*future internet*

MDPI

*Article*

# Analysis of ICS and SCADA Systems Attacks Using Honeypots

**Mohamed Mesbah [1], Mahmoud Said Elsayed [2,*], Anca Delia Jurcut [2] and Marianne Azer [3]**

[1] School of Information Technology and Computer Science, Nile University, Cairo 12677, Egypt; m.mesbah@nu.edu.eg
[2] School of Computer Science, University College Dublin, D04 V1W8 Dublin, Ireland; anca.jurcut@ucd.ie
[3] National Telecommunication Institute, Nile University, Cairo 12677, Egypt; mazer@nu.edu.eg
* Correspondence: eng.mahmoud101@gmail.com

**Abstract:** Supervisory control and data acquisition (SCADA) attacks have increased due to the digital transformation of many industrial control systems (ICS). Operational technology (OT) operators should use the defense-in-depth concept to secure their operations from cyber attacks and reduce the surface that can be attacked. Layers of security, such as firewalls, endpoint solutions, honeypots, etc., should be used to secure traditional IT systems. The three main goals of IT cybersecurity are confidentiality, integrity, and availability (CIA), but these three goals have different levels of importance in the operational technology (OT) industry. Availability comes before confidentiality and integrity because of the criticality of business in OT. One of the layers of security in both IT and OT is honeypots. SCADA honeypots are used as a layer of security to mitigate attacks, known attackers' techniques, and network and system weaknesses that attackers may use, and to mitigate these vulnerabilities. In this paper, we use SCADA honeypots for early detection of potential malicious tampering within a SCADA device network, and to determine threats against ICS/SCADA networks. An analysis of SCADA honeypots gives us the ability to know which protocols are most commonly attacked, and attackers' behaviors, locations, and goals. We use an ICS/SCADA honeypot called Conpot, which simulates real ICS/SCADA systems with some ICS protocols and ICS/SCADA PLCs.

**Keywords:** critical infrastructure; cyber security; Conpot; defense in depth (DiD); honeynet; operational technology (OT); industrial control systems (ICS); incident response; PLC; SCADA



**Citation:** Mesbah, M.; Elsayed, M.S.; Jurcut, A.D.; Azer, M. Analysis of ICS and SCADA Systems Attacks Using Honeypots. *Future Internet* **2023**, *15*, 241. https://doi.org/10.3390/fi15070241

Academic Editor: Claude Chaudet

Received: 26 May 2023
Revised: 9 July 2023
Accepted: 11 July 2023
Published: 14 July 2023



## 1. Introduction

Power plants and water treatment facilities are examples of traditional industrial systems that were designed to operate in highly controlled and separated settings. However, the recent exposure of industrial control systems (ICSs) to the Internet has made access and technological adaptation easier, which has led to the exploitation of security holes by attackers to launch attacks against ICSs [1]. These attacks can significantly impact the economics and national security of countries [2]. To identify possible threats and comprehend the terrain of these assaults, ICS honeypots are deployed [3]. One of the primary targets of these attacks is supervisory control and data acquisition (SCADA) systems [4]. There are two different kinds of honeypots: production honeypots and research honeypots. Honeypots may be categorized as low-interaction, medium-interaction, or high-interaction honeypots based on their design and deployment. For this paper, a low-interaction honeypot will be employed.

### *Paper Contribution*

This research paper provides a comprehensive overview of the current state of OT cybersecurity and the importance of addressing this critical issue. The paper highlights the potential impact of OT cyber attacks on national security and the economy, and provides valuable insights into the various components of OT networks, including PLCs, RTUs, and HMIs. Additionally, the study explores the use of honeypot technology as a security

layer, and emphasizes the importance of investing in new security technologies. The paper concludes by discussing some of the most notable OT incidents and underscores the need for organizations to prioritize OT cybersecurity and take steps to prevent these attacks. The paper also discusses experimental work on the OT honeypot (Conpot), including its deployment architecture, running PLCs, and the percentage of cyber-attacks against various protocols and from different countries.

The contributions of this paper are as follows:

- It provides an in-depth analysis of the current state of OT cybersecurity, including the latest trends and challenges.
- It highlights the potential impact of OT cyber attacks, which can cause widespread disruption to critical infrastructure, including power grids, transportation systems, and communication networks. These attacks have a direct impact on national security and the economy as a whole.
- It explains the various components of OT networks, including PLCs, RTUs, and HMIs, and identifies potential security weaknesses that attackers can exploit.
- It explores the IoT landscape, including the various types of IoT devices and how they are classified. It highlights the differences between IT and OT systems, and the unique security considerations that each requires.
- It highlights the fact that while IT systems are primarily focused on protecting data and information, OT systems are concerned with the operational processes of physical assets and the protection of industrial control systems.
- It discusses the most famous OT incidents that have taken place in recent years, including Stuxnet, BlackEnergy, and Triton. These incidents have exposed the critical need for robust OT cybersecurity measures, and underscore the importance of investing in the research and development of new security technologies.
- It explores the use of honeypot technology as a valuable tool for detecting and mitigating OT cyber threats. Honeypots are simulated systems or network segments that are designed to appear vulnerable, thereby luring attackers into a controlled environment wherein they can be monitored and analyzed. The paper also outlines different types of honeypots and their respective benefits.

In this study, we utilized Conpot as an ICS/SCADA honeypot to detect potential malicious tampering and identify which protocols are most targeted, and determine the countries that are most susceptible to attacks. The experiment was deployed on local servers connected to the internet through a firewall, with honeypot software installed to act as fake systems for attacks. The experiment lasted for 45 days, during which logs were collected from servers and applications from day one to the last day. The logs were forwarded to a Splunk SIEM solution for monitoring and correlation.

The remainder of this paper is organized as follows:

Section 2 presents related work in the field of OT cybersecurity. Section 3 provides background information about ICS/SCADA components and functions, as well as ICS/SCADA honeypots. The main differences between IT and OT systems are also discussed, and famous OT cyber incidents are highlighted in Sections 4 and 5, respectively. In Section 6, we discuss the experimental setup and present the experimental results in Sections 6.1 and 6.2. Section 7 analyzes the results obtained from the experiment. Finally, we present our conclusions and future work in Section 8.

## 2. Related Work

In 2021, Nikolaos Pitropakis conducted a study focusing on the analysis of honeypots on different cloud platforms. The author deployed honeypots on popular cloud providers in North America, Europe, and Asia to study the techniques employed by threat actors. The results show regional differences in activity, with evidence of automated activity targeting popular protocols such as remote desktop sharing. The authors found that attackers targeted assets irrespective of the cloud provider's popularity, and that exit nodes originated from both common and uncommon sources. The study highlights the importance of

rigorous patch management and threat intelligence feeds for organizations that operate online, and provides insights into adversarial activity that can inform situational awareness operations [5].

In 2022, Elisavet Grigoriou and his team conducted a study protecting ICS/SCADA systems with honeypots; the results of their research showed that an increasing number of interconnected industrial control systems (ICS) are exposed to the internet without adequate security measures, and this has made them vulnerable to attacks with potentially catastrophic outcomes. The authors enhanced and implemented low-interaction honeypots to collect unsolicited traffic aimed at ICS devices, and analyzed the received traffic to determine who is engaging with vulnerable ICS devices and how. The authors encouraged the industry to strengthen its efforts to secure ICSs and continue monitoring new risks as they emerge [6].

In 2023, Ya Kong conducted research regarding an interactive honeypot-based approach to network threat management; this paper proposes a modular design approach to create a highly interactive honeypot threat management system that achieves active defense measures for the network environment while withstanding continuous attacks. The system's structure includes information collection, connection control, honeypot deployment, and data analysis and processing modules. Practical tests were conducted to assess the model's practicability, and the system was compared with other network threat management methods. The system uses high-interaction honeypots as information collection tools, formats collected data utilizing the attacker's IP address as the primary key for classification, and offers a user-friendly web interface. The system adapts to a variety of operating systems, and shows significant improvements in security and proactivity when compared to traditional network threat management systems. The study demonstrates that the system achieved its security and seduction objectives, and promotes the more widespread application of honeypot technology [7].

There are numerous research papers available on the topic of operational technology (OT) cybersecurity attacks, as well as techniques to protect against them. These research papers cover many OT cybersecurity threats, such as malware attacks, network attacks, physical attacks, and insider threats.

- Malware attacks are a significant concern for OT systems, as they can cause serious disruptions to critical infrastructure and industrial processes. Malware can infect OT systems through various vectors, such as phishing emails, compromised software updates, or infected devices. Examples of OT-specific malware include Stuxnet, Triton, and Industroyer.
- OT systems often have complex networks that can be vulnerable to various types of network attacks, such as denial of service (DoS) attacks, distributed denial of service (DDoS) attacks, and man-in-the-middle (MITM) attacks.
- Physical attacks against OT systems refer to any attempt to physically damage, manipulate, or interfere with the devices and equipment that make up an OT system. These attacks can have serious consequences, including loss of control over critical infrastructure and industrial processes, data theft, and physical harm to people and equipment.
- Insider threats against OT systems refer to any malicious actions taken by individuals within an organization that can compromise the security and availability of critical infrastructure and industrial processes. These actions can be intentional or accidental, and can have serious consequences.

To detect OT attacks, researchers use two types of models. The first model uses a real environment with real PLCs, HMIs, historians, etc., and starts to capture, monitor, and correlate these logs based on use cases. The second model uses a low-level interaction honeypot solution to simulate real PLCs, HMIs, and OT protocols such as MODBUS, BACnet, S7comm, etc., and performs the same functions mentioned previously, capturing, monitoring, and correlating these logs based on use cases. In this paper, the researchers use model two because Conpot is easy to deploy, modify and extend, and is also cost-effective.

In this paper, we use model two, because Conpot is easy to deploy, modify, and extend, and is cost-effective. There are several types of supervisory control and data acquisition (SCADA) deployment, which are as follows:

- Centralized SCADA: All field devices and control panels are connected to a central computer, which acts as the SCADA server. This type of deployment is suitable for large systems with multiple field devices and control panels.
- Distributed SCADA: The SCADA system is divided into multiple subsystems, each with its own server and field devices. This type of deployment is suitable for large systems with multiple locations, or for systems that need to be distributed over a wide geographical area.
- Hybrid SCADA: The SCADA system is a combination of centralized and distributed SCADA. This type of deployment is suitable for systems that have a combination of centralized and distributed components.
- Web-based SCADA: The SCADA system is accessed through a web browser. This type of deployment is suitable for systems that need to be accessed remotely or for systems that need to be accessed by multiple users.
- Cloud-based SCADA: The SCADA system is hosted on a cloud computing platform. This type of deployment is suitable for systems that need to be accessed remotely or for systems that need to be accessed by multiple users.

## 3. Background

In this section, we present the components and functions of ICS/SCADA systems, as well as honeypot definitions and types. ICS and SCADA systems are used to control and monitor industrial processes and infrastructure. These systems typically consist of the following components and features:

- Sensors and actuators: These are devices that measure physical quantities such as temperature, pressure, and flow rate, and control equipment such as valves and pumps.
- Control hardware: This includes controllers, programmable logic controllers (PLCs), and distributed control systems (DCS) that execute control logic and communicate with field devices.
- Communication infrastructure: This includes networks, protocols, and communication devices that enable the control hardware and field devices to communicate with each other and with the SCADA software.
- SCADA software: This is software that runs on a computer or server and is used to monitor and control the industrial process. It typically includes a human–machine interface (HMI) for operators to view and control the process, as well as tools for data analysis and reporting.
- Security measures: ICS and SCADA systems are vulnerable to cyber attacks, so it is important to implement measures such as firewalls, intrusion detection systems, and secure authentication to protect against unauthorized access. The main components of SCADA systems are presented in Table 1.

**Table 1.** SCADA systems' main components.

| Component | Acronym | Function |
| --- | --- | --- |
| Programmable Logic Controller | PLC | Used as local controllers for monitoring and running the different processes. This is accomplished using feedback tools such as sensors and actuators [8]. |
| SCADA Server or Master Terminal Unit | MTU | In charge of giving directions to the field's RTU [9]. |
| Remote Terminal Unit | RTU | Receiving and transmitting data to MTU is the responsibility of the control field feedback device [10]. |
| Human Machine Interface | HMI | Used as an interface to connect the ICS operator and control hardware. It allows the display of information, whether related to status or data gathered in the ICS Environment [11]. |
| Communication Infrastructure: | | The network infrastructure that connects systems. |

- Industrial control systems (ICS) protocols can be categorized into two types: transmission control protocols (TCP) and user datagram protocols (UDP). TCP-based protocols typically establish a standard connection before transmitting data, providing an opportunity for authentication from the sender. This makes TCP-based protocols reliable and secure for host-to-host communication. In contrast, UDP-based protocols do not require a standard connection before sending data, resulting in no authentication for process-to-process communication. According to [12] this makes UDP-based protocols less secure [13].
- ICS threats and vulnerabilities can be exploited: the following are some of the vulnerabilities in industrial control systems (ICS) that can be exploited by cyber-attacks. Insecure interfaces and device vulnerabilities are among them, which include legacy control interfaces that are connected to the Internet, industrial Internet of Things (IIoT) devices, and various bring your own devices (BYODs) such as tablets and smartphones. These devices can serve as entry points to the system and introduce vulnerabilities [12].

Communication vulnerabilities that are insecure include insecure protocols and direct access to field devices. The ModBus protocol is an example of an insecure protocol lacking encryption, integrity, and authentication measures, which make it vulnerable to various attacks. In terms of wireless communication, some plants may use weaker Wi-Fi encryption protocols. Additionally, it has been found that a significant number of programmable logic controllers (PLCs) are directly connected to the Internet [13].

All of the aforementioned factors create vulnerabilities in the communication systems of industrial plants. Insecure software vulnerabilities arise from the absence of access control in real-time operating systems used in programmable logic controllers (PLCs) and remote terminal units (RTUs). This lack of access control provides all users with root access, thereby leaving the system open to various attacks. Insecure software vulnerabilities can also stem from vulnerabilities in Windows and Linux. Stuxnet is an example of a cyber-attack that exploited Windows vulnerabilities, such as Windows Server Service remote code execution. Additionally, buffer overflow vulnerabilities are common [14]. Software applications are also vulnerable to attacks due to the absence of digital signatures, which exacerbates the problem of vulnerabilities in the software.

Honeypots can be thought of as traps to attract attackers. They emulate physical or virtual network devices to help monitor attackers' behaviors. Honeypots help security administrators to identify and study their enemies. Additionally, honeypots help determine how attackers can gain access and escalate their privileges, what attackers leave in the attacked network to come back again (e.g., rootkits, Trojans, and exploits), and how to defend against these attacks [14].

The authors divided honeypots and honeynets for IoT, IIoT, and CPS into several categories based on their function, level of interaction, scalability, resource level, source code accessibility, and application, as shown in Figure 1 [15]. They also considered simulated services, connections between honeypots and honeynets based on inheritance, the platforms on which they were built, and the programming languages used. Additionally, honeypots may be categorized based on their level of interaction, ranging from low to high, as shown in Table 2 [16].

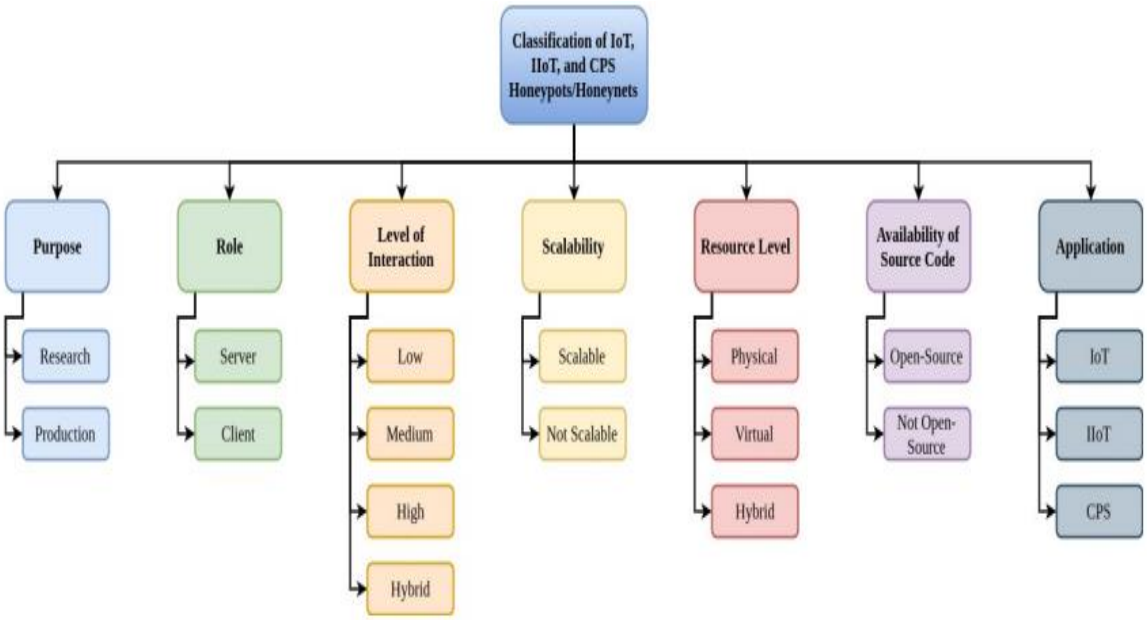


**Figure 1.** Types of IoT, IIoT, and CPS honeypots and honeynets [17].

**Table 2.** Classification of honeypots based on the level of interactivity with the attackers [18].

| Level of Interactivity with Attacker | Interact with Host | Interact with Program | Write Programs |
|---|---|---|---|
| Low | √ | x | x |
| Medium | √ | √ | x |
| High | √ | √ | √ |

## 4. Main Differences between IT and OT

Information technology (IT) and operational technology (OT) systems serve different purposes and have different characteristics, making them distinct from one another. Understanding the differences between IT and OT systems is critical for ensuring their security and availability, as well as for making informed decisions about the use of technology in different environments. Table 3 presents the key differences between IT and OT.

IT systems are typically used to manage and process data, such as in business systems, whereas OT systems are used to control and monitor industrial processes and equipment. IT systems have a focus on confidentiality and integrity, while OT systems prioritize availability and safety. The approach to change is also different, with IT systems being more flexible and able to adapt to rapid change, while OT systems are designed for controlled and predictable change. OT systems are also less dependent on connectivity and are more time-sensitive than IT systems.

**Table 3.** Main differences between IT and OT.

| Item | IT | OT |
|---|---|---|
| Purpose | Managing and processing data | Controlling and monitoring |
| Examples | Computers, servers, networks | PLCs, DCS, SCADA systems |
| Security focus | Confidentiality, integrity | Availability, safety |
| Approach to change | Rapid, flexible | Controlled, predictable |
| Dependency on connectivity | High | Low |
| Time sensitivity | Low | High |

The confidentiality, integrity, availability (CIA) model is a common framework for understanding and managing the security of information systems. It refers to the three key aspects of security: confidentiality, which ensures that information is only accessible to authorized individuals; integrity, which ensures that information is accurate and has not been tampered with; and availability, which ensures that information is accessible when needed.

- Confidentiality: This is safeguarding against unauthorized access to or disclosure of sensitive information.
- Integrity: This is the safeguarding of data against unauthorized alteration or manipulation.
- Availability: This describes the readiness of the information system for usage by authorized users.

The availability, integrity, confidentiality (AIC) model is a similar framework, but the focus is on the three key aspects of security for the availability of data and systems. The AIC model is often used in the context of information security and privacy, especially in the OT industries.

## 5. OT Famous Cyber Incidents

OT and ICS systems are critical to the operation of many industries, but they also present unique cybersecurity risks because they were not originally designed with cybersecurity in mind. As a result, OT and ICS systems have been targeted by cyberattacks in the past, with some high-profile incidents causing significant damage. The following are some examples of famous OT/ICS cyber incidents.

- Stuxnet: In 2010, the Stuxnet worm was discovered to have infected industrial control systems in Iran, causing damage to the country's nuclear program. It is believed to have been created by the US and Israeli governments as a cyber weapon. Stuxnet was able to infect the ICS equipment of its targets and manipulate the systems to cause physical damage. This was accomplished by exploiting vulnerabilities in the systems and modifying the firmware of programmable logic controllers (PLCs) that were used to control the physical processes. The result of this manipulation was that the systems failed, causing significant physical damage to the equipment. The impact of Stuxnet was significant, as it demonstrated the potential for cyberattacks to cause physical harm and the importance of securing industrial control systems and critical infrastructure. Since its discovery, Stuxnet has inspired other state-sponsored cyberattacks and served as a wake-up call for organizations to improve their cybersecurity practices.
- Ukraine power grid attack (BlackEnergy): The Ukraine power grid attack refers to a cyberattack that took place on 23 December 2015, in which hackers caused widespread power outages across the Ukrainian capital of Kyiv and surrounding areas. This was the first known instance of a cyberattack causing widespread disruption to a power grid. The attack was carried out by using malware to gain remote access to the systems of the Ukrainian power grid and to manipulate the operational technology (OT) systems that control the distribution of electricity. The attackers were able to cause significant damage to the systems and cause widespread power outages, affecting hundreds of thousands of people. The attack was significant because it demonstrated the vulnerability of critical infrastructure to cyberattacks and the potential for such attacks to cause widespread disruption. It also highlights the need for organizations to secure their OT systems, as well as their information technology (IT) systems, and to implement robust cybersecurity practices and incident response plans.
- Triton: Triton is a type of malware that was discovered in 2017. It is believed to be state-sponsored, and is specifically designed to target industrial control systems (ICS) such as those used in critical infrastructure, e.g., power plants and water treatment facilities. Triton is capable of compromising the safety systems of ICS, and can cause physical damage to equipment by exploiting vulnerabilities in the systems and manipulating

the control logic. The malware is highly sophisticated and is designed to evade detection by traditional cybersecurity measures.

- Cyberattacks on the USA energy sector: In 2021, the energy sector in the United States continued to be a target of cyberattacks. The COVID-19 pandemic has made the sector even more vulnerable, as many companies have shifted to remote work and have become reliant on digital systems and networks to support their operations. The energy sector in the United States has been a target of numerous cyberattacks in recent years. These attacks have ranged from simple spear-phishing campaigns to sophisticated malware attacks that have impacted the operational technology (OT) systems used to control the production and distribution of energy. As a result of energy sector attacks, the US government has established the Department of Energy's Cybersecurity for Energy Delivery Systems (CEDS) program, which provides guidance and support to energy companies on how to improve their cybersecurity practices and protect against cyberattacks. The program also works to establish national and international standards for the protection of critical infrastructure against cyberattacks.

The Table 4 explains the famous and latest OT in 2021; these attacks demonstrate the potential impact of OT attacks on critical infrastructure and essential services. In the case of the Oldsmar water treatment plant attack, the attacker attempted to poison the water supply, which could have had significant public health consequences. The Colonial Pipeline ransomware attack disrupted the supply of fuel to millions of people, leading to widespread fuel shortages and economic disruption. The JBS meat processing plant cyberattack disrupted the food supply chain, potentially leading to shortages of meat products. The Kaseya VSA ransomware attack affected thousands of businesses that rely on managed service providers for IT services, leading to significant disruption of their operations. These attacks highlight the importance of securing OT systems against a range of threats, and the need for organizations to implement robust security measures to protect critical infrastructure and essential services.

**Table 4.** 2021 Famous OT attacks: targets and impacts.

| Date | Attack | Targeted System | Impact |
|---|---|---|---|
| February 2021 | Oldsmar Water Treatment Plant Attack | Water Treatment Plant | Attempted poisoning of water supply |
| May 2021 | Colonial Pipeline Ransomware Attack | Oil and Gas Pipeline | Disruption of fuel supply, widespread fuel shortages |
| June 2021 | JBS Meat Processing Plant Cyberattack | Food Processing Plant | Disruption of operations, potential food shortages |
| July 2021 | Kaseya VSA Ransomware Attack | Managed Service Provider (MSP) | Disruption of services for thousands of businesses |

## 6. Experiment

In this section, we present our experimental findings. The setup and results are presented respectively.

### *6.1. Experimental Set-Up*

ICS/SCADA honeypots try to emulate real SCADA systems with protocols, PLC, and HMI. In this experiment, we used Conpot [17], classified as a low-interaction side ICS. This honeypot contains different ICS/SCADA protocols such as Modbus, S7comm, etc. This is in addition to some TCP/IP protocols such as HTTP and SNMP. Conpot has different PLCs, such as S7-200 and S7-300, from vendors such as Siemens and Schneider. Figures 2 and 3 depict an ICS/SCADA honeypot architecture. We created a virtual server and four virtual machines. All these machines have Ubuntu 16.04 as the operating system, and all these machines are assigned public IP addresses from one of the service providers. Conpot software was installed on these machines. In the first phase, we started with only

two machines, one with a PLC—Siemens S7-200, and the other with a Siemens S7-300. We collected the log files and forwarded them to the Splunk SIEM solution, as well as the MISP Threat Intelligence platform. After Conpot was successfully installed on the virtual machine, we shut it down and took a clone image from it to redeploy it to another virtual machine. We used SSH to access it and carry out our work. After accessing each Conpot machine via SSH, the following commands were utilized to start the Conpot with the desired template.

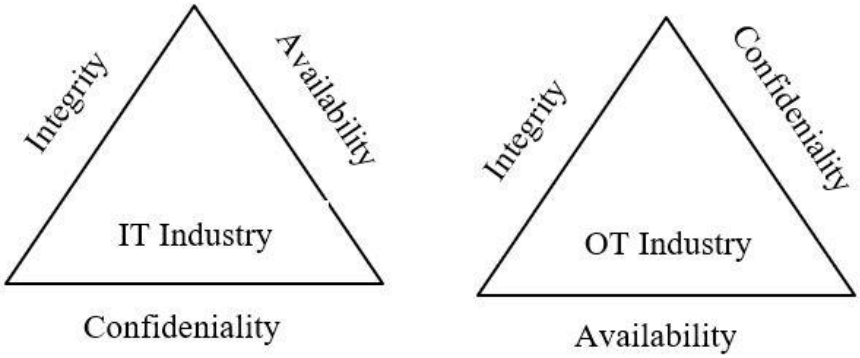


**Figure 2.** CIA in the IT industry vs. AIC in the OT industry.

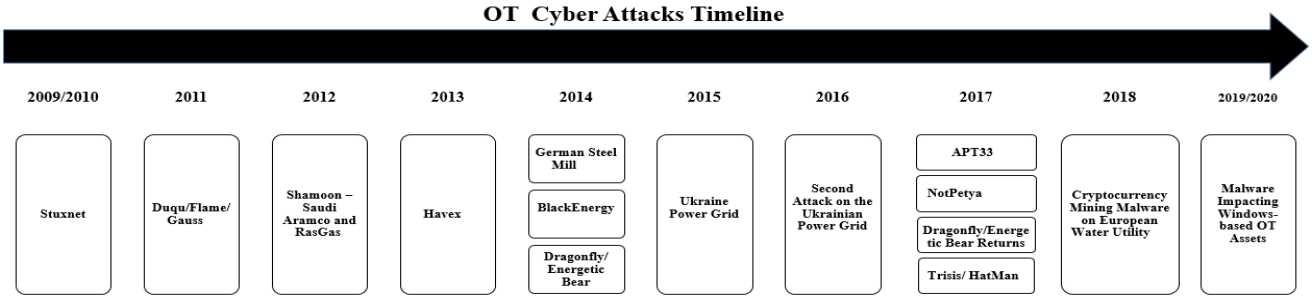


**Figure 3.** OT history of cyber attacks.

The default option runs if the template name is not selected; Figure 4 is S7-200 from Siemens.

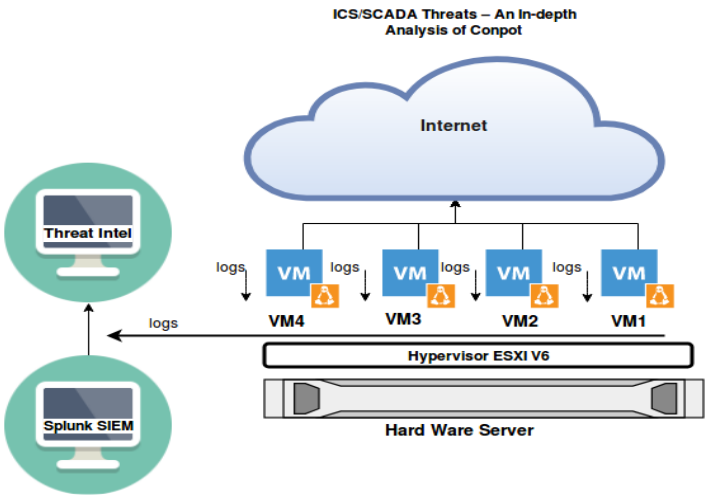


**Figure 4.** ICS/SCADA honeypot architecture.

The experimental work runs in one phase:

- In this phase, there are two machines: one is the default PLC S7-200, and the other one is the S7-300.

All of these machines have public IPs and are hosted on one hardware server, and they are managed through SSH.

Table 5 summarizes the deployed Conpot honeypots with their IP addresses and template details.

**Table 5.** Conpot available templates.

| Template | Unite | Protocols |
|---|---|---|
| -template proxy | Non-proxy | proxy |
| -template guardian_ast | Guardian—Guardian AST tank monitoring system | guardian_ast |
| -template default | -S7-200 | HTTP, MODBUS, s7comm, SNMP |
| -template kamstrup_382 | Kamstrup—382 | Kamstrup |
| -template IEC104 | -S7-300 | IEC104, SNMP |
| -template IPMI—371 | IPMI—371 | IPMI |

As previously mentioned, there are currently only two running machines which have a public IP address of 41.38.171.244, and another running machine with a public IP address of 41.38.171.245.

#### 6.1.1. Experimental Component

SIEM Solution: The use of security information and event management (SIEM) solutions in detecting and responding to cyber attacks is becoming increasingly important, especially in operational technology (OT) environments. One notable SIEM solution that has gained popularity in recent years is Splunk. Splunk can be used to collect and analyze data from various sources, including OT devices and applications, in order to identify anomalies and security events that could indicate a security breach. During this experimental work, it was used as a virtual machine to collect and analyze logs from both machines.

#### 6.1.2. Threat Intelligence

MISP (Malware Information Sharing Platform) is an open-source threat intelligence platform that enables organizations/researchers to collect, share, and collaborate on indicators of compromise (IOCs) and other security-related information. It was developed by the MISP Project, which is a community-driven initiative aimed at improving threat intelligence sharing across organizations.

Key Features of MISP:

- Threat Intelligence Feeds: MISP allows you to integrate with external threat intelligence feeds to enrich your data and automatically import indicators from trusted sources. It supports various feed formats and provides customization options for managing feed subscriptions.
- Visualization and Analysis: MISP offers visualizations and analytics capabilities to help users understand the relationships between different indicators and events. It includes tools for graph visualization, timeline analysis, and statistical reporting

#### 6.1.3. Security Assessment and Scanning Tool

Nessus is a well-known vulnerability scanner and security assessment tool developed by Tenable, Inc. Nessus is widely used by security professionals, researchers, and IT departments to identify vulnerabilities and security issues in computer systems, networks, and applications.

Nessus can perform a variety of security scans, including vulnerability scans, configuration audits, malware detection, and web application scanning. The tool uses a database of known vulnerabilities and security issues to identify potential security problems in target systems. Nessus can also provide detailed reports and remediation advice to help IT teams address any issues identified during the scanning process.

Nessus has modules for OT network vulnerability scanning, which are customized to discover OT vulnerability scanning in different OT applications.

### *6.2. Experimental Results*

To scan open ports on these honeypots, we used some tools; Nmap [18] is one such tool which searches for open ports in the target machine. Nmap has different scanning techniques, as summarized in Table 6.

**Table 6.** Honeypots' deployment setup.

| Location | Name | IP | Template |
|---|---|---|---|
| Location 1 | Conpot 1 | 41.38.171.244 | Default S7-200 |
| Location 2 | Conpot 2 | 41.38.171.245 | S7-300 |

There are many scripting and advanced techniques used by Nmap for carrying out advanced and deep scanning for target machines. The above scripting is just an example. After scanning with these scripts, the honeypot's open ports are summarized in Table 7, and the ports' function can be described as follows. Port 80 is an HTTP port used to access Conpot through the web. SSH commonly uses port 22 to allow users to log in and issue commands on distant machines. Port 161 is used by firewalls, routers, and other hardware and software to utilize the Simple Network Management Protocol (SNMP) to send logging and management data to remote monitoring software. The Modbus protocol on port 502 is used for field device communication, while the ASF Remote Management and Control Protocol (ASF-RMCP) and the Intelligent Platform Management Interface (IPMI) Remote Management Protocol over UDP both officially use port 623. S7 Communication is carried out using port 102 (S7comm). Programmable logic controllers (PLCs) of the Siemens S7-300/400 series communicate with one another via the proprietary S7comm protocol.

**Table 7.** Nmap scanning techniques.

| Result | Script |
|---|---|
| Scan a single IP | Nmap [IP address] |
| Scan a subnet | Nmap [IP address/Subnet] |
| Detect OS and services | Nmap—A [IP Address] |
| Version detection | Nmap—A—V [IP Address] |
| Doing ping during the scan | Nmap—A—V-PN [IP Address] |

Shodan [19] is a search engine that obtains all connected devices' IP addresses and their banners. These devices can be routers, servers, switches, cameras, etc., and the banners might include information about the server's operating system, active programs, open ports, the features it supports, a welcome message, or anything else the client can learn before interacting with the server. Additionally, Shodan looks for any potential security holes in these systems, and accesses the exploits for such holes.

## 7. Results Analysis

The honeypots were active for one month with public IP addresses from one of the service providers; hence we have one month of data. The protocols analyzed are HTTP, SNMP, Modbus, BACnet, and S7Comm. The number of IP addresses from each country is summarized in Table 8.

**Table 8.** Honeypot open ports.

| Honeypot Type | Open Ports |
|---|---|
| Siemens S7-200 | 80, 22, 161, 502, 623, 102 and 6009 |
| Siemens S7-300 | 20, 22, 502, 161 and 102 |

These IP addresses are the highest in some countries (Table 9), but some countries also have IP addresses under ten, such as Chile, Colombia, Ecuador, Georgia, Germany, India, and Japan. Figure 5 illustrates the percentages of countries.

**Table 9.** Number of IP addresses from each country.

| Country | Number of IPs |
|---|---|
| Iran | 18 |
| Russia | 21 |
| Netherland | 28 |
| Brazil | 36 |
| China | 750 |
| USA | 250 |
| Ukraine | 89 |
| Italy | 125 |
| France | 778 |
| Egypt | 537 |

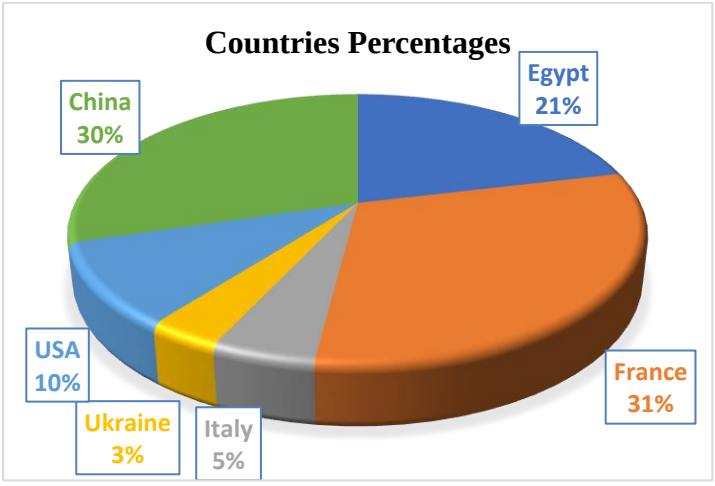


**Figure 5.** Number of IP addresses from each country.

In the second stage analysis for IP addresses per port, we found that the most accessed protocol is HTTP, followed by SNMP, Modbus, S7comm, and then Bacnet. Below are some IP addresses that tried to access these ports. Figure 6 illustrates a comparison between the protocols addressed in the top countries.

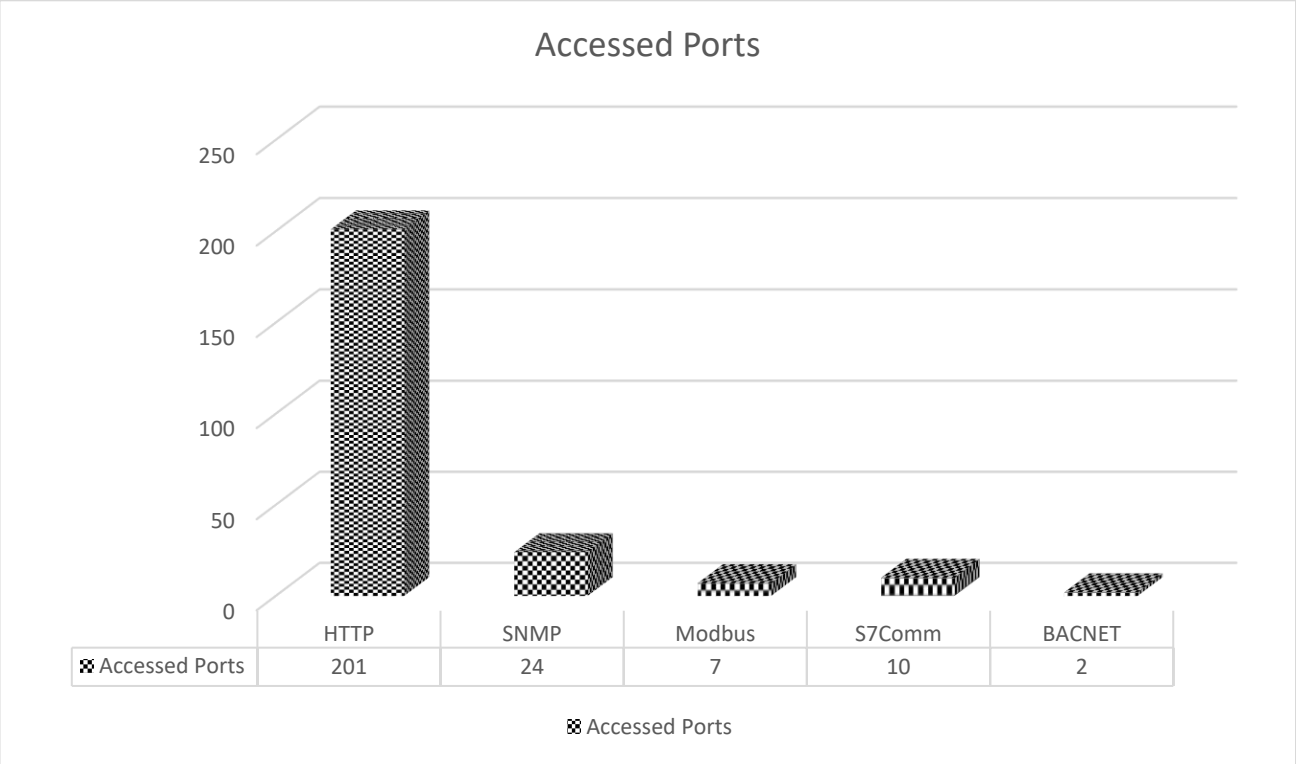


**Figure 6.** Protocols accessed by top countries.

- **HTTP: 201 IPs**
  - (102.134.73.30).
  - (103.23.34.14).
  - (103.50.7.115).
  - (103.65.193.129).
  - (103.87.170.210).
  - (104.152.52.31).
- **SNMP: 24 IPs**
  - (100.27.12.73).
  - (104.131.145.116).
  - (104.131.145.165).
  - (129.250.206.86).
  - (184.105.139.67).
- **Modbus: 7 IPs**
  - (104.131.132.215).
  - (105.42.161.219).
  - (154.129.241.152).
  - (196.52.43.116).
  - (196.52.43.88).
  - (198.108.66.16).
  - (50.116.23.165).
- **S7comm: 10 IPs**
  - (104.131.131.237).
  - (105.42.161.219).
  - (122.228.19.79).
  - (125.64.94.197).
  - (139.162.99.243).

- (154.131.238.4).
- (178.73.215.171).
- (198.108.66.224).
- (198.20.99.130).
- (71.6.199.23).

- **BACnet: 2 IPs**
  - (185.35.62.20).
  - (196.52.43.84).

Table 10 shows some of the most well-known industrial control systems (ICS)' vulnerabilities, their impact, and possible mitigation solutions or services.

**Table 10.** Some of the most well-known industrial control systems (ICS).

| Vulnerability | Impact |
|---|---|
| Insecure Protocols (e.g., Modbus) | Lack of encryption, integrity, and authentication measures, making them vulnerable to attacks |
| Insecure Interfaces | Legacy control interfaces that connect to the internet, connected industrial IoT devices, and various BYOD devices can serve as entry points to the system and introduce vulnerabilities |
| Insecure Software | Lack of access control in real-time operating systems, and vulnerabilities in Windows and Linux |
| Weak Encryption | Use of weaker Wi-Fi encryption protocols |
| Insufficient Physical Security | Lack of physical security measures for devices and systems |
| Lack of Network Segmentation | Systems are not segmented, allowing an attacker to move laterally and gain access to critical systems |
| Lack of Monitoring | Insufficient monitoring of network traffic and system activity |

Mitigation solutions/services may vary depending on the specific system and context. However, overall it is important to regularly update and patch systems, implement network segmentation and access controls, and monitor network traffic and system activity to mitigate the risk of cyber-attacks on ICS (as shown in Table 11).

**Table 11.** List of Modbus, S7comm, and BACnet protocols and their potential impact if accessed by attackers.

| Protocol | Purpose | Vulnerabilities | Impact |
|---|---|---|---|
| Modbus | Communication protocol for industrial control systems | Lack of encryption, authentication, and integrity measures | Attackers can tamper with or disrupt data communication, modify system settings, and execute unauthorized commands |
| S7comm | Communication protocol for Siemens programmable logic controllers | Vulnerable to man-in-the-middle attacks, weak encryption, lack of authentication | Attackers can intercept and modify data, execute unauthorized commands, and cause system outages |
| BACnet | Communication protocol for building automation and control systems | Vulnerable to buffer overflow attacks, insecure authentication mechanisms | Attackers can exploit vulnerabilities to gain unauthorized access to the system, modify system settings, and cause system outages |

To protect operational technology (OT) systems against cyberattacks, several national and international standards can be adopted by organizations. These standards provide guidelines and best practices for securing OT systems and ensuring their availability, reliability, and security. Some of the most commonly used standards include:

- IEC 62443 series: Developed by the International Electrotechnical Commission (IEC), this series of standards provides comprehensive guidelines for securing industrial control systems (ICS) and OT systems.
- NIST SP 800-82: Developed by the National Institute of Standards and Technology (NIST), this standard provides guidelines for securing ICS and OT systems, including network security, access control, and incident response.
- ISO/IEC 27001: This international standard provides a framework for information security management systems (ISMS), including guidelines for protecting OT systems.
- ENISA's OT Cybersecurity Recommendations: Developed by the European Union Agency for Cybersecurity (ENISA), this document provides recommendations for securing OT systems, including threat intelligence, network security, and incident response.

Adopting these standards can help organizations and companies ensure the security and availability of their OT systems, as well as comply with regulatory requirements and industry best practices. However, it is important to note that following these standards is only the first step in protecting against cyberattacks. Organizations also need to implement strong security controls, regularly assess and monitor their systems, and have an incident response plan in place. Also, organizations should build an OT cyber security strategy and road map to achieve these objectives and reduce the surface of OT networks that is vulnerable to attacks.

## 8. Conclusions and Future Work

The risk of attacks on industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems is significant and growing. These systems are used to control critical infrastructure and industrial processes, making them valuable targets for cybercriminals and nation-state actors who seek to cause disruption, theft, or damage. These systems are also often legacy systems that were not designed with security in mind, making them vulnerable to a range of cyber threats, such as malware infections, unauthorized access, and denial-of-service attacks. If these systems are compromised, there may be serious consequences, including loss of service, financial losses, environmental damage, and even loss of life. To mitigate the risk of ICS/SCADA system attacks, it is important to implement strong security measures, such as network segmentation, secure remote access, and regular software updates. Regular risk assessments and security audits should also be conducted.

To mitigate the risks of OT attacks, organizations can use techniques such as network segmentation, access controls, and intrusion detection systems. Additionally, organizations can use honeypots, which are decoy systems designed to lure attackers away from real assets, to gather information about the types of attacks that are being launched against their systems. By analyzing the data collected from honeypots, organizations can better understand the nature of OT attacks and develop more effective strategies for defending against them.

ICS/SCADA honeypots are useful for security administrators to identify vulnerabilities in these systems. By deploying ICS/SCADA honeypots in a controlled environment, security administrators can simulate a target for attackers and monitor their behavior, helping to identify new attack techniques and understand the methods used by attackers. This information can be used to improve the security of the actual ICS/SCADA systems by patching vulnerabilities and implementing stronger security measures. However, it is important to note that deploying ICS/SCADA honeypots can also increase the risk of cyberattacks, as they may attract more attention from attackers. Therefore, it is crucial to deploy these honeypots securely and monitor them closely.

Different organizations should invest in OT cyber security. Here are some key recommendations for securing operational technology (OT) systems:

- Network Segmentation: Segregate the OT network from the IT network to reduce the risk of cross-contamination. This can help prevent malware infections from spreading from the IT network to the OT network.

- Secure Remote Access: Implement secure remote access protocols and restrict access to only authorized personnel. This can help prevent unauthorized access to the OT network.
- Regular Software Updates: Keep all software and systems up to date with the latest security patches and updates. This can help prevent attacks that exploit known vulnerabilities.
- User Awareness Training: Provide regular training to all personnel who interact with the OT network to help raise awareness of cyber security threats and the best practices for avoiding them.
- Asset Inventory: Maintain an accurate inventory of all assets connected to the OT network, including hardware, software, and configuration details. This can help identify and remediate vulnerabilities more quickly.
- Regular Risk Assessments: Conduct regular risk assessments and security audits of the OT network to identify and prioritize vulnerabilities. This can help ensure that security measures are up-to-date and effective.
- Incident Response Plan: Develop and regularly review an incident response plan, to ensure that your organization is prepared to respond quickly and effectively in the event of a cyber attack.
- Third-Party Security: Consider the security of third-party systems and services that may have access to or impact the OT network. Ensure that they are secured and maintained to a high standard.

By implementing these recommendations, organizations can significantly reduce the risk of cyber attacks on their operational technology systems, and protect their critical infrastructure and industrial processes.

In the future, our team will look more closely at OT attacks targeting critical infrastructure, and at study attackers' motivations, how the attack has been launched, which vulnerabilities have been exploited, the attack's impact on the target, and the lessons learned for future mitigation.

**Author Contributions:** Conceptualization, M.M. and M.A.; methodology, M.S.E.; software, A.D.J.; validation, M.M., M.A. and M.S.E.; formal analysis, A.D.J.; investigation, M.M.; resources, M.A.; data curation, M.S.E.; writing—original draft preparation, M.M.; writing—review and editing, M.A.; visualization, A.D.J.; supervision, A.D.J.; project administration, M.M.; funding acquisition, M.M., M.S.E., A.D.J. and M.A. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** Data in this research paper will be shared upon request made to the corresponding author.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Arafune, M.; Rajalakshmi, S.; Jaldon, L.; Jadidi, Z.; Pal, S.; Foo, E.; Venkatachalam, N. Design and Development of Automated Threat Hunting in Industrial Control Systems. In Proceedings of the 2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), Pisa, Italy, 21–25 March 2022; IEEE: Manhattan, NY, USA; pp. 618–623.
2. Lehto, M. Cyber-Attacks Against Critical Infrastructure. In *Cyber Security*; Springer: Cham, Switzerland, 2022; pp. 3–42.
3. Rashid, S.M.; Haq, A.; Hasan, S.T.; Furhad, M.H.; Ahmed, M.; Barkat Ullah, A.S. Faking Smart Industry: A Honeypot-Driven Approach for Exploring Cyber Security Threat Landscape. In Cognitive Radio Oriented Wireless Networks and Wireless Internet, Proceedings of the International Conference on Cognitive Radio Oriented Wireless Networks, International Wireless Internet Conference, Virtual, 11 December 2021; Springer: Cham, Switzerland, 2022; pp. 307–324.
4. Ara, A. Security in Supervisory Control and Data Acquisition (SCADA) based Industrial Control Systems: Challenges and Solutions. In *IOP Conference Series: Earth and Environmental Science*; IOP Publishing: Bristol, UK, 2022; Volume 1026, p. 012030.
5. Kelly, C.; Pitropakis, N.; Mylonas, A.; McKeown, S.; Buchanan, W.J. A Comparative Analysis of Honeypots on Different Cloud Platforms. *Sensors* **2021**, *21*, 2433. [CrossRef] [PubMed]
6. Grigoriou, E.; Liatifis, A.; Grammatikis, P.R.; Lagkas, T.; Moscholios, I.; Markakis, E.; Sarigiannidis, P. Protecting IEC 60870-5-104 ICS/SCADA Systems with Honeypots. In Proceedings of the 2022 IEEE International Conference on Cyber Security and Resilience (CSR), Rhodes, Greece, 27–29 July 2022; pp. 345–350. [CrossRef]

7. Yang, X.; Yuan, J.; Yang, H.; Kong, Y.; Zhang, H.; Zhao, J. A Highly Interactive Honeypot-Based Approach to Network Threat Management. *Future Internet* **2023**, *15*, 127. [CrossRef]
8. Mellado, J.; Núñez, F. Design of an IoT-PLC: A containerized programmable logical controller for the industry 4.0. *J. Ind. Inf. Integr.* **2022**, *25*, 100250. [CrossRef]
9. Sibai, F.N.; Mohammad, N.; Muhammad, S. Probabilistic Modeling and Study of Cybersecurity Attacks in Industrial Control Systems of Plants. In Proceedings of the 2020 IEEE Conference on Application, Information and Network Security (AINS), Kota Kinabalu, Malaysia, 17–19 November 2020.
10. Leverett, E.; Wightman, R. Vulnerability Inheritance in Programmable Logic Controllers. In Proceedings of the 2013 GreHack Conference, Grenoble, France, 15 November 2013.
11. ICS-CERT. *Common Cybersecurity Vulnerabilities in Industrial Control Systems*; U.S. Department of Homeland Security: Washington, DC, USA, 2011.
12. Yang, Y.S.; Lee, S.H.; Chen, W.C.; Yang, C.S.; Huang, Y.M.; Hou, T.W. Securing SCADA Energy Management System under DDos attacks using token verification approach. *Appl. Sci.* **2022**, *12*, 530. [CrossRef]
13. Kumar, A.; Bhushan, B.; Malik, A.; Kumar, R. Protocols, Solutions, and Testbeds for Cyber-Attack Prevention in Industrial SCADA Systems. In *The Internet of Things and Analytics for Agriculture*; Springer: Singapore, 2022; Volume 3, pp. 355–380.
14. Polat, H.; Türkoğlu, M.; Polat, O.; Şengür, A. A novel approach for accurate detection of DDoS attacks in SDN-based SCADA systems based on deep recurrent neural networks. *Expert Syst. Appl.* **2022**, *197*, 116748. [CrossRef]
15. Franco, J.; Aris, A.; Canberk, B.; Uluagac, A.S. A survey of honeypots and honeynets for the Internet of Things, industrial internet of Things, and cyber-physical systems. *IEEE Commun. Surv. Tutor.* **2021**, *23*, 2351–2383. [CrossRef]
16. Lau, S.; Klick, J.; Arndt, S.; Roth, V. POSTER: Towards highly interactive honeypots for industrial control systems. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 1823–1825.
17. Cabral, W.Z.; Valli, C.; Sikos, L.F.; Wakeling, S.G. Analysis of Conpot and its BACnet features for cyber-deception. In *Advances in Security, Networks, and Internet of Things 2021*; Springer: Cham, Switzerland, 2021; pp. 329–339.
18. Kang, K.D.; Park, G.; Kim, H.; Alian, M.; Kim, N.S.; Kim, D. NMAP: Power Management Based on Network Packet Processing Mode Transition for Latency-Critical Workloads. In Proceedings of the MICRO-54: 54th Annual IEEE/ACM International Symposium on Microarchitecture, Virtual Event, 18–22 October 2021; pp. 143–154.
19. Zolotykh, M. Study of Crawlers of Search Engine 'Shodan. io'. In Proceedings of the 2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT), Yekaterinburg, Russia, 13–14 May 2021; IEEE: Manhattan, NY, USA; pp. 419–422.