MITRE ATT&CK-mapped rule-based SIEM detection and a machine learning autoencoder module deployed at the edge, ensuring both rapid identification of known threats and adaptive detection of novel anomalies.
3) **Practical Deployment and Benchmarking:** Our framework supports real-world industrial settings,

This work was executed in the project "KISTE - AI-powered SIEM System for Highly Reliable Industrial IoT Networks and Fieldbuses", supported by the German Federal Ministry for Economic Affairs and Climate Action(BMWK), based on a decision of the German Bundestag under grant number "KK5189606RG4".

integrating data from OT and IT networks for centralized analysis and edge-based inference.

4) **Scalable Data Processing Pipeline:** We develop a pipeline transforming raw network, host, and protocol data into actionable features, enabling efficient ingestion, enrichment, and indexing within the SIEM environment.

II. Literature Review

Public IIoT/IoT security datasets (Table I) provide valuable benchmarks but typically capture only isolated views—network flows (NetFlow), host events (Auditd), or protocol messages (e.g., via Zeek)—rather than the end-to-end, multi-layer telemetry needed for comprehensive threat detection. Recent advances in IoT security datasets have demonstrated the limitations of traditional approaches, particularly in industrial environments where multi-modal sensing is critical [12].

Contemporary intrusion detection systems face fundamental architectural challenges when deployed across diverse network environments including cloud computing, virtualized networks, IoT, and industrial control systems. As highlighted in recent comprehensive reviews, the integration of AI and ML technologies has shown promise but continues to struggle with scalability, performance optimization, and the persistent challenge of reducing false positives and negatives [13].

Effective IIoT attack detection further faces three intertwined challenges. First, **multi-modal data fusion** requires consistent feature extraction across heterogeneous sources (network, host, sensor, protocols). The complexity of this challenge is amplified in edge-of-things environments where traditional signature-based and anomaly detection approaches must adapt to resource-constrained deployment scenarios [13]. Second, **timeliness and scalability** demand lightweight models capable of real-time inference on resource-constrained edge devices, as demonstrated by federated learning approaches that achieve sub-20ms inference latency while maintaining high detection accuracy [12]. Third, **protocol awareness** is often lacking: many ML methods treat all traffic uniformly and ignore IIoT-specific semantics (e.g., Modbus function codes, MQTT topics), reducing detection precision for subtle control-plane attacks.

To address these, hybrid architectures that combine rule-based SIEM alerts (e.g., MITRE ATT&CK–mapped correlations) with unsupervised edge-deployed autoencoders have shown promise. Modern SIEM correlation engines utilizing advanced pattern matching libraries like Hyperscan have demonstrated significant performance improvements in multi-layered attack detection, achieving parallel log scanning capabilities that can process thousands of events per second while maintaining low latency [14]. However, their validation is hindered by the absence of high-fidelity, cross-layer datasets and by inference engines that understand protocol semantics.

Contemporary approaches in intrusion detection have increasingly adopted ensemble learning methods, combining deep learning techniques with traditional machine learning algorithms. Ensemble frameworks utilizing artificial neural networks, support vector machines, and random forest meta-classifiers have achieved detection accuracies exceeding 99% on benchmark datasets, while incorporating explainable AI techniques to address the black-box nature of deep learning models [15]. These systems demonstrate the effectiveness of hybrid approaches in balancing detection performance with interpretability requirements, a critical consideration for industrial environments where false positives can trigger costly operational disruptions.

We thus identify three key gaps that align with broader challenges identified in recent IDS literature [13]:

- **Lack of Integrated Datasets:** No public dataset unifies flow, host, sensor, and protocol telemetry for end-to-end IIoT modeling, despite the recognized need for comprehensive test environments that span cloud, IoT, and industrial control system scenarios.
- **Poor Cross-Domain Generalization:** Models trained on narrow or synthetic data fail to adapt to diverse, multi-stage attack chains, despite advances in federated learning approaches that handle non-IID data distributions in distributed IoT environments [12]. This challenge is particularly acute for zero-day attacks that exploit previously unknown vulnerabilities.
- **Edge Deployment Constraints:** Few approaches consider the CPU, memory, and energy limits of IIoT endpoints, hindering real-time, on-device detection, although recent federated learning frameworks have shown promise with deployment on resource-constrained devices like Raspberry Pi and Jetson Nano [12].

These observations motivate our SIEM-centric, hybrid anomaly detection framework, which (i) generates a unified multi-layer dataset addressing the comprehensive testing needs identified in current IDS research [13], (ii) fuses SIEM rule-based alerts with edge autoencoder inference for low-latency response, leveraging advanced correlation engines for parallel log scanning [14], and (iii) supports realistic, multi-stage attack scenarios for rigorous evaluation using ensemble learning principles that balance accuracy with explainability [15].

III. Proposed Framework Design

A. Framework Components:

Our proposed framework addresses the identified challenges by tightly integrating SIEM and AI-based anomaly detection to generate a comprehensive, multi-layer dataset. The corresponding architecture is depicted in Fig. 1. Key components include:

Table I. COMPARISON OF PUBLIC IIOT/IOT SECURITY DATASETS

Dataset	Data Features	Attack Types	Format	Limitations
IoTID20 [3]	Flow data (packet header-derived)	D/DoS, MITM, scanning	CSV	Lacks sensor, host and modbus/MQTT protocol data
Kitsune [4]	Flow data (packet header-derived)	DDoS, MITM, injection, recon.	pcap, CSV	Lacks sensor, host and modbus/MQTT protocol data; no raw traffic packets
PAN2020_ICS [5]	Sensor telemetry, actuator states, HMI, PLC cmds, Modbus/TCP logs	Unauthorized access, Modbus attacks, control manipulation, replay	NA	Closed access limits utility
ICS Security [6]	SCADA time-series	Cmd injection, replay, unauthorized access	CSV	Lacks network and host data
TON_IoT [7]	Telemetry, flow, OS logs	DoS, DDoS, ransomware, web attacks	Logs, CSV	Lacks modbus/MQTT protocol data and limited host data
CIC IoT 2023 [8]	Flow data	D/DoS, recon, brute force, spoofing, Mirai	pcap, CSV	Lacks sensor, host and modbus/MQTT protocol data; no raw traffic packets
CIC APT 2024 [9]	Flow and host logs	APT (collection, exfiltration, discovery, lateral, evasion, persistence)	pcap, CSV, graphs	Lacks sensor and modbus/MQTT protocol data. Limited host data in the form of provenance logs
Edge-IIoTset [10]	Sensor data, alerts, resource logs, flow data	DoS, MITM, injection, malware	pcap, CSV	Lacks sensor and host data
X-IIoTID [11]	Flow, host logs, alerts	MITRE ATT&CK for ICS	CSV	Lacks sensor and modbus/MQTT protocol data
Our Work	Flow, sensor, host data, alerts, logs	Attacks mapped to MITRE ATT&CK for ICS	CSV, pcap	Under development; aims to integrate correlated telemetry

- **Multi-Layer Data Collection:** The framework employs Elastic Agents integrated with Zeek, NetFlow, and Auditd across industrial control devices in the OT field network. This setup captures:
  - **Network Layer (NetFlow):** Captures source/destination IPs, ports, flow duration, packet/byte counts, and flow direction—vital for identifying traffic patterns and anomalies.
  - **Protocol Layer (Zeek):** Extracts protocol-specific details including Modbus transactions (function codes, register addresses, request/response messages) and other protocol events (HTTP, DNS, SSL/TLS) to detect misuse or subtle attacks.
  - **Host Layer (Auditd):** Records host-level events such as process creation, file access/modifications, authentication events, and security alerts, critical for detecting insider threats and lateral movement.

  Correlating these diverse data sources, the SIEM-based framework consolidates cross-layer telemetry into a rich dataset for anomaly detection.
- **Edge-Centric Data Processing:** Lightweight processing on edge devices (e.g., Raspberry Pis, IoT sensors, HMI interfaces) enables initial filtering and real-time responsiveness, mitigating resource constraints while ensuring high-fidelity data capture.
- **Integrated Attack Simulation with MITRE Caldera:**
  - **Adversary Emulation Framework:** The framework leverages MITRE Caldera—an open-source adversary emulation platform [16]—configured with OT-specific plugins (e.g., `CALDERA-for-ICS`) to simulate multi-stage cyberattacks aligned with MITRE ATT&CK for ICS. This replaces simplistic fuzzing with behavior-driven threat replication.
  - **OT Attack Vector Simulation:** Caldera executes ICS-targeted tactics including:
    - **Initial Access (TA0101):** Phishing campaigns against HMIs or engineering workstations using malicious ladder logic files.
    - **Lateral Movement (TA0108):** Protocol exploitation (e.g., S7Comm, Modbus/TCP) to pivot between PLCs and SCADA servers.
    - **Impact (TA0109):** Manipulation of safety instrumented systems (SIS) or ransomware deployment (e.g., LogicLocker-style payloads).
  - **Key Advantages:**
    - **ATT&CK Alignment:** All activities are tagged with MITRE technique IDs (e.g., T0883: *Modbus/TCP Command Injection*), enabling supervised learning with threat intelligence context.
    - **Reproducible Scenarios:** Pre-built Caldera profiles ensure standardized benchmarking across ICS environments.
    - **Behavioral Fidelity:** Emulates attacker dwell time (e.g., reconnaissance $\rightarrow$ exploitation $\rightarrow$ persistence phases) missing in synthetic anomaly generators.

  Implementation: Caldera agents deploy on OT boundary devices (e.g., HMIs) to execute attack playbooks while logging all activities into Elastic-

search via Elastic Agents. This generates labeled alerts where each entry maps to ATT&CK tactics and techniques, host/network observables, and protocol-layer payloads.

- **Hybrid Data Analysis and Federated Learning Prospect:** Data is ingested by Elastic Agents and analyzed with Elastic Security using both rule-based detection (aligned with the MITRE ATT&CK framework) and AI-based techniques. In parallel, a prospective FL module at the PLC level is planned, where local quantized autoencoder models optimized for resource-constrained PLCs, learn normal operational patterns and share model updates (without transmitting raw data) to a central aggregator. This dual approach is expected to enhance detection accuracy and responsiveness.

B. Data Pipeline

Our robust data pipeline transforms raw data into actionable features through the following stages:

1) **Data Collection and Ingestion:** Elastic Agents at the network edge capture raw network packets, protocol messages, and host logs via Zeek, NetFlow, and Auditd. Initial parsing with personalized Elastic Agents ensure that only relevant data is forwarded.
2) **Data Enrichment and Preprocessing:** The raw data is transmitted to a central logging infrastructure and ingested into Elasticsearch using tailored pipelines (via native elastic ingest nodes). This stage involves:
   - **Normalization:** Standardizing log formats from diverse sources.
   - **Parsing:** Extracting key-value pairs, timestamps, and identifiers using Elasticsearch's JSON mappings.
   - **Enrichment:** Augmenting data with contextual information (e.g., geolocation from IP addresses, device identifiers) and mapping protocol-specific fields into unified feature sets.
3) **Feature Extraction:** Enriched data is processed to extract features critical for anomaly detection. For example:
   - **NetFlow:** Calculating flow duration, packet inter-arrival times, and byte-to-packet ratios.
   - **Zeek:** Extracting protocol-specific metrics such as transaction IDs, error codes, and response times.
   - **Auditd:** Deriving system call sequences, user session patterns, and anomalous process trees.
4) **Data Storage and Indexing:** Processed datasets are indexed in Elasticsearch for efficient querying and correlation, essential for both historical analysis and real-time threat detection.
5) **Visualization and Export:** Kibana creates interactive dashboards and reports to visualize correlations among network, protocol, host, and application events. Data can also be exported (e.g. as CSV or JSON) for offline analysis, AI model training, or integration with other security systems.

This comprehensive pipeline transforms raw network, host, and protocol data into high-fidelity, actionable features—bridging gaps in existing dataset collection efforts.

C. Security Threat Analysis of Framework Components

The monitoring framework itself is a high-value target. We now examine potential attack vectors and vulnerabilities associated with each pipeline component, along with corresponding mitigation strategies.

- **Elastic Agent Compromise**
  - *Attack Vector:* Adversaries exploit agent misconfigurations to inject false logs or disable telemetry [17].
  - *Mitigations:* Certificate-based authentication; TLS 1.3 mutual authentication; runtime integrity attestation; least-privilege enforcement.
- **Zeek Parser Exploits**
  - *Attack Vector:* Crafted ICS packets cause buffer overflows in protocol parsers, enabling remote code execution or denial-of-service [18].
  - *Mitigations:* Keep parsers up to date; use memory-safe languages for plugins; sanitize inputs; run under unprivileged accounts.
- **Elasticsearch/Kibana Attacks**
  - *Attack Vector:* Unauthenticated indices allow data exfiltration or ransomware encryption; prototype-pollution in visualization modules leads to RCE [19].
  - *Mitigations:* Enforce strong ACLs; segment networks; apply patches promptly; use encrypted backups and immutable indices.
- **Data Poisoning of ML Models**
  - *Attack Vector:* Poisoned training samples degrade model accuracy or implant backdoors [20].
  - *Mitigations:* Track data provenance; detect outliers statistically; apply differential privacy to federated updates; enable model version rollback.
- **Supply-Chain Component Tampering**
  - *Attack Vector:* Malicious code injection in third-party Beats or container images during CI/CD compromises collectors [21].
  - *Mitigations:* Audit SBOMs; sign artifacts; scan dependencies continuously; use air-gapped build environments.
- **Edge Device Intrusions**
  - *Attack Vector:* Physical tampering or weak credentials on edge hardware enable lateral movement into OT networks [22].
  - *Mitigations:* Implement secure boot; encrypt storage; use HSMs for key protection; enforce strict access controls and tamper-evident enclosures.
- **SIEM Rule Evasion & Misconfiguration**

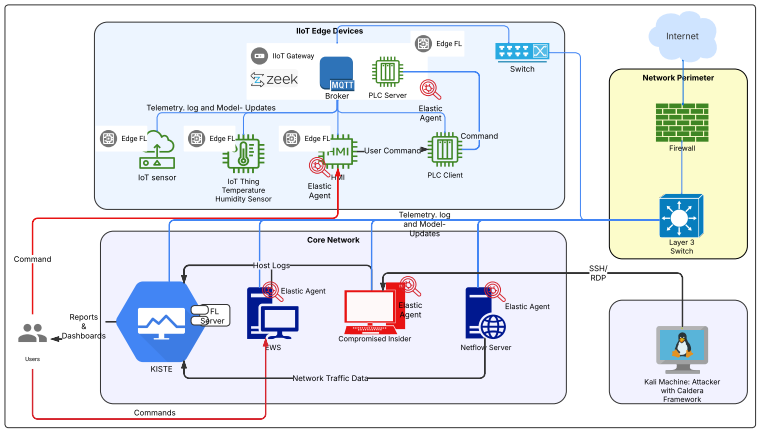

Figure 1. Network Architecture for Federated and SIEM-Based IIoT Security Monitoring

– *Attack Vector:* Crafted traffic patterns bypass static rules; parser mismatches cause silent alert failures [23].
– *Mitigations:* Automate rule-health tests; validate schemas; monitor coverage metrics; supplement with ML-driven anomaly scoring.

IV. Data Analysis

Secure analysis of multi-layer data are achieved via a hybrid detection workflow leveraging SIEM-based rules which are triggered on known IOCs and carriage patterns, while autoencoders at the edge evaluate reconstruction errors for novel anomalies. Correlated alerts are visualized in Kibana and routed to incident responders.

Data analysis therefore integrates rule-based SIEM detection with the autoencoder module. Local ML models are trained on benign data to establish baseline behavior and detect anomalies; and when Federated Learning is enabled, thresholds are determined locally, and aggregated model updates enable detection of both known and novel threats. Regardless of the integration of Federated Learning, this hybrid approach is expected to enhance real-time detection while minimizing latency and integrating multiple data levels.

V. Conclusion and Future Work

This work introduces a SIEM-centric framework augmented with edge-based autoencoder anomaly detection to generate and leverage a comprehensive, multi-layer IIoT dataset. By unifying network, protocol, and host telemetry, we overcome limitations of existing datasets and detection approaches. The proposed hybrid detection methodology demonstrates the potential for enhanced threat visibility across OT and IT network boundaries while maintaining operational continuity in industrial environments. Future planned directions include the following:

- **Real Industrial Environment Validation:** A critical next step involves comprehensive validation in operational industrial environments to assess the framework's effectiveness, reliability, and scalability under real-world conditions. We plan to:
  – Deploy the framework in multiple industrial sectors including manufacturing, energy, and water treatment facilities to evaluate cross-domain generalizability
  – Conduct long-term studies (6-12 months) to assess system stability, resource utilization, and maintenance requirements under continuous operation
  – Collaborate with industrial partners to establish baseline performance metrics and acceptable false positive/negative rates for different operational contexts
  – Evaluate the framework's impact on network latency, device performance, and operational safety systems during peak production periods
  – Develop industry-specific deployment guidelines and best practices based on empirical findings
- **Extended Protocol Support and Attack Scenario Coverage:** To enhance the framework's applicability across diverse industrial environments, future work will expand protocol support and attack scenario modeling:
  – **Additional Industrial Protocol Integration:**
    * Add support for emerging IoT protocols such as CoAP, MQTT-SN, OPC UA, EtherCAT...
    * Create protocol-agnostic detection mechanisms for proprietary industrial communication standards
  – **Advanced Attack Scenario Modeling:**
    * **Supply Chain Attacks:** Develop detection capabilities for compromised firmware, malicious software updates, and third-party component vulnerabilities affecting industrial devices

    - ∗ **Complex Persistent Threats:** Model advanced persistent threats (APTs) with extended dwell times, multi-stage attack chains, and sophisticated evasion techniques
    - ∗ **Insider Threat Scenarios:** Enhanced modeling of malicious insider activities, including credential abuse and privileged access misuse
- **Federated Learning Integration:** Future work will explore integrating federated learning at the edge to enable collaborative model refinement while improving privacy, scalability, and resilience in distributed IIoT environments:
    - Developing privacy-preserving aggregation algorithms suitable for industrial environments
    - Creating secure model update mechanisms that prevent adversarial manipulation
    - Establishing trust frameworks for multi-organization collaborative learning
    - Optimizing federated learning algorithms for resource-constrained industrial devices
- **Advanced Analytics and AI Integration:**
    - Implement explainable AI techniques to provide interpretable threat analysis for industrial operators
    - Develop adaptive threshold mechanisms that automatically adjust to changing operational conditions
    - Integrate graph neural networks for improved understanding of complex industrial network topologies
    - Create predictive maintenance capabilities that correlate security events with equipment health indicators

These research directions will collectively advance the state of industrial cybersecurity monitoring and contribute to the development of more resilient, secure, and scalable OT/IIoT environments.

Declaration on Generative AI

During the preparation of this work, the author(s) used Grammarly in order to: Grammar and spelling check, Paraphrase and reword. After using this tool/service, the author(s) reviewed and edited the content as needed and take(s) full responsibility for the publication's content.

References

[1] D. Formby, S. Durbha, and R. Beyah, "Out of control: Ransomware for industrial control systems," in *RSA conference*, vol. 4, 2017, p. 8.

[2] M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis *et al.*, "Understanding the mirai botnet," in *26th USENIX security symposium (USENIX Security 17)*, 2017, pp. 1093–1110.

[3] R. A. Labib, M. A. Rahman, N. U. Pathan, M. A. Hossain, M. M. Alam, and M. A. Razzaque, "A scheme for generating a dataset for anomalous activity detection in iot networks," in *Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA)*, 2020, pp. 539–552.

[4] Y. Mirsky, T. Doitshman, Y. Elovici, and A. Shabtai, "Kitsune: An ensemble of autoencoders for online network intrusion detection," in *Proceedings of the Network and Distributed System Security Symposium (NDSS)*, 2018.

[5] Y. Pan, J. White, D. C. Schmidt, S. Neema, and J. Sztipanovits, "Industrial control system simulation and data logging for intrusion detection system research," *ACM Transactions on Cyber-Physical Systems*, vol. 4, no. 2, pp. 1–28, 2020.

[6] G. B. Gaggero, A. Armellin *et al.*, "Industrial control system-anomaly detection dataset (ICS-ADD) for cyber-physical security monitoring in smart industry environments," *IEEE Access*, 2024. [Online]. Available: https://dl.acm.org/doi/10.1016/j.cose.2024.104143

[7] N. Moustafa, "A new distributed architecture for evaluating ai-based security systems at the edge: Network ton_iot datasets. sustain. cities soc. 72, 102994 (2021)," 2021.

[8] E. C. P. Neto, S. Dadkhah, R. Ferreira, A. Zohourian, R. Lu, and A. A. Ghorbani, "Ciciot2023: A real-time dataset and benchmark for large-scale attacks in iot environment," *Sensors*, vol. 23, no. 13, p. 5941, 2023.

[9] E. Ghiasvand, S. Ray, S. Iqbal, S. Dadkhah, and A. A. Ghorbani, "Cicapt-iiot: A provenance-based apt attack dataset for iiot environment," *arXiv preprint arXiv:2407.11278*, 2024.

[10] M. A. Ferrag, O. Friha, D. Hamouda, L. Maglaras, and H. Janicke, "Edge-iiotset: A new comprehensive realistic cyber security dataset of iot and iiot applications for centralized and federated learning," *IEEE Access*, vol. 10, pp. 40 281–40 306, 2022.

[11] M. Al-Hawawreh, E. Sitnikova, and N. Aboutorab, "X-iiotid: A connectivity-agnostic and device-agnostic intrusion data set for industrial internet of things," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3962–3977, 2021.

[12] A. Alabdulatif, "Edge-flguard: A federated learning framework for real-time anomaly detection in 5g-enabled iot ecosystems," *Applied Sciences*, vol. 15, no. 12, p. 6452, 2025.

[13] L. Diana, P. Dini, and D. Paolini, "Overview on intrusion detection systems for computers networking security," *Computers*, vol. 14, no. 3, p. 87, 2025.

[14] M. Sheeraz, M. H. Durad, M. A. Paracha, S. M. Mohsin, S. N. Kazmi, and C. Maple, "Revolutionizing siem security: An innovative correlation engine design for multi-layered attack detection," *Sensors*, vol. 24, no. 15, p. 4901, 2024.

[15] A. Alabdulatif, "A novel ensemble of deep learning approach for cybersecurity intrusion detection with explainable artificial intelligence," *Applied Sciences*, vol. 15, no. 14, p. 7984, 2025.

[16] MITRE, "MITRE ATT&CK Caldera Framework," 2023. [Online]. Available: https://github.com/mitre/caldera

[17] J. Smith and M. Lee, "Security analysis of elastic agents in operational environments," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 2, pp. 345–358, 2024.

[18] M. Jones and R. Patel, "Buffer overflow vulnerabilities in ics protocol parsers," in *2023 ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec)*, 2023, pp. 112–124.

[19] X. Wang and R. Gupta, "An empirical study of elasticsearch and kibana security breaches," *Journal of Information Security*, vol. 14, no. 4, pp. 219–237, 2023.

[20] H. Nguyen and L. Tran, "A survey of data poisoning attacks and defenses on machine learning," *ACM Computing Surveys*, vol. 56, no. 1, pp. 1–36, 2024.

[21] K. Tsiknas, K. Demertzis, and C. Skianis, "Cyber threats to industrial iot: A survey on attacks and countermeasures," *Sensors*, vol. 21, no. 4, p. 1123, 2021.

[22] V. Karthik and L. Smith, "Edge computing security challenges in industrial iot environments," *IEEE Internet of Things Journal*, vol. 12, no. 3, pp. 445–460, 2025.

[23] A. García and M. Robinson, "Detecting evasions of siem rules in enterprise networks," in *ArXiv preprint arXiv:2311.10197*, 2023.