INTELLITHINGS
Artificial Intelligence | Internet of Things

Vol. 1 No. 1, 2024 p-ISSN: xxxx-xxxx e-ISSN: xxxx-xxxx https://doi.org/xxxxxxxxx

Lightweight Edge-Based Security System Design for DDoS Attack Mitigation in Industrial IoT Infrastructure

Ata Amrullah

Department of Informatics, Darul Ulum Islamic University, East Java, Indonesia

Received: 2 December 2023
Accepted: 9 January 2024
Published: 29 February 2024

Keywords:
Industrial IoT (IIoT);
Edge Computing;
DDoS Attack Mitigation;
Lightweight Security;
Anomaly Detection.

Corresponding author:
Ata Amrullah
ata@unisda.ac.id

Abstract

The rapid integration of the Industrial Internet of Things (IIoT) into industrial control systems (ICS) has greatly improved automation and operational efficiency, but it has also introduced new cybersecurity risks for critical infrastructure. Distributed Denial of Service (DDoS) attacks, in particular, pose a significant threat by potentially disrupting real-time operations, compromising safety, and causing physical damage. Traditional centralized methods for mitigating DDoS attacks often do not meet the low-latency, high-reliability, and resource-constrained requirements of IIoT environments. To address these challenges, this paper proposes a lightweight, edge-based security system specifically designed for real-time DDoS mitigation in IIoT infrastructures. The proposed architecture leverages the local processing capabilities of edge gateways, integrates efficient machine learning models for anomaly detection, and implements rapid response mechanisms. By focusing on resource efficiency and effective threat neutralization close to the source, the system aims to safeguard the integrity and availability of critical industrial processes. This paper outlines the system's main components, highlights its lightweight design, and discusses ongoing challenges, providing a foundational framework for enhancing IIoT security against the growing landscape of cyber threats.

1. Introduction

The Industrial Internet of Things (IIoT) is revolutionizing industries such as manufacturing, energy, transportation, and critical infrastructure by extending the core concepts of IoT into these sectors [1]. Through the integration of sensors, actuators, control systems, and advanced data analytics, IIoT enables unprecedented automation, predictive maintenance, remote monitoring, and operational efficiency. However, as operational technology (OT) merges with information technology (IT) in IIoT environments, the resulting interconnected systems become increasingly complex and exposed to a wide range of cyber threats [2].

Among these threats, Distributed Denial of Service (DDoS) attacks are particularly concerning for IIoT infrastructure. Unlike attacks focused on stealing data or conducting espionage, DDoS attacks flood systems or networks with excessive traffic, making them inaccessible to legitimate users. In the context of IIoT, the impact of a successful DDoS attack can be severe, potentially causing real-time control processes to fail and halt production, compromising safety systems and leading to physical or environmental harm, disrupting the flow of critical sensor data needed for decision-making, and resulting in significant financial losses due to downtime and recovery efforts [3].

The specific nature of IIoT environments—characterized by the need for real-time,

deterministic operations, the presence of legacy devices with minimal security, and often remote or harsh deployment conditions—makes traditional, centralized security solutions less effective or even impractical. For example, cloud-based DDoS mitigation can introduce unacceptable delays for time-sensitive industrial processes, and routing all traffic through the cloud can be costly in terms of bandwidth [4]. Additionally, installing heavy security software on IIoT devices is often not an option due to their limited resources.

Given these challenges, there is a clear need for lightweight, edge-based security solutions that can detect and mitigate DDoS attacks right at the network's edge—on gateways or local processing units. By moving security intelligence closer to where data is generated and control actions are taken, these systems can provide real-time protection, minimize network overhead, and serve as a first line of defense before threats reach critical controllers or cloud infrastructure.

In this paper, we introduce a lightweight, edge-based security system designed specifically to counter DDoS attacks in IIoT environments. Our main contributions are as follows:

- To present an architectural framework for an edge-focused DDoS mitigation system tailored to IIoT;
- To outline the lightweight design principles and intelligent anomaly detection methods suitable for resource-limited edge devices;
- To discuss strategies for real-time response and mitigation that can be executed directly at the edge;
- To identify key challenges and suggest future research directions for enhancing IIoT security against DDoS threats;

The rest of this paper is organized as follows: Section 2 reviews IIoT security and current DDoS mitigation approaches. Section 3 details the proposed lightweight edge-based security system. Section 4 covers performance evaluation and ongoing challenges. Finally, Section 5 concludes the paper.

2. Background and Related Work

2.1. Industrial IoT (IIoT) Infrastructure and Vulnerabilities

Industrial IoT (IIoT) systems are fundamentally different from traditional IT and consumer IoT networks because of their critical operational roles and strict performance demands [5]. These environments are characterized by the need for real-time, deterministic operations—such as motion control and robotic processes—where even a millisecond of delay can result in catastrophic failures. IIoT infrastructures often incorporate legacy industrial control systems (ICS) and supervisory control and data acquisition (SCADA) components, many of which were not originally designed with modern cybersecurity considerations, leaving them particularly vulnerable to attacks [6]. Communication within IIoT frequently depends on proprietary industrial protocols like Modbus, OPC UA, and PROFINET, which may lack strong security features. Moreover, cyberattacks targeting IIoT can have direct physical consequences, potentially causing equipment damage, environmental harm, or risks to human safety. These unique characteristics make IIoT environments especially susceptible to Distributed Denial of Service (DDoS) attacks, which can disrupt network availability, compromise the integrity of control systems, or target specific application services running on industrial controllers [7].

2.2. DDoS Attacks in IIoT Context

DDoS attacks are designed to overwhelm a target system by flooding it with excessive traffic, depleting essential resources such as bandwidth, CPU, memory, and connection tables, ultimately rendering the system unavailable. In the context of IIoT, these attacks can take several forms: volumetric attacks that saturate network bandwidth through methods like UDP or ICMP floods [8]; protocol attacks that exploit vulnerabilities in network protocols, such as SYN floods or fragmented packet attacks [9]; and application-layer attacks that focus on specific application services, often using seemingly legitimate requests to drain server resources, for example, HTTP floods directed at OPC UA servers [10]. In IIoT environments, even low-volume, highly targeted DDoS attacks aimed at critical control messages or specific device endpoints can cause disproportionately severe disruptions.

2.3. Traditional DDoS Mitigation Approaches and Their Limitations for IIoT

Cloud-based mitigation services work by redirecting traffic to scrubbing centers in the cloud, which can be highly effective against large-scale volumetric attacks targeting IT infrastructure. However, for real-time IIoT operations, these services often introduce unacceptable latency and require all IIoT traffic to be routed through external networks, raising significant privacy and compliance issues [11]. On-premise DDoS appliances, which are hardware solutions installed at the network perimeter, offer lower latency compared to cloud-based options but tend to be costly, resource-intensive, and may struggle to scale effectively against the vast array of potential attack vectors present in IIoT environments without substantial investment [12]. Traditional intrusion detection systems (IDS), whether signature-based or anomaly-based, are also commonly used. Signature-based IDSs depend on known attack patterns, making them ineffective against new, previously unseen DDoS variants. Anomaly-based IDSs, which often utilize machine learning (ML), can identify novel attacks but typically demand considerable computational resources for both training and inference. This can result in high power consumption and an increased risk of false positives, which may disrupt critical industrial processes [13]. As a result, deploying such systems directly on resource-constrained IIoT edge devices is often impractical.

2.4. Role of Edge Computing in IIoT Security

Edge computing presents a promising approach to strengthening IIoT security by positioning computational resources closer to where data is generated [14]. This proximity allows for real-time threat analysis and mitigation without the delays associated with sending data to the cloud, significantly reducing latency. By processing information locally, edge computing also helps conserve bandwidth by minimizing the amount of data that needs to be transmitted to the core network. Additionally, it enables early detection of malicious activity by identifying abnormal patterns right at the point of entry. Furthermore, edge computing facilitates rapid isolation and containment of compromised devices or network segments, helping to prevent attacks from spreading laterally across the IIoT environment.

Recent studies have begun to investigate the potential of edge-based security solutions for IoT environments. For instance, [15] introduced an edge-based intrusion detection system that utilizes lightweight machine learning techniques for general IoT networks. Another study [16] explored the application of federated learning at the edge to enable distributed anomaly detection, a method that holds promise for adapting to DDoS scenarios. Meanwhile, [17] examined AI-driven anomaly detection approaches for IIoT, though these efforts do not always prioritize lightweight deployment specifically tailored for DDoS mitigation on resource-constrained edge devices. Despite these advancements, there is still a notable gap in the development of a comprehensive, lightweight, edge-based security system that is purpose-built for DDoS mitigation in IIoT, taking into account the sector's unique real-time operational demands and limited resources.

3. Proposed Lightweight Edge-Based Security System Design

To tackle the specific challenges of DDoS mitigation in IIoT environments, we propose a lightweight, edge-based security system that brings together intelligent monitoring, anomaly detection, and rapid response functions directly on edge gateways. This approach is carefully designed to deliver effective real-time protection while remaining efficient and practical for deployment in resource-constrained settings.

3.1. System Architecture

The proposed system functions at the edge layer, typically running on dedicated edge gateways that are strategically placed at the interface between IIoT devices or controllers and the wider enterprise or cloud network. This setup is depicted in the conceptual architecture shown in Figure 1.

IIoT devices and controllers, such as industrial sensors, actuators, PLCs, and RTUs, are responsible for generating and receiving operational data within the system. The edge gateway, equipped with networking capabilities, serves as a local computing device that hosts the Lightweight Security Module, acting both as a data aggregation point and the

first line of defense against potential threats. At the heart of this setup is the Lightweight Security Module, which provides the core intelligence for monitoring and protection directly on the edge gateway. Supporting this architecture, 5G and other network infrastructure deliver high-speed, low-latency connectivity for IIoT traffic and facilitate communication between the edge and the cloud. The cloud layer, meanwhile, is utilized for global threat intelligence, long-term data storage, and centralized management and reporting.

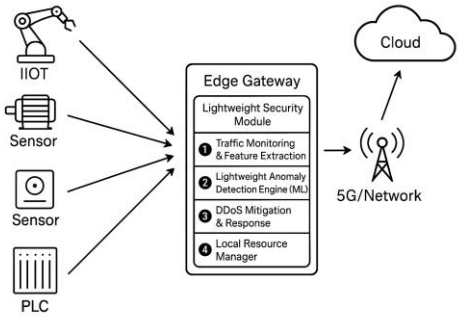

Figure 1. Edge-Based Security System Design

3.2. Components of the Lightweight Security Module

a. Traffic Monitoring and Feature Extraction

The system begins with packet capture and flow export, continuously monitoring all incoming and outgoing traffic on the edge gateway by capturing packet headers or generating flow records similar to NetFlow or IPFIX, all while operating at a low level to keep overhead minimal [18]. Instead of performing deep packet inspection on every packet, the lightweight feature extraction component focuses on gathering only the most essential features needed for effective DDoS detection. These features include packet-level details such as source and destination IP addresses, port numbers, protocol types (TCP, UDP, ICMP), and packet sizes; flow-level metrics like the number of packets or bytes per flow, flow duration, connection states, and the distribution of flags (such as SYN and ACK for TCP); and time-series characteristics, including the rate of new connections, packets per second, and the entropy of source or destination IPs and ports over short time intervals [19]. Additionally, the system incorporates IIoT protocol awareness by performing basic parsing of common industrial protocols like Modbus TCP and OPC UA, enabling it to identify control messages and detect anomalies specific to these protocols, such as an unusually high frequency of Write Coils requests.

b. Lightweight Anomaly Detection Engine (ML-Based)

The primary goal of this component is to detect deviations from typical IIoT traffic patterns that could signal a DDoS attack, including previously unseen, zero-day variants. To achieve this, the system prioritizes machine learning models that have low computational and memory requirements, making them suitable for deployment at the edge. For identifying known types of DDoS attacks, lightweight supervised learning algorithms such as Decision Trees (DT), Random Forests (RF), or Support Vector Machines (SVM) with optimized kernels are used, as they offer faster inference times compared to deep neural networks [20]. To uncover novel or unknown DDoS patterns, unsupervised learning methods like Isolation Forest, One-Class SVM, or k-Means Clustering are employed to spot outliers in the extracted feature sets, eliminating the need for pre-labeled attack data [21]. The models are further optimized through techniques such as quantization, which reduces the precision of model weights (for example, from 32-bit floats to 8-bit integers) to decrease model size and accelerate inference without significantly sacrificing accuracy [22], and pruning, which removes unnecessary connections or neurons from the model. Additionally, online or continual learning is incorporated to allow the model to adapt to changing IIoT traffic patterns and emerging attack types without the need for complete retraining [23]. Finally, dynamically adjusted thresholds for anomaly scores are used to minimize false positives, which is especially important in the context of IIoT operations.

c. DDoS Mitigation and Response

When a DDoS attack is detected, the system can take immediate action at the local level by enforcing Access Control Lists (ACLs) or firewall rules to block malicious source IP addresses or specific traffic patterns [24]. It can also implement rate limiting to throttle the flow of suspicious connections or packets, thereby protecting targeted IIoT devices or services.

Additionally, the system is capable of filtering out packets that match known attack signatures or that exceed predefined thresholds. To ensure coordinated defense, alerts are generated and sent to central security operations in the cloud layer, providing detailed information about the detected attack and the mitigation steps taken. In more severe scenarios, the system can initiate network segmentation to isolate the affected IIoT subnet, effectively containing the attack and preventing it from spreading to other critical parts of the infrastructure.

d. Local Resource Manager

The system continuously monitors the edge gateway's CPU, memory, and power usage to ensure that the security module does not negatively impact the performance of the industrial applications it is designed to protect. It also dynamically adjusts the level of monitoring and anomaly detection based on current resource availability, always prioritizing the smooth operation of critical IIoT processes.

3.3. Lightweight Design Principles

The "lightweight" nature of the system is achieved through several deliberate design choices. First, data processing is kept minimalist by focusing only on the essential features needed for DDoS detection, rather than performing exhaustive deep packet inspection. The machine learning models used are carefully selected and optimized to ensure low resource consumption. Event-driven processing is employed, meaning data is only analyzed when specific triggers or anomalies are detected, which helps reduce continuous overhead. The system also adopts a stateless or low-state design, minimizing the amount of state information stored on the edge gateway for greater efficiency. For highly critical deployments, optional dedicated hardware acceleration—such as tinyML or specialized AI accelerators—can be used to significantly boost ML inference performance while keeping power usage low. By embedding these capabilities directly at the edge, the proposed system delivers a vital, real-time defense layer against DDoS attacks, helping to protect the operational integrity and safety of IIoT infrastructure.

4. Performance Evaluation and Challenges

The effectiveness of the proposed lightweight edge-based security system for DDoS mitigation in IIoT needs to be thoroughly assessed using key performance indicators, while also taking into account the practical challenges that may arise during real-world deployment.

4.1. Key Performance Metrics

Key performance indicators for evaluating the proposed system include the Detection Rate (DR) or True Positive Rate (TPR), which measures the percentage of actual DDoS attacks accurately identified. Equally important is the False Positive Rate (FPR), representing the proportion of legitimate traffic or normal IIoT operations mistakenly flagged as attacks; keeping this rate low is essential to prevent unnecessary disruptions to critical processes [25]. Mitigation Time, or the interval between attack detection and the execution of mitigation actions, must be extremely short—ideally within milliseconds—to meet real-time IIoT requirements. Resource consumption, including CPU, memory, and power usage, is another crucial metric, as the security module must remain lightweight to be practical for edge deployment. Additionally, Throughput Under Attack assesses how much legitimate IIoT traffic the gateway can process and forward during a DDoS incident, while Latency Impact measures any extra delay the security module introduces to normal IIoT communications. Finally, Scalability evaluates the system's ability to maintain its performance as the number of IIoT devices, traffic volume, and the scale of DDoS attacks grow.

4.2. Evaluation Methodology

To thoroughly evaluate the system, a combination of testbed simulation and real hardware deployment is recommended. IIoT-specific network simulators, such as OMNeT++ or Mininet-WiFi configured with industrial protocols, can be used to model IIoT infrastructure, generate realistic traffic, and simulate a variety of DDoS attack scenarios. For more precise measurements of resource consumption and latency, the system should also be tested on a physical edge gateway connected to actual IIoT devices like PLCs and sensors in a controlled environment. Additionally, training and testing the machine learning models require datasets that accurately

represent both normal IIoT operations and a range of DDoS attack patterns targeting IIoT protocols. However, the scarcity of publicly available IIoT datasets presents a significant challenge in this area [26].

4.3. Persistent Challenges

There are several IIoT-specific constraints that must be carefully considered. First, real-time determinism is essential—the security system cannot introduce unpredictable delays or jitters that might disrupt critical control loops, so all security operations must be both highly predictable and extremely fast. Second, many IIoT devices rely on outdated software or firmware and are unable to support complex security agents, meaning the edge gateway must provide robust protection without requiring any modifications to these legacy devices. Third, the safety-critical nature of IIoT environments means that false positives, which could result in legitimate traffic being blocked, have the potential to cause serious safety hazards, such as failures in emergency shutdown procedures. Striking the right balance between security and operational safety is therefore crucial. Finally, the use of proprietary protocols in IIoT makes deep packet inspection for DDoS detection both complex and resource-intensive, which can conflict with the system's goal of remaining lightweight.

Balancing the need for lightweight operation with the effectiveness of DDoS detection presents a significant challenge. Achieving high detection accuracy for complex and evolving DDoS attacks is difficult when working within strict resource limitations, as overly simplified machine learning models may fail to identify more sophisticated threats. Additionally, there is a delicate trade-off between minimizing false positives—which is crucial in IIoT environments to avoid disrupting essential operations—and ensuring a high detection rate across all types of attacks. Careful tuning and optimization are required to strike the right balance between these competing priorities.

One major challenge is the limited availability of public, high-quality datasets that accurately represent IIoT network traffic, particularly those that include real-world DDoS attack scenarios involving industrial protocols and environments. This scarcity makes it difficult to train and validate machine learning models effectively [27]. Additionally, while simulated attack data can be useful, it often fails to capture the full complexity and subtlety of real-world threats, potentially limiting the robustness of the security system.

Detecting zero-day attacks remains a significant challenge, as even though anomaly-based machine learning models can identify previously unseen threats, their ability to catch highly novel or evasive DDoS techniques still demands ongoing research and rapid adaptation to emerging attack patterns. Additionally, the security of the edge security module itself is crucial, as it becomes a high-value target for attackers. The system must be robust against direct attacks, such as evasion tactics or attempts to tamper with the ML model, and its integrity should be protected, for example, by using trusted execution environments. Finally, as the deployment of edge gateways scales up, effectively coordinating their threat intelligence and mitigation actions—such as sharing blacklists of malicious IP addresses—without causing excessive communication overhead presents another layer of complexity.

Overcoming these challenges calls for a multidisciplinary approach, bringing together knowledge from cybersecurity, machine learning, industrial control systems, and network engineering. As IIoT threats continue to evolve, it is essential to develop adaptive and resilient security solutions that can effectively respond to new and emerging attack techniques.

5. Conclusion

The integration of industrial control systems with the Internet of Things, known as Industrial IoT (IIoT), has greatly improved efficiency but also created new cybersecurity risks. DDoS attacks are especially dangerous for IIoT because they can disrupt real-time operations, threaten safety, and even cause physical damage. Traditional, centralized methods for stopping DDoS attacks often do not meet the strict needs of IIoT, such as low latency and limited resources. To address this, this paper introduced a lightweight security system that works at the edge, close to IIoT devices. The system uses local processing on edge gateways, efficient machine learning models for detecting unusual activity, and quick response actions, all while keeping resource use low.

The paper discussed important ways to measure the system's performance, like how well it detects attacks, how often it makes mistakes, how quickly it responds, and how much computing power it uses. There are still challenges, such as making sure the system does not interfere with critical operations, finding the right balance between being lightweight and effective, and dealing with the lack of real-world IIoT attack data. Future research should focus on creating smarter and more efficient AI models, using collaborative learning between edge devices, improving system security, and developing standard tests for IIoT security. In the end, keeping IIoT systems safe will require ongoing, adaptive, and edge-focused security solutions.

References

[1] M. Javaid, Abid Haleem, R. Pratap Singh, S. Rab, and R. Suman, "Upgrading the manufacturing sector via applications of Industrial Internet of Things (IIoT)," *Sensors Int.*, vol. 2, p. 100129, 2021, doi: https://doi.org/10.1016/j.sintl.2021.100129.

[2] J. Kim, J. Park, and J.-H. Lee, "Analysis of Recent IIoT Security Technology Trends in a Smart Factory Environment," in *2023 International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*, 2023, pp. 840–845. doi: 10.1109/ICAIIC57133.2023.10067004.

[3] A. H. Eyeleko and T. Feng, "A Critical Overview of Industrial Internet of Things Security and Privacy Issues Using a Layer-Based Hacking Scenario," *IEEE Internet Things J.*, vol. 10, no. 24, pp. 21917–21941, 2023, doi: 10.1109/JIOT.2023.3308195.

[4] Y. Li, Y. Zhao, J. Li, X. Yu, Y. Zhao, and J. Zhang, "DDoS Attack Mitigation Based on Traffic Scheduling in Edge Computing-Enabled TWDM-PON," *IEEE Access*, vol. 9, pp. 166566–166578, 2021, doi: 10.1109/ACCESS.2021.3134671.

[5] S. F. Ahmed *et al.*, "Industrial Internet of Things enabled technologies, challenges, and future directions," *Comput. Electr. Eng.*, vol. 110, p. 108847, 2023, doi: https://doi.org/10.1016/j.compeleceng.2023.108847.

[6] M. Sverko, T. G. Grbac, and M. Mikuc, "SCADA Systems With Focus on Continuous Manufacturing and Steel Industry: A Survey on Architectures, Standards, Challenges and Industry 5.0," *IEEE Access*, vol. 10, pp. 109395–109430, 2022, doi: 10.1109/ACCESS.2022.3211288.

[7] S. Chaudhary and P. K. Mishra, "DDoS attacks in Industrial IoT: A survey," *Comput. Networks*, vol. 236, p. 110015, 2023, doi: https://doi.org/10.1016/j.comnet.2023.110015.

[8] A. Lohachab and B. Karambir, "Critical Analysis of DDoS—An Emerging Security Threat over IoT Networks," *J. Commun. Inf. Networks*, vol. 3, no. 3, pp. 57–78, 2018, doi: 10.1007/s41650-018-0022-5.

[9] M. Arif, G. Wang, M. Zakirul Alam Bhuiyan, T. Wang, and J. Chen, "A survey on security attacks in VANETs: Communication, applications and challenges," *Veh. Commun.*, vol. 19, p. 100179, 2019, doi: https://doi.org/10.1016/j.vehcom.2019.100179.

[10] F. De Keersmaeker, Y. Cao, G. K. Ndonda, and R. Sadre, "A Survey of Public IoT Datasets for Network Security Research," *IEEE Commun. Surv. Tutorials*, vol. 25, no. 3, pp. 1808–1840, 2023, doi: 10.1109/COMST.2023.3288942.

[11] A. Bhardwaj *et al.*, "IIoT: Traffic Data Flow Analysis and Modeling Experiment for Smart IoT Devices," 2022. doi: 10.3390/su142114645.

[12] A. Ashraf and W. M. Elmedany, "IoT DDoS attacks detection using machine learning techniques: A Review," in *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 2021, pp. 178–185. doi: 10.1109/ICDABI53623.2021.9655789.

[13] I. A. Mahar, W. Libing, G. A. Rahu, Z. A. Maher, and M. Y. Koondhar, "Feature Based Comparative Analysis of Traditional Intrusion Detection System and Software-Defined Networking Based Intrusion Detection System," in *2023 IEEE 8th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*, 2023, pp. 1–5. doi: 10.1109/ICETAS59148.2023.10346497.

[14] Z. Lin, J. Liu, J. Xiao, and S. Zi, "A Survey: Resource Allocation Technology Based on Edge Computing in IIoT," in *2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI)*, 2020, pp. 1–5. doi: 10.1109/CCCI49893.2020.9256663.

[15] H. Bangui and B. Buhnova, "Lightweight intrusion detection for edge computing networks using deep forest and bio-inspired algorithms," *Comput. Electr. Eng.*, vol. 100, p. 107901, 2022, doi: https://doi.org/10.1016/j.compeleceng.2022.107901.

[16] W. Marfo, D. K. Tosh, and S. V Moore, "Network Anomaly Detection Using Federated Learning," in *MILCOM 2022 - 2022 IEEE*

Military Communications Conference (MILCOM), 2022, pp. 484–489. doi: 10.1109/MILCOM55135.2022.10017793.

[17] K. DeMedeiros, A. Hendawi, and M. Alvarez, "A Survey of AI-Based Anomaly Detection in IoT and Sensor Networks," *Sensors*, vol. 23, no. 3, 2023, doi: 10.3390/s23031352.

[18] M. Fejrskov, J. M. Pedersen, and E. Vasilomanolakis, "Detecting DNS hijacking by using NetFlow data," in *2022 IEEE Conference on Communications and Network Security (CNS)*, 2022, pp. 273–280. doi: 10.1109/CNS56114.2022.9947264.

[19] Z. Liu, Y. Wang, F. Feng, Y. Liu, Z. Li, and Y. Shan, "A DDoS Detection Method Based on Feature Engineering and Machine Learning in Software-Defined Networks," *Sensors*, vol. 23, no. 13, 2023, doi: 10.3390/s23136176.

[20] S. Sadhwani, B. Manibalan, R. Muthalagu, and P. Pawar, "A Lightweight Model for DDoS Attack Detection Using Machine Learning Techniques," *Appl. Sci.*, vol. 13, no. 17, 2023, doi: 10.3390/app13179937.

[21] E. H. Budiarto, A. Erna Permanasari, and S. Fauziati, "Unsupervised Anomaly Detection Using K-Means, Local Outlier Factor and One Class SVM," in *2019 5th International Conference on Science and Technology (ICST)*, 2019, pp. 1–5. doi: 10.1109/ICST47872.2019.9166366.

[22] S. Liu, L. Liu, and Y. Yi, "Quantized Reservoir Computing on Edge Devices for Communication Applications," in *2020 IEEE/ACM Symposium on Edge Computing (SEC)*, 2020, pp. 445–449. doi: 10.1109/SEC50012.2020.00068.

[23] S. A. Bakhsh, M. A. Khan, F. Ahmed, M. S. Alshehri, H. Ali, and J. Ahmad, "Enhancing IoT network security through deep learning-powered Intrusion Detection System," *Internet of Things*, vol. 24, p. 100936, 2023, doi: https://doi.org/10.1016/j.iot.2023.100936.

[24] W. Zahwa, A. Lahmadi, M. Rusinowitch, and M. Ayadi, "Automated Placement of In-Network ACL Rules," in *2023 IEEE 9th International Conference on Network Softwarization (NetSoft)*, 2023, pp. 486–491. doi: 10.1109/NetSoft57336.2023.10175436.

[25] N. Anjum, Z. Latif, C. Lee, I. A. Shoukat, and U. Iqbal, "MIND: A Multi-Source Data Fusion Scheme for Intrusion Detection in Networks," *Sensors*, vol. 21, no. 14, 2021, doi: 10.3390/s21144941.

[26] D. Atzeni, R. Ramjattan, R. Figliè, G. Baldi, and D. Mazzei, "Data-Driven Insights through Industrial Retrofitting: An Anonymized Dataset with Machine Learning Use Cases," *Sensors*, vol. 23, no. 13, 2023, doi: 10.3390/s23136078.

[27] 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. 40281–40306, 2022, doi: 10.1109/ACCESS.2022.3165809.