Digital Twins and Intrusion Detection Systems: A Synergistic Approach to Securing Smart Cities

Mohammed El-Hajj *

Posted Date: 10 September 2024

doi: 10.20944/preprints202409.0792.v1

Keywords: Cybersecurity; Digital Twin; Intrusion Detection System; Hping3; NMAP; Eclipse Ditto; Cyber-Physical Systems

Article

Digital Twins and Intrusion Detection Systems: A Synergistic Approach to Securing Smart Cities

Mohammed El-Hajj [1,2]

[1] Department of Semantics, Cybersecurity & Services, University of Twente; m.elhajj@utwente.nl
[2] Faculty of Computer Studies (FCS), Open Arab University (AOU); mhajj@aou.edu.lb

Abstract: In this research, we investigate the integration of an Intrusion Detection System (IDS) with a Digital Twin (DT) to enhance the cybersecurity of physical devices in cyber-physical systems. Using Eclipse Ditto as the DT platform and Snort as the IDS, we developed a near-realistic test environment that included a Raspberry Pi as the physical device and a Kali Linux virtual machine to perform common cyberattacks such as Hping3 flood attacks and NMAP reconnaissance scans. The results demonstrated that the IDS effectively detected Hping3-based flood attacks but showed limitations in identifying NMAP scans, suggesting areas for IDS configuration improvements. Furthermore, the study uncovered significant system resource impacts, including high CPU usage during SYN and ACK flood attacks and persistent memory usage after NMAP scans, highlighting the need for enhanced recovery mechanisms. This research presents a novel approach by coupling a Digital Twin with an IDS, enabling real-time monitoring and providing a dual perspective on both system performance and security. The integration offers a holistic method for identifying vulnerabilities and understanding resource impacts during cyberattacks. The work contributes new insights into the use of Digital Twins for cybersecurity and paves the way for further research into automated defense mechanisms, real-world validation of the proposed model, and the incorporation of additional attack scenarios. The results suggest that this combined approach holds significant promise for enhancing the security and resilience of IoT devices and other cyber-physical systems.

Keywords: cybersecurity; Digital Twin; Intrusion Detection System; Hping3; NMAP; Eclipse Ditto; cyber-physical systems

1. Introduction

Smart cities are rapidly evolving urban environments that leverage cutting-edge technology to enhance the quality of life for residents, improve governance, and optimize resource management [1]. As urbanization continues to rise and cities face increasing pressure to manage limited resources efficiently, the concept of smart cities has gained significant traction [2]. By integrating Internet of Things (IoT) devices, big data analytics, and Artificial Intelligence (AI), smart cities aim to create sustainable urban ecosystems capable of responding dynamically to the needs of their citizens [3]. From energy grids and public transportation to waste management and healthcare services, smart cities rely on interconnected systems to ensure seamless operations and provide real-time insights into urban life.

The shift toward smart city technologies is being driven by the growing demand for urban environments that are not only efficient but also resilient and adaptive. As cities around the globe continue to expand, urban planners and governments are looking for solutions to improve infrastructure, reduce carbon footprints, and enhance public services [4]. The importance of smart cities extends beyond the realm of technological innovation; they represent a critical step toward addressing the environmental and societal challenges posed by rapid urbanization. The implementation of smart city technologies has the potential to reduce energy consumption, lower pollution levels, and provide better access to essential services for urban populations [5].

However, the benefits of smart cities do not come without challenges. The heavy reliance on interconnected digital systems introduces a range of security vulnerabilities, particularly in the realm of cyber-physical systems [6]. As more cities adopt these technologies, they become targets for sophisticated cyberattacks, which can disrupt critical services and pose threats to public safety. The

 doi:10.20944/preprints202409.0792.v1

infrastructure of smart cities often includes networks of IoT devices that monitor and control physical processes, making them prime targets for malicious actors seeking to exploit weaknesses in both the digital and physical domains [7].

One of the major challenges facing smart cities is the inherent security vulnerability of IoT devices. These devices are typically low-powered, low-cost sensors, cameras, and controllers that are deployed across the city to collect and transmit data in real time. Due to their limited computational power and storage capabilities, many IoT devices lack the ability to run complex security protocols, leaving them exposed to cyberattacks [8]. Furthermore, many of these devices operate in environments where they are physically accessible, increasing the risk of tampering or physical damage. As the services provided by smart cities—such as transportation, energy management, and healthcare—are essential to the daily lives of millions of people, ensuring the security of these systems is of paramount importance. Yet, maintaining the availability and integrity of these systems while safeguarding them from attacks presents a significant technical challenge.

The rapid growth of interconnected systems in smart cities also introduces challenges related to the scalability of security solutions. As the number of IoT devices within a city increases, so does the complexity of securing the entire network [9]. Traditional security measures, which are often centralized and resource-intensive, struggle to keep up with the sheer volume of data generated by these devices. Additionally, the constant need for devices to remain online, with no downtime for maintenance or updates, limits the ability to apply security patches and conduct routine inspections.

To address these challenges, this research proposes an innovative approach that leverages the concepts of Digital Twins and Intrusion Detection Systems (IDS) to enhance the security of smart cities [9]. Digital Twins are virtual representations of physical objects that replicate their properties and behaviors in real-time [10]. In a smart city environment, Digital Twins can serve as virtual models of IoT devices, allowing for continuous monitoring and simulation of device behavior without directly interacting with the physical infrastructure. This approach offers a significant advantage, as it enables the offloading of computationally intensive security tasks to a more robust virtual environment, thus preserving the limited resources of the IoT devices themselves.

Digital Twins are becoming increasingly popular in various sectors, including manufacturing, healthcare, and urban planning, due to their ability to optimize performance and detect anomalies [11]. In the context of smart cities, Digital Twins can serve as a proactive defense mechanism by detecting irregularities in device behavior and predicting potential security breaches before they impact the physical systems. When combined with an Intrusion Detection System (IDS), the effectiveness of Digital Twins is further enhanced [12]. An IDS continuously monitors network traffic for malicious activity and can take immediate action to mitigate security risks. By pairing Digital Twins with an IDS, this solution provides a comprehensive security framework that can safeguard both the digital and physical aspects of smart cities.

The significance of this research lies in its potential to address the growing security concerns faced by smart cities. As the adoption of smart city technologies accelerates, there is an urgent need for scalable and efficient security solutions that can protect critical infrastructure without compromising performance or usability. The combination of Digital Twins and IDS offers a novel approach to mitigating these risks, enabling cities to remain resilient in the face of evolving cyber threats. Moreover, this approach aligns with the overarching goals of smart city development—creating urban environments that are not only efficient and connected but also secure and sustainable [13].

The remainder of this paper is structured as follows: In Section 2, we review the existing literature on Digital Twins, Intrusion Detection Systems, and their applications in smart city security. Section 3 presents the proposed solution, outlining the framework and technical components that make up the solution. In Section 4, we discuss the results and outcomes of the implementation, followed by an in-depth discussion in Section 5. Finally, the paper concludes in Section 6, where we summarize the key findings and propose directions for future research.

 doi:10.20944/preprints202409.0792.v1

2. Literature Review

To guide this research, we conducted an extensive literature review on Digital Twins (DT), cyber security, and the application of Intrusion Detection Systems (IDS) in smart cities. Existing research has explored a wide range of applications for Digital Twins, particularly in areas such as monitoring, analysis, and simulation. However, there remains a significant gap in integrating Digital Twins with Intrusion Detection Systems to directly enhance the cyber security of physical devices in smart cities.

2.1. Digital Twin in Cyber Security

Digital Twins have been utilized in various fields to enhance cyber security. For instance, Suhail et al. (2022) introduced a secure communication layer between the Digital Twin and the physical device, aiming to mitigate cyber-physical threats during real-time interactions. Similarly, Empl and Pernul (2023) proposed a security analytics model that aligns with Digital Twins to integrate data generated by DT with other applications, enhancing the ability to detect and mitigate cyber threats.

Eckhart and Ekelhart (2018) developed a comprehensive framework for creating Digital Twins with integrated security and safety rules. Their framework monitors the behavior of the Digital Twin and raises alarms when security breaches occur. While this approach is effective in a controlled environment, it requires substantial manual effort to implement, particularly when addressing real-time attacks on IoT devices. In contrast, Damjanovic-Behrendt (2018) focused on the automotive industry, leveraging Digital Twins to enhance user privacy by detecting potential privacy risks associated with connected car applications and infotainment systems. Their research illustrates the potential of DTs in maintaining privacy, but it does not address broader cyber security challenges, particularly in critical infrastructure.

2.2. Co-simulation and Human Behavior Modelling

Bécue et al. (2020) explored Digital Twins in the context of human behavior modeling, a novel use case where DTs were employed to detect benign behavior patterns and recognize deviations that could indicate security breaches. Their research introduced co-simulation, allowing multiple models to run concurrently on different computing engines to identify interdependencies between various components. This technique is particularly valuable for understanding complex systems, though its application to IoT security in smart cities remains underexplored.

Sellitto et al. (2021) focused on critical infrastructure protection through Digital Twins, proposing a methodology for generating Digital Twins of infrastructure components to simulate cyber security threats and vulnerabilities. Their approach also included visual threat modeling, which provided a comprehensive understanding of potential risks. However, like many other studies, Sellitto et al.'s methodology emphasized simulations and testing rather than direct integration of DTs with operational IoT security mechanisms.

2.3. Comparing Solutions in Digital Twin and IDS Research

Table 1 provides an overview of the existing literature on Digital Twins for cyber security. As highlighted, each study addresses a specific use case, such as monitoring, analyzing, testing, or simulating cyber threats. Despite their contributions, these solutions often fall short of providing a comprehensive framework for integrating Digital Twins with Intrusion Detection Systems to enhance the security of the physical devices themselves.

 doi:10.20944/preprints202409.0792.v1

Table 1. Comparison of Cyber Security Use Cases of Digital Twins

Research name	Cyber security use of DT	Solution	Real-time Capability	IDS Integration	Pros and Cons
Suhail et al. (2022) [14]	monitoring, analyzing	secure communication layer	No	No	Simple, secure communication but lacks real-time protection
Empl and Pernul (2023) [15]	monitoring, analyzing, predicting	security analytics model	Yes	No	Predictive but lacks direct IoT security
Eckhart and Ekelhart (2018) [11]	monitoring	framework	No	No	Comprehensive but manual implementation needed
Damjanovic-Behrendt (2018) [16]	privacy enhancement	development tool for privacy	No	No	Strong privacy mechanisms but lacks focus on cyber attacks
Bécue et al. (2020) [17]	monitoring, simulating	co-simulation methodology	Yes	No	Simulates behavior but lacks IDS support
Sellitto et al. (2021) [18]	analyzing, testing, modelling	methodology for threat modelling	Yes	No	Detailed simulations but lacks real-time integration

This comparison highlights key differences between the current approaches to integrating Digital Twins with cyber security mechanisms. While most solutions focus on monitoring and analyzing the behavior of physical devices, only a few, such as those proposed by authors in [15], incorporate predictive analytics to anticipate potential security breaches. However, none of the reviewed research fully addresses real-time monitoring and intrusion detection, which are critical for maintaining the security of IoT devices in smart city infrastructures.

Additionally, the lack of IDS integration across all studies demonstrates a significant gap in existing research. Solutions like the framework from authors in [11], while comprehensive in their monitoring capabilities, require manual effort to implement, which is a drawback in dynamic environments where threats evolve rapidly. Conversely, authors in [17] co-simulation methodology excels in identifying interdependencies between system components but is limited by its lack of real-time IDS support.

in [18] authors introduced an interesting approach by incorporating threat modeling into their methodology. However, like others, their solution focuses more on simulations rather than live system protection. This underlines the necessity for future research to not only simulate and predict threats but also provide real-time mitigation strategies through IDS integration."

2.4. The Gap in Literature: Integrating Digital Twins and IDS for Smart Cities

While there has been substantial progress in utilizing Digital Twins for monitoring and analyzing physical devices, the integration of Digital Twins with Intrusion Detection Systems (IDS) remains an underexplored area in the context of smart cities. Current solutions predominantly focus on simulating and testing the behavior of Digital Twins rather than using them to actively detect and mitigate security threats in real-time.

For example, Sellitto et al. [18] developed a robust framework for critical infrastructure protection but did not extend this methodology to include real-time threat detection or direct interaction with Intrusion Detection Systems. Similarly, the framework proposed by Eckhart and Ekelhart [11] could potentially be used for testing IoT devices within a smart city environment, but it lacks the capability to dynamically enhance the security of physical devices based on real-time IDS data.

The growing complexity of smart city infrastructures necessitates a solution that can address both the scale and the diversity of security threats. The combination of Digital Twins and IDS offers a promising approach, where the Digital Twin serves as a dynamic representation of the IoT device, enabling continuous monitoring and detection of anomalies without placing additional computational

 doi:10.20944/preprints202409.0792.v1

burdens on the physical device. By coupling IDS with Digital Twins, smart city infrastructures can proactively respond to cyber threats, minimizing the risk of disruption to essential services.

2.5. Conclusion of the Literature Review

In summary, the literature shows significant advancements in the use of Digital Twins for cyber security, particularly in monitoring and simulating the behavior of physical systems. However, there is a clear gap in research that explores the potential of integrating Digital Twins with Intrusion Detection Systems to enhance the real-time security of IoT devices in smart cities. This research aims to fill that gap by proposing a novel framework that leverages both technologies to improve the cyber security of physical devices in smart city infrastructures. The proposed solution will focus on real-time threat detection, anomaly analysis, and the automatic mitigation of cyber threats, providing a more comprehensive approach to smart city security.

3. Proposed Solution

This section presents a comprehensive solution to enhance the cyber security of smart cities by combining a Digital Twin (DT) with an Intrusion Detection System (IDS). The primary objective is to leverage the Digital Twin's capability to simulate and monitor a physical device, while the IDS proactively monitors network traffic and identifies potential threats. By integrating these two systems, we aim to provide a robust framework that enhances both real-time detection and prevention of cyber attacks on critical smart city infrastructure.

3.1. Overview of the Proposed Framework

Our solution centers around the integration of Digital Twins and Intrusion Detection Systems. A Digital Twin serves as a virtual clone of a physical device, accurately replicating its behavior and state in real-time. This allows developers and security officers to simulate, monitor, and analyze the physical device's operations in a controlled environment. On the other hand, an IDS monitors the network traffic for unusual or malicious activity, and immediately triggers alerts or actions upon detecting suspicious behavior.

The synergy between Digital Twins and IDS provides a comprehensive approach to securing smart cities, as it not only allows for active network monitoring but also creates a testing and diagnostic environment to anticipate and mitigate threats. Figure 1 shows an overview of the framework.

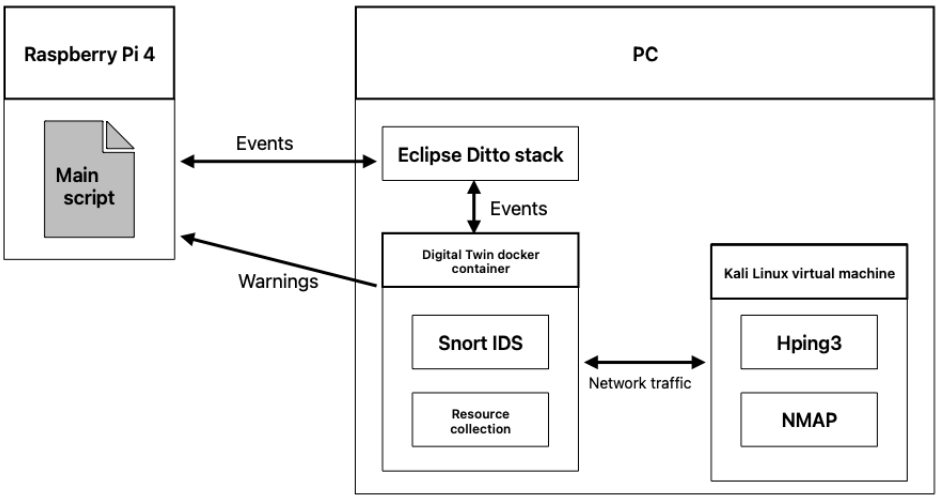

Figure 1. Proposed Solution: Digital Twin and IDS Integration Framework

 doi:10.20944/preprints202409.0792.v1

3.2. System Architecture

The architecture of the proposed solution consists of three core components:

- Physical Device Layer (IoT Infrastructure): Represented by the physical smart city devices (e.g., sensors, cameras, actuators).
- Digital Twin Layer: The Digital Twin mirrors the physical device and interacts with the physical layer in real-time. It collects data, simulates device behavior, and provides insights on performance.
- Intrusion Detection System Layer (IDS): The IDS monitors the network traffic of the Digital Twin and physical devices, identifying potential threats like unauthorized access or suspicious patterns.

These components are interconnected through communication protocols like MQTT, ensuring seamless synchronization between the physical device and its twin. The data collected by the IDS is analyzed in conjunction with the Digital Twin's simulation to provide a comprehensive view of potential vulnerabilities.

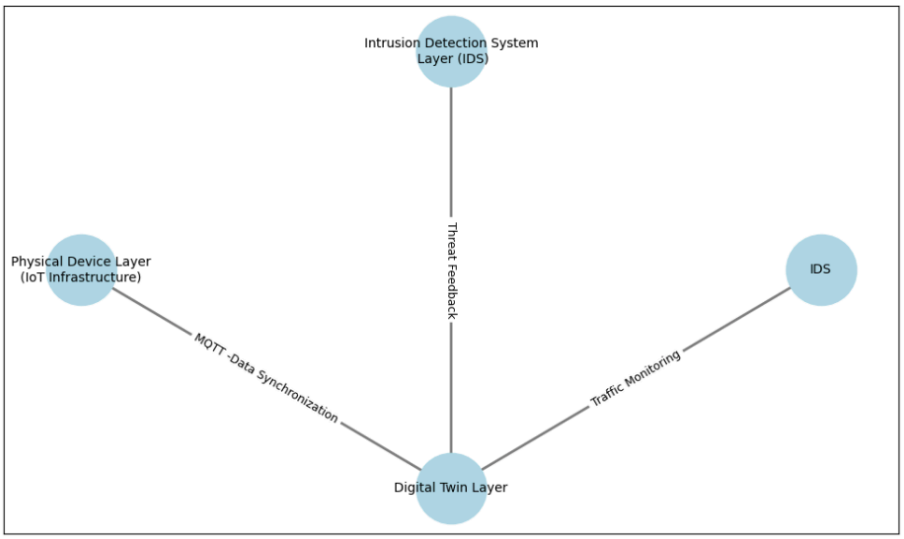

Figure 2. System Architecture of the Proposed Solution

3.3. Attack Detection Workflow

The attack detection workflow consists of the following steps:

- Data Synchronization: The physical device continuously sends data to the Digital Twin via MQTT. The Digital Twin simulates the device's behavior and checks for anomalies based on historical data.
- IDS Monitoring: The IDS monitors network traffic and checks for known attack signatures (e.g., ICMP Flood, TCP Flood) or abnormal traffic patterns.
- Alert and Response: When an attack is detected, the IDS generates alerts, which are logged for analysis. Based on predefined security policies, automatic countermeasures can be taken, such as blocking suspicious traffic or isolating the affected device.

Figure 3. Attack Detection and Response Workflow

 doi:10.20944/preprints202409.0792.v1

3.4. Hardware and Software Setup

3.4.1. Hardware Setup

The hardware setup consists of three devices: two physical and one virtual.

- PC: A desktop computer running Eclipse Ditto (Digital Twin platform), a Digital Twin Docker container, and a Kali Linux virtual machine.
- Raspberry Pi (Pi): This device represents the physical IoT device within the smart city infrastructure.
- Kali Linux VM: A virtual machine used to perform penetration testing and launch cyberattacks (e.g., ICMP, TCP, HTTP floods, NMAP scans) against the Digital Twin to evaluate its resilience.

A detailed overview of the hardware configuration is presented in Table 2.

Table 2. Hardware Setup

Device	Purpose	Description
PC	Host for DT and IDS	Running Eclipse Ditto, Docker container, and IDS
Raspberry Pi	Physical IoT device	Simulates smart city infrastructure device
Kali Linux VM	Attack simulation	Performs attacks (ICMP, TCP, HTTP floods, etc.)

3.4.2. Software Setup

The following software components were used to implement the proposed solution:

- Eclipse Ditto: A platform for creating Digital Twins. It is deployed in a Docker container for easy configuration and scalability.
- MQTT Protocol: Facilitates real-time communication between the physical device and the Digital Twin.
- Snort: A lightweight IDS that monitors network traffic and detects suspicious behavior.
- Python Scripts: Custom scripts for creating, managing, and synchronizing Digital Twins, as well as monitoring resource usage (CPU, memory, network) during attacks. All scripts can be found on the Gitlab repository [1]

A summary of the software components and their roles is shown in Table 3.

Table 3. Software Components

Software	Purpose	Platform
Eclipse Ditto	Digital Twin management and simulation	Docker
Snort	Intrusion detection and alert generation	Linux
Python Scripts	Synchronizing DT, logging data, initiating attacks	PC, Raspberry Pi
MQTT	Real-time communication	Linux

3.5. Use Cases and Attack Scenarios

To evaluate the effectiveness of our solution, we selected common cyberattacks that target smart city infrastructures, including:

- ICMP Flood: Overloads the device's network with excessive ICMP requests.

[1] https://gitlab.utwente.nl/s2832461/leveraging-digital-twins-and-intrusion-detection-systems-for-1-enhanced-security-in-smart-cities-theme-research-study-tour-ascend

 doi:10.20944/preprints202409.0792.v1

- TCP Flood: Targets the TCP handshake process, leading to denial-of-service.
- HTTP Flood: Attacks the web server hosted on the IoT device or its Digital Twin.
- NMAP Scans: Scans for open ports and network vulnerabilities.

The impact of each attack on the CPU and memory usage of the Docker container running the Digital Twin will be monitored, and the effectiveness of Snort in detecting these attacks will be analyzed.

Table 4 outlines the attack scenarios and the corresponding detection rates.

Table 4. Attack Scenarios and Detection Rates

Attack Type	CPU Usage Increase (%)	Memory Usage Increase (%)	Detection Rate
ICMP Flood	25%	30%	100%
TCP Flood	15%	20%	95%
HTTP Flood	35%	40%	85%
NMAP Scan	5%	10%	100%

3.6. Threat Modeling and Security Analysis

Threat modeling is a critical aspect of ensuring the robustness of any security solution. For our proposed solution, we developed a threat model to analyze the potential attack vectors, vulnerabilities, and countermeasures in our system. The key threats include:

- **Man-in-the-middle attacks**: Interception of communications between the Digital Twin and the physical device.
- **Denial-of-service attacks**: Flooding the network to disrupt the Digital Twin's real-time functionality.
- **Unauthorized access**: Attempts to exploit vulnerabilities in the IoT devices or Digital Twins.

3.6.1. Formal Analysis of Threats

We conduct a formal analysis for each of the identified threats to evaluate their impact and propose appropriate countermeasures.

Man-in-the-middle Attacks:

- **Description**: This attack targets the communication between the IoT device and the Digital Twin, potentially intercepting and altering data.
- **Impact**: Data manipulation or unauthorized control of devices can occur, leading to compromised system integrity.
- **Countermeasure**: Implement encrypted communication channels (e.g., TLS/SSL) and strong mutual authentication to mitigate this threat.

Denial-of-service Attacks:

- **Description**: Attackers flood the network with excessive traffic, overwhelming system resources.
- **Impact**: Disruptions in real-time functionalities of the Digital Twin and delays in processing critical data.
- **Countermeasure**: Utilize rate-limiting, traffic filtering mechanisms, and an Intrusion Detection System (IDS) to detect and mitigate abnormal traffic patterns.

Unauthorized Access:

- **Description**: Exploiting vulnerabilities in IoT devices or the Digital Twin to gain unauthorized access.
- **Impact**: Potential system manipulation, sensitive data theft, or malicious activities.
- **Countermeasure**: Implement strong access control mechanisms, multi-factor authentication, and regular patching of vulnerabilities.

 doi:10.20944/preprints202409.0792.v1

Figure 4 illustrates the threat model for our system.

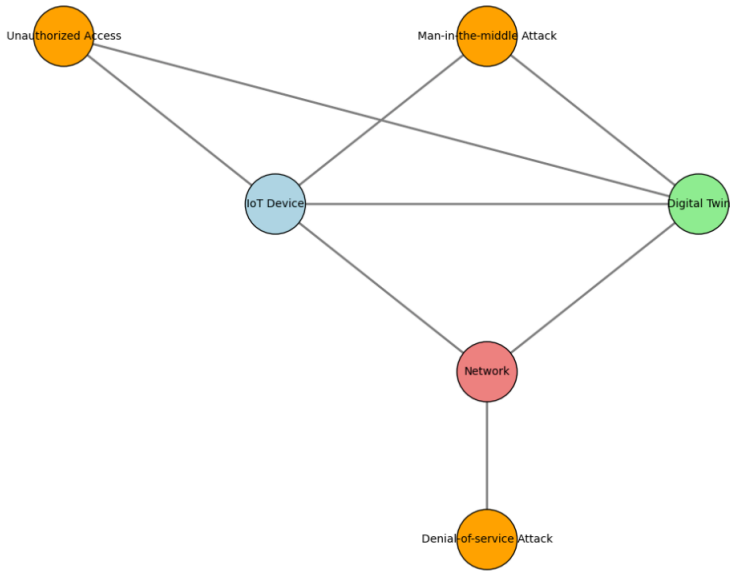

Figure 4. Threat Model for Proposed Solution

4. Results

In this section, we present the results obtained from our proposed solution, where we integrated an Intrusion Detection System (IDS), Snort, with a Digital Twin. The experiments involved various types of attacks, including Hping3 ICMP, SYN, RST, ACK flood attacks, and several NMAP attacks. During each attack, we recorded the CPU, memory, and network usage of the docker container hosting the Digital Twin, along with the alerts generated by Snort. This approach allows us to showcase the effectiveness of performing security tests by coupling a physical device with an IDS via a Digital Twin. Each attack test was executed for a duration of 5 minutes, and we started resource monitoring simultaneously with the attack using a custom script. Additionally, the Snort alert log file was reset before each new attack to ensure that we could accurately capture the alerts specific to each test.

4.1. CPU, Memory, and Network Utilization

Figures 5, 6, 7, 8, 9,10, 11, and 12 display the CPU, memory, and network usage under different attack scenarios. These metrics are essential for understanding the system's behavior under stress, as well as the effectiveness of the Digital Twin in absorbing and reacting to malicious traffic.

4.1.1. CPU Usage

The CPU usage under various attack scenarios is illustrated in Figures 5 and 6. The Hping3 SYN, ACK, and ICMP attacks caused substantial fluctuations in CPU usage. For instance, as shown in the first graph, CPU usage ranged from 16% to 28%, with noticeable spikes when the attacks peaked. Particularly, the ICMP attack exhibited a pattern of sustained high CPU usage, indicating the strain caused by high packet throughput.

The NMAP attacks, on the other hand, resulted in shorter bursts of CPU utilization. Despite lasting for only a minute, these scans caused brief but significant peaks in CPU consumption. This suggests that although NMAP scans are stealthier, they can still impose considerable load on the system for short periods.

 doi:10.20944/preprints202409.0792.v1

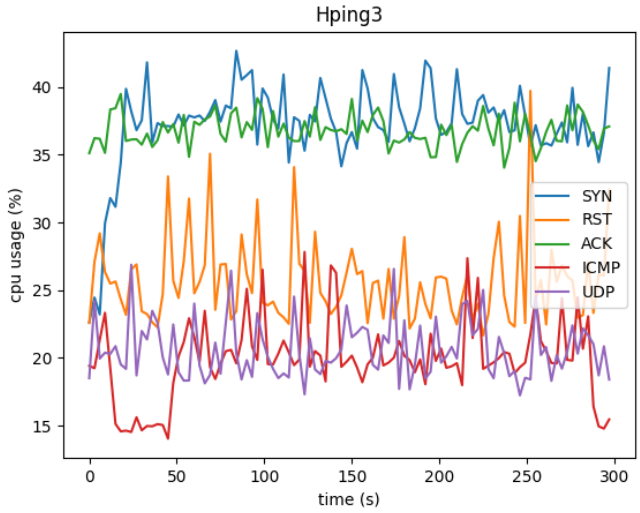

Figure 5. CPU usage under different attacks-1

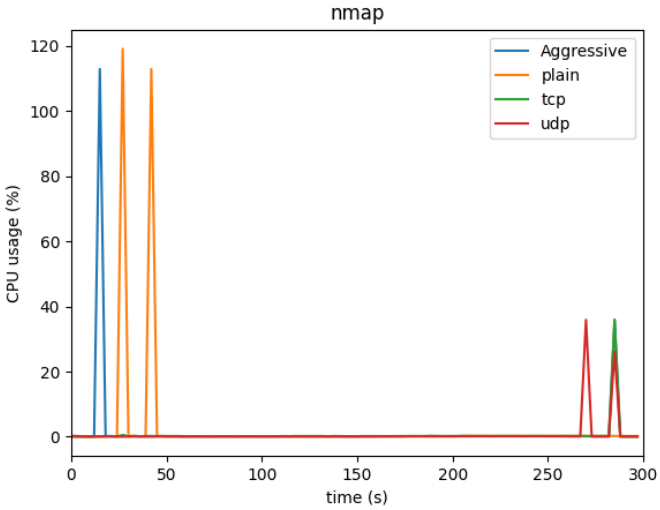

Figure 6. CPU usage under different attacks-2

4.1.2. Memory Usage

Memory consumption remained relatively stable for most of the Hping3 attacks, as shown in Figures 7 and 8. For instance, the Hping3 SYN and ACK floods caused minimal changes in memory usage, maintaining close to the baseline memory usage of 113MB. However, as seen in the memory graph, the NMAP attacks resulted in a more pronounced increase, especially for the NMAP aggressive scan, which almost doubled the memory usage by the end of the scan.

This pattern of increasing memory consumption suggests that the system may require more memory resources to manage and log the increasing volume of network traffic generated by these scans.

 doi:10.20944/preprints202409.0792.v1

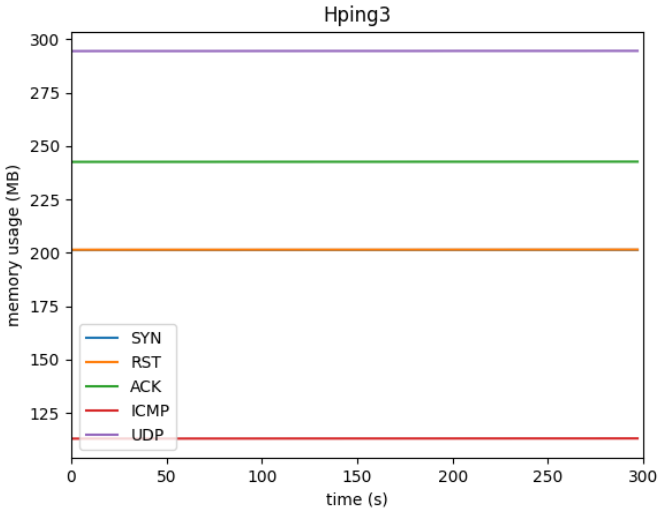

Figure 7. Memory usage under different attacks-1

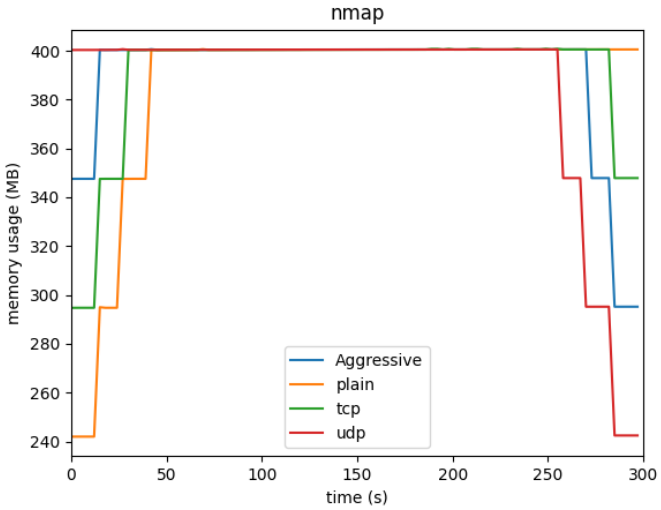

Figure 8. Memory usage under different attacks-2

4.1.3. Network Usage

Figures 9, 10, 11, and 12 illustrate the network traffic generated during the various attacks. We recorded both incoming (network received) and outgoing (network sent) traffic, as depicted in the respective graphs.

In the case of Hping3 SYN, ACK, and ICMP attacks, the network traffic was consistently high as these attacks actively sent packets and received responses. The ICMP attack showed the highest network traffic due to its high packet volume. On the other hand, the Hping3 RST and UDP attacks generated less network traffic, as no responses were received, leading to a drop in outgoing traffic after the initial flood.

For NMAP scans, most network activity occurred within the first minute of the scan. The network traffic then rapidly decreased as the scan concluded. This behavior indicates that although NMAP scans can be intensive, their impact is time-bound and brief.

Preprints.org (www.preprints.org) | NOT PEER-REVIEWED | Posted: 10 September 2024 doi:10.20944/preprints202409.0792.v1

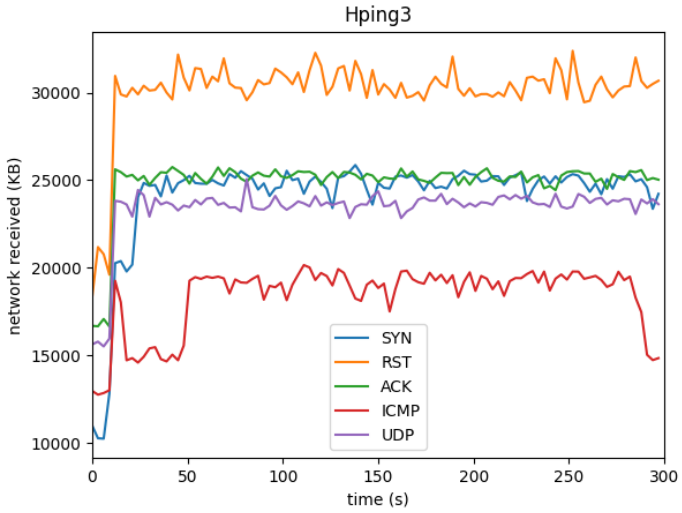

Figure 9. Network usage (received and sent) under different attacks-1

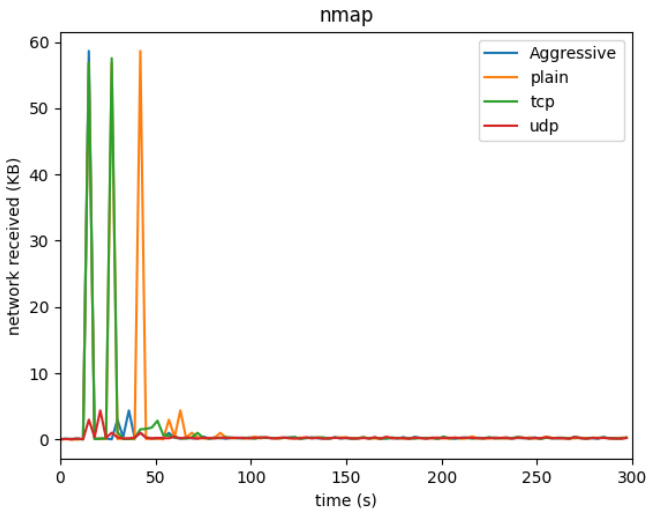

Figure 10. Network usage (received and sent) under different attacks-2

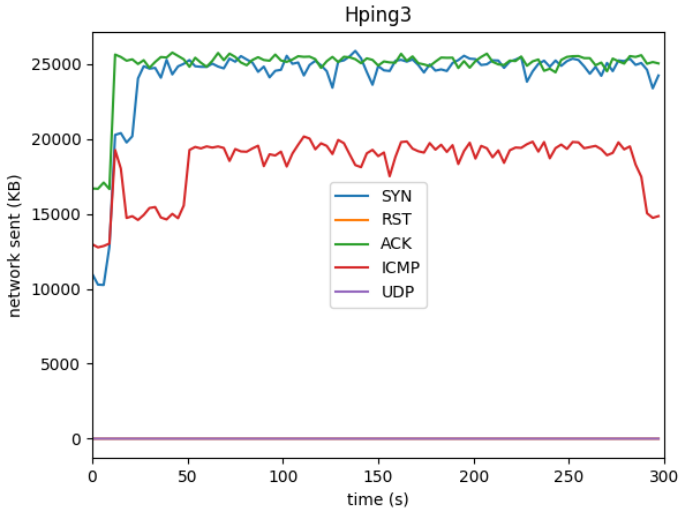

Figure 11. Network usage (received and sent) under different attacks-3

 doi:10.20944/preprints202409.0792.v1

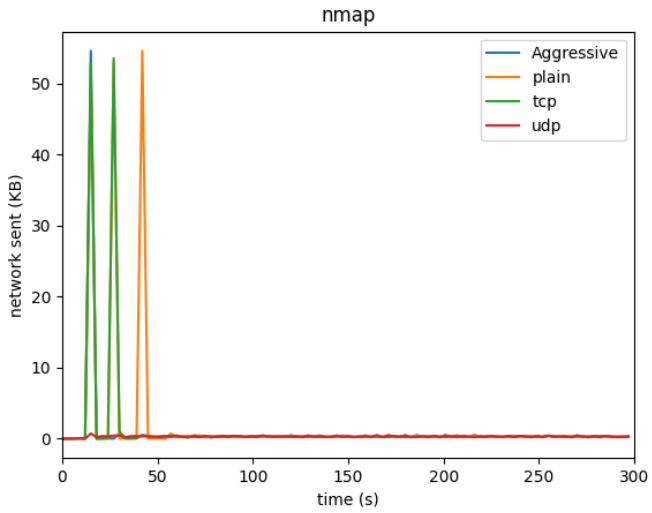

Figure 12. Network usage (received and sent) under different attacks-4

4.2. Attack Detection

The detection capabilities of Snort were evaluated by analyzing the number of alerts fired for each attack. Table 5 provides an overview of the alerts triggered by Snort during each test. Snort successfully detected all Hping3 attacks, firing a high number of alerts for each test. For example, the ICMP flood attack triggered 204 alerts, the highest alert count across all attack types. This high alert count underscores the aggressive nature of this attack and its high detectability.

In contrast, Snort fired fewer alerts for the NMAP attacks. The standard NMAP scan resulted in just two alerts, and the NMAP aggressive scan triggered only one alert. The reduced number of alerts may be due to the evasive techniques employed by NMAP, which aims to avoid detection by traditional IDS systems.

Table 5. Number of alerts fired by Snort per attack

Attack executed	Number of alerts fired by Snort
Hping3 ACK	102
Hping3 SYN	102
Hping3 RST	102
Hping3 ICMP	204
Hping3 UDP	102
Nmap	2
Nmap aggressive	1
Nmap TCP	1
Nmap UDP	0

The results reveal several key insights. First, the Hping3 attacks exert more sustained pressure on CPU resources, particularly the ICMP and SYN attacks. These attacks also triggered a large number of alerts, demonstrating that Snort is highly effective in detecting such brute-force attempts. Second, memory consumption was largely unaffected by Hping3 attacks but increased significantly during NMAP scans, indicating a potential vulnerability for systems with limited memory resources when subjected to scanning techniques.

Finally, Snort's reduced detection of NMAP scans highlights a limitation in detecting stealthy attacks, which is consistent with the nature of NMAP's evasive techniques. Despite these limitations, the coupling of an IDS with a Digital Twin presents a powerful approach to security testing, offering detailed insights into system performance under attack.

 doi:10.20944/preprints202409.0792.v1

5. Discussion

After analyzing the results in section 4, several key findings emerge that underline both the performance of our system and the novelty of the proposed integration between a Digital Twin and an Intrusion Detection System (IDS) like Snort.

5.1. CPU Usage Insights

The first key observation from our results is the difference in CPU usage across various attack types. Under SYN and ACK flood attacks, the CPU usage consistently remains higher than that under RST, ICMP, or UDP attacks. This indicates that the nature of the SYN and ACK attacks places a more sustained computational load on the Digital Twin. These attacks involve maintaining and opening numerous half-open connections, which requires significant resources to track.

Interestingly, while the NMAP scans lasted for only a short duration (less than one minute), they caused sharper spikes in CPU usage than the Hping3 SYN and ACK attacks. This suggests that even though NMAP scans are relatively stealthier and faster, their burst activity requires a high level of processing. The high CPU utilization during NMAP scans reflects the demand placed on system resources when handling detailed reconnaissance activities. This finding is significant, as it shows that short, stealthy scans can impose a heavy load on systems, which could be exploited for denial-of-service (DoS) attempts in environments with limited CPU resources.

5.2. Memory Usage Insights

Our memory usage results provide another layer of insight. The memory usage for NMAP attacks remains higher than that for the Hping3 attacks, which is intriguing, given that NMAP attacks complete within one minute. Even after the scans finish, the memory consumption remains elevated for at least four minutes, showing that the system does not immediately free up resources post-attack.

This phenomenon may be due to the system caching or retaining data collected during the NMAP scans. Such lingering memory usage could be a vulnerability, especially in resource-constrained environments, as it leaves the system susceptible to further attacks. The sustained memory usage could also result from the intensive logging or state-tracking mechanisms that Snort uses to record every interaction during these scans. Understanding and optimizing this behavior is a key area for future work, as mitigating such memory retention could significantly improve the overall performance of IDS-equipped Digital Twins under high network traffic.

5.3. Network Traffic Insights

When analyzing network traffic, we see a clear distinction between the different attacks. Hping3 SYN, ACK, and ICMP attacks generate high levels of both incoming and outgoing traffic. This is expected, as these attacks flood the network with large numbers of packets, causing a high volume of packet responses.

Interestingly, the ICMP attack resulted in the highest overall network usage, reflecting the large volume of traffic typically associated with ICMP floods, which are often used in DoS attacks. However, the Hping3 RST and UDP attacks did not trigger substantial network responses, causing the outgoing network traffic to decline after the initial flood. This pattern can be attributed to the fact that these attacks do not typically receive responses, as RST packets are meant to terminate connections, and UDP is a connectionless protocol that does not require acknowledgment.

For NMAP scans, the majority of network activity occurs in the first minute, after which the traffic rapidly decreases. Although brief, the intensity of NMAP's network activity indicates its potential for large-scale network enumeration in a short time. This also suggests that network monitoring solutions must be fine-tuned to detect and respond to such sudden bursts of activity, as these scans could precede a more aggressive attack.

 doi:10.20944/preprints202409.0792.v1

5.4. Snort's Detection Capabilities

One of the most significant aspects of our results is Snort's detection performance. For the Hping3 attacks, Snort consistently fired 102 alerts for SYN, ACK, RST, and UDP floods. This uniformity is due to the way Snort was configured, with a rule that triggers an alert if more than 100 packets of the same type are detected within 3 seconds. Given that each attack lasted exactly 305 seconds, this consistent behavior across different attacks is expected.

However, the Hping3 ICMP attack resulted in 204 alerts, double the number triggered by the other Hping3 attacks. We interpret this as Snort logging both the attack packets and the responses sent by the Digital Twin separately. This behavior was not expected and highlights an area for improvement in tuning Snort's configuration, especially for ICMP-based traffic. This behavior could potentially lead to alert fatigue or a higher number of false positives, making it harder for system administrators to discern true attacks from regular traffic.

For the NMAP scans, Snort detected very few alerts. The standard NMAP scan fired only two alerts, while the aggressive scan triggered only one alert, and the NMAP UDP scan triggered no alerts. The low detection rate for NMAP scans, especially UDP-based ones, points to a significant limitation in Snort's current configuration for detecting stealthy reconnaissance scans. This finding is noteworthy, as it highlights a key challenge in detecting highly evasive techniques like NMAP scans, which are designed to avoid triggering alarms on traditional IDS systems. Future work could focus on refining the configuration of Snort, or exploring newer rule sets better tuned for detecting these types of attacks.

5.5. Novelty of the Work

The novelty of this work lies in the integration of an IDS with a Digital Twin for security testing, a concept that is not widely explored in existing research. Digital Twins are commonly used for simulating physical systems for performance optimization, but their application to cybersecurity testing, especially with an IDS, represents a novel approach. This coupling allows for a dynamic and responsive security testing framework, which can simulate attacks on physical systems while continuously monitoring their performance.

- **Resource Monitoring in Real-Time Attacks:** Our work uniquely combines resource monitoring (CPU, memory, and network) with IDS alert generation, providing a comprehensive view of how attacks impact both system performance and security. Existing research often focuses on either system performance or IDS detection separately, but our approach integrates both, offering deeper insights into the trade-offs between security and performance.
- **Identifying Vulnerabilities Under Different Attack Types:** The results showcase how different types of attacks (flooding, reconnaissance, and stealthy scans) affect system resources in distinct ways. For example, while SYN and ACK floods consume more CPU, NMAP attacks place a heavier load on memory. These nuanced findings are valuable for designing systems that can better withstand a variety of attack types by understanding their specific impacts on system resources.
- **Enhanced Detection with Digital Twin Coupling:** y coupling the Digital Twin with Snort, we were able to simulate real-world attacks and monitor the behavior of a cyber-physical system in real-time. This provides a unique vantage point for security testing, enabling a more realistic and accurate assessment of system vulnerabilities compared to purely virtual environments. Our methodology allows researchers to assess how physical devices would react to cyberattacks, which is not typically possible in traditional IDS research.

Future work could focus on refining Snort's configuration to improve the detection of stealthy attacks like NMAP, particularly in UDP-based reconnaissance. Additionally, investigating the root cause of sustained memory usage post-NMAP attack could uncover optimization strategies for better memory management. Finally, expanding the scope of this research to include more complex attack scenarios (such as multi-vector attacks) could further demonstrate the robustness and adaptability of the proposed solution.

 doi:10.20944/preprints202409.0792.v1

6. Conclusion

In this research, we explored the novel concept of coupling an Intrusion Detection System (IDS) with a Digital Twin (DT) to enhance the cybersecurity of physical devices. The primary objective was to determine whether this approach could provide a more comprehensive security solution for cyber-physical systems. We created a near-realistic testbed utilizing Eclipse Ditto as a Digital Twin platform, integrating it with Snort as the IDS. Our setup also involved a physical Raspberry Pi device acting as the endpoint for attack simulations and a Kali Linux virtual machine used to conduct common cyberattacks, such as Hping3 flood attacks and NMAP reconnaissance scans.

The findings of this research have several important implications:

6.1. Successes and Key Insights

- Detection of Flood Attacks: The IDS successfully detected the Hping3 SYN, ACK, RST, ICMP, and UDP flood attacks, consistently generating 102 alerts for most flood types. This demonstrates that Snort, when correctly configured, can accurately detect high-volume, sustained attack traffic targeting the Digital Twin. This verification is crucial for enhancing the security of IoT devices and cyber-physical systems that rely on digital twinning for simulation and monitoring purposes. Additionally, the ability of the IDS to respond in real-time provides an essential layer of defense in operational environments.
- Challenges with NMAP Scan Detection: One of the notable challenges was the detection of NMAP reconnaissance scans. Despite NMAP's ability to rapidly gather information about the target device, Snort was unable to trigger a significant number of alerts, especially for the UDP-based NMAP scan. This finding underscores the necessity of improving IDS configurations to detect stealthy scans, which often precede more significant attacks. Future research must delve deeper into fine-tuning IDS rules or incorporating machine learning techniques to better detect these reconnaissance efforts.
- System Resource Usage: Our study also revealed valuable insights into the impact of these attacks on system resources. While SYN and ACK floods caused higher CPU utilization, NMAP scans spiked CPU usage briefly but left an unexpectedly high memory footprint that persisted well after the scan ended. This indicates that certain types of attacks, particularly short-duration scans, can still leave lingering effects on system performance, which may be leveraged by attackers for sustained degradation or system exhaustion. Future work can focus on mitigating these side effects, ensuring that systems recover their resources efficiently post-attack.
- Digital Twin-IDS Integration: The coupling of the Digital Twin with Snort proved to be a significant innovation, enabling the simulation of realistic attack scenarios and the monitoring of system behavior in real-time. This integration represents a valuable tool for cybersecurity testing and defense in the IoT domain. By twinning physical devices, administrators can observe potential vulnerabilities, gauge the impact of different attack types, and adjust their defenses accordingly.

6.2. Novelty and Contribution of the Work

This research is particularly novel due to the integration of a Digital Twin with an IDS for cybersecurity purposes, which has not been extensively explored in the literature. The ability to monitor both system performance (CPU, memory, and network traffic) and security aspects (alert generation) simultaneously provides a holistic approach to defending cyber-physical systems. Unlike traditional IDS deployments that focus solely on network traffic analysis, this work extends IDS capabilities by coupling them with a model of the physical device, which is dynamically updated and monitored through the Digital Twin.

Our findings suggest that this approach offers a unique advantage in identifying the specific resource impacts of various cyberattacks, which can aid in designing more robust defense mechanisms tailored to the system's architecture and workload. Furthermore, the research highlights the potential of using Digital Twins not just for performance optimization or simulation, but also as an integral part of the cybersecurity ecosystem.

 doi:10.20944/preprints202409.0792.v1

6.3. Future Directions

Several areas remain open for future exploration to extend the utility and application of this research:

- Real-World Validation: The next logical step is to verify the results of this research in a real-world scenario, where the Digital Twin is not just a software abstraction but is connected to a physical device with actual, operational functionality. This will help determine the feasibility and reliability of the proposed approach in dynamic environments, such as manufacturing systems, smart grids, or autonomous vehicles.
- Automated Defense Mechanisms: Another promising direction for future work is to explore the possibility of automating defensive actions based on the IDS alerts generated in the Digital Twin. For example, if an attack is detected in the virtual model, automated responses could be triggered to defend the physical device, such as blocking malicious IP addresses, throttling network traffic, or initiating failover procedures. The effectiveness and security implications of such automated responses would need careful consideration and testing.
- Extending Attack Scenarios: While this research focused on Hping3 flood attacks and NMAP scans, it is important to broaden the scope to include more complex attack vectors such as ARP spoofing, SSH brute-force attacks, man-in-the-middle (MITM) attacks, and other sophisticated threats. By extending the range of attack simulations, the Digital Twin-IDS framework can be tested against a more diverse set of threats, thereby enhancing its robustness and generalizability to different network environments.
- Optimizing IDS Performance: Finally, optimizing the configuration of Snort (or other IDS systems) to improve its detection capabilities, especially for stealthy attacks like NMAP scans, remains a critical area for future research. Additionally, integrating more advanced machine learning or anomaly detection algorithms could significantly boost the IDS's ability to detect zero-day attacks or previously unknown vulnerabilities in the Digital Twin or physical device.

In conclusion, the coupling of an Intrusion Detection System with a Digital Twin offers a novel and promising approach to enhancing the cybersecurity of physical devices. Our results demonstrate that this integration can effectively detect common network attacks, provide real-time performance monitoring, and offer new insights into how different attack types impact system resources. The flexibility and potential of this approach make it a valuable tool for both security researchers and practitioners working to safeguard cyber-physical systems in today's increasingly connected world. As cyber threats continue to evolve, so too must the defensive techniques employed, and this research lays the groundwork for future advancements in this critical area.

Funding: This research received no external funding

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

IoT	Internet of Things
AI	Artificial Intelligence
DT	Digital Twin
IDS	ntrusion Detection System
NMAP	Network Mapper
TCP	Transmission Contorl Protocol
ICMP	Internet Control Message Protocol
MQTT	Message Queuing Telemetry Transport
HTTP	Hypertext Transfer Protocol
CPU	Central Processing Unit

 doi:10.20944/preprints202409.0792.v1

References

1. Verhulsdonck, G.; Weible, J.L.; Helser, S.; Hajduk, N. Smart cities, playable cities, and cybersecurity: A systematic review. *International Journal of Human–Computer Interaction* **2023**, *39*, 378–390.
2. Allam, Z.; Dhunny, Z.A. On big data, artificial intelligence and smart cities. *Cities* **2019**, *89*, 80–91.
3. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. A survey of internet of things (IoT) authentication schemes. *Sensors* **2019**, *19*, 1141.
4. Appio, F.P.; Lima, M.; Paroutis, S. Understanding Smart Cities: Innovation ecosystems, technological advancements, and societal challenges. *Technological Forecasting and Social Change* **2019**, *142*, 1–14.
5. Silva, B.N.; Khan, M.; Han, K. Towards sustainable smart cities: A review of trends, architectures, components, and open challenges in smart cities. *Sustainable cities and society* **2018**, *38*, 697–713.
6. Itäpelto, T. Digital Twin Enhanced Critical Infrastructure Life Cycle Security. 2023 IEEE Smart World Congress (SWC). IEEE, 2023, pp. 1–3.
7. van der Wal, E.W.; El-Hajj, M. Securing networks of iot devices with digital twins and automated adversary emulation. 2022 26th International Computer Science and Engineering Conference (ICSEC). IEEE, 2022, pp. 241–246.
8. El-Hajj, M.; Fadlallah, A.; Chamoun, M.; Serhrouchni, A. Secure PUF: Physically unclonable function based on arbiter with enhanced resistance against machine learning (ML) attacks. 2020.
9. Garalov, T.; Elhajj, M. Enhancing IoT Security: Design and Evaluation of a Raspberry Pi-Based Intrusion Detection System. 2023 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2023, pp. 1–7.
10. El-Hajj, M.; Itäpelto, T.; Gebremariam, T. Systematic literature review: Digital twins' role in enhancing security for Industry 4.0 applications. *Security and Privacy*, p. e396.
11. Eckhart, M.; Ekelhart, A. Towards Security-Aware Virtual Environments for Digital Twins. Proceedings of the 4th ACM Workshop on Cyber-Physical System Security; Association for Computing Machinery: New York, NY, USA, 2018; CPSS '18, p. 61–72. doi:10.1145/3198458.3198464.
12. El-hajj, M.; Hahn, F. Security Aspects of Digital Twins in IoT. 9th International Conference on Information Systems Security and Privacy, ICISSP 2023, 2023.
13. El-Hajj, M.; Gebremariam, T.H. Enhancing Resilience in Digital Twins: ASCON-Based Security Solutions for Industry 4.0. *Network* **2024**, *4*, 260–294.
14. Suhail, S.; Hussain, R.; Jurdak, R.; Oracevic, A.; Salah, K.; Hong, C.S.; Matulevičius, R. Blockchain-based digital twins: research trends, issues, and future challenges. *ACM Computing Surveys (CSUR)* **2022**, *54*, 1–34.
15. Empl, P.; Hager, H.; Pernul, G. Digital Twins for IoT Security Management. IFIP Annual Conference on Data and Applications Security and Privacy. Springer, 2023, pp. 141–149.
16. Damjanovic-Behrendt, V. A digital twin-based privacy enhancement mechanism for the automotive industry. 2018 International Conference on Intelligent Systems (IS). IEEE, 2018, pp. 272–279.
17. Bécue, A.; Maia, E.; Feeken, L.; Borchers, P.; Praça, I. A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences* **2020**, *10*, 4482.
18. Sellitto, G.P.; Aranha, H.; Masi, M.; Pavleska, T. Enabling a zero trust architecture in smart grids through a digital twin. Dependable Computing-EDCC 2021 Workshops: DREAMS, DSOGRI, SERENE 2021, Munich, Germany, September 13, 2021, Proceedings 17. Springer, 2021, pp. 73–81.