Mandalapu Rohit, Akinremi Taiwo, Appiah Joel, and Said Hazem

Virtual cybersecurity testbeds for industrial Internet of Things

Abstract: Modern industrial equipment are networked to interact with both internal and external systems, enabling automated decision-making with minimal or no human intervention. While this new environment creates efficiencies, it exposes the environment to cyber threats. This chapter explores the use of cybersecurity testbeds to study best practices in architecting and defending environments that contain industrial systems. Cybersecurity testbeds – physical, virtual, and hybrid – are used in different sectors for research and validation. Virtual testbeds hold promise as they enable design flexibility, reconfiguration, and scale to support various types of research studies. This chapter discusses the value of virtual cybersecurity testbeds and demonstrates a case study on the use of virtual testbeds using a simple industrial control system and a common attack. The concepts apply to more complex set ups and more complex attack structures. Virtual cybersecurity testbed can support researchers, practitioners, and educators interested in defending critical infrastructure environments and industrial systems.

Keywords: Industry 4.0, SCADA, PLC, factory I/O, cloud, virtualization, IOT

1 Introduction

The US Cybersecurity and Infrastructure Security Agency (CISA) defines critical infrastructure as “sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the country that their incapacitation or disruption would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof” [1]. Critical Infrastructure includes power plants, tele-

Acknowledgment: The Ohio Cyber Range Institute (OCRI) provided the infrastructure to host the testbed and supported the second and third authors.

Mandalapu Rohit, School of Information Technology, University of Cincinnati, Cincinnati, OH 45206, USA, e-mail: mandalrt@ucmail.uc.edu
Akinremi Taiwo, School of Information Technology, University of Cincinnati, Cincinnati, OH 45206, USA, e-mail: akinretp@mail.uc.edu
Appiah Joel, School of Information Technology, University of Cincinnati, Cincinnati, OH 45206, USA, e-mail: appiahjk@mail.uc.edu
Said Hazem, School of Information Technology, University of Cincinnati, Cincinnati, OH 45206, USA, e-mail: saidhm@ucmail.uc.edu

https://doi.org/10.1515/9783111436548-012

communications, chemical facilities, oil refineries, food and water systems, emergency services, security services, public health services, and financial systems [2, 1].

At the heart of critical infrastructure is the industrial Internet of Things (IIoT) which is an interconnected network of sensors, devices, machines, and communication systems used in industrial processes to improve efficiency, productivity, and automation [3]. IIoT systems are deployed across various sectors, especially in manufacturing, making it possible for predictive maintenance, real-time monitoring of data, and system optimization [4]. However, the interconnectedness of IIoT subjects these systems to cyberattacks, leading to short- and long-term disruption. Notable examples include cyberattacks against industrial infrastructure such as the largest blackout in the history of the United States of America (USA) and Canada in August 2003 [2]; the release of 3,622,639 liters of oil into the river Fork Shoals, South Carolina, USA, in 1996 when the operator acted on inaccurate data on the human-computer interaction (HCI) module [2]; and the slammer worm attack on nuclear power plant in Oak Harbor, Ohio, USA, which disabled the safety monitoring system of the power plant for five hours [2]. Recently, the world experienced cyberattacks being used as part of warfare when Russia attacked Ukraine's power grids and communication systems [5]. When war is combined with cyberattacks, the weapons move at the speed of light [6], making it difficult to understand the magnitude of the attack to plan, communicate, and execute a defense strategy, unless plans were put in place beforehand [1].

The rise in cyberattacks on critical infrastructure shows the importance of studying current vulnerabilities in industrial systems. Industry 4.0, or the fourth industrial revolution, involves the integration of industrial equipment over interconnected networks, significantly expanding the attack surface [7]. As Mandalapu and Said [1] noted, Industry 4.0 advances – such as cloud computing, IoT, and machine learning – enable industrial equipment to make autonomous decisions, but these innovations also heighten vulnerability to cyberattacks [1]. Davis & Mahoney [8] reported a 110% increase in cyberattacks on industrial control systems from 2015 to 2016 [3], with these attacks evolving into advanced persistent threats that are challenging to counter. Given the potential societal impact of such attacks [8], there is a critical need for new strategies to understand and address cybersecurity vulnerabilities in the Industrial Internet of Things [1].

One approach for addressing the need for cybersecurity in IIoT systems is the use of cybersecurity testbeds [9, 10]. These testbeds are used for assessing vulnerabilities, conducting cybersecurity testing, and understanding, mitigating, and preventing cyber threats in the evolving landscape of IIoT [11]. They play a pivotal role due to the complex interconnectivity and critical nature of industrial systems.

Al-Hawawreh and Sitnikova [12] demonstrated the use of a cybersecurity testbed in evaluating security controls, analyzing attack landscapes, and extracting threat intelligence [11]. Similarly, Siboni et al. [4] and Berhanu et al. [11] have shown the effectiveness of cybersecurity testbeds in testing vulnerabilities and evaluating system resilience against cyber threats in industrial settings [13, 14].

Researchers and industry professionals noted that cybersecurity testbeds could be valuable for replicating the complex networks of IIoT devices to understand security threats, assess vulnerabilities, and validate the effectiveness of defensive technologies [25, 1].

Ukwandu et al. [16] provide an overview of cybersecurity testbeds, emphasizing their role in cybersecurity training and research by detailing various configurations and their significance through realistic scenario simulations [16]. Holm et al. [17] compiled a comprehensive list of platforms for industrial control systems' (ICS) security research. They analyzed current issues, challenges, and the pros and cons of four typical ICS testbeds, and identified 30 testbeds aimed at facilitating vulnerability analysis, education, and defense testing [11]. Chih-Che Sun [18] explored the cybersecurity challenges specific to power grids and reviewed technological solutions to mitigate these threats [10]. Kayan et al. [19] examined security threats and countermeasures in the context of IIoT security, contributing to the understanding of IIoT's security dynamics [9].

Geng et al. [20] presented an overview of ICS testbeds and their design, contributing to the knowledge base on ICS testbeds [21]. Kampourakis et al. [22] conducted a systematic literature review on wireless security testbeds in cyber-physical systems, focusing on the evaluation of wireless communications security and highlighting the need for broader research on cybersecurity testbeds within IIoT settings [13]. Alves et al., [23] demonstrated both a localized virtual testbed and a physical testbed, noting that discrepancies in resource allocation between the virtual and physical environments affected by the impact of denial-of-service (DoS) and man-in-the-middle (MiTM) attacks [2].

According to Mandalapu and Said [1], cybersecurity testbeds can be categorized into three primary models: physical systems, virtual environments, and hybrid solutions [1]. Akinremi et al. [24] conducted a systematic literature review on cybersecurity testbeds. Physical testbeds replicate entire IIoT systems using real hardware and network configurations, offering high fidelity [24]. However, physical testbeds can be expensive and time-consuming to set up and modify [24]. Virtual testbeds, in contrast, use software to simulate industrial environments, providing high flexibility and scalability, though they are sometimes considered less realistic [24]. Hybrid testbeds combine physical and virtual components, offering a balance between fidelity – how accurately the system reflects real-world conditions – and flexibility [24].

In their study, Akinremi et al. identified several use cases where cybersecurity testbeds were used. It includes simulating IIoT in agriculture crop monitoring, understanding brownfield IIoT, assessing cyberattacks on building automation systems, examining the safety of ICSs on naval warships, and testing the behavior of energy generation and distribution systems during cyberattacks. In addition, they observed additional use cases in transportation, water treatment plants, and in manufacturing [24].

Cybersecurity testbeds are used primarily in the analysis and assessment of cyberattacks [24]. In addition, it is used for cybersecurity threat detection, training, forensic investigation, data security, and security testing and validation [24].

Akinremi et al. reported that cybersecurity testbeds were used to understand more than 50 different types of attacks. They categorized those attacks into different categories that included DoS attacks, data and information attacks, network attacks, malware and malicious software attacks, and system and hardware attacks. In addition, cybersecurity testbeds can be used to observe and understand advance persistent threats, service disruption, and safety system manipulation attacks. Furthermore, authorization and authentication attacks, and software and data integrity attacks are among various types of attacks that can be simulated on cybersecurity testbeds [24]. Evaluating cybersecurity threats in the evolving IIoT landscape continues to be a challenge due to the intricate security and infrastructure complexities [20, 10]. As the range of cybersecurity threats targeting industrial interconnected systems continues to expand [16], there is an increasing need for enhanced security measures for the IIoT [25].

The next section demonstrates the construction and use of a virtual cybersecurity testbed. It uses a simple case study to draw the reader's attention to the steps needed to build the testbed. Scaling the testbed to more complex environments and subjecting it to more complex attack scenarios will follow the same steps. The authors hope that researchers and practitioners can build on this work by examining how cybersecurity testbeds, particularly virtual ones, can be utilized to understand cyberattacks in industrial smart environments.

2 Case study

The case study explores the development of a virtual cybersecurity testbed using software and virtualization tools on a cloud environment to simulate cyberattacks. To identify the requirements for creating the testbed, this study builds on the work done by Mandalapu and Said [1], which used the modular design illustrated in Figure 1, which was first suggested by Cantera (2020). The testbed includes network equipment that connects components such as supervisory control and data acquisition (SCADA) systems, programmable logical controllers (PLCs), and human-machine interface (HMI). These components control, monitor, and manage sensors and actuators in physical infrastructure through remote telemetry units (RTUs) [26]. Intelligent electronic devices (IEDs) like PLC and RTU can use Modbus TCP protocol over a network interface for communication with the SCADA [27].

OpenPLC software is used to represent the PLC component, following the approach outlined by Alves et al. [28]. OpenPLC is an open-source virtual PLC designed to be interchangeable with other PLCs that adhere to the same standard [28]. ScadaBR simulates a SCADA system with more features than a conventional HMI [29]. Factory I/O simulates the factory by constructing subsystems from a library of standardized parts of the physical industry and interacting with physical or digital PLC through RTU simulation drivers [30].

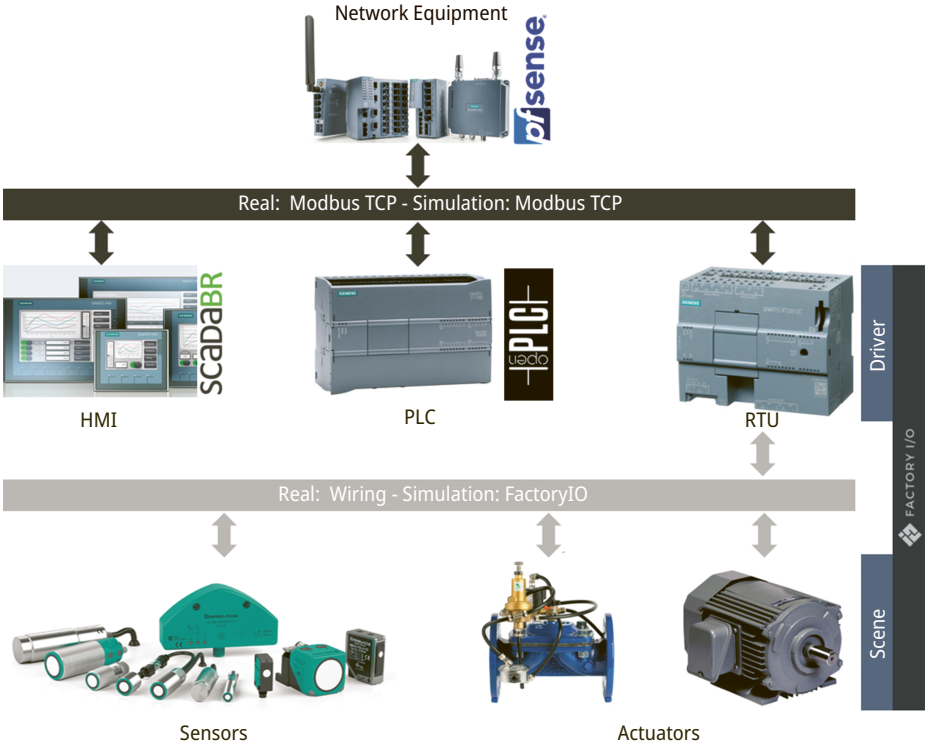


Figure 1: A modular diagram to understand the physical industry [31].

The case study uses a simple conveyor belt example with one programmable logic controller. For the attacks, it simulates a DoS attack from a compromised system within the network, case a, and from a system external to the network, case b. In both simulations, key indicators of the cyberattacks are identified.

2.1 Method

The existing literature primarily emphasizes experimental results rather than the setup process of virtual testbeds, which are typically developed on local machines and thus limit researcher access. Additionally, there is a lack of references on the implementation and setup processes of these testbeds. Understanding the setup process and reliability of industrial testbeds is crucial for effective cybersecurity research. This study will outline the process of setting up an industrial testbed in a cloud environment, facilitating team collaboration and evaluating its reliability.

This study investigated the design of a virtual industrial testbed within a cloud environment, featuring a conveyor belt system that transports loads from point A to

point B. The setup includes a piston at point B, which activates to drop the load onto a crate, when detected by a sensor near the piston. Once the load is removed from the belt, the conveyor resumes operation, continuing its cycle. Secondly, it also explored the placement of the attacker machine to simulate a compromised machine in the industrial network and an attacker machine outside the industrial network to simulate an external cyberattack. Additionally, this study conducted a DoS attack to identify indicators of a cyberattack on the testbed. Experiments are defined by borrowing the guidelines from Trochim et al. [30] for pretest and posttest comparison [21]. This experiment is based on a testbed; hence, no population is involved in the grouping, so sampling has been eliminated from the borrowed guidelines.

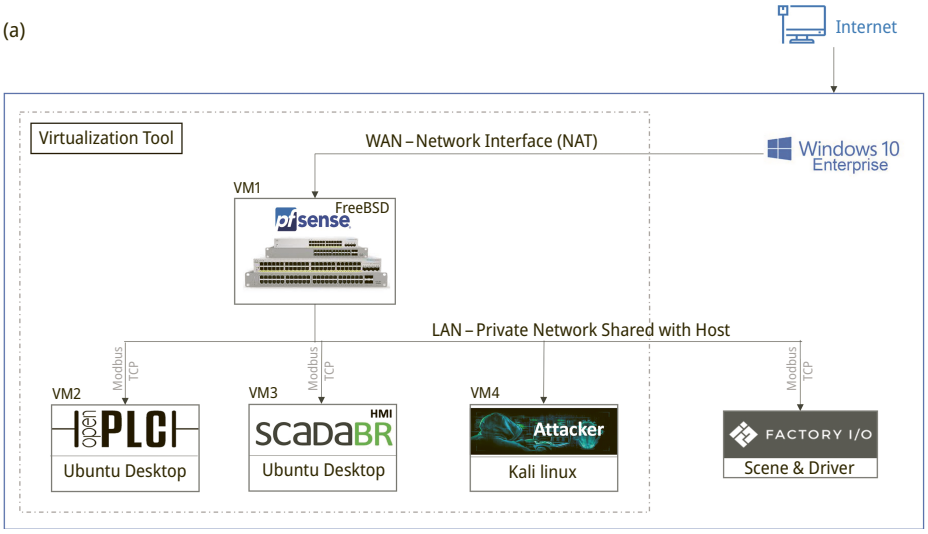
2.1.1 Virtual industrial testbed for cybersecurity

This study used a virtual testbed for its flexibility and adaptability, particularly noting the benefits observed in the study conducted by Mandalapu and Said [1]. In addition, Shi et al. [6] note that performing cybersecurity research using virtual platforms allows researchers to study a complicated industrial system and to comprehend their weaknesses [7].

To explore the implementation of an industrial testbed for cybersecurity in a cloud environment, this study adapted the network diagram used from Mandalapu and Said [1], employing OpenPLC to simulate the physical PLC, ScadaBR to manage the HMI system, and Factory I/O to create the industrial scenario with sensors and actuators connected via the built-in RTU simulator [1]. These tools have previously demonstrated their effectiveness as viable options for setting up a virtual testbed for industrial cybersecurity research. PFSense was utilized to virtualize the network and connect all the components. The study examined the virtualization tools listed in Table 1 to develop a stable testbed by borrowing the model from Mandalapu and Said [1]. Deploying an attacker machine externally connected to the base machine over the same network would violate the cloud usage policy [1]. Figure 2a represents the network diagram borrowed from Mandalapu and Said [1] to represent a compromised system inside the industrial network. This is built on the network diagram to facilitate the research design of exploring placement of attacker machine for simulating external cyberattacks, which is represented in Figure 2b.

The VMware ESXi server, provided by the Ohio Cyber Range Institute at the University of Cincinnati, hosted the base system for the testbed. The base system configuration has been borrowed from Mandalapu and Said [1], as represented in Table 2 [1]. This virtual testbed is configured to replicate the industrial setup depicted in Figure 1, where each system corresponds to a module within the industry, and the network connections simulate the physical wiring.

(a)



(b)

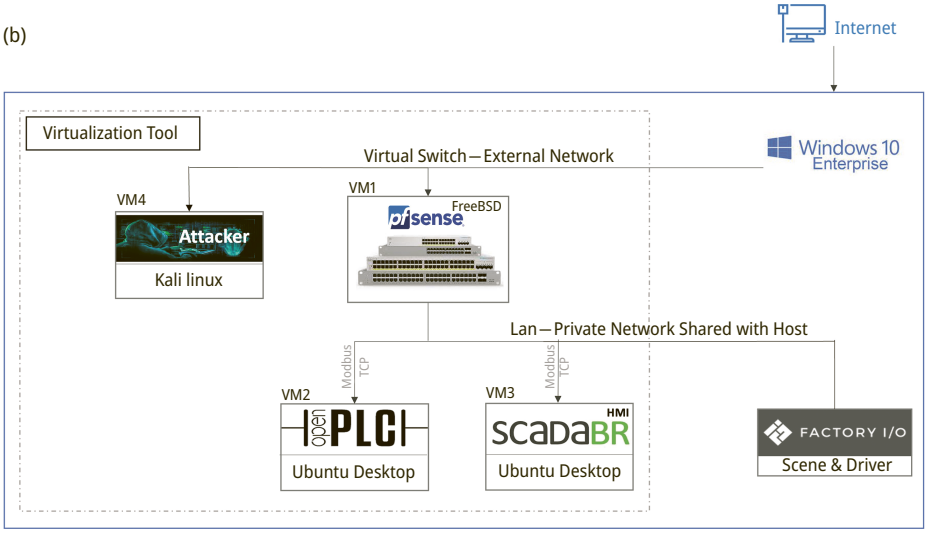


Figure 2: (a) Network diagram for implementing cloud-based virtual industrial testbed [1]. (b) Network diagram for implementing cloud-based virtual industrial testbed with attacker machine, inside and externally.

Table 1: Virtualization tools used [1].

ID	Virtualization tool name
1	VirtualBox
2	Microsoft Hyper-V
3	VMware Workstation Pro 16

Table 2: System configuration of the base system [1].

Items	Values
Processor	2 x Intel Xenon Platinum 8,168 CPU @ 2.70 GHz, 2,694 MHz. 5Core(s) 5 logical processors(s)
RAM	32.0 GB
Storage	298 GB
Operating system	Microsoft Windows 10 Enterprise

In the process of exploring the testbed setup, three sets of testbeds were developed per the setup defined in Figure 2a and b. All testbed setups are subjected to a pretest and a posttest. The pretest is conducted by validating the testbed over the checklist mentioned in Table 3, adopted from Mandalapu and Said [1]. For conducting the posttest, the virtual testbed was subjected to vigorous configuration changes, as defined in Table 4, which was adopted from the study of Mandalapu and Said [1]. These changes were repeated ten times on each VM before validating the testbed for the posttest using Table 3, as defined in the study by Mandalapu and Said [1]. Pretests and posttests were conducted to assess the stability and reliability of the testbed under configurational changes as part of the calibration process [1]. The pretest and posttest help validate the fidelity of the environment developed during the study of Mandalapu and Said [1] with the current environment.

Table 3: Pretest and posttest checklist [1].

Checklist ID	Items
TBV01	PFSense is working as expected and can connect with an external network from the host machine to access the internet.
TBV02	PFSense is working as expected and is connected with a virtual private network.
TBV03	Open PLC host is connected to the Internet through PFSense over the private network and is working as expected.
TBV04	SCADABR host is connected to the Internet through PFSense over the private network and is working as expected.
TBV05	Kali Linux VM is connected to the Internet through PFSense over the private network and is working as expected.
TBV06	Factory I/O is connected to the private network over the Modbus TCP and is working as expected.
TBV07	Virtual machines and host machines can ping each other.

Table 4: Pretest and posttest checklist [1].

ID	Item
1	Increase the RAM and restart the system.
2	Increase the CPU and restart the system.
3	Decrease the RAM and restart the system.
4	Decrease the CPU and restart the system.
5	Increase the CPU and RAM, and then restart the system.
6	Decrease the CPU and RAM, and then restart the system.

2.1.2 Denial-of-service (DoS) attack

DoS attacks have long been a well-known type of cyberattack [12], primarily aimed at making systems unresponsive to legitimate users. In the current study, both pretest and posttest procedures were utilized to identify indicators of a cyberattack on the testbed. The pretest involved recording initial data on VM resource utilization and network packets using Wireshark, with readings taken after 5 min of the factory operating under ideal conditions.

At the 10-min mark, ideal conditions were disrupted by administering a DoS attack. This was executed using hping3 and the Metasploit framework, with ten instances of each attack targeting ports 80 and 502 on the PLC host machine. Following the attack, the same indicators from the pretest were captured every 5 min to serve as posttest results. These were recorded 10 mins after the attack successfully halted the conveyor belt.

The experiment was conducted with a scenario involving an attack originating from outside the industry network, as depicted in Figure 2b. Results from a DoS attack on a compromised system within the industry network, as shown in Figure 2a, were sourced from the study by Mandalapu and Said [1] to evaluate the fidelity of the testbed setup defined in Figure 2b.

3 Results

This study adopted the methodology of Mandalapu and Said [1] for data collection and maintenance. Data from the pretest and posttest were organized in Excel files, named according to their timestamps [1]. Wireshark data was saved in a folder, with a clear naming convention to ensure proper organization, and the file paths were recorded in Excel [1]. Following the completion of the experiments, all data in Excel was analyzed [1]. Post the successful cyberattack, we decided to exclude the 10 min of additional data from the analysis, as it showed no significant differences compared to the data collected when the conveyor belt setup ceased operation.

3.1 Virtual industrial testbed for cybersecurity

Six different combinations of virtual industrial testbeds were created using the virtualization tools outlined in Table 1, following the network diagrams illustrated in Figure 2a and b.

3.1.1 Testbed setup with VirtualBox

The results of the pretest and posttest for this setup are detailed in Table 5. The posttest revealed that all the virtual machines became corrupted after undergoing significant configuration changes, rendering the host machine unable to connect to them. However, since the Factory I/O was hosted on the machine, it remained unaffected by these changes, as indicated by TBV07 in Table 5.

Table 5: Pretest and posttest observations for testbed setup with VirtualBox.

Checklist ID	Pretest	Posttest for Figure 2a setup	Posttest for Figure 2b setup
TBV01	Yes	No (system corrupted)	No (system corrupted)
TBV02	Yes	No (system corrupted)	No (system corrupted)
TBV03	Yes	No (system corrupted)	No (system corrupted)
TBV04	Yes	No (system corrupted)	No (system corrupted)
TBV05	Yes	No (system corrupted)	No (system corrupted)
TBV06	Yes	Yes	Yes
TBV07	Yes	No	No

3.1.2 Testbed setup with Hyper-V

The findings from the pretest and posttest are summarized in Table 6. While the virtual machines generally remained stable despite rigorous changes, connectivity issues arose with the factory I/O and the virtual network adapters configured by Hyper-V. Specifically, the base machine experienced problems with the network adapter, preventing the RTU simulator within the factory I/O from connecting to the testbed network.

3.1.3 Testbed setup with VMware workstation Pro 16

The observations from the pretest and posttest are detailed in Table 7. The virtual testbed remained stable despite extensive configuration changes. Based on these findings, VMware Workstation Pro 16 is recommended as the preferred virtualization tool for the testbed setup outlined in Figure 2. This configuration was subsequently used

Table 6: Pretest and posttest observations for testbed setup with Hyper-V.

Checklist ID	Pretest	Posttest for Figure 2a setup	Posttest for Figure 2b setup
TBV01	Yes	Yes	Yes
TBV02	Yes	Yes	Yes
TBV03	Yes	Yes	Yes
TBV04	Yes	Yes	Yes
TBV05	Yes	Yes	Yes
TBV06	Yes	No	No
TBV07	Yes	Yes	Yes

for additional experiments involving cyberattacks to identify key indicators within the virtual industrial testbed, as described in the design section.

Table 7: Pretest and posttest observations for testbed setup with VMware Workstation Pro 16.

Checklist ID	Pretest	Posttest for Figure 2a setup	Posttest for Figure 2b setup
TBV01	Yes	Yes	Yes
TBV02	Yes	Yes	Yes
TBV03	Yes	Yes	Yes
TBV04	Yes	Yes	Yes
TBV05	Yes	Yes	Yes
TBV06	Yes	Yes	Yes
TBV07	Yes	Yes	Yes

3.2 Denial-of-service (DoS) attack

The DoS attack was performed on the test bed using the attacker machine defined in the design section in Figure 2b. According to Mandalapu and Said [1], the initial attack had no impact on the testbed because the firewall integrated into PFSense and the operating systems of the PLC virtual machines effectively blocked the intrusion [1]. The DoS attack is one of the most well-known attacks, and the most updated firewalls are able to block the attack. Much industrial equipment, however, use older operating systems and are still vulnerable. Considering the facts, we temporarily disabled the built-in firewall to conduct the DoS attack on the testbed. This approach was used to simulate older equipment and to effectively showcase the functionality of the testbed for this experiment.

After disabling the firewall, the external attacker machine initiated a DoS attack on the PLC machine, with the entire experiment spanning 40 min. The initial 10 min featured the conveyor belt setup operating under ideal conditions. At the 10-min mark, the DoS attack commenced, becoming effective by the 30th minute, which rendered the PLC machine unresponsive and halted the conveyor belt. The actual attack

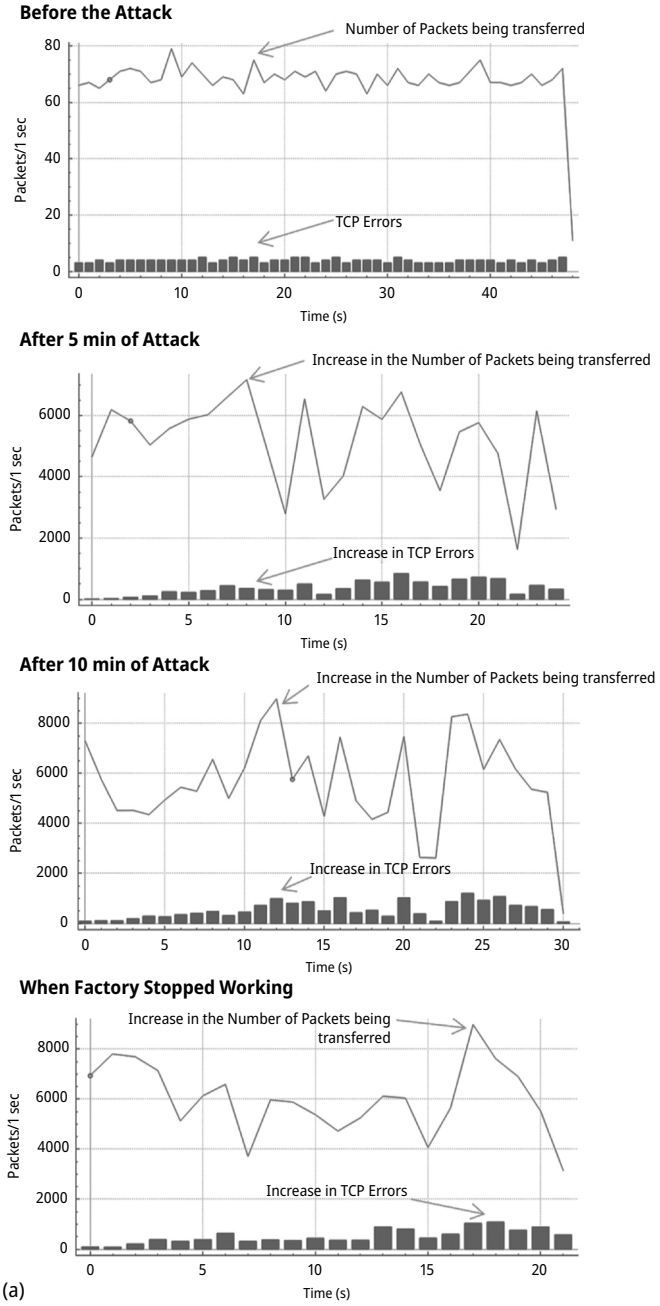
lasted 20 min, during which time the PLC host machine's performance and network traffic were monitored using Wireshark every 5 min, starting from the 5th minute of the conveyor belt operation. Figures 3b, 4b, 5b, and 6b display snapshots taken before the attack and at 4-min intervals following its initiation. Figures 3a, 4a, 5a, and 6a are borrowed from the study conducted by Mandalapu and Said [1] to compare the setup and its results with those from a DoS attack.

Network packet data collected from Wireshark can be used to generate various graphs to visualize the network traffic. Firstly, I/O Graphs with TCP errors can be generated for the entire data set to visualize the number of packets being transferred over time, along with any TCP errors. Figure 3 is a visual representation of the packets transmitted over time before and during the attack, along with the TCP errors. The line graph represents the number of packets being transferred at a time, and the bar graph represents the TCP errors recorded at that time interval. Figure 3 shows that the number of packets being transferred and TCP errors in the network increased drastically during the attack. Figure 3a shows that the number of packets transferred increased from 80 packets per second to 8,000 packets per second before the conveyor belt stopped working. Similarly, Figure 3b demonstrates that during an external cyberattack, the number of packets transferred rose from 350 to 2000 packets per second. From Figures 3a and 3b, we can also observe that number of TCP errors had drastically increased.

When the testbed is exposed to a DoS attack, a delay in the conveyor belt's operation becomes apparent. From Figure 4a and 4b, roundtrip time graph illustrates this by showing the response time for each request. During the attack, the response time between the conveyor belt and the PLC increased significantly, indicating a lag in factory operations. Even after the factory ceased functioning, communication continued between the factory I/O and the PLC, with the factory I/O still attempting to receive commands from the PLC, which had stopped responding. This ongoing communication explains the observed decrease in roundtrip time after the factory's operation ceased.

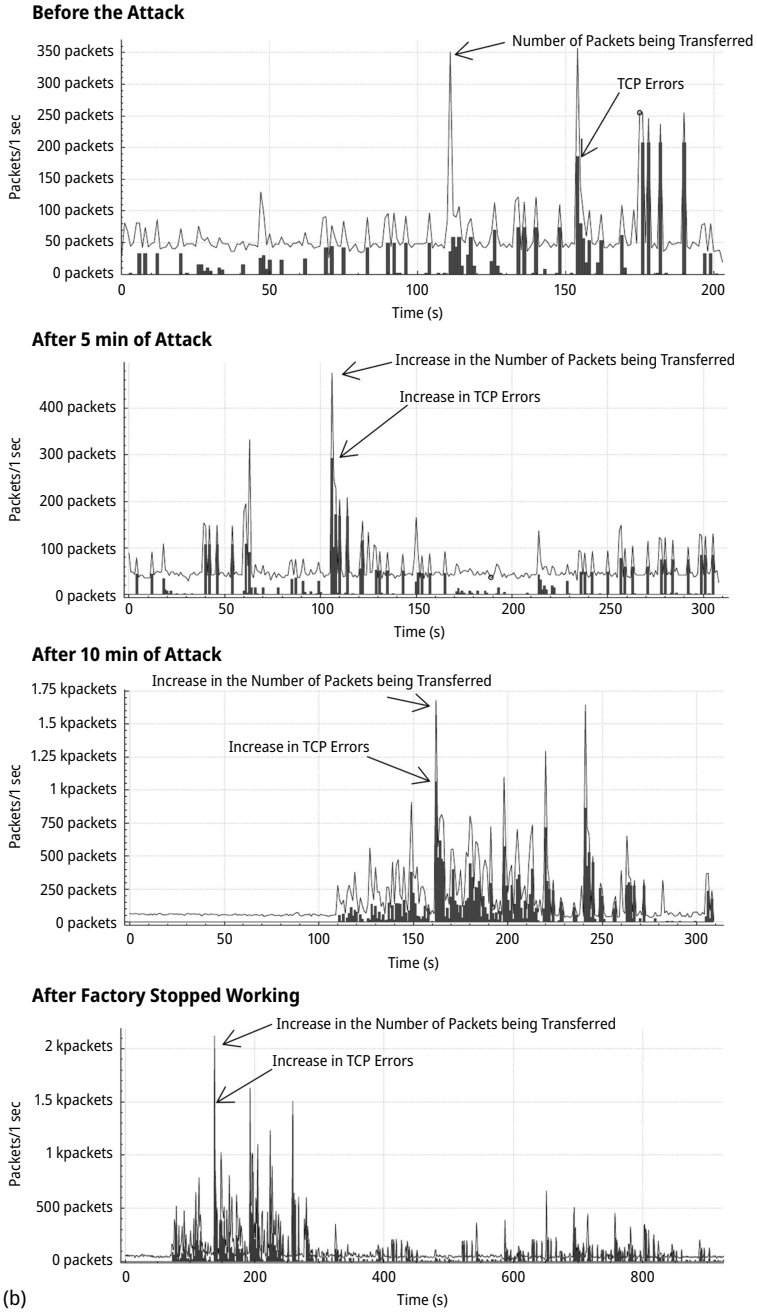
Figure 5a and b depicts the CPU usage of the PLC host machine. It shows a rise in CPU utilization during the attack. In contrast, the memory usage of the PLC host machine remained stable and did not show any observable change before or during the attack.

Figure 6a displays the network utilization of the PLC host machine during the attack. Initially, the machine sent more data than it received. However, once the attack commenced, this pattern reversed, with the machine receiving more data than it transmitted. Consequently, network traffic was disrupted, leading to the PLC host machine becoming unresponsive.



(a)

Figure 3: Snapshots of packet transmission and TCP errors during DoS attack. **(a)** Results of attack from compromised machine in the network – 5 s increments [1]. **(b)** Results of external cyberattack simulation – 50 s increments.



(b)

Figure 3 (continued)

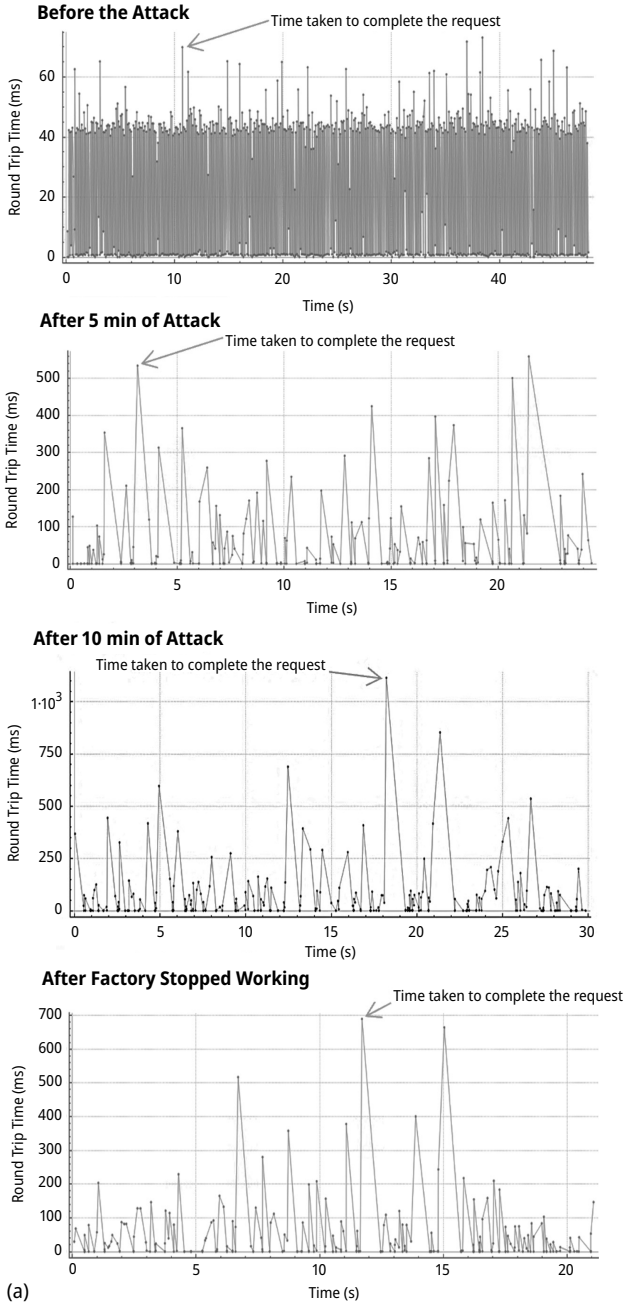
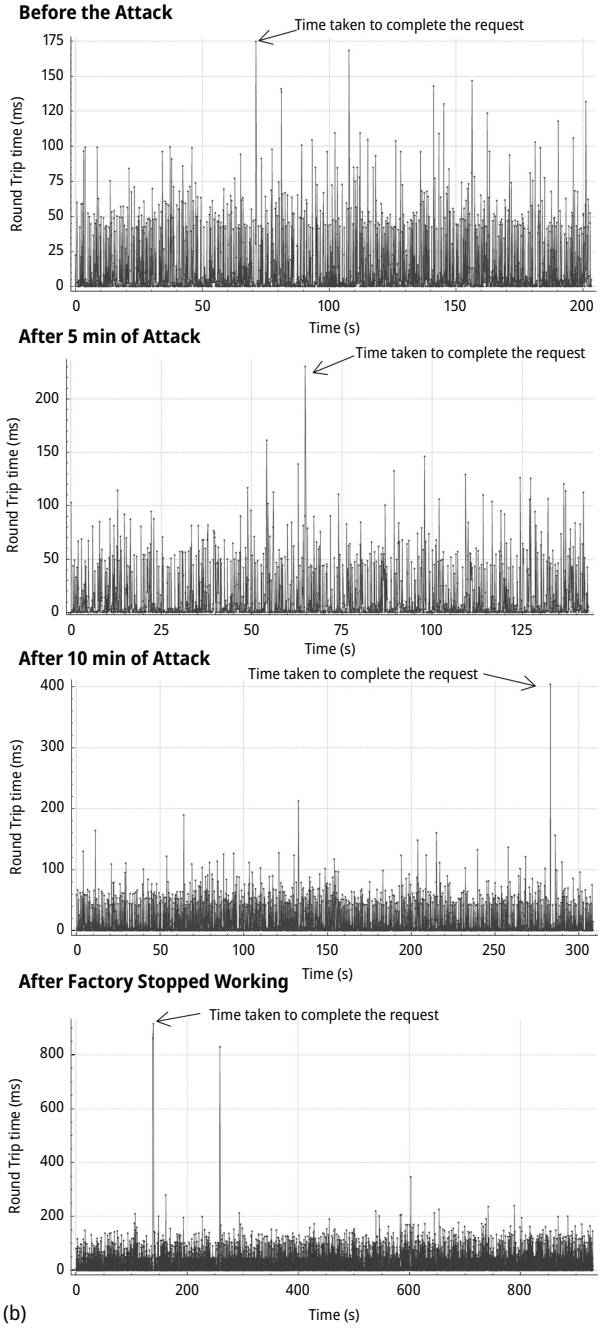
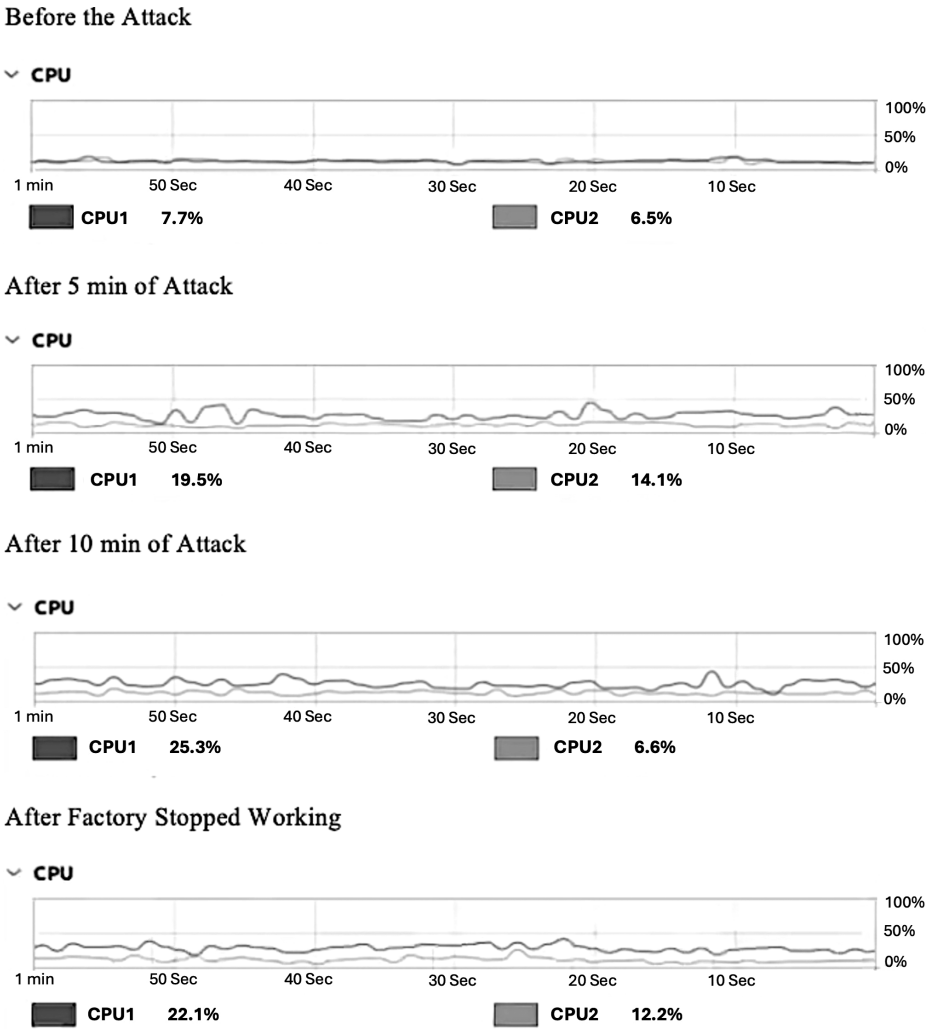


Figure 4: Round trip/time graph between factory I/O and PLC during the DoS attack. **(a)** Results of the attack from the compromised machine in the network [1] – 5 s increments. **(b)** Results of the external cyberattack simulation – 50 s increments.



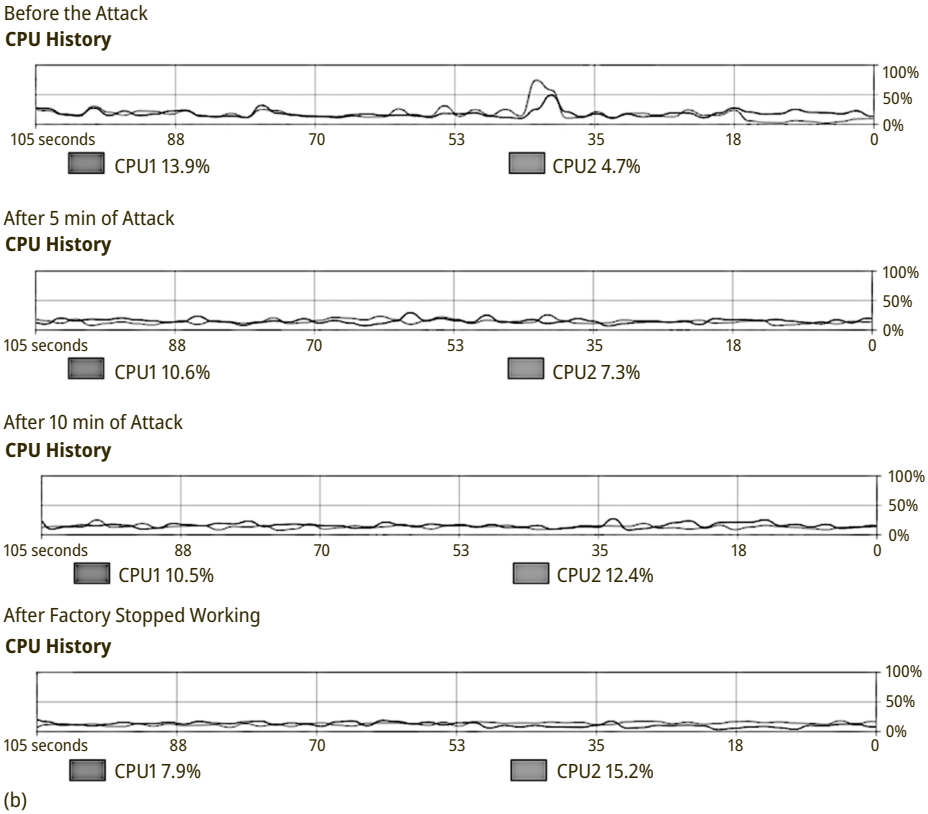
(b)

Figure 4 (continued)



(a)

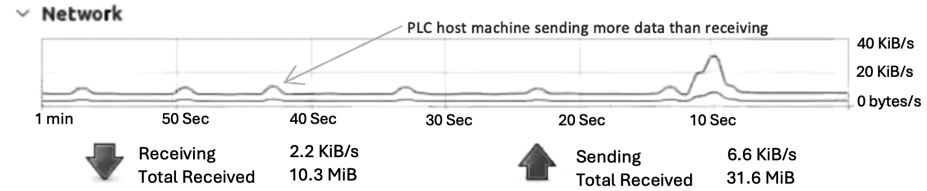
Figure 5: CPU Utilization of the PLC host machine. (**a)** Results of the attack from the compromised machine in the network [1]. (**b)** Results of the external cyberattack simulation.



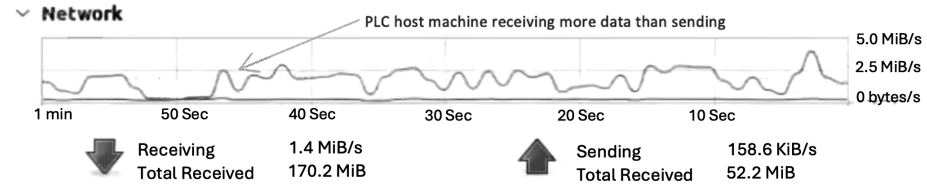
(b)

Figure 5 (continued)

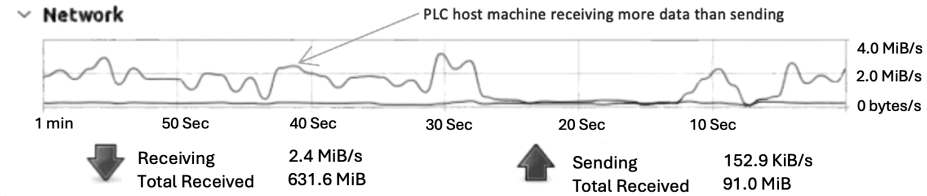
Before the Attack



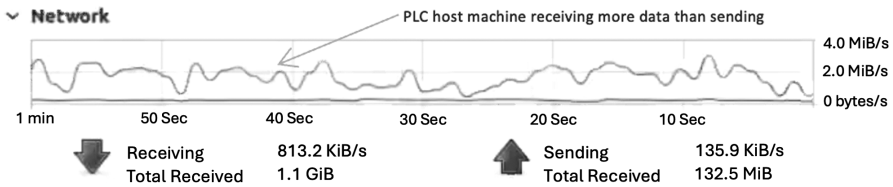
After 5 min of Attack



After 10 min of Attack

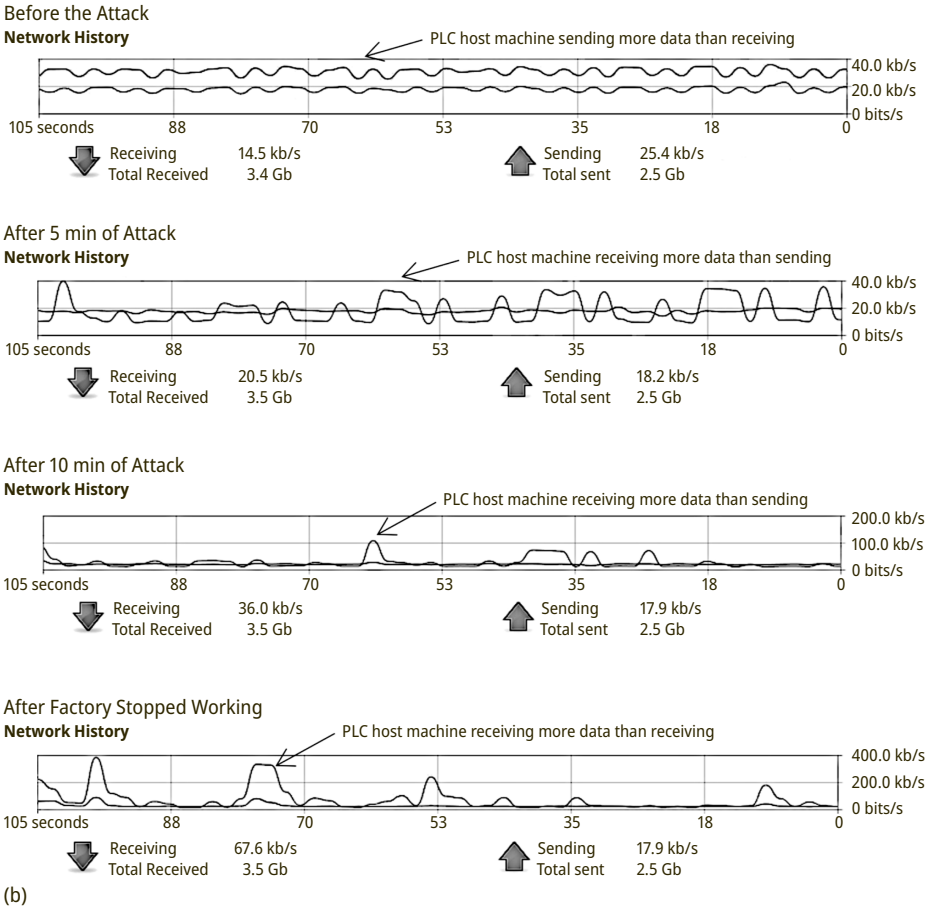


After Factory Stopped Working



(a)

Figure 6: PLC host machine network usage. **(a)** Results of the attack from the compromised machine in the network [1]. **(b)** Results of the external cyberattack simulation.



(b)

Figure 6 (continued)

4 Discussion and conclusion

The case study highlights the significant advantages of virtual cybersecurity testbeds. It underscores their ability to be easily reconfigured and repurposed for various research needs, unlike physical or hybrid systems. The study also demonstrates that virtual testbeds, which do not require expensive hardware, can be quickly set up to evaluate the impact of cyberattacks.

4.1 Findings

This study identified the placement of attacker machine for simulating the external cyberattack study and confirmed the findings of Mandalapu and Said [1] that VMware Workstation Pro is a stable and reliable tool for developing cybersecurity testbeds. Additionally, it also confirmed the work of Mandalapu and Said [1], which highlights that virtual cybersecurity testbed is still relevant for simulating industrial systems, while allowing both researchers and practitioners to assess vulnerabilities, conduct security testing, detect threats, and develop cyber safety measures for safeguarding critical industrial process and systems.

The current study validated cyberattack identifiers from a previous study conducted by Mandalapu and Said [1]. It explored various indicators for identifying cyberattacks, including network I/O graphs with TCP errors, roundtrip/time graphs, and resource utilization metrics of PLC host machines. The analysis of the I/O graph with TCP errors revealed a significant increase in network usage and flagged miscellaneous packets, which serves as a primary indicator of potential malicious activity. The roundtrip/time graph confirmed a lag in the virtual conveyor belt's operation, consistent with the observed delays. Additionally, the study found that CPU utilization of the PLC host machine increased during the attack, likely due to the higher volume of requests being processed. During normal operation, the PLC machine sent more data than it received. However, this pattern reversed under a DoS attack, causing the

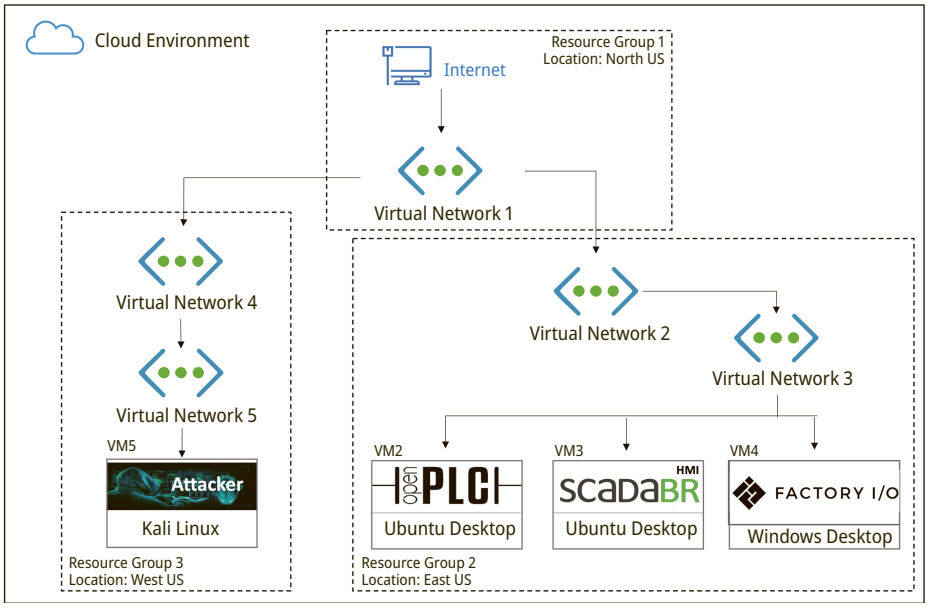


Figure 7: Proposed setup of virtual testbed on cloud environment for individual system access.

PLC to fail in responding to legitimate requests. These results collectively indicate that the performance monitoring of the PLC host machine can effectively signal malicious activity, corroborating the findings of the previous study.

The study aligns with previous research, including works by Dietz et al. [28] and Cantera [7], reiterated the utility of virtual testbeds in industrial cybersecurity research. The cloud-based nature of this testbed provides flexibility, enabling the simulation of various cyber threats in an industrial environment.

This study demonstrated the effectiveness of a cloud-based virtual environment through a case study involving a PLC and a virtual conveyor belt setup with an attacker machine simulating external and internal cyberattacks, as shown in Figure 2a and b, and it confirms the viability of such testbeds. However, it notes that the number of PLCs in a real industrial setup varies by industry size, and the current scope is limited to simulating external cyberattacks.

Challenges remain, such as the availability of specific software for certain systems or applications. Yet, as the software industry progresses, simulation and virtualization tools will advance, leading to greater adoption of virtual cybersecurity testbeds. These testbeds offer flexibility and adaptability, essential for keeping pace with evolving cyber threats, particularly in IIoT. They provide a scalable and collaborative environment for researchers to assess vulnerabilities and strengthen IIoT systems.

This study opens avenues for collaborative research, allowing multiple institutions and locations to access, modify, and experiment with the same testbed remotely. This collaborative capability is crucial for advancing cybersecurity knowledge, enabling diverse teams to simulate various use cases and cyberattack scenarios without geographic constraints. Researchers can simulate multiple industrial scenarios, such as energy grids or water treatment plants, compare outcomes, identify common vulnerabilities, and develop robust defense mechanisms.

4.2 Future work

Future work will focus on exploring how virtual cybersecurity testbeds can facilitate collaboration among researchers and institutions, both domestically and internationally. This collaborative approach could significantly enhance the development of comprehensive cybersecurity solutions and advance the field. Figure 7 illustrates a potential network diagram for a cloud environment designed to simulate external cyberattacks. In this setup, V-Net 1 represents the internet source, while V-Nets 2 and 4 function as separate local ISPs. The attacker machine is connected to the local area network V-Net 5 via ISP V-Net 4. Virtual machines deployed for the industry setup are connected through local network V-Net 3 to ISP V-Net 2. This configuration could enable individual researchers to access dedicated systems, facilitating real-time data sharing and collaborative development of robust defense mechanisms. Such a setup holds promise for advancing research on testbeds by allowing global researchers to work together effectively.

Next work will focus on further developing virtual cybersecurity testbeds, which are vital for investigating and testing known cyberattacks on IIoT systems. Key areas for expansion include scaling the testbed to simulate a factory environment with multiple PLCs and incorporating sophisticated attack scenarios. Additionally, expanding the library of attack types will be a priority.

Once different cyberattack indicators in industrial settings are well understood, future studies will explore automating cybersecurity measures using artificial intelligence and machine learning based on these indicators and collected data. Research collaboration will also be crucial for effectively assessing, detecting, and responding to cybersecurity threats in industrial systems.

4.3 Conclusion

The impact of the study lay in highlighting the need for flexible and cost-effective solutions for researching and investigating cyberattacks on critical infrastructure. Virtual cybersecurity testbeds, as demonstrated through the case study, offers a scalable and affordable approach. The study showcased a cloud-based test environment that was accessible to both practitioners and researchers.

This testbed enabled researchers to collect log data, analyze behaviors, and evaluate protocols for assessing cyberattacks, particularly in small- and medium-sized factory settings. Additionally, the cloud infrastructure supported collaborative activities among researchers and practitioners from various institutions, enhancing their ability to address cybersecurity challenges through shared knowledge and resources.

References

[1] R. Mandalapu, and H. Said, “Towards a Virtual Cloud-Based Smart Factory Testbed forCybersecurity,” In *2023 Congress in Computer Science, Computer Engineering, & Applied Computing (CSCE)*. NV, USA, Las Vegas, 2023, pp. 909–915, doi: 10.1109/CSCE60160.2023.00154.

[2] K. Conger, “Ukraine says it thwarted a sophisticated Russian cyberattack on its power grid,” *The New York Times*, Vol. 12, 2022.

[3] T. Gebremichael, L. P. I. Ledwaba, M. H. Eldefrawy, G. P. Hancke, N. Pereira, M. Gidlund, and J. Akerberg, “Security and privacy in the industrial internet of things: Current standards and futurechallenges,” *IEEE Access*, vol. 8, 152351–152366, 2020.

[4] S. Siboni, V. Sachidananda, Y. Meidan, M. Bohadana, Y. Mathov, S. Bhairav, A. Shabtai, and Y. Elovici “Security testbed for internet-of-things devices,” *IEEE Transactions on Reliability*, vol. 68, no. 1, 23–44, 2018.

[5] B. Smith, *Defending Ukraine: Early Lessons from the Cyber War*. Microsoft, June 22, 2022.

[6] L. Shi, S. Krishnan, and S. Wen, “Study Cybersecurity of Cyber Physical System in the VirtualEnvironment: A Survey and New Direction,” In *Proceedings of the 2022 Australasian Computer Science Week*. 2022, pp. 46–55.

[7] R. Cantera, “Virtual Industrial Cybersecurity Lab – Part 0: Road to Virtualization,” Rodrigo Cantera, Dec. 31, 2020. https://rodrigocantera.com/en/virtual-industrial-cybersecurity-part-0-road-tovirtualization/(accessed Aug. 24, 2022).

[8] J. Davis, and T. Mahoney. Cybersecurity for manufacturers: Securing the digitized and connected factory. MForesight: Alliance for manufacturing foresight report MF-TR-2017–0202 (2017).

[9] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, “Cybersecurity for industrial control systems: A survey,” *Computers & Security*, vol. 89, 101677, 2020.

[10] T. Vaiyapuri, Z. Sbai, H. Alaskar, and N. A. Alaseem, “Deep learning approaches for intrusion detection in IIoT networks– Opportunities and future directions,” *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, 2021.

[11] Y. Berhanu, H. Abie, and M. Hamdi, “A testbed for adaptive security for IoT in eHealth,” In *Proceedings of the International Workshop on Adaptive Security*. 2013, pp. 1–8.

[12] M. Al-Hawawreh, and E. Sitnikova “Developing a security testbed for industrial internet of things,” *IEEE Internet of Things Journal*, vol. 8, no. 7, 5558–5573, 2020.

[13] G. Bernieri, F. P. Estefanía Etchevés Miciolino, and R. Setola, “Monitoring system reaction in cyberphysical testbed under cyber-attacks,” *Computers & Electrical Engineering*, vol. 59, 86–98, 2017.

[14] R. Trifonov, G. Tsochev, R. Y. Slavcho Manolov, and G. Pavlova. “Cyber trends in industrial control systems,” In *2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC)*. 2021, pp. 41–45.

[15] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri “The cyber security landscape in industrial control systems,” *Proceedings of the IEEE*, vol. 104, no. 5, 1039–1057, 2016.

[16] E. Ukwandu, M. A. B. Farah, H. Hindy, D. Brosset, D. Kavallieros, R. Atkinson, C. Tachtatzis, M. Bures, I. Andonovic, and X. Bellekens, “A review of cyber-ranges and test-beds: Current and future trends,” *Sensors*, vol. 20, no. 24, 7148, 2020.

[17] H. Holm, M. Karresand, A. Vidström, and E. Westring. “A Survey of Industrial Control System Testbeds,” in *Secure IT Systems: 20th Nordic Conference, NordSec 2015, Stockholm, Sweden: Springer, October 19–21, 2015, Proceedings*. 2015, pp. 11–26.

[18] C.-C. Sun, A. Hahn, and C.-C. Liu, “Cyber security of a power grid: State-of-the-art,” *International Journal of Electrical Power & Energy Systems*, vol. 99, 45–56, 2018.

[19] H. Kayan, M. Nunes, O. Rana, P. Burnap, and C. Perera “Cybersecurity of industrial cyber-physical systems: A review,” *ACM Computing Surveys (CSUR)*, vol. 54, no. 11, 1–35, 2022.

[20] Y. Geng, Y. Wang, W. Liu, Q. Wei, K. Liu, and W. Haolan, “A Survey of Industrial Control System Testbeds,” In *IOP Conference Series: Materials Science and Engineering*. vol. 569, IOP Publishing, 2019, p. 042030.

[21] Wikipedia Contributors, “Denial of service attack,” Wikipedia, Apr. 17 2019, https://en.wikipedia.org/wiki/Denial-of-service_attack (accessed Jan. 09, 2023).

[22] V. Kampourakis, V. Gkioulos, and S. Katsikas, “A systematic literature review on wireless security testbeds in the cyber-physical realm,” *Computers & Security*, 103383, 2023.

[23] T. Alves, R. Das, and T. Morris, “Virtualization of Industrial Control System Testbeds for Cybersecurity,” in *Proceedings of the 2nd Annual Industrial Control System Security Workshop*. 2016, December, pp. 10–14.

[24] T. P. Akinremi, J. K. Appiah, R. Asadi, O. Ibitoye, H. M. Jayathilake, and H. Said, “Systematic literaturereview of cybersecurity testbeds for industrial internet of things,” *Submitted to ACM Computing Surveys, under Review*, 2024.

[25] A. Mumrez, M. M. Roomi, H. C. Tan, D. Mashima, G. Elbez, and V. Hagenmeyer, “Comparative study on smart grid security testbeds using MITRE ATT&CK matrix,” In 2023 *IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE 2023, pp. 1–7.

[26] B. Chen, N. Pattanaik, A. Goulart, K. L. Butler-Purry, and D. Kundur, "Implementing Attacks for Modbus/TCP Protocol in a Real-Time Cyber Physical System Test Bed," In 2015 *IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*. IEEE, 2015, May, pp. 1–6.

[27] T. Alves, T. Morris, and S. M. Yoo, "Securing Scada Applications Using OpenPLC with End-to-End Encryption," In *Proceedings of the 3rd Annual Industrial Control System Security Workshop*. 2017, December, pp. 1–6.

[28] M. Dietz, L. Hageman, C. Von Hornung, and G. Pernul, "Employing Digital Twins for Security-by-Design System Testing," In *Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*. 2022, April, pp. 97–106.

[29] A. Philippot, B. Riera, M. Koza, R. Pichard, R. Saddem, F. Gellot, ... F. Emprin, "HOME I/O and FACTORY I/O: 2 Pieces of Innovative PO Simulation Software for Automation Education," In 2017 *27th EAEEIE Annual Conference (EAEEIE)*. 2017, June, pp. 1–6.

[30] W. M. Trochim, J. P. Donnelly, and K. Arora, Research Methods: The Essential Knowledge Base, 2016.

[31] T. Alves, R. Das, A. Werth, and T. Morris, "Virtualization of SCADA testbeds for cybersecurity research: A modular approach," *Computers & Security*, vol. 77, 531–546, 2018.