A Data Rate Monitoring Approach for Cyberattack Detection in Digital Twin Communication

Cláudio H. Albuquerque Rodrigues *, Waldir S. S. Júnior, Wilson Dias de Oliveira, Isomar Silva

Posted Date: 10 November 2025

doi: 10.20944/preprints202510.1127.v2

Keywords: Digital Twins; Data Rate; Cyberattacks; IIoT Security

Article

A Data Rate Monitoring Approach for Cyberattack Detection in Digital Twin Communication

Cláudio Rodrigues [1,2,*], Waldir S. S. Júnior [2], Wilson Oliveira [3] and Isomar Silva [1]

[1] Conecthus Institute - Technology and Biotechnology of Amazonas
[2] Federal University of Amazonas - UFAM
[3] Ulbra Manaus - Universidade Luterana do Brasil
* Correspondence: claudio.rodrigues@conecthus.org.br; Tel.: +55-92-98113-4537

Abstract

The growing integration of Digital Twins (DTs) in Industry 4.0 environments exposes the physical–virtual communication layer as a critical vector for cyber vulnerabilities. While most studies focus on complex and resource-intensive security mechanisms, this work demonstrates that the inherently predictable nature of DT communications allows simple statistical metrics—such as the $\mu + 3\sigma$ threshold—to provide robust, interpretable, and computationally efficient anomaly detection. Using a Docker-based simulation, we emulate Denial-of-Service (DoS), Man-in-the-Middle (MiTM), and intrusion attacks, showing that each generates a distinct statistical signature (e.g., a 50-fold increase in packet rate during DoS). The results confirm that data rate monitoring offers a viable, non-intrusive, and cost-effective first line of defense, thereby enhancing the resilience of IIoT-based Digital Twins.

Keywords: digital twins; data rate; cyberattacks; IIoT security

1. Introduction

The adoption of Digital Twins (DTs) has become a cornerstone of Industry 4.0, transforming how complex systems are monitored, analyzed, and optimized in real time [1,2]. By creating dynamic, high-fidelity virtual replicas of physical assets or processes, DTs enable precise and proactive decision-making, with applications spanning from manufacturing to critical infrastructure management [3,4]. This technology operates through a continuous, bidirectional data stream that synchronizes the states of the physical and digital entities, ensuring real-time consistency.

Despite its operational advantages, this persistent interconnection introduces a novel and critical vector for cyber vulnerabilities. The communication layer, responsible for transporting data from Industrial Internet of Things (IIoT) sensors and Programmable Logic Controller (PLC) commands, becomes a primary attack surface where the integrity, confidentiality and availability of data can be compromised [5,6]. Attacks targeting this channel can corrupt the fidelity of the Digital Twin and may also trigger hazardous actions within the physical system, potentially resulting in severe operational disruptions and safety risks.

Recent studies have explored multiple strategies to mitigate these threats, including Machine Learning (ML)-based detection and blockchain-enabled authentication mechanisms [7–9]. However, as emphasized in our systematic review (Section 2), these methods frequently impose substantial computational overhead, rendering them less practical for resource-constrained edge environments. Conversely, traditional low-cost defenses, such as static firewall rules, remain inadequate against novel (zero-day) attacks. This observation reveals a crucial research gap: the absence of detection mechanisms that are both computationally efficient and behaviorally resilient, specifically designed for the unique communication dynamics of IIoT-based Digital Twins.

To bridge this gap, the core contribution of this study is to demonstrate that the inherent regularity of IIoT and Digital Twin communication can serve as its own most effective line of defense.

 doi:10.20944/preprints202510.1127.v2

Unlike conventional IT networks, which exhibit irregular and stochastic traffic, IIoT environments are characterized by cyclical, deterministic, and highly predictable communication patterns—such as periodic sensor data reporting and command delivery to actuators. We argue that this predictability enables the use of lightweight, statistically grounded techniques—exemplified by our non-intrusive approach based on the $\mu + 3\sigma$ threshold—for robust anomaly detection. The findings of this work validate that data rate monitoring, when tailored to this specific context, constitutes a transparent, interpretable, and computationally efficient first layer of cyber defense.

The remainder of this paper is organized as follows. Section 2 presents the conceptual background for this work. Section 3 presents a critical review of the literature and defines the research gaps. Section 4 details the methodology used, including the detection approach and experimental setup. Section 5 presents and discusses the results obtained from the simulation experiments. Finally, Section 6 concludes the paper, summarizing the findings, discussing the limitations, and suggesting directions for future research.

2. Background

The transition to cyber-physical production systems enabled by Digital Twins relies critically on maintaining the integrity, confidentiality, and availability of the data streams that link the physical and virtual domains. This section provides the necessary conceptual background for this work. It first defines Digital Twin technology, architectures, and connectivity challenges. It then examines the broader cybersecurity landscape in Operational Technology (OT) and IIoT environments, concluding with a review of emerging threats that target these systems.

2.1. Digital Twins: Concepts, Architectures, and Connectivity Challenges

A Digital Twin (DT) is a dynamic, high-fidelity virtual representation of a physical asset, process, or system [1]. This digital model is continuously synchronized through real-time data collection from sensors and other sources in the physical environment, enabling it to replicate the behavior and characteristics of its physical counterpart for observation, analysis, and operational optimization [3,19]. A fundamental pillar of this technology is the bidirectional interaction between the physical domain and its digital counterpart: real-world data feed the virtual model, which, in turn, generates insights that influence the physical system, establishing a continuous cycle of control and improvement [1,29]. The implementation of DTs is facilitated by the convergence of technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and Machine Learning (ML) [30,31]. Their inherently connected nature and reliance on data exchange underscore the critical importance of communication security [5,6,32].

Building an effective Digital Twin (DT) requires a robust and well-defined architecture. Although various models have been proposed in the literature [3,19,33], a fundamental set of core components is commonly shared. Conceptually, a DT architecture can be structured into several key layers. The first layer is the physical entity, representing the real-world system and including the sensors and actuators responsible for data collection and interaction [5,6]. The second layer is the virtual model—a digital representation comprising components ranging from 3D models to AI algorithms used to process data, simulate scenarios, and optimize operations [30,34]. Serving as the bridge between these layers, the data connection layer enables the bidirectional flow of information, in which IoT and communication network technologies play a crucial role [5,6,32]. Finally, the service and application layer leverages the insights generated by the DT to deliver value through control dashboards, predictive maintenance tools, and decision-support systems [19,33].

The seamless integration of these layers facilitates the successful application of DTs across domains ranging from manufacturing to smart city management [3,4]. It is evident that the data connection layer functions as the central nervous system of the entire architecture. Its integrity and availability are not only critical functional requirements but also represent the primary potential attack surface. Therefore, understanding the security challenges inherent to this connectivity is a prerequisite for developing more resilient DT systems.

 doi:10.20944/preprints202510.1127.v2

2.2. Cybersecurity and Threat Detection in IIoT/OT Environments

Securing Operational Technology (OT) and Industrial Internet of Things (IIoT) environments presents a unique set of challenges distinct from those found in traditional IT systems [35]. Ensuring the availability and integrity of critical physical processes—often operating in real time—must coexist with the proliferation of resource-constrained devices and heterogeneous communication protocols, including legacy systems [5,35]. This complex scenario demands security strategies that extend beyond conventional network perimeters, focusing on the detection of anomalies and malicious behaviors directly within data traffic and system operations.

The research community has focused on developing increasingly sophisticated Intrusion Detection Systems (IDS) for these environments. Many proposed solutions employ machine learning and deep learning techniques to analyze network traffic and identify deviations from normal behavior [16]. However, the complexity of these detection mechanisms introduces new vulnerabilities. Studies such as [36] have demonstrated that deep learning–based detection systems can be susceptible to evasion attacks, in which adversaries deliberately manipulate input data to deceive the detection model. This underscores that, despite technological advances, threat detection in complex distributed systems remains an ongoing challenge.

2.3. Emerging Cyber Threats and Their Impacts

Digital Twin (DT) security addresses not only known threats but also an ever-evolving attack landscape. The increasing sophistication of threats such as Advanced Persistent Threats (APTs) and AI-driven attacks—designed to remain stealthy and persistent—poses a particular challenge. Such attacks may not seek immediate service disruption but instead aim for continuous data exfiltration or the subtle, long-term manipulation of physical operations by corrupting the data stream that feeds the Digital Twin.

This new generation of threats tests the limits of existing detection mechanisms. Evasion attacks, for instance, are intentionally crafted to circumvent AI-based systems by subtly manipulating input data so that it is misclassified as benign traffic [36]. Moreover, these advanced attack capabilities exacerbate systemic concerns about data privacy and security in Digital Twins, potentially leading to large-scale data manipulation or critical information leakage, as discussed in [37].

The impact of these emerging threats on the physical–virtual communication flow is therefore direct. A sophisticated attack may not produce an obvious traffic spike, as in a DDoS event, but it can alter the frequency, size, or regularity of data packets, causing subtle deviations from the operational baseline. This underscores the need for monitoring approaches sensitive to fundamental variations in the communication channel.

3. Related Work

To contextualize the contribution of this work, we conducted a critical review of the state-of-the-art in DT intrusion detection. A structured and reproducible search methodology was developed and applied across major scientific databases, including IEEE Xplore and the ACM Digital Library. The search string employed was: ("digital twin" OR "digital twins") AND ("intrusion detection" OR "attack detection" OR "anomaly detection" OR "threat detection" OR detection) AND ("industrial IoT" OR IIoT OR "industrial control system"). Following the initial retrieval, the resulting corpus was subjected to a multi-stage screening process designed to ensure both temporal relevance and thematic precision. Publications from 2020 onward were prioritized, with inclusion criteria focusing on the explicit occurrence of search terms within titles and abstracts. After applying these filters, a final corpus of 22 articles was selected, representing the most relevant state-of-the-art research at the intersection of Digital Twin technology and cyberattack detection. Table 1 summarizes the main features of these studies and serves as the analytical foundation for the discussion presented in the following subsections.

 doi:10.20944/preprints202510.1127.v2

Table 1. Systematic Review of Anomaly Detection Methods in IIoT and Digital Twins. This table summarizes key studies in the field, emphasizing the prevailing reliance on complex, high-overhead approaches (e.g., ML/DL). The review highlights the research gap addressed in this paper—the experimental validation of lightweight, data-rate-based detection methods.

Reference	System Type	Security Focus	Detection	Monitor. Metric	Technique	Attacks	Validation
[9]	IIoT	D, P	AN	DR, SC	FL, DL	DDoS	Simulation
[7]	Industrial	I, R, A	PR	SC, NF	BC	DI, FR	Theoretical
[10]	IIoT	D, I	CA	NF	BC, ML	GA	Simulation
[11]	ICS	D	AN	SC	DT, ML	GA	Simulation
[12]	ICS	D	AN(S)	SC	DT, Sim.	GA	Simulation
[13]	CPS	D	AN	SC	ML, DT	GA	Simulation
[8]	IIoT	D, P, R	CA	NF, SC	FL	IN	Simulation
[14]	CPS	D	AN(C)	NF	DT	GA	Simulation
[15]	IIoT	D, I	AD	NF	Testbed	DA	Testbed
[16]	CPS	D	TD	SC	DRL, IoT, DT	TCPS	Simulation
[17]	ICS	D	AN	SC	DT, DL	GA	Simulation
[18]	CPS	D, R	HY(A)	SC, NF	DT, Hybrid	GA	Simulation
[19]	IIoT	D	AN(B)	SC	DT, ML	GA	Simulation
[20]	IIoT	D	AN	SC	DT, ML	GA	Simulation
[21]	ICS	D	IN(A)	SC	DT, ML	IN	Simulation
[22]	ICS	D	AN(D)	SC	DT, ML	CA	Simulation
[23]	ICS	C, I, D	SA	SC, NF	DT, Data	GT	Simulation
[24]	Industrial	P	AN	SC	HMMs	FA	Dataset
[25]	Industrial	A, I	PD	SC	BC, AI	FR	Simulation
[26]	ICS	D	FD	SC	DT	CA	Simulation
[27]	IIoT	C, A	TM	SC	DT, BC	MB	Simulation
[28]	Industrial	D	AN(SH)	SC	DT, ML	GT	Simulation

System Type: IIoT (Industrial Internet of Things), ICS (Industrial Control System), CPS (Cyber-Physical System).
Security Focus: C (Confidentiality), I (Integrity), D (Availability), P (Privacy), R (Resilience), A (Authenticity).
Detection: AN (Anomaly), PR (Prevention), CA (Collab. Anomaly), AN(S) (Anomaly, Sim.), AN(C) (Anomaly, Collab.), AD (Attack Detection), TD (Threat Detection), HY(A) (Hybrid, Anomaly), AN(B) (Anomaly, Behav.), IN(A) (Intrusion, Anomaly), AN(D) (Anomaly, Defense), SA (Situational Aware.), PD (Prediction), FD (Fault Detection), TM (Trust Management), AN(SH) (Anomaly, Self-heal.).
Monitoring Metric: DR (Data Rate), SC (System Comp.), NF (Network Flow).
Technique: ML (Machine Learning), DL (Deep Learning), FL (Federated Learning), BC (Blockchain), DRL (Deep Reinforcement Learning).
Attacks: DI (Data Injection), FR (Fraud), GA (Generic Attacks), IN (Intrusions), DA (Diverse Attacks), TCPS (Threats in CPS), CA (Cyberattacks), GT (Generic Threats), FA (Faults), MB (Malicious Behavior).

3.1. Intrusion Detection in the Physical–Virtual Communication of Digital Twins

The fidelity and utility of a Digital Twin (DT) are directly proportional to the integrity of its bidirectional communication with the physical counterpart. As highlighted previously, ensuring the Confidentiality, Integrity, and Availability (CIA) of this channel is imperative [5,6]. Any compromise of this data stream—whether through manipulation, interception, or disruption—can invalidate the virtual model and lead to erroneous or hazardous operational decisions in the physical environment [37]. Therefore, this subsection focuses on studies that directly address threat detection within this communication layer.

Recent literature proposes several strategies to mitigate these challenges. A major line of research employs machine learning and deep learning techniques for anomaly detection. For example, [7] explores the use of Federated Learning to train intrusion detection models in a distributed manner, thereby preserving data privacy. Others, such as [9], adopt a similar approach with a specific focus on detecting Distributed Denial-of-Service (DDoS) attacks in IIoT networks supporting Digital Twins. In parallel, there is growing interest in leveraging blockchain technology to ensure the integrity and traceability of exchanged data. Studies such as [8,10] propose architectures in which data transactions between the physical and virtual domains are immutably recorded, preventing undetected manipulation.

 doi:10.20944/preprints202510.1127.v2

3.2. Literature Gaps and Proposed Contribution

A critical analysis of these contributions reveals a notable gap. Although effective against certain attack classes, many of these approaches introduce considerable computational and latency overheads (as in the case of blockchain) or require extensive labeled datasets for training (as with supervised deep learning). More importantly, few studies investigate low-level network metrics—such as throughput—as primary indicators of security anomalies. The hypothesis that subtle or abrupt variations in the volume and frequency of data packets can signal different types of attacks—ranging from DoS disruptions to reconnaissance or false data injection—remains relatively underexplored. This shortcoming justifies the investigation of a lightweight, computationally efficient detection method focused directly on the fundamental behavior of the communication channel.

The literature analysis reveals a vibrant research field with significant progress in defining Digital Twin (DT) architectures and applying techniques such as machine learning and blockchain to enhance security in IIoT environments. Despite these advances, our systematic review highlights critical gaps that remain and motivate the present investigation. The main identified gaps are as follows:

- **Architectures with reactive security:** Most architectural models treat security as an external or adjunct layer rather than as an intrinsic design principle. There is a lack of proposals for architectures conceived from the outset to facilitate intrusion detection within communication flows while considering the performance constraints of IIoT systems.
- **Focus on complex, high-level methods:** Predominant detection strategies rely on computationally intensive approaches (e.g., deep learning, federated learning, blockchain) or on system-level behavioral analysis, often neglecting fundamental, low-cost communication channel metrics.
- **Lack of throughput-focused detection:** Specifically, the exploration of data throughput as a primary indicator for detecting a wide range of attacks—from service disruptions to subtle manipulations—remains notably underexplored in the Digital Twin literature.
- **Limited validation against emerging threats:** There is a pressing need for experimental validation of detection strategies capable of operating in real time and maintaining DT resilience under sophisticated, stealthy attacks that target data integrity rather than merely causing denial of service.

In light of these gaps, this study proposes and validates an approach for detecting cyberattacks in the communication of industrial Digital Twins, based on monitoring and analyzing anomalies in data throughput. The proposed method aims to provide a non-intrusive, computationally lightweight, and complementary solution to existing strategies, thereby contributing to the development of more secure and resilient Digital Twin architectures within IIoT environments.

4. Methodology

This section details the methodology used to validate the proposed detection approach. It is structured to first explain the conceptual foundation of the method and then describe the experimental implementation.

4.1. Detection Approach

The central hypothesis of this work is that the *inherent predictability* of IIoT and Digital Twin communication makes it an ideal subject for statistical anomaly detection. Unlike traditional IT networks, which often exhibit irregular and stochastic traffic, DT environments are characterized by cyclical, deterministic, and highly predictable data flows (e.g., sensors reporting at fixed intervals).

Given this predictability, any significant deviation from a stable baseline can serve as a robust indicator of an anomaly. Our approach, therefore, is grounded in establishing this baseline and applying a lightweight, statistically rigorous threshold.

First, the benign (normal operation) workload was characterized to establish this baseline. As illustrated in the sequence diagram (Figure 3), this workload consists of the device container (simulating sensors such as temperature and humidity) periodically sending telemetry data via MQTT to

 doi:10.20944/preprints202510.1127.v2

the mqtt_broker, which then forwards it to the digital_twin. This stable, cyclical baseline traffic was recorded for 60 minutes without any faults or attacks. Data rate metrics—Packets per Second (PPS) and Bytes per Second (BPS)—were recorded in one-second time windows. The mean (μ) and standard deviation (σ) of these metrics were then computed to establish the statistical baseline (as detailed in Table 2).

Second, anomaly detection is implemented based on this baseline. For each new data rate measurement collected during fault and attack scenarios, an anomaly is flagged whenever the observed value exceeds a defined threshold. As an initial criterion, a threshold of three standard deviations ($\mu \pm 3\sigma$) was adopted, a common practice in statistical process control for identifying statistically significant deviations. This "white box" method is computationally efficient, requires no training, and is highly interpretable, making it ideal for resource-constrained edge devices.

4.2. Experimental Setup and Implementation

The experimental environment was developed using Docker containerization technology. This platform was selected for its ability to create isolated, lightweight, and reproducible environments, making it ideal for simulating the complex architecture of a Digital Twin (DT) system. The simulation architecture consisted of three main container types, each fulfilling a specific role:

- **Simulated physical device containers:** These containers emulate the behavior of Programmable Logic Controllers (PLCs) and Industrial Internet of Things (IIoT) devices.
- **Digital Twin container:** This container hosts the virtual representation of the physical devices and functions as a system capable of receiving, processing, and storing data across various communication protocols.
- **Monitoring container (Sniffer):** Operating as a dedicated component, this container is responsible for capturing and analyzing network traffic without interfering with the primary data flow.

An overview of the proposed method is presented in Figure 1. The monitoring system (Sniffer) non-intrusively observes the communication channel that connects the physical world and its digital representation—the Digital Twin—to detect anomalies that may indicate a cyberattack.

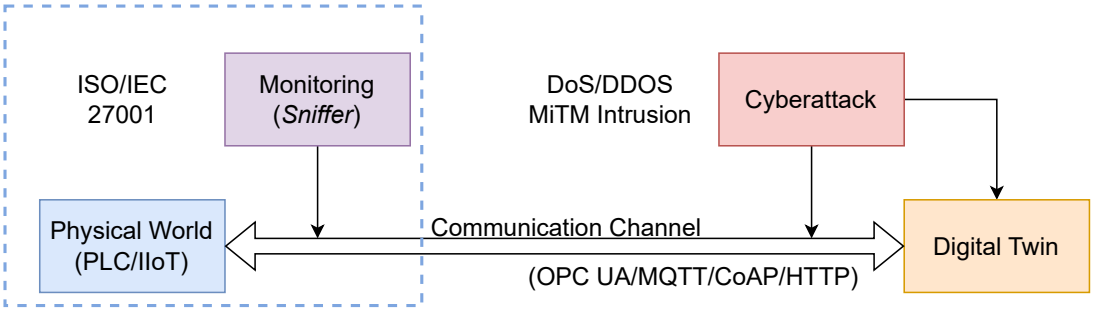

Figure 1. Conceptual architecture of the non-intrusive monitoring approach. The diagram illustrates the communication flow between the physical world (PLC/IIoT) and the Digital Twin, which relies on a communication channel (e.g., OPC UA/MQTT). This channel is identified as the primary attack vector for threats such as DoS, MiTM, and intrusion. The core component of our method, the "Monitoring (Sniffer)," is strategically positioned to non-intrusively capture data rate metrics from this channel for anomaly detection.

The monitoring system (Sniffer) non-intrusively observes the communication channel linking the physical world (simulated by PLC and IIoT devices) and its digital representation—the Digital Twin (DT). The Sniffer continuously analyzes the data rate, expressed in Packets per Second (PPS) and Bytes per Second (BPS), to detect anomalies that may indicate a cyberattack. It operates within a conceptual security perimeter aligned with international standards such as ISO/IEC 27001 [38].

It is important to clarify the relationship between the conceptual architecture (Figure 1) and the logical implementation (Figure 2). The conceptual method itself (Figure 1) is protocol-agnostic, as it monitors only data rates (PPS/BPS), not packet content, a strength we discuss in the Discussion

 doi:10.20944/preprints202510.1127.v2

(Section 5). For the experimental validation, however, a specific protocol stack had to be implemented. We selected MQTT as the primary communication channel for our logical architecture (Figure 2), as it is a dominant and representative standard in IIoT environments.

The detailed logical architecture of the simulation environment is shown in Figure 2. The diagram illustrates the interactions among the main containerized services, grouped into three functional domains: Main Flow, Monitoring, and Attack Vectors. The main operational flow (Main Flow) consists of data and command exchanges via MQTT between the Device and the Digital Twin, mediated by the MQTT Broker. The Monitoring component (Sniffer/IDS) passively observes this traffic, while the Attack Vectors represent the various entry points for simulated attacks, including direct assaults on the Digital Twin's API and interception of MQTT traffic through a proxy (MiTM Proxy).

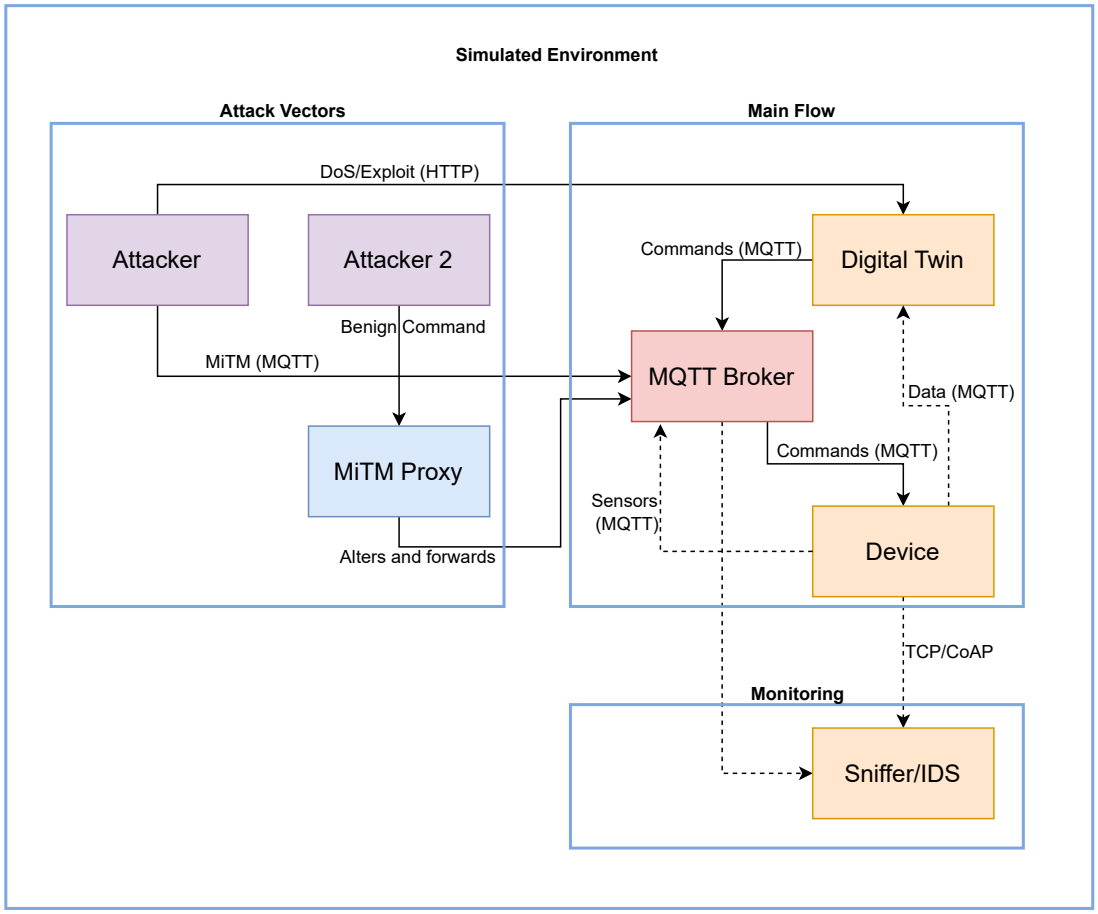

Figure 2. Logical architecture of the simulation environment. The flowchart details the experimental setup used to validate the proposed detection method. It illustrates the interactions among key components, including the simulated Device (sensors), the MQTT Broker, and the Digital Twin. Crucially, it identifies the injection points for attack vectors (DoS and MiTM) and the strategic placement of the "Monitoring (Sniffer/IDS)" component, which non-intrusively captures all network traffic for data rate analysis.

The experiments were conducted in a controlled environment. The host operating system was Ubuntu 24.04.3 LTS. Containerization was managed using Docker Engine version 28.4.0 and Docker Compose version 2.39.4. All scripts were developed in Python version 3.12. The system's functionality relied on several key libraries, whose versions are essential for reproducibility: Paho-MQTT 1.6.1, Requests 2.32.3, Python-OPC-UA 0.98.13, and aiocoap 0.4.3. This documented configuration provides a solid foundation for replicating the experiments, enabling other researchers to reproduce and extend the proposed scenarios. The complete source code is available as detailed in the Data Availability Section.

 doi:10.20944/preprints202510.1127.v2

4.3. Scenario Simulation and Validation

A fundamental step of our methodology involved simulating different operational scenarios to characterize the impact of anomalous events on transmission data rates. The objective was to establish a comparative basis for distinguishing anomalies resulting from malicious cyberattacks. To this end, the following types of communication faults were simulated:

- **Loss of connectivity:** Simulation of temporary and permanent interruptions in the communication of specific devices or in the connection with the Digital Twin.
- **Network latency:** Introduction of variable network delays to observe their effect on response time and data transfer rates.
- **Transmission errors:** Simulation of packet transmission errors to induce retransmissions and observe the consequent variations in the data rate, mimicking potential data corruption.
- **Bandwidth limitation:** Introduction of artificial network bottlenecks to reduce transmission capacity and simulate congestion conditions.

For each type of fault, specific network control methods were applied using the Linux tc (traffic control) utility with netem (Network Emulator) within the Docker environment. For example, Network Latency was introduced by applying netem delay rules via the tc utility, and Bandwidth Limitation was simulated using a tbf (Token Bucket Filter). Parameters such as duration and intensity were varied based on a risk analysis and common faults observed in industrial and IIoT systems. The analysis of the data collected during these simulations enabled the identification of specific patterns used later to distinguish operational faults from cyberattacks.

To investigate the sensitivity of the data rate as an indicator of malicious activity, several types of cyberattacks were simulated, targeting both the communication between the simulated physical elements and the Digital Twin, and the Digital Twin itself. The main targets were the communication channel and the Digital Twin container, with the goal of compromising the integrity and availability of the exchanged data. The simulated attacks included:

- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS):** These attacks aim to render the system unavailable by overwhelming communication resources or the Digital Twin itself with excessive requests or malicious traffic. This was implemented using a custom Python script that leveraged multi-threading to generate high volumes of `HTTP` GET requests directed at the Digital Twin's API.
- **Man-in-the-Middle (MiTM):** This attack seeks to intercept communication between the physical devices and the Digital Twin, with the potential to read or modify data in transit. This was simulated using a custom Python-based `TCP` proxy (as seen in Figure 2), which positioned itself at the communication layer to intercept traffic.
- **Intrusion and asset compromise:** This attack targets system vulnerabilities to gain unauthorized access to the Digital Twin, sending malicious commands (e.g., shutting down sensors) to the physical asset. This scenario, simulating an exploit, was implemented by sending malicious commands (e.g., 'shut-down') via unauthorized `HTTP` POST requests to the Digital Twin's API, simulating a sabotage attack.

For each attack type, parameters such as intensity and activity characteristics were varied. This allowed us to evaluate whether the anomalies in the data rate could be detected under different conditions and intensity levels, in order to determine detection thresholds and assess the sensitivity of the proposed method to diverse classes of threats.

The bidirectional communication flow during normal operation is illustrated in the sequence diagram shown in Figure 3. The simulated physical device sends telemetry data to the Digital Twin (step 1), which, in turn, can issue actuation commands to the device (step 3). The monitoring component (Sniffer), positioned within the communication channel, passively captures and analyzes all traffic (steps 2 and 4).

 doi:10.20944/preprints202510.1127.v2

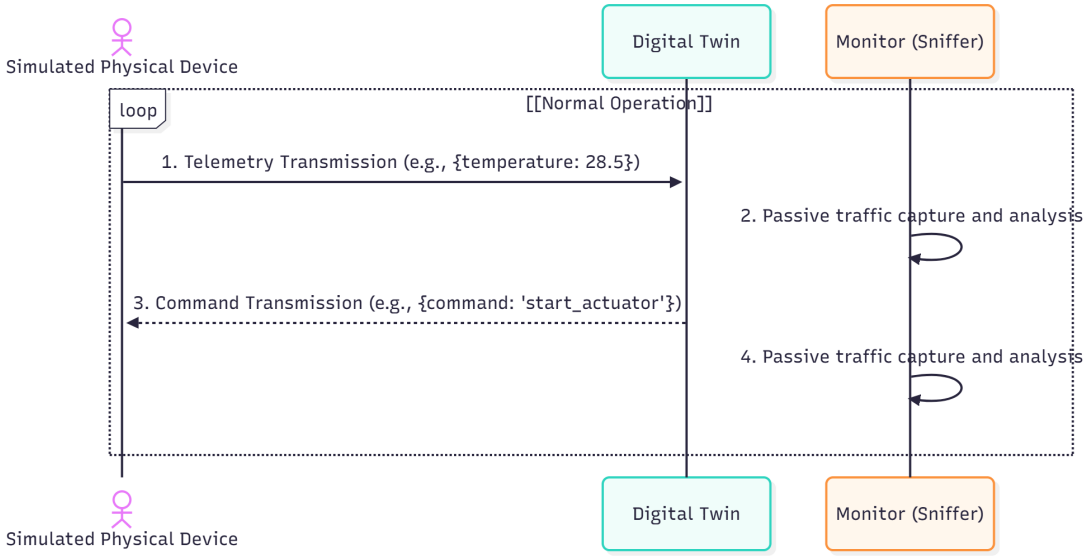

Figure 3. UML Sequence Diagram of the Non-Intrusive Monitoring Logic. This diagram depicts the standard MQTT publish/subscribe communication flow among the Device, MQTT Broker, and Digital Twin. It explicitly illustrates the role of the Monitoring (Sniffer) component, which operates in parallel to non-intrusively capture all network traffic. The Sniffer performs continuous data rate analysis (PPS/BPS) and, upon detecting a statistical anomaly (i.e., a threshold breach), triggers an alert to the Digital Twin, demonstrating the method's passive detection capability.

The third and final stage consisted of validating the methodology by verifying the correlation between the detected anomalies and the simulated events. This validation was performed by overlaying time series graphs, plotting the data rate alongside visual indicators marking the start and end of each fault or attack. This temporal analysis confirmed whether the detected anomalies coincided with the simulated events, thereby validating the method's ability to accurately identify abnormal activities.

The attack scenarios presented in Section 5 were executed under the following parameters: the Denial-of-Service (DoS) attack (Figure 4) was generated using 50 concurrent threads, resulting in an increased packet rate averaging approximately 800 PPS; the Man-in-the-Middle (MiTM) attack (Figure 5) was modeled to simulate the overload caused by a malicious proxy, increasing the packet rate to an average of 60 PPS; and the Intrusion attack (Figure 6) consisted of a 5-second burst of activity, with packet rates peaking at 150 PPS to simulate the sending of sabotage commands.

5. Results and Discussion

This section presents the experimental results obtained and discusses their implications. Subsection 5.1 first describes the quantitative outcomes of the simulations, demonstrating the effectiveness of the proposed data-rate monitoring approach in detecting the three attack scenarios. Subsection 5.2 then provides a comparison with state-of-the-art (SOTA) methods. Subsequently, Subsection 5.3 interprets these findings, situating the contributions of this work within the existing literature, highlighting its advantages, and acknowledging its limitations.

5.1. Results

The proposed data-rate monitoring approach was evaluated across three distinct cyberattack scenarios. The results show a strong correlation between the simulated attacks and statistically significant anomalies in network-traffic metrics, thereby validating the method's effectiveness. A detailed statistical analysis is presented in Table 2, while the temporal behavior of the traffic is illustrated in Figures 4, 5, and 6.

 doi:10.20944/preprints202510.1127.v2

Table 2. Statistical Baseline Parameters for Anomaly Detection. Descriptive statistics—mean (μ) and standard deviation (σ)—for the normal-operation baseline ($t < 40$ s) across all three simulated attack scenarios (DoS, MiTM, and Intrusion). These baseline values form the basis for computing the $\mu + 3\sigma$ statistical thresholds used to detect anomalous traffic, as visualized in Figures 4–6.

Attack Type	Period	Mean PPS	Std. Dev. PPS	Mean BPS	Std. Dev. BPS
DoS	Normal	13.75	4.27	7309.92	3082.47
DoS	Attack	779.30	156.03	50904.75	15049.37
MiTM	Normal	12.70	4.59	7085.28	2656.04
MiTM	Attack	65.68	14.97	25445.80	8674.89
Intrusion	Normal	14.95	5.08	7721.48	3213.76
Intrusion	Attack	21.52	55.55	3664.50	10141.59

As shown in Table 2, network traffic under normal operating conditions exhibited a stable and consistent baseline across all experiments, with an average packet rate ranging between 12.70 and 14.95 PPS. This baseline served as a reliable reference for detecting deviations.

In the first scenario, the initiation of the Denial-of-Service (DoS) attack (Figure 4) resulted in the immediate detection of a drastic anomaly. Table 2 quantifies this event: the average packet rate increased from a baseline of 13.75 PPS to 779.30 PPS—a surge of over 50-fold. The plots clearly illustrate this traffic flood, where both packets per second (a) and bytes per second (b) escalate sharply to sustained extreme levels, confirming the method's reliability in identifying volumetric attacks.

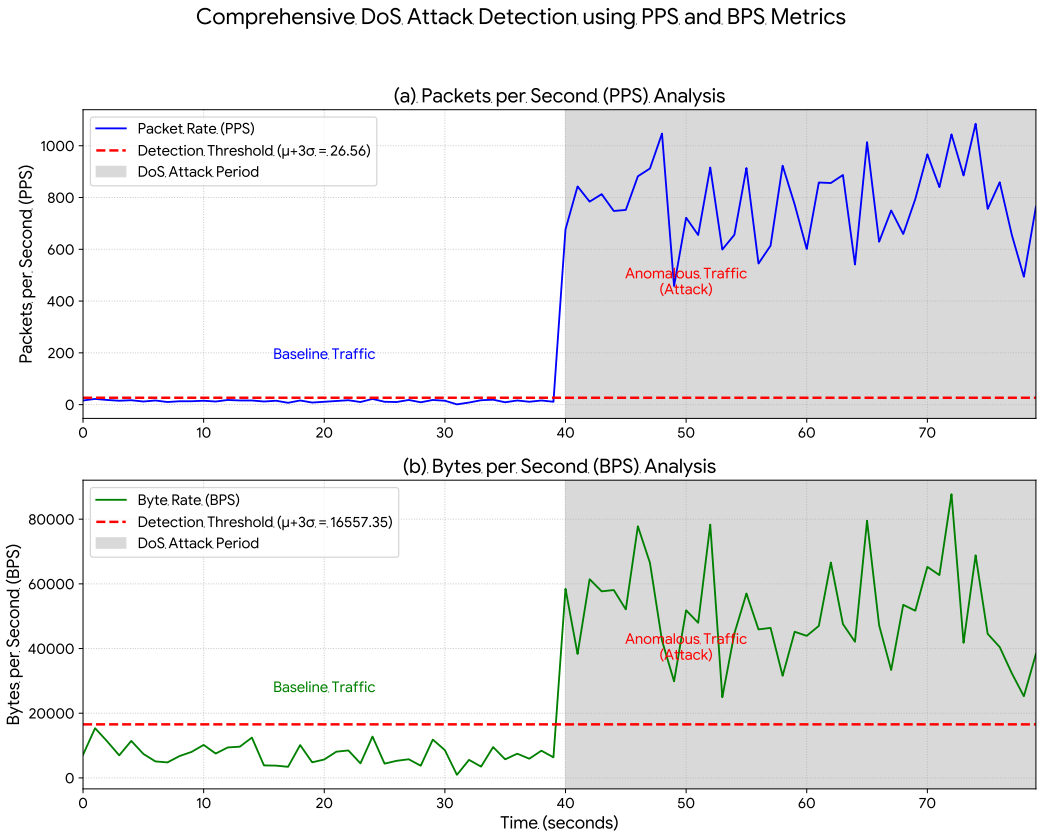

Figure 4. DoS Attack Detection Using PPS and BPS Metrics. Detection of a DoS attack (shaded region, $t \geq 40$ s) through data-rate monitoring. A baseline statistical threshold (red dashed line), corresponding to $\mu + 3\sigma$, was established based on normal operation ($t < 40$ s). Upon attack initiation at $t = 40$ s, both (a) Packets per Second (PPS) and (b) Bytes per Second (BPS) exhibit immediate and significant spikes that exceed the threshold, validating the method's effectiveness in identifying high-volume attacks.

 doi:10.20944/preprints202510.1127.v2

The Man-in-the-Middle (MiTM) attack (Figure 5) exhibited a more subtle yet clearly detectable signature. The average packet rate increased from 12.70 PPS to 65.68 PPS (Table 2). Although less pronounced than the DoS attack, this anomaly demonstrates the system's sensitivity in detecting not only flooding events but also traffic manipulations indicative of communication interception.

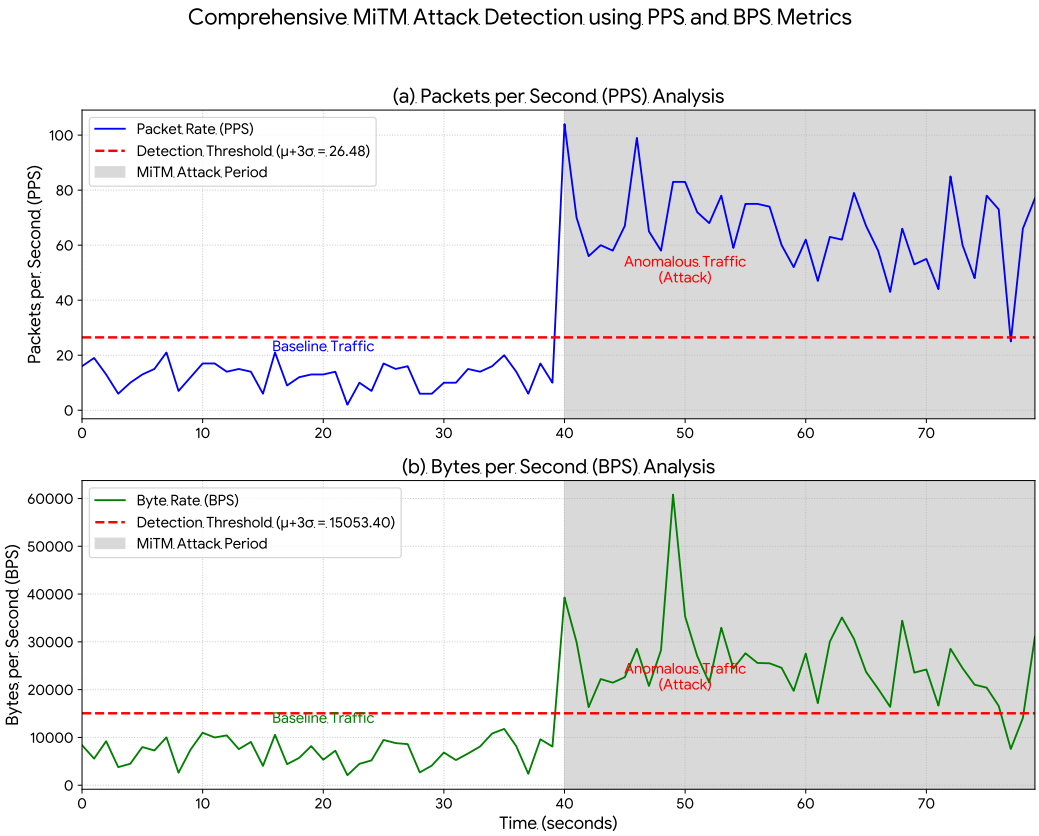

Figure 5. MiTM Attack Detection Using PPS and BPS Metrics. Detection of a Man-in-the-Middle (MiTM) attack initiated at $t = 40$ s (shaded region). Although its statistical signature is more subtle than that of the DoS attack, the anomalous traffic promptly exceeds the established $\mu + 3\sigma$ threshold (red dashed line) for both (a) Packets per Second (PPS) and (b) Bytes per Second (BPS). This result highlights the method's sensitivity in identifying attacks that attempt to blend with normal traffic patterns.

The intrusion attack (Figure 6) exhibited a distinctive statistical signature. As shown in Table 2, although the mean PPS showed only a modest increase (from 14.95 to 21.52), the standard deviation rose sharply from 5.08 to 55.55. This high variance corresponds to the behavior depicted in the plot: a brief, high-intensity traffic peak (command injection) followed by an almost complete collapse in communication. These results demonstrate that the method can detect anomalies not only in traffic volume but also on instability and abrupt state changes within the communication channel.

 doi:10.20944/preprints202510.1127.v2

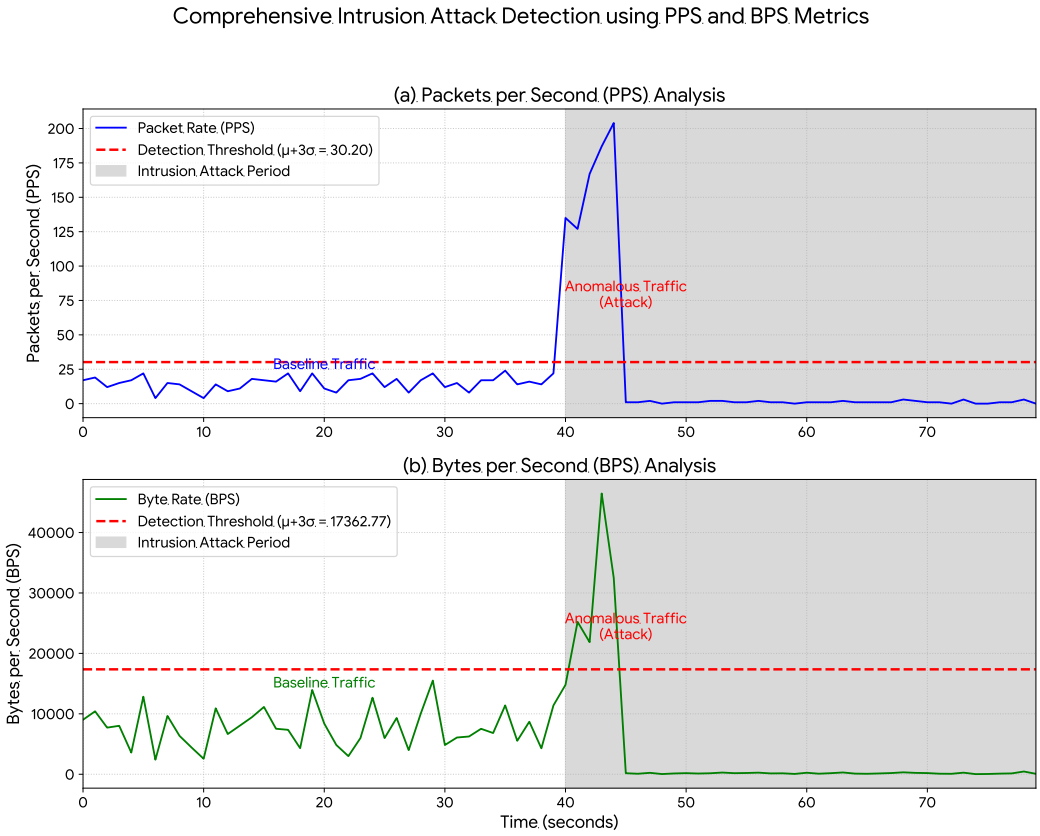

Figure 6. Intrusion Attack Detection Using PPS and BPS Metrics. Results from the intrusion attack simulation (shaded region, $t \geq 40$ s). The attack produces a distinct, short-duration traffic spike that markedly exceeds the $\mu + 3\sigma$ statistical baseline (red dashed line) for both (a) Packets per Second (PPS) and (b) Bytes per Second (BPS). This clear threshold violation confirms the method's capability to identify unauthorized intrusion events based on their data-rate footprint.

5.2. Comparison with State-of-the-Art Methods

A critical analysis of the literature necessitates comparing the proposed method with state-of-the-art (SOTA) approaches, particularly those based on Machine Learning (ML) and Deep Learning (DL), which have been extensively studied (as summarized in Table 1).

Table 3 synthesizes this comparison, focusing on two key metrics essential for a fair assessment: detection performance and computational efficiency (overhead).

It is important to note, as indicated by the asterisk (*) in Table 3, that the "Detection Performance" metrics of the SOTA methods and the proposed approach are not directly comparable. The SOTA values (e.g., 99.98%) typically refer to classification accuracy achieved on static benchmark datasets (e.g., KDD, CIC-IDS) following extensive training and feature extraction phases.

In contrast, the 100% value reported for our method represents the detection success rate within the simulated attack scenarios (Figures 4–6). Notably, this success rate (True Positive Rate) was achieved with a 0% False Positive Rate (FPR) during the normal operation period. As shown in Figures 4–6, the baseline traffic ($t < 40$ s) consistently remained below the $\mu + 3\sigma$ detection threshold. This distinction is critical: while SOTA approaches focus on complex traffic classification, our method—achieving 100% success in tests—emphasizes efficient, real-time detection of anomalous events in the IIoT context.

 doi:10.20944/preprints202510.1127.v2

Table 3. Comparison with State-of-the-Art (SOTA) Anomaly Detection Methods in IIoT. This table contrasts the proposed low-overhead statistical approach ($\mu + 3\sigma$ threshold) with state-of-the-art methods based on Machine Learning (ML) and Deep Learning (DL) identified in the literature. The comparison focuses on detection performance and computational efficiency, highlighting the trade-off between model complexity and suitability for resource-constrained IIoT environments.

Reference	SOTA Technique	Performance Metric	Computational Cost (Overhead)	Suitability for IIoT/Edge
[9]	FL, DL	99.98%(Accuracy)	High	Low
[26]	DL	99.87%(Accuracy)	High	Low
[21]	ML	99.64%(Accuracy)	Medium-High	Medium-Low
[17]	DL	99.60%(Accuracy)	High	Low
[20]	DL	99.45%(Accuracy)	High	Low
[11]	ML	98.77%(Accuracy)	Medium-High	Medium-Low
This paper	SDRM	100%(Detection Rate)*	Very Low	High

SOTA Technique: ML (Machine Learning), DL (Deep Learning), FL (Federated Learning), SDRM (Statistical Data Rate Monitoring).
Computational Cost (Overhead):
High: Refers to DL methods (FL, GANs, CNN-LSTM, Graph Models) that require intensive training and/or specialized hardware (GPU).
Medium-High: Refers to ML methods (GCN, Multiples) that require training and significant feature extraction.
Very Low: Refers to the proposed method, which requires no training and uses only simple statistical operations.
* The 100% metric represents the Detection Success Rate of the method in the three simulated attack scenarios (DoS, MiTM, Intrusion), where the statistical threshold was violated in all events.

The analysis of Table 3 reveals a fundamental *trade-off*:

1. **Accuracy vs. Complexity:** SOTA methods such as [9,26] indeed achieve very high detection accuracies, often exceeding 99.5% in classifying anomalous traffic. However, this performance entails significant computational overhead, requiring intensive training, complex preprocessing and feature extraction, and frequently specialized hardware (e.g., GPUs) for real-time inference—requirements our method eliminates, as demonstrated in Section 4 and validated in Figures 4–6.
2. **Efficiency in IIoT Contexts:** This high computational overhead makes complex ML/DL models impractical or undesirable in many IIoT and Digital Twin scenarios, where devices such as PLCs or edge sensors possess limited resources.

Strengths and Limitations.

The principal strength of our approach, as supported by Table 3, lies in its exceptional computational efficiency. Calculating a $\mu + 3\sigma$ threshold is a straightforward statistical operation that can be executed on a lightweight network sniffer or edge device with minimal resource consumption and without adding latency to the system. The main limitation of the approach is its specialization in detecting anomalies that affect data-rate metrics. However, as demonstrated in Figures 4–6, a wide range of attacks (DoS, MiTM, and Intrusion) generate distinct and detectable statistical signatures within these metrics. In conclusion, although SOTA ML/DL methods may achieve higher accuracy in classifying complex attack types, the proposed low-cost statistical approach offers a more efficient, interpretable, and context-aware solution for Digital Twin security—serving as a robust first line of defense.

5.3. Discussion

The presented results provide compelling evidence supporting the viability of data-rate analysis as a primary indicator for detecting cyberattacks in Digital Twin (DT) communication channels. However, the significance of these findings extends beyond simple anomaly detection and can be interpreted through three complementary perspectives: the diagnostic versatility of the method, its operational implications for industrial environments, and its role as a lightweight and robust security mechanism.

 doi:10.20944/preprints202510.1127.v2

The central implication of this study lies in demonstrating that fundamental network metrics—such as packet and byte rates—serve not only as performance indicators but also as valuable sources of security information. The method's ability to detect three fundamentally distinct attack classes—a volumetric attack (DoS), an interception attack (MiTM), and a sabotage attack (Intrusion)—attests to its robustness and generalizability. Rather than being a threat-specific solution, this approach functions analogously to a "nervous system" for the communication channel, exhibiting sensitivity to multiple types of disturbances.

Each attack produced a distinct statistical signature, as detailed in Table 2. The DoS attack manifested as a substantial increase in mean PPS, while the MiTM attack exhibited a more moderate rise. The Intrusion attack, in contrast, was characterized not by an increase in the mean but by a sharp rise in variance (standard deviation). This observation is crucial: data-rate monitoring provides not only a binary alert (normal vs. anomalous) but also a foundation for preliminary threat characterization and classification, offering an operational advantage for prioritizing incident response.

This ability to support threat characterization underscores a fundamental contrast with many state-of-the-art (SOTA) approaches in the literature. While machine learning (ML) and deep learning (DL) methods have demonstrated high proficiency in detecting complex anomalies, they often entail significant computational costs [9,11,17,21,26] and suffer from limited interpretability—the so-called "black box" problem [9,20,26]. In Operational Technology (OT) environments, where computational resources are limited and rapid, transparent diagnostics are essential, AI-based alerts lacking causal explanations can be problematic. Operators need not only to know that an anomaly has been detected, but also why it was detected, as the underlying rationale determines the appropriate incident response.

It is important to clarify *why* these attacks generated these signatures. The **MiTM** attack (Figure 5) was not a passive eavesdropping attack, but an active `TCP` proxy. While the data volume might be similar, the proxy implementation inherently introduces significant *protocol overhead* (e.g., additional packet handshakes, acknowledgments, and proxy processing), which results in the moderate but clearly detectable increase in PPS and BPS. The **Intrusion** scenario (Figure 6) was simulated as a high-intensity *burst* of unauthorized `HTTP POST` commands designed for rapid sabotage. This burst (and not a "low-and-slow" attack) is what creates the distinct, short-duration, high-volume spike that our method detected.

In contrast, the approach proposed in this work is grounded in the principle of direct interpretability—a "white box" design. The cause of each alert is explicitly tied to a violation of a statistical threshold in fundamental and intuitive metrics, such as packets or bytes per second. This simplicity constitutes a strategic advantage rather than a limitation. The modest computational requirements for calculating means and standard deviations in real time make the method suitable for deployment on edge devices or resource-constrained gateways, serving as an efficient, low-latency first line of defense. This approach therefore directly addresses the trade-off identified in Table 3, prioritizing high adequacy and low overhead for IIoT contexts over the costly, high-precision classification of SOTA methods.

Additionally, the proposed approach is largely application-protocol agnostic. While many Intrusion Detection Systems (IDS) rely on specific parsing rules for protocols such as MQTT, OPC UA, or HTTP [35], data-rate monitoring operates at a lower abstraction level, remaining sensitive to anomalies regardless of the communication protocol employed. This grants greater flexibility and adaptability, especially in heterogeneous industrial ecosystems where legacy and modern technologies coexist.

6. Conclusion

This study demonstrates the viability of a non-intrusive and computationally lightweight approach for detecting cyberattacks in Digital Twin (DT) communication channels—an increasingly critical threat vector in Industrial Internet of Things (IIoT) environments. Through a controlled simulation environment, we demonstrated that monitoring and statistically analyzing fundamental network metrics—specifically packet rate (PPS) and byte rate (BPS)—is highly effective for identifying a diverse

 doi:10.20944/preprints202510.1127.v2

range of malicious activities. The method proved robust, achieving a 100% Detection Success Rate (True Positive Rate) across the three simulated attack classes (DoS, MiTM, and Intrusion), with a 0% False Positive Rate (FPR) during normal operation (baseline).

The principal contribution of this work lies in validating that data-rate analysis can serve as a robust and interpretable first line of defense. More importantly, the study highlights that the intrinsically predictable and deterministic nature of IIoT traffic enables a simple statistical threshold ($\mu + 3\sigma$) to act as a high-fidelity anomaly detector. This approach addresses a critical gap in the literature, which largely focuses on computationally intensive methods (e.g., ML/DL), by offering a low-overhead alternative ideally suited for this context. The results indicate that this strategy can significantly enhance the resilience and security of Digital Twin systems by providing an effective early-warning mechanism.

In practical terms, this method can be deployed as a lightweight network sensor that monitors traffic at critical points within OT/IT networks. The generated anomaly alerts can be seamlessly integrated into existing Security Information and Event Management (SIEM) platforms, thereby enriching situational awareness without overburdening the control infrastructure. Future work will focus on validating the approach in physical testbeds and exploring adaptive thresholding techniques to further improve detection sensitivity.

Despite its effectiveness and advantages, certain limitations must be acknowledged, which also define opportunities for future research. The primary limitation arises from the experimental setup, as validation was performed within a controlled Docker-based simulation. Although this approach ensures reproducibility and controlled variable isolation, it cannot fully capture the complexity and unpredictability of physical industrial networks, including hardware jitter, electromagnetic interference, and the heterogeneous behavior of legacy components.

Furthermore, while the tested attack scenarios encompass distinct threat classes, they are not exhaustive. More sophisticated threats—such as low-and-slow or Advanced Persistent Threats (APT)—may induce data-rate anomalies that remain below simple statistical thresholds. Detecting such stealthy attacks will require more sensitive and adaptive analytical strategies beyond fixed-threshold monitoring.

Building upon these findings, future research can advance in three main directions. The first is the validation of the proposed method in physical testbeds integrating industrial hardware such as programmable logic controllers (PLCs), sensors, and network switches to evaluate real-world performance. The second involves expanding the detection scope by assessing sensitivity to a broader range of stealthy or evolving threats. Finally, the third direction entails exploring hybrid architectures, in which data-rate monitoring serves as a low-cost preliminary trigger that activates more computationally intensive analyses—such as deep packet inspection or ML-based classifiers—upon the detection of an initial anomaly, enabling an efficient, layered, and resilient defense system.

Overall, the proposed statistical data-rate monitoring approach offers a practical pathway toward more interpretable, efficient, and resource-aware cybersecurity in Industrial Digital Twin systems.

Data Availability Statement: The complete source code, Docker configuration files ($docker - compose.yml$), and scripts used to generate the results presented in this article are publicly available in a GitHub repository at the following address: Github.

Abbreviations

The following abbreviations are used in this manuscript:

DT	Digital Twin
DTs	Digital Twins
IIoT	Industrial Internet of Things
OT	Operational Technology
DoS	Denial-of-Service
MiTM	Man-in-the-Middle

 doi:10.20944/preprints202510.1127.v2

PPS	Packets Per Second
BPS	Bytes Per Second
SIEM	Security Information and Event Management
APT	Advanced Persistent Threat
IDS	Intrusion Detection System
CIA	Confidentiality, Integrity, and Availability
PLC	Programmable Logic Controller

References

1. Grieve, M. W. *Digital Twin: Manufacturing Excellence through Virtual Prototyping*; University of Michigan, 2003; White Paper.
2. Tao, F.; Cheng, J.; Qi, Q.; Zhang, M. Digital twin-driven product design, manufacturing and service with big data. *Int. J. Adv. Manuf. Technol.* **2018**, *94*(5–8), 1509–1520. https://doi.org/10.1007/s00170-017-0233-1.
3. Botín-Sanabria, D.M.; García-Méndez, L.C.; Gaviria-López, C.A.; Muñoz-Guerrero, J.D.; Arango-Serna, M. Digital twins for smart cities: a review of current applications and future trends. *Sustain. Cities Soc.* **2024**, *109*, 105652. https://doi.org/10.1016/j.scs.2024.105652.
4. Hosamo, H.; Al-Hussein, M.; Almashaqbeh, A.; Al-Kasasbeh, B. A Review of the Digital Twin Technology in the AEC-FM Industry. *Adv. Civ. Eng.* **2022**, *2022*, 2185170. https://doi.org/10.1155/2022/2185170.
5. Al-Fawwaz, A.; Al-Qaralleh, A.; Al-Majali, A.; Qadan, M. A Comprehensive State-of-the-Art Review for Digital Twin: Cybersecurity Perspectives and Open Challenges. *Sensors* **2023**, *23*(8), 4635. https://doi.org/10.3390/s23084635.
6. Bhushan, M.; Kumar, A.; Kumar, A.; Prakash, S. Advancing Security with Digital Twins: A Comprehensive Survey. *arXiv* **2025**, arXiv:2505.17310.
7. Liu, C.; Ren, Y.; Wang, H.; Yu, G.; Xu, X.; Su, B. Federated Learning for Intrusion Detection in Industrial IoT and Digital Twin. *IEEE Trans. Ind. Informatics* **2024**, *20*(8), 9205–9215. https://doi.org/10.1109/TII.2023.3330386.
8. Liu, W.; Li, D.; Guo, Q.; Zhang, H.; Lv, Y.; Chen, J. Blockchain-Enabled Digital Twin for Secure and Resilient Industrial Systems. *IEEE Trans. Ind. Informatics* **2024**, *20*(4), 3841–3852. https://doi.org/10.1109/TII.2023.3303721.
9. Belay, M.A.; Rasheed, A.; Rossi, P.S. Digital Twin Knowledge Distillation for Federated Semi-Supervised Industrial IoT DDoS Detection. *IEEE Internet Things J.* **2025**, doi:10.1109/JIOT.2024.3402120.
10. Zainudin, A.; Paramartha Putra, M.A.; Alief, R.N.; Kim, D.S.; Lee, J.M. Blockchain-aided Collaborative Threat Detection for Securing Digital Twin-based IIoT Networks. In Proceedings of the ICC 2024 - IEEE International Conference on Communications, Denver, CO, USA, 9–13 June 2024; pp. 4656–4661.
11. Li, S.; Zhang, Z.; Shi, H.; Wang, X. A Digital Twin Anomaly Detection Method Based on a Spatiotemporal Fusion Graph Convolutional Network. *Sensors* **2024**, *24*(4), 1253. https://doi.org/10.3390/s24041253.
12. Pan, J.; Chen, J.; Su, Z. Digital Twin-Based Anomaly Detection in Industrial Control Systems. *IEEE Trans. Ind. Informatics* **2023**, *19*(12), 11571–11580. https://doi.org/10.1109/TII.2023.3270921.
13. Yu, G.; Zhang, J.; Cao, Y.; Yu, H.; Zhang, Y. A Survey on Digital Twin-Empowered Anomaly Detection in Cyber-Physical Systems. *IEEE/CAA J. Autom. Sin.* **2024**, *11*(4), 833–852. https://doi.org/10.1109/JAS.2024.124231.
14. Wang, L.; Liu, C.; Li, Y.; Li, B. Digital Twin-Based Collaborative Anomaly Detection for Industrial IoT. *IEEE Internet Things J.* **2023**, *10*(13), 11466–11477. https://doi.org/10.1109/JIOT.2023.3243177.
15. Koroniotis, N.; Moustafa, N.; Schiliro, F.; Gauravaram, P.; Janicke, H. A holistic review of cybersecurity and intrusion detection systems in securing smart cities: a survey and future directions. *J. Netw. Comput. Appl.* **2023**, *213*, 103607. https://doi.org/10.1016/j.jnca.2023.103607.
16. Xie, J.; Zuo, H.; Fu, S.; Liu, S. IoT and Digital Twin assisted Deep Reinforcement Learning for Cyber-Physical Industrial Control Systems Security. *IEEE Trans. Ind. Informatics* **2023**, *19*(12), 11571–11580. https://doi.org/10.1109/TII.2023.3248888.
17. Zuo, H.; Xie, J.; Fu, S. Digital Twin-Driven Threat Detection for Industrial Control Systems via Dynamic Graph Learning. *IEEE Trans. Ind. Cyber-Phys. Syst.* **2024**, doi: 10.1109/TICPS.2024.3364741.
18. Liang, Z.; Tang, B.; Liu, Y.; Wang, S.; Chen, S. Hybrid Anomaly Detection for Industrial Control System Based on Digital Twin. *IEEE Trans. Circuits Syst. II Express Briefs* **2024**, *71*(2), 999–1003. https://doi.org/10.1109/TCSII.2023.3305459.

19. Wang, J.; Li, W.; Li, X.; Li, M. Digital Twin—A Review of the Evolution from Concept to Technology and Its Analytical Perspectives on Applications in Various Fields. *Sensors* **2024**, *24*(13), 5454. https://doi.org/10.3390/s24135454.
20. Yang, Y.; Wang, H.; Li, M.; Liu, Z.; Zhang, C. Anomaly detection in industrial IoT based on digital twin and deep learning. *Digit. Commun. Netw.* **2023**, *9*(5), 1276–1286. https://doi.org/10.1016/j.dcan.2022.11.002.
21. Li, H.; Ota, K.; Dong, M. Digital Twin-Based Intrusion Detection for Industrial Cyber-Physical Systems. *IEEE Netw.* **2023**, *37*(4), 180–186. https://doi.org/10.1109/MNET.2023.3259837.
22. Li, S.; Zhang, Z.; Shi, H.; Wang, X. A Digital Twin Anomaly Detection Method Based on a Spatiotemporal Fusion Graph Convolutional Network. *Sensors* **2024**, *24*(4), 1253. https://doi.org/10.3390/s24041253.
23. Ma, R.; Labbe, A.; Malo, A.; G-B. de Lamotte, F. Digital twin for situational awareness in industrial cybersecurity: A review and a new concept. *Comput. Ind.* **2023**, *148*, 103901. https://doi.org/10.1016/j.compind.2023.103901.
24. Puerto-Santana, F.; Puerto-Santana, E.; O'Leary, P.; Gutierrez-Estevez, M. A Digital Twin with HMMs for Industrial Anomaly Detection. *Sensors* **2022**, *22*(19), 7436. https://doi.org/10.3390/s22197436.
25. Shukla, S.; L-F. Pau, L.F.; Balasubramaniam, S.; Mustafa, M.A. Digital Twin-Based Anomaly Prediction in Industrial Control Systems. In Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 29–31 October 2021; pp. 836–845.
26. Abolfazi, S.A.; Tabaee, T.; G-B. de Lamotte, F. Digital-Twin-Enabled Intrusion Detection System for Industrial Control Systems: A GAN-Based Implementation. *Sensors* **2023**, *23*(6), 3209. https://doi.org/10.3390/s23063209.
27. Gnanaprakasam, A.; Anand, S.J.S.; Balasubramanian, S.; Akila, D. A trust management model using digital twin and blockchain for industrial IoT networks. *Peer-to-Peer Netw. Appl.* **2024**, *17*, 118. https://doi.org/10.1007/s12083-024-01648-z.
28. Sharma, A.; Singh, H. Digital Twin Empowered Autonomic Security Management in Industrial IoT Network. *IEEE Internet Things J.* **2024**, doi: 10.1109/JIOT.2024.3390890.
29. Niyonzuima, R.; Al-Maqbali, A.; Al-Bahri, Y.; Al-Barami, B.; Al-Hinai, M. Digital twin: a unified definition, issues, challenges, and opportunities. *J. Cyber Secur. Data Prot.* **2024**, *1*(1), 1–15.
30. Zhang, S.; Yang, J.; Hu, Z.; Yan, S.; Liu, Y. A systematic review of the digital twin technology in buildings, landscape and urban environment from 2018 to 2024. *Buildings* **2024**, *14*(11), 3475. https://doi.org/10.3390/buildings14113475.
31. Niyonzuima, R.; Al-Maqbali, A.; Al-Bahri, Y.; Al-Barami, B.; Al-Hinai, M. Digital twin: a unified definition, issues, challenges, and opportunities. *J. Cyber Secur. Data Prot.* **2024**, *1*(1), 1–15.
32. National Institute of Standards and Technology (NIST). Security and trust considerations for digital twin technology. *NISTIR 8356* **2025**. https://doi.org/10.6028/NIST.IR.8356.
33. Digital Twin Consortium. Understanding DTC's digital twin platform stack architectural framework. Technical Report, November 2023. Available online: https://www.digitaltwinconsortium.org/2023/11/understanding-dtcs-digital-twin-platform-stack-architectural-framework/.
34. Orange, J. Network digital twin: concepts and reference architecture. *IETF Internet-Draft draft-irtf-nmrg-network-digital-twin-arch-10* **2025**. Expires August 31, 2025.
35. Tange, K.; De Donno, M.; Fafoutis, X.; Dragoni, N. A systematic survey of industrial internet of things security: requirements and fog computing opportunities. *IEEE Access* **2020**, *8*, 123456–123478.
36. Herath, J.D.; Yan, G. Real-Time Evasion Attacks against Deep Learning-Based Anomaly Detection from Distributed System Logs. In Proceedings of the Eleventh ACM Conference on Data and Application Security and Privacy, Virtual Event, USA, 26–28 April 2021; pp. 29–40.
37. Rasheed, A.; Javed, A. R.; Habib, M. F.; Abbas, S.; Fatima, T.; Farooq, M. S. Privacy and security challenges of the digital twin: systematic literature review. *J. Univers. Comput. Sci.* **2024**, *30*(13), 1782–1806. https://doi.org/10.3897/jucs.114607.
38. International Organization for Standardization. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. ISO, 2022.