Towards a Virtual Cloud-based Smart Factory Testbed for Cybersecurity

Rohit Mandalapu
S. of Information Technology
University of Cincinnati
Cincinnati, OH, USA
mandalrt@ucmail.uc.edu

Hazem Said
S. of Information Technology
University of Cincinnati
Cincinnati, OH, USA
saidhm@ucmail.uc.edu

***Abstract*— Today's industrial equipment is connected over a network to communicate with external systems and make decisions without human intervention, making it vulnerable to cyberattacks and showing the importance of research. This study explored the implementation of a cloud-based virtual testbed for a smart factory for cybersecurity testing and research. As a first step, this paper reports on developing an environment with one programmable logic controller (PLC) simulating a conveyor belt setup. The study examined different virtualization platforms and network designs. In addition, it executed a denial-of-service attack and identified its signature indicators. The study found that VMware Workstation Pro is the most suitable virtualization platform and that network input and output are the DoS attack's signature indicators.**

***Keywords*— Industry 4.0, SCADA, PLC, Factory I/O, Cloud, Virtualization**

I. 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, telecommunication, chemical plants, oil refiners, food and water, emergency services, security services, public health, and financial systems [1] [2]. It is evident from recent times that these critical industries are subjected to cyberattacks leading to disrupted human activity and long-term health issues. Popular examples of cyberattacks include the largest blackout in the history of the United States of America (USA) and Canada in August 2003 [2]; 3,622,639 liters of oil was released into the nearby river Fork Shoals, South Carolina, USA, in 1996 when operator acted on inaccurate data on the Human-Computer Interaction (HCI) module [2]; nuclear powerplant in Oak Harbor, Ohio, USA, was attacked with the Slammer SQL server worm, which disabled the safety monitoring system of the powerplant for five hours [2]. Recently, we have also seen cyberattacks used as part of warfare when Russia attacked Ukraine's power grids and communication systems [3]. When war is combined with cyberattacks, the weapons move at the speed of light [4], making it difficult to understand the magnitude of the attack, plan, communicate and execute a defense strategy unless plans were put in place beforehand.

The growing number of cyberattacks in critical industries shows the importance of studying current industrial revolution cyber vulnerabilities. Industrial equipment interconnected over a network with abilities to communicate with external systems has been named Industry 4.0, i.e., the fourth industrial revolution [5]. It represents an evolution to a smart factory environment with the prevalence of cloud computing, IOT, and machine learning; industrial equipment is connected with the capability of making its own decisions without human intervention. While most of the literature focused on physical testing environments, virtualized environments were also explored. Alves et al., 2016 demonstrated a localized virtual testbed and a physical testbed. Their experiment included a Denial of Service (DoS) and Man in the middle (MiTM) attacks; they noted the importance of configuring the virtual environment to be similar to the physical environment; for example, in their testbed, the virtual machine for the OpenPLC was much more resourced than the physical machine, and as a result, when subjected to DoS attack there was no effect noted [2].

To understand the requirements to develop a smart factory testbed, this study used a blog by Cantera (2021), which suggested modular design, as shown in Fig 1 [6]. The testbed includes network equipment that connects components such as Supervisory control and data acquisition (SCADA) systems, Programmable logical controllers (PLC), and Human-machine interface (HMI). These components control, monitor, and manage sensors and actuators in physical infrastructure through Remote Telemetry Units (RTU) [7]. Intelligent Electronic Devices (IED) like PLC and RTU can use Modbus TCP protocol over a network interface for communication between the SCADA [8].

This study uses the design in Fig. 1 to create a cloud-based virtualized testbed. The OpenPLC software is used following Alves et al. [9] to represent the PLC component. OpenPLC is an open-source virtual PLC designed to be interchangeable with other PLCs that adhere to the same standard [9]. ScadaBR simulates a Supervisory Control and Data Acquisition (SCADA) system with more features than a conventional HMI [10]. 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 [11].

Funded by The Ohio Cyber Range Institute and The University of Cincinnati Office of Research.

979-8-3503-2759-5/23/$31.00 ©2023 IEEE
DOI 10.1109/CSCE60160.2023.00154

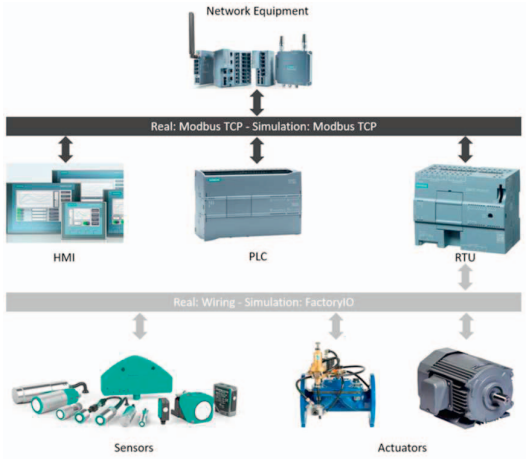

Fig. 1. A modular diagram to understand Physical industry [6]

This study reports the first steps towards implementing a virtual cyber security testbed in a cloud environment. In addition to setting up the virtual environment, the study reports on the first experiment to explore implementing a cyberattack machine to launch a DoS attack on the environment. Furthermore, this study examines indicators to identify if a cyberattack is taking place.

The following three sections will first discuss the design choices for setting up the virtual testbed, followed by the results of conducting the testbed's first experiment and the attack machine's placement. The experiment conducts a denial-of-service attack on a conveyor belt controlled by a PLC. The last section discusses what was learned and the next steps.

II. Design

The literature available is more focused on the experiment and the results of the experiment. Virtual testbed setups discussed in the literature are developed on a local machine limiting access to a researcher. At the same time, no reference is available explaining their testbed's implementation and the process they followed to implement the testbed. To conduct cybersecurity research on industrial testbeds, it is essential to understand the process of setting up the testbed and its reliability. This study will detail the setup of the industrial testbed on a cloud environment enabling the collaboration of teams of researchers and the process it adopted to determine reliability.

This study will conduct two experiments; first, it will set up an industrial testbed for cyber security study in a cloud environment. Secondly, it will conduct a DoS attack on a testbed to explore indicators of a cyberattack on the testbed. Experiments are defined by borrowing the guidelines from the research methods book [12] for pre-test and post-test comparison. This experiment is based on a testbed; hence, no population is involved in the grouping, so sampling has been eliminated from the borrowed guidelines.

A. Virtual Industrial Testbed for Cybersecurity

Shi et al., 2022 proposed to perform cybersecurity research using virtual platforms to study complicated industrial systems in connection to cybersecurity and comprehend their weaknesses [5]. To explore the implementation of an industrial testbed for cybersecurity in a cloud environment, this study adapted the network diagram used to implement the virtual testbed on a local environment from a blog by Rodrigo Cantera [6]. The study utilizes OpenPLC to replicate the physical PLC and ScadaBR to facilitate the HMI system. Factory I/O is used to develop the industrial scenario with sensors and actuators connected through the inbuilt RTU simulator, as these have been previously used and proved to be a viable option for the setup of a virtual testbed for industrial cybersecurity research. PFSense was used to virtualize the network and connect all the components over a network. This study considered the virtualization tools mentioned in Table I to explore the stable testbed. Fig 2 represents the network diagram borrowed from Cantera (2021) and tweaked to facilitate the research design of exploring the cloud-based virtual testbed.

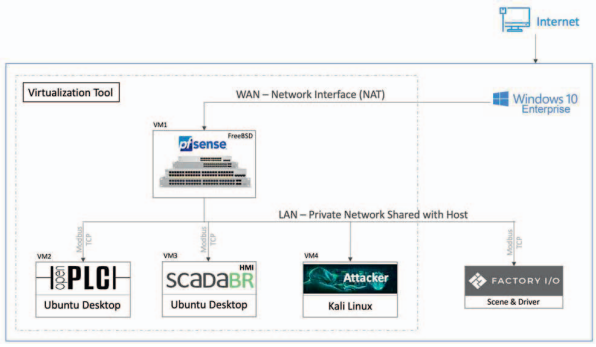

Fig. 2. Network diagram for implementing cloud-based virtual industrial testbed [6].

TABLE I. Virtualization Tools Used

ID	Virtualization Tool Name
1	VirtualBox
2	Microsoft Hyper-V
3	VMware Workstation Pro 16

VMware ESXi server from the Ohio Cyber Range Institute at the University of Cincinnati was used as the host of the base system for the testbed with the system configuration as in Table II. The virtual Testbed is designed to replicate the industrial setup shown in Fig 1.; each system represents a module in an industry, and network connections represent the physical wiring.

TABLE II. System Configuration of Base System

Items	Values
Processor	2 x Intel Xenon Platinum 8168 CPU @ 2.70GHz, 2694Mhz. 5Core(s) 5 Logical Processors(s)
RAM	32.0 GB
Storage	298 GB
Operating System	Microsoft Windows 10 Enterprise

Deploying an attacker machine connected to the base machine externally over the same network will breach the cloud

usage policy. To explore the placement of the attacker machine inside the base machine, this study considered the case of having a compromised system within the network of the industrial testbed, as shown in Fig 2. This machine will act as an attacker machine for further experiments.

In the process of exploring the testbed setup, three sets of testbeds were developed. All testbed setups are subjected to a pretest and posttest. Pretest is conducted by validating the testbed over the checklist mentioned in Table III. For conducting the posttest, the virtual testbed was subjected to vigorous configuration changes as defined in Table IV. These changes were repeated ten times on each VM before validating the testbed for posttest using Table III. The pretest and post-test have been conducted to test the stability and reliability of the testbed when subjected to configurational changes as part of the calibration.

TABLE III. CHECKLIST OF PRETEST AND POSTTEST

Check List 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 connected with virtual private network
TBV03	Open PLC host connected to internet through PFSense over private network and working as expected
TBV04	SCADABR host connected to internet through PFSense over private network and working as expected
TBV05	Kali Linux VM connected to internet through PFSense over private network and working as expected
TBV06	Factory I/O connected to private network over the Modbus TCP and working as expected
TBV07	Virtual machines and host machines can ping each other

TABLE IV. CHECKLIST OF PRETEST AND POSTTEST

ID	Items
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, then restart the system.
6	Decrease the CPU and RAM, then restart the system.

B. Denial of Service (DoS) Attack

Denial of service attacks have been a popularly known cyberattack over the decades [13]; as the name suggests, its main intention is to attack a system to make it unresponsive for its legitimate users. The current study planned the attack with a pretest and a posttest procedure to identify the indicators of a cyberattack on the testbed. The pretest was conducted by collecting initial readings of VM resource utilization and the network packets using Wireshark Software. The pretest results were captured after 5 minutes of allowing the factory to run in ideal conditions.

Ideal conditions were interrupted at the 10th minute, and a posttest was administered by a DoS attack using hping3 and Metasploit framework with ten instances of each attack on ports 80 and 502 of the PLC host machine. After the launch of the attack, the same indicators as the pretest were captured every 5 minutes and considered post-test results. Posttest results are captured until 10 minutes after the cyber-attack was successful in bringing the conveyor belt to a complete stop.

III. RESULTS

The data from the pretest and posttest were collected in Excel files that were named according to the timestamp. The Wireshark data was saved in a folder with an identifiable naming convention to gather all the data appropriately, and the file's path was entered in Excel. After the experiments had been concluded, all the data available in Excel were analyzed. The 10 minutes of excess data collected after the successful cyberattack was omitted as no significant difference was observed when compared to the data captured when the conveyor belt setup stopped working.

A. Virtual Industrial Testbed for Cybersecurity

A total of three combinations of virtual industrial testbeds were developed by implementing the virtualization tools mentioned in Table I with the network diagram shown in Fig 2.

1) Testbed setup with VirtualBox

The pretest and posttest of this setup are presented in Table V. It was observed from the posttest that all the virtual machines deployed were corrupted when subjected to vigorous configuration changes, leaving the host machine unable to establish a connection to them. Since the host machine hosted the Factory I/O, it had no effect after the posttest, which can be observed from TBV07 in Table V.

TABLE V. PRETEST AND POSTTEST OBSERVATIONS FOR TESTBED SETUP WITH VIRTUALBOX

Checklist ID	Pretest	Posttest
TBV01	Yes	No (System corrupted)
TBV02	Yes	No (System corrupted)
TBV03	Yes	No (System corrupted)
TBV04	Yes	No (System corrupted)
TBV05	Yes	No (System corrupted)
TBV06	Yes	Yes
TBV07	Yes	No

2) Testbed setup with Hyper-V

The results of the pretest and posttest are presented in Table VI. The virtual machines were observed to be stable when subjected to vigorous changes. Still, there was an issue with the connectivity of the Factory I/O with the virtual network adaptors that Hyper-V created. The Base machine had accessibility issues with the network adaptor, and hence the RTU simulator within the Factory I/O could not connect with the testbed network.

TABLE VI. PRETEST AND POSTTEST OBSERVATIONS FOR TESTBED SETUP WITH HYPER-V

Checklist ID	Pretest	Posttest
TBV01	Yes	Yes
TBV02	Yes	Yes
TBV03	Yes	Yes
TBV04	Yes	Yes
TBV05	Yes	Yes
TBV06	Yes	No
TBV07	Yes	Yes

3) Testbed setup with VMware Workstation Pro 16

The pretest and posttest observations are presented in Table VII. The virtual testbed was observed to be stable after vigorous configurational changes. Based on these results, the VMWare Workstation Pro 16 is recommended as the virtualization tool for the testbed setup as defined in the Fig 2 network diagram. This setup was used to conduct further experiments with a cyber-attack to identify the indicators in a virtual industrial testbed, as defined in the design section.

TABLE VII. PRETEST AND POSTTEST OBSERVATIONS FOR TESTBED SETUP WITH VMWARE WORKSTATION PRO 16

Checklist ID	Pretest	Posttest
TBV01	Yes	Yes
TBV02	Yes	Yes
TBV03	Yes	Yes
TBV04	Yes	Yes
TBV05	Yes	Yes
TBV06	Yes	Yes
TBV07	Yes	Yes

B. Denial of Service (DoS) Attack

The DoS attack was performed two times on the test bed using the attacker machine defined in the design section. In the initial attack, there was no effect on the testbed. The firewall built in the PFSense and the PLC virtual machine operating systems successfully blocked the attack. The DoS attack is one of the most known attacks, and the most updated firewalls are able to block the attack. Much industrial equipment, however, uses older operating systems and is still vulnerable.

We shut down the built-in firewall to conduct the DoS attack on the testbed. This is an assumption for this experiment to simulate older equipment and to enable us to demonstrate the use of the testbed.

After shutting down the firewall, the attacked machine launched a DoS attack on the PLC machine. This experiment lasted a total of 40 minutes. The first 10 minutes consisted of the testbed with the conveyor belt setup running in ideal condition. On the 10th minute, the DoS attack was launched, which was successful at the 30th minute, causing the PLC machine to become unresponsive and the conveyor belt to stop working. The recording was taken for 10 more minutes after the attack. The actual attack lasted 20 minutes until the conveyor belt setup stopped working. The PLC host machine performance and network packets were captured with Wireshark every 5 minutes during the process, starting at the 5th minute of running the conveyor belt. Figs 4, 5, 6, and 7 show four snapshots of time before the attack and every five minutes after the launch of the 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. Fig 4. It 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. Fig 4 shows that the number of packets being transferred and TCP errors in the network increased drastically during the attack. From Fig 4 we can observe that the number of packets being transferred has increased from a range of 80 packets per second to 8000 packets per second by the time the conveyor belt stopped working.

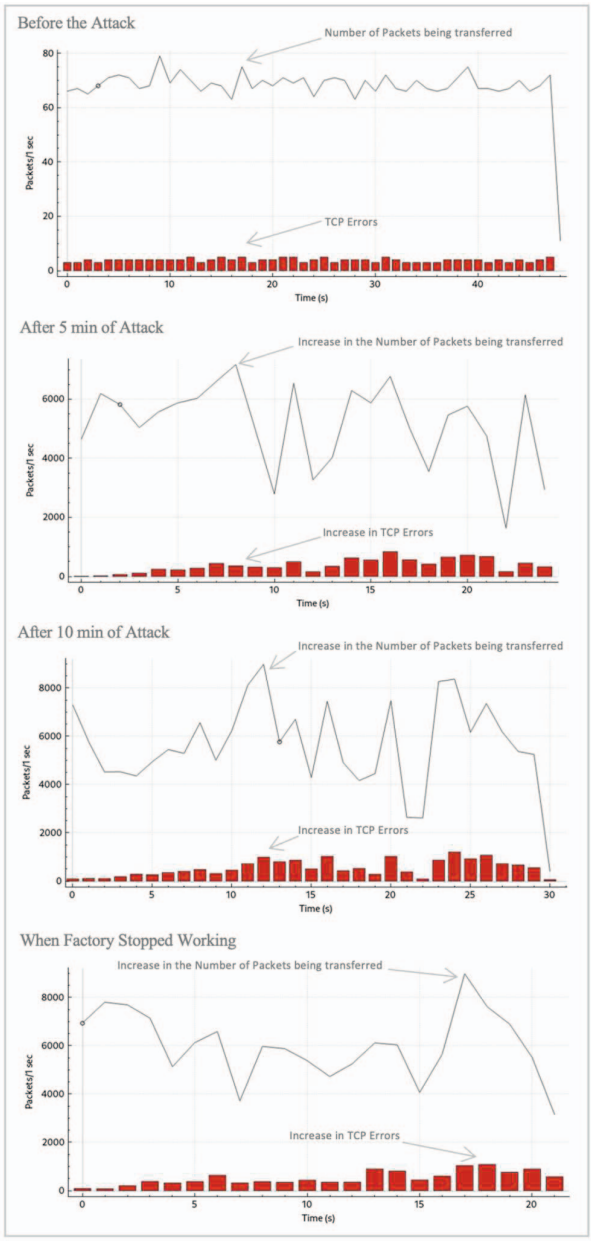

Fig. 3. Snapshots of packet transmission and TCP errors during DoS attack.

A delay in the operation of the conveyor belt has been observed when the testbed is subjected to the DoS attack. This can be observed from the roundtrip/Time graph in Fig 5. This graph visualizes the time taken to complete the response per request. The response time between the conveyor belt and the PLC increased exponentially during the attack. This shows that the response time has increased, so the factory operation lag was observed. It can be observed that after the Factory stopped

working, there was still communication going on between the Factory I/O and PLC, as the Factory I/O was still seeking further commands from the PLC while the PLC was no longer responding. This is the reason behind the decrease in round trip time after the factory stopped working.

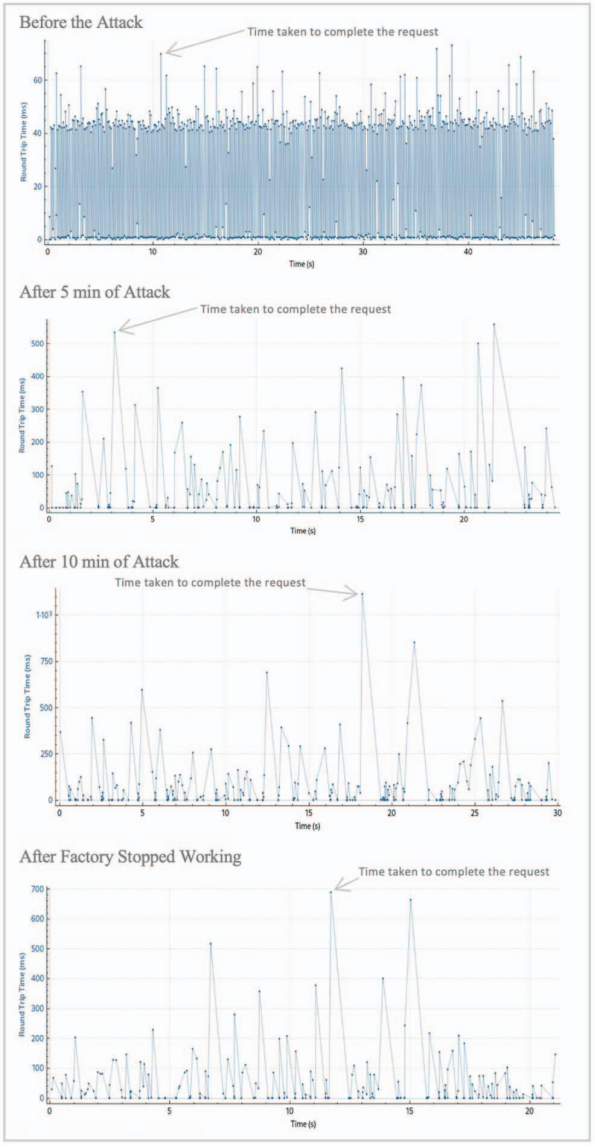

Fig. 4. Round trip / Time graph between Factory I/O and PLC during DoS attack.

CPU usage of the PLC host machine is represented in Fig 6. It can be observed that the CPU utilization increased during the attack. It was observed that the memory of the PLC host machine was stable and remained unchanged before and during the attack.

Fig. 5. CPU Utilization of the PLC host machine

Network utilization of the PLC host machine during the attack was recorded and presented in Fig 7. Before the attack started, the PLC machine sent more data than it received. Once the attack started, this was reversed, with the machine receiving more data than it sent. As a result, the network traffic was disrupted, and the PLC host machine became unresponsive.\

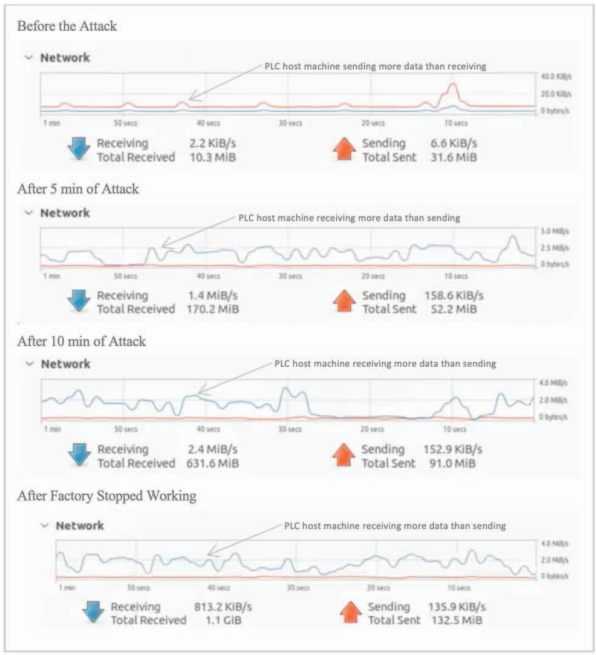

Fig. 6. PLC host machine network usage

IV. Discussion and Conclusion

This study explored the implementation of a virtual industrial testbed on a cloud environment using the network setup in Fig 2. The study found that the VMware Workstation Pro is a stable virtualization tool and reliable for use for the testbed.

In the testbed setup with VirtualBox, it's observed that all VMs hosted with VirtualBox crashed when subjected to a series of changes in the configuration of the VM; this kind of environment will not be sustainable with the testbeds as they may be subjected to changes during the calibration process to match the performance of physical testbed. For the Hyper-V environment, the Factory I/O could not connect with the testbed as the virtual network created was not accessible to the base machine. Testbed setup with VMware workstation hosting the VMs was found to be stable when subjected to the configuration changes, and such setup is deemed suitable for testbed setup.

In addition, the study explored the implementation of the cyberattack machine to be inside the testbed connected over the testbed network simulating the case study of a compromised machine in the network, as shown in Fig 2. This implementation is helpful to avoid any breach of the cloud usage policy set by the provider.

Furthermore, it explored the indicators to identify cyberattacks, include network I/O graphs with TCP errors, Round trip/Time graphs, and resource utilization of PLC host machines. From the I/O graph with TCP errors, it is evident that there has been a sudden increase in network usage and flagged miscellaneous packets; this can be used as a primary indicator of possible malicious activity in the network. A lag in the virtual conveyor belt operation was identified, and this was confirmed from the roundtrip/time graph. The CPU utilization of the PLC host machine has increased during the attack; this can be due to the number of requests the host machine is processing during the attack. The results show that the PLC machine sent more data than it received during its normal operation. However, this was reversed when the PLC was subjected to a DoS attack resulting in the PLC failing to respond to legitimate requests. Performance monitoring of the PLC host machine directly indicates malicious activity.

Alves et al., 2016 stated that no effect was observed when their industrial testbed was subjected to an attack. They speculated that their virtual system must be over-resourced than the physical PLC [2]. However, this may have been a result of the firewall in their virtual machines, as the study experienced a similar outcome when the DoS attack was launched the first time when all the firewalls were enabled. The DoS attack was successful when all built-in firewalls were disabled.

This study confirmed the viability of a cloud-based virtual environment for a smart-factory testbed for cybersecurity by considering a case study of having one PLC running a virtual conveyor belt setup with an attacker machine inside the factory network. However, the number of PLCs in an industry setup can depend on the industry and its size. The scope of this study is to simulate the cyberattack on the testbed considering an internally compromised machine; however, cyberattacks can happen by gaining access to the industrial network from external devices connected through the internet.

Future work will expand the environment to a factory with multiple PLCs and a way to simulate the external attack on the testbed. In addition, future work will expand the library of attacks that could be launched. Once the identifiers for different cyber-attack in the industrial environment have been explored, a study can be conducted on automating cybersecurity in an industry using artificial intelligence and machine learning with the identified indicators and the data collected.

The broader impact of this study is to make available to practitioners and researchers a cloud-based test environment for cybersecurity. This testbed environment will enable researchers to collect log data, study behaviors, or evaluate protocols for assessing cyberattacks in small and medium-sized factory environments. The cloud infrastructure will facilitate collaborative activities among researchers and practitioners in different institutions.

Acknowledgment

The Ohio Cyber Range Institute (OCRI) provided the infrastructure to host the testbed. The University of Cincinnati Office of Research provided a Digital Futures Graduate Fellowship for the first author to complete this work.

References

[1] CISA, “Critical Infrastructure Sectors,” Cybersecurity and Infrastructure Security Agency, Oct. 21, 2020. https://www.cisa.gov/critical-infrastructure-sectors (accessed Aug. 30, 2022).

[2] T. Alves, R. Das, and T. Morris, “Virtualization of Industrial Control System Testbeds for Cybersecurity,” Proceedings of the 2nd Annual Industrial Control System Security Workshop, pp. 10–14, Dec. 2016, doi: https://doi.org/10.1145/3018981.3018988.

[3] K. Conger, “Ukraine Says It Thwarted a Sophisticated Russian Cyberattack on Its Power Grid,” The New York Times, Apr. 2022. Accessed: Aug. 30, 2022. [Online]. Available: https://www.nytimes.com/2022/04/12/us/politics/ukraine-russian-cyberattack.html

[4] B. Smith, “Defending Ukraine: Early Lessons from the Cyber War,” Microsoft On the Issues, Jun. 22, 2022. https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/ (accessed Aug. 30, 2022).

[5] L. Shi, S. Krishnan, and S. Wen, “Study Cybersecurity of Cyber Physical System in the Virtual Environment: A Survey and New Direction,” Australasian Computer Science Week 2022, pp. 46–55, Feb. 2022, doi: https://doi.org/10.1145/3511616.3513098.

[6] 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-to-virtualization/ (accessed Aug. 24, 2022).

[7] T. Alves, R. Das, A. Werth, and T. Morris, “Virtualization of SCADA testbeds for cybersecurity research: A modular approach,” Computers & Security, vol. 77, pp. 531–546, Aug. 2018, doi: https://doi.org/10.1016/j.cose.2018.05.002.

[8] 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,” IEEE Xplore, May 01, 2015. https://ieeexplore.ieee.org/abstract/document/7129084 (accessed Aug. 30, 2022).

[9] T. Alves, T. Morris, and S.-M. Yoo, “Securing SCADA Applications Using OpenPLC With End-To-End Encryption,” Proceedings of the 3rd Annual Industrial Control System Security Workshop, pp. 1–6, Dec. 2017, doi: https://doi.org/10.1145/3174776.3174777.

[10] M. Dietz, L. Hageman, C. von Hornung, and G. Pernul, “Employing Digital Twins for Security-by-Design System Testing,” Proceedings of the 2022 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems, Apr. 2022, doi: https://doi.org/10.1145/3510547.3517929.

[11] A. Philippot et al., “HOME I/O and FACTORY I/O : 2 Pieces of innovative PO simulation software for automation education,” 2017 27th EAEEIE Annual Conference (EAEEIE), Jun. 2017, doi: https://doi.org/10.1109/eaeeie.2017.8768639.

[12] W. M. K. Trochim, J. P. Donnelly, and K. Arora, Research methods : the essential knowledge base. Boston, Ma: Cengage Learning, 2016.

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