computers

MDPI

Article

A Survey of Security Challenges in Cloud-Based SCADA Systems

Arwa Wali *,† **and Fatimah Alshehry** †

Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah 21589, Saudi Arabia
* Correspondence: amwali@kau.edu.sa
† These authors contributed equally to this work.

Abstract: Supervisory control and data acquisition (SCADA) systems enable industrial organizations to control and monitor real-time data and industrial processes. Migrating SCADA systems to cloud environments can enhance the performance of traditional systems by improving storage capacity, reliability, and availability while reducing technical and industrial costs. However, the increasing frequency of cloud cyberattacks poses a significant challenge to such systems. In addition, current research on cloud-based SCADA systems often focuses on a limited range of attack types, with findings scattered across various studies. This research comprehensively surveys the most common cybersecurity vulnerabilities and attacks facing cloud-based SCADA systems. It identifies four primary vulnerability factors: connectivity with cloud services, shared infrastructure, malicious insiders, and the security of SCADA protocols. This study categorizes cyberattacks targeting these systems into five main groups: hardware, software, communication and protocol-specific, control process, and insider attacks. In addition, this study proposes security solutions to mitigate the impact of cyberattacks on these control systems.

Keywords: cloud security; cloud-based SCADA systems; cyberattacks

Citation: Wali, A.; Alshehry, F. A Survey of Security Challenges in Cloud-Based SCADA Systems. *Computers* **2024**, *13*, 97. https://doi.org/10.3390/computers13040097

Academic Editor: Leandros Maglaras

Received: 14 March 2024
Revised: 7 April 2024
Accepted: 8 April 2024
Published: 11 April 2024

1. Introduction

Supervisory control and data acquisition (SCADA) represents a control system architecture essential for operating critical infrastructure in industrial sectors, including electric generation, oil, gas, and manufacturing plants. This system facilitates the operation by controlling and monitoring real-time data and processes, either locally or remotely. It utilizes various components such as sensors, actuators, switches, and valves [1]. SCADA systems have transitioned from stand-alone, isolated environments (e.g., monolithic or distributed) with limited functionalities and proprietary communication protocols to network-based platforms utilizing wide-area networks (WANs) with open communication protocols and standards [2]. At present, SCADA systems have evolved into open systems connected to the Internet, fully integrated with corporate information technology (IT) networks, and support various facilities, software, and Internet protocols, such as TCP/IP [2,3].

As complex industrial operations necessitate advanced and efficient environments and handle vast amounts of data, the literature has proposed migrating SCADA systems to the cloud [4]. Cloud computing, employing parallel and distributed systems, offers IT resources under specific service-level agreements between customers and service providers [5]. Cloud systems can enhance traditional system performance by reducing technical and industrial costs. These sophisticated systems bolster computing environment attributes, including quality of service, reliability, flexibility, and communication efficiency. In addition, they ensure appropriate system configuration and maintenance [6].

According to Stojanović [4], two methods exist for integrating SCADA systems with cloud computing technologies. The first method involves utilizing public cloud infrastructure, where SCADA applications are executed within companies or organizations' premises.

Although the control functions of SCADA applications remain isolated in the controller network, they are directly connected to cloud services for data transfer, storage, and distribution. The second method employs private or hybrid cloud infrastructures, in which SCADA applications are entirely cloud-executed, while the controller units are remotely linked to these applications via WAN connections. Importantly, ensuring robust security measures, minimal latency, and high service availability is crucial when transitioning SCADA critical infrastructure to a cloud environment [7].

Although the use of cloud-based SCADA systems is increasing across various industrial sectors, these systems face the same cybersecurity challenges as other cloud-integrated systems. Data in the cloud are often accessible and located in an open, distributed environment [8]. The features of cloud-based SCADA systems, such as real-time monitoring and/or the control of processes, data transmission over the Internet, and remote access, create numerous security vulnerabilities that potential attackers can exploit. These vulnerabilities allow attackers to inject malware, modify control data, or block data transfer [4]. In addition, the public cloud environment exposes these systems to other security threats, including denial-of-service (DoS) attacks, distributed DoS (DDoS), and man-in-the-middle (MITM) attacks [9].

Researchers in previous studies have extensively reviewed cloud-based SCADA frameworks and their primary components, as highlighted in references [8,10–12]. However, in recent years, there is limited scientific research specifically addressing the security challenges inherent in these crucial infrastructures. To mention a few, the authors in [13,14] generally addressed the broad vulnerabilities and cyberattacks of cloud-based SCADA systems including the limited security controls over the data, loss of connection, lack of security standardization, and lack of sufficient authentication and encryption mechanisms. The authors suggest various cybersecurity measures, such as encryption, intrusion detection systems, and secure architecture design to detect and mitigate cyber threats in cloud-based environments. Additionally, the paper [14] emphasizes the importance of regular log analysis, the application of blockchain-based security solutions for enhanced data integrity and control, and the necessity of thorough data backup and recovery practices. Sajid et al. [15] outline the security vulnerabilities and threats to SCADA systems in Internet of Things (IoT) cloud environments, including security risks related to data logging, the lack of authentication and encryption mechanisms, and the threats of the lack of protecting the embedded devices at the core of industrial IoT-based SCADA systems.

Other studies classify various attacks based on specific criteria. Maglaras et al. [16] discuss threats to critical infrastructures, presenting various attacks on SCADA systems, critical infrastructure attack analysis, and IoT-enabled attack vectors, including their impact on healthcare, transportation systems, and 5G cellular infrastructure. To protect critical information assets, the paper outlines cybersecurity measures classified according to legal, technical, organizational, capacity building, and cooperation aspects. It highlights the significance of cyber threat intelligence for preemptive countermeasures against potential attacks.

In addition, Pliatsios et al. [17] provide a survey of various high-impact security threats on SCADA protocols (i.e., Modbus, DNP3, etc.). The authors recommend exploring novel SCADA protocols designed to meet the demands of Industry 4.0, integrating IoT concepts, leveraging virtualization technologies like Software Defined Networking (SDN) and Network Function Virtualization (NFV), the application of big data analytics in enhancing SCADA security, and the adoption of a SCADA cyber hygiene framework. Similarly in [18], the paper presents a classification of attacks based on security needs and network protocol layers of SCADA systems. This classification covers attacks on hardware, software, and network connections. It reviews numerous security schemes proposed to address SCADA network vulnerabilities, organizing them based on current standards, detection, and prevention of attacks.

In general, the scope of the existing research on cloud-based SCADA systems security is often narrowed to specific types of attacks, with the results being scattered throughout

numerous publications. Addressing this gap, our research aims to offer a comprehensive survey of the main vulnerabilities and cyberattacks targeting cloud-based SCADA systems. Furthermore, it will examine the range of existing security solutions developed to strengthen these systems against such threats.

This paper is organized into eight sections, beginning with this introduction. Section 2 presents a brief background for the main architecture and technologies of both traditional and cloud-based SCADA systems. Section 3 describes the research's survey methodology. Section 4 identifies the primary vulnerabilities in cloud-based SCADA systems. Sections 5 and 6 offer reviews of cyberattacks on these systems and the tactics employed, respectively. Section 7 discusses security solutions from the existing literature applicable to such systems. This paper concludes in Section 8 with a discussion of the limitations and recommendations for future research.

2. Background

To understand the vulnerabilities and cyberattacks described later, this section offers a brief overview of the architecture of traditional and cloud-based SCADA systems, as well as the main technologies used in both systems.

2.1. Traditional SCADA Systems Architecture

Traditional SCADA systems consist of an integration of hardware components, software programs, and communication links that facilitate the monitoring, controlling, and management of industrial processes. Hardware includes remote terminal units (RTUs), programmable logic controllers (PLCs), intelligent electronic devices (IEDs), master terminal units (MTUs), and actuators and sensors. Software encompasses the human–machine interface (HMI), a central database (Historian), and other user software [2]. RTUs collect real-time data from sensors in the physical environment via LAN/WAN links and transmit this information to the MTU. Along with PLCs and IEDs, RTUs locally control actuators and monitor SCADA sensors [4]. RTUs also transfer the current status data of connected physical devices. The MTU acts as the central monitoring station, issuing commands to RTUs, responding to their messages, processing and storing data, analyzing information, and generating reports for future communication.

The HMI acts as the interface between SCADA hardware and software, facilitating control, monitoring, and communication between RTUs and the MTU. The Historian is responsible for storing communication data, events, and alarms and serves as a centralized database or server. It supports the HMI by providing data for graphical trend analysis. The communication network enables interactions between SCADA components, utilizing either wireless or wired media. Wireless communication is often preferred for its efficiency in connecting geographically distributed and remote areas. This network is typically isolated from external networks to reduce cybersecurity risks. Traditional SCADA systems operate independently on-site and often use closed, vendor-specific, and real-time proprietary communication protocols (e.g., TCP/IP, Modbus), which enhance security through obscurity but may limit interoperability. Figure 1 shows the overall architecture of a traditional SCADA system's framework. For more information, we refer the reader to [2,4].

2.2. Cloud-Based SCADA System Architecture

In a cloud-based SCADA system, the architecture typically involves integrating SCADA applications with cloud services to enhance scalability, accessibility, and cost-effectiveness [19]. In addition to the various traditional components of SCADA systems, the cloud architecture is responsible for more extensive data processing, storage, and advanced analytics [2]. It provides global access to data, supports large-scale computational tasks, and hosts applications that require significant processing power. Controllers such as RTUs and PLCs are connected via WAN links to SCADA applications executed in the cloud [15].

Cloud-based SCADA systems incorporate Cyber–Physical Systems (CPSs)/IoT integration, enabling the connection of a vast array of sensors and devices and facilitating real-time data collection and automation. Hosting services like fog nodes—which include industrial controllers, routers, and embedded servers—act as intermediaries, processing data closer to its source to enhance real-time processing, reduce latency, and support local data analytics and storage [2,20]. Additionally, control functions within the SCADA application are segregated in the controller network, while the application itself is connected to cloud services for visualization, reporting, and remote access [4]. Communication networks in cloud-based SCADA systems support various protocols and standards (e.g., distributed network protocol (DNP3)), ensuring interoperability and secure data exchange between devices and the cloud [21]. The infrastructure also integrates security technologies such as firewalls—which control incoming and outgoing network traffic—and includes encryption, authentication, intrusion detection systems, and access control mechanisms to safeguard against cyber threats [22].

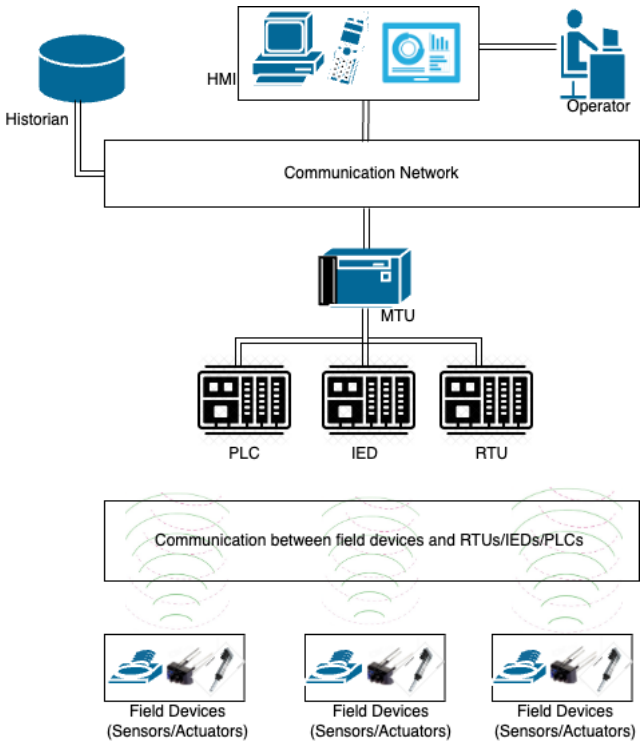

Figure 1. Architecture of traditional SCADA systems (inspired by [2]).

In general, cloud computing systems offer four main layers of services for SCADA applications, each structured hierarchically as follows [4,19]:

1. The hardware layer, located within data centers, consists of essential physical components such as processors, memory, storage, and bandwidth.
2. The infrastructure layer introduces virtualization and provides infrastructure as a service (IaaS), featuring a pool of virtual machines (VMs) that host SCADA applications and can be provisioned on demand to IT users.
3. The platform layer builds upon the infrastructure services to offer platform as a service (PaaS), enabling software development and delivery over the web, and
4. The software layer delivers ready-to-use software and applications, meeting various business needs and providing software as a service (SaaS) by utilizing the platform layer's components and services.

Figure 2 illustrates the overall architecture of a cloud-based SCADA system.

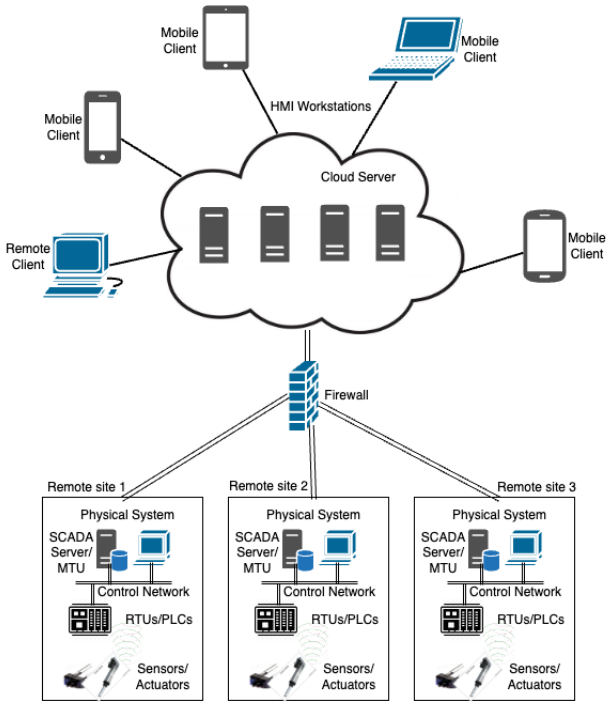

Figure 2. Architecture of cloud-based SCADA systems (inspired by [15]).

The transition to cloud-based SCADA systems from traditional architectures marks a significant shift toward more integrated, intelligent, and flexible industrial control systems. While cloud-based systems offer numerous advantages, they also introduce new challenges, especially concerning cybersecurity and data privacy. In both architectures, the emphasis on security—whether through cyber or physical means—remains paramount, underscoring the critical importance of protecting industrial processes and infrastructure.

3. Research Methodology

We conducted this research by gathering information on the security challenges and threats compromising cloud-based SCADA systems, followed by a discussion of various security solutions to mitigate their adverse impacts. To achieve this, relevant articles published in top venues from 2016 to 2024 were collected using search keywords including "security of cloud-based SCADA systems," "cyberattacks on cloud-based SCADA systems," "cloud-based SCADA system security challenges," and "cloud-based SCADA system security issues." In addition, these keywords were utilized to search for scientific papers across various scientific databases and platforms, such as Google Scholar, ResearchGate, the Institute of Electrical and Electronics Engineers, and ACM.

To ensure each article was of high quality and directly relevant to the subject of cloud-based SCADA system security, our criteria for article selection included the following key components:

- English peer-reviewed studies: We prioritized articles published in well-respected, peer-reviewed journals, conference proceedings, and book chapters. This ensures the reliability and academic integrity of the information presented.
- Relevance to cloud-based SCADA systems: We selected articles based on their focus on security issues specifically related to cloud-based SCADA systems. We carefully reviewed abstracts, keywords, and conclusions to determine the direct relevance of each study to our research topic.
- Recency of publication: Given the rapidly evolving nature of cybersecurity, we gave preference to articles published within the last five to seven years. This helped ensure that the findings and discussions in our review reflect the current challenges and solutions in the field, and

- Citation count and impact factor: we also considered the citation count and the publishing journal's impact factor as indicators of the article's influence and relevance to the academic community in the field of cybersecurity.

Employing an inductive generalization approach, we reviewed the selected articles and analyzed them to identify patterns in security challenges, particularly focusing on vulnerabilities and cyberattacks in cloud-based SCADA systems. This approach enables the transition from specific instances to a broader generalization. We then formulated themes by grouping and classifying analogous patterns and labeling them according to the frequency of cyberattacks.

This research identified four primary vulnerability factors: connectivity with cloud services, shared infrastructure, malicious insiders, and the security of SCADA protocols. In addition, five categories of cyberattacks were outlined: hardware, software, communication and protocol-specific, control process, and insider attacks. Within these, software attacks are further classified as industrial control systems (ICSs) that are vulnerabilities-based or cloud-specific. The most prevalent tactics in various cyberattacks impacting the security of cloud-based SCADA systems are DoS, MITM, and advanced persistent threat (APT) attacks. Figure 3 illustrates the general classification of vulnerability factors, cyberattacks, and their common tactics, derived from an inductive generalization approach applied to related studies. Finally, this paper discusses several suitable security solutions for cloud computing in general and cloud-based SCADA systems in particular, recommending their application for the detection and prevention of cyberattacks.

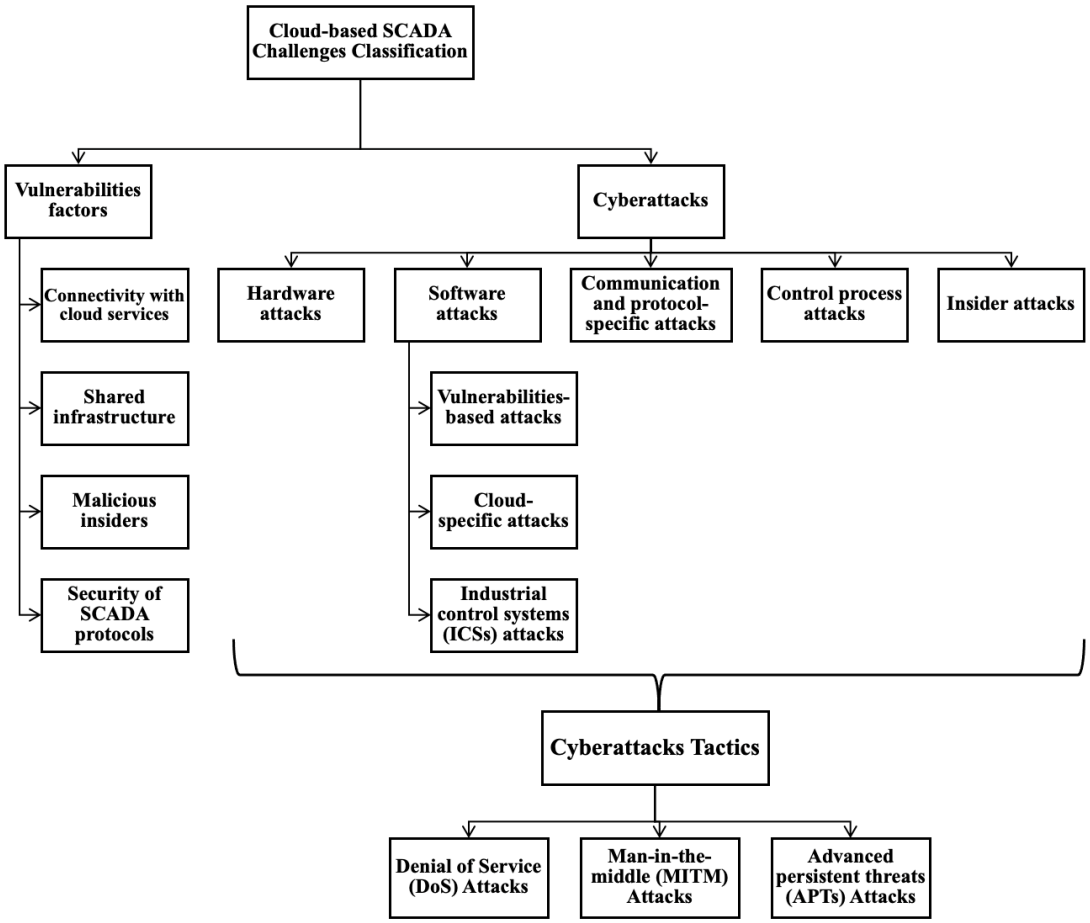

Figure 3. Classification of the security challenges of cloud-based SCADA systems.

4. Cloud-Based SCADA Systems Vulnerabilities

Previous studies have explored general vulnerability factors and security challenges in cloud-based SCADA systems. These challenges range from human errors and insuffi-

cient resources for physical devices to proprietary protocols and insecure legacy systems. Insecure legacy control interfaces, connections to the internet, connected industrial IoT (IIoT) devices, and various bring-your-own devices (BYODs) [23], along with accidents due to negligence and equipment failures [24], can all serve as entry points to the systems for cyberattacks, introducing vulnerabilities. In addition, unprotected virtual machines, the unavailability of cloud infrastructure [25], account or service traffic hijacking [26], security concerns of industrial automation and analysis devices, inadequate software security mechanisms in many industrial sensors running real-time processes [23], and the omission of proper backdoor capabilities by some manufacturers for managing and updating industrial devices [27] are significant vulnerability factors that organizations need to consider after transitioning to a cloud-based infrastructure.

The analysis of cyberattacks targeting cloud-based SCADA systems identified four prevalent vulnerabilities: (1) the interconnectivity between SCADA systems and cloud services, (2) the use of shared infrastructure, (3) the presence of malicious insiders, and (4) the security robustness of SCADA protocols. The subsequent subsections provide brief overviews of these factors.

4.1. SCADA Systems and Cloud Service Connectivity

Traditional SCADA systems, designed as closed systems without Internet connectivity, serve as a protective mechanism. However, migrating these systems to the cloud exposes them to complex network environments, thereby increasing security threats, similar to those faced by any cloud infrastructure [4,15]. In cloud-based SCADA systems, local devices may lose connectivity with remote components, leading to delays in production processes, data loss, and error propagation in other system components [13]. This is attributed to the required connectivity with cloud data centers, a critical argument against adopting cloud computing [12]. Deploying data and applications to the cloud and accessing them via the Internet inherently increases system vulnerability to attacks by malicious users [25].

Unlike traditional systems, components of cloud-based SCADA systems do not adhere to a uniform security framework, resulting in an inconsistent operational performance [13]. This necessitates considering additional security concerns, including hacker tracking, information leakage, latency issues, and privacy concerns [2]. Table 1 summarizes the significant impacts of vulnerabilities arising from the connectivity between SCADA systems and cloud services on cloud-based SCADA systems.

Table 1. "Connectivity between SCADA system and cloud service" vulnerability impacts on cloud-based SCADA systems based on articles between the years of 2016 and 2024.

Vulnerability Impact	Article Reference	Authors, Year
The dependence on cloud communication renders the SCADA system more vulnerable to external access.	[15]	Sajid et al., 2016
Security threats increase due to the required connectivity to the public cloud.	[12]	Yi et al., 2017
Increasing risks that can potentially affect the security of cloud-based SCADA systems.	[4]	Stojanović et al., 2019
The loss of connection leads to delayed processes, data loss, and privacy issues.	[13]	Bhamare et al., 2020
Communication through a public cloud exposes the SCADA system to potential cyberattacks.	[25]	Nazir et al., 2020
The reliance on cloud communication can expose SCADA to denial-of-service (DoS) attacks and man-in-the-middle (MITM) attacks	[2]	Yadav et al., 2021

4.2. Shared Infrastructure

Sharing an infrastructure with external, unidentified users presents various threats to such systems [4]. In particular, the risks stem from the potential of sharing hardware infrastructure, like physical servers, with other entities, such as businesses or competitors. These entities might employ command/response injection techniques for system attacks. This leads to several consequences, potentially impacting cloud-based SCADA systems

in their critical, real-time applications [25]. The multi-tenancy feature in cloud-shared technologies presents significant risks, particularly if the hypervisor, or virtual machine monitor, lacks robust protection. Intrusions into virtual machines on the same hypervisor may enable malicious activities, compromising the integrity and confidentiality of critical infrastructure data [26]. The major vulnerability impacts of shared infrastructure on cloud-based SCADA systems are summarized in Table 2.

Table 2. "Shared Infrastructure" vulnerability impacts on cloud-based SCADA systems based on articles between the years of 2016 and 2024.

Vulnerability Impact	Article Reference	Authors, Year
Security risks emerge due to the multi-tenancy feature inherent in cloud technologies.	[26]	Cerullo et al., 2016
Sharing the infrastructure with external parties exposes the system to command/response injections, including DoS and MITM attacks.	[4]	Stojanović et al., 2019
Cloud vendors do not guarantee that SCADA resources will not be shared with other businesses, potentially leading to threats to the system	[25]	Nazir et al., 2020

4.3. Malicious Insiders

Malicious insiders are commonly regarded as the most severe threat to any system, notably critical systems like SCADA systems, which oversee industrial operations. Malicious insiders may include former employees, system administrators, or cloud service providers with privileged access to system resources. These insiders introduce inherent security vulnerabilities to the systems. [15,26]. Various security threats posed by malicious insiders include unauthorized access and control, data breaches, data theft, data manipulation, and data exploitation [13].

These security threats can lead to intentional or unintentional errors, potentially causing significant damage to the system. This risk is heightened as insiders possess detailed knowledge of the system's operations [25]. In the context of the Internet of Things (IoT) within cloud-based SCADA systems, employees, vendors, and suppliers often have their connections to these systems. They may be authorized to access or control network sensors, enabling them to add or update functionalities and to access production data and statistics. Efforts to block or stop these forms of authorized access could lead to a shutdown of the entire organization's cloud-based SCADA system [27]. Table 3 summarizes the major vulnerability impacts caused by the malicious insiders' factor in cloud-based SCADA systems.

Table 3. "Malicious Insiders" vulnerability impacts on cloud-based SCADA systems based on articles between the years of 2016 and 2024.

Vulnerability Impact	Article Reference	Authors, Year
Malicious administrators at the cloud provider (CP) or any other user with privileged access to resources will consistently threaten the system.	[26]	Cerullo et al., 2016
Threats associated with external individuals and cloud service providers.	[15]	Sajid et al., 2016
Employees and vendors associated with the cloud might have authorized access to and/or control over sensors on the network, potentially leading to various security risks.	[27]	Ulltveit-Moe et al., 2016
Other remote cloud users are abusing the system's flaws.	[13]	Bhamare et al., 2020
The loss of access to SCADA system resources can be caused either by employees of CPs with malicious intentions or by innocent mistakes.	[25]	Nazir et al., 2020

4.4. SCADA Protocols Security

Another factor contributing to the vulnerability of cloud-based SCADA systems to various security threats is the lack of protection in some traditional SCADA communication protocols, such as Modbus/TCP , International Electrotechnical Commission (IEC) 60870-5 series, IEC 61850, and DNP3 [15]. These protocols do not support authentication and

encryption mechanisms [4,23] and suffer from a lack of protection controls [2]. As a result, these protocols expose system applications running on the cloud to attackers and permit intruders' easy access to private credentials, such as IP addresses and usernames, during cloud use. Moreover, the inadequate security in protocols like the IEC 61850 standard, used for intelligent electronic devices at electrical substations, capitalizes on SCADA systems' vulnerabilities and introduces key management challenges for SCADA networks [15]. Table 4 outlines the primary impacts of these security vulnerabilities on cloud-based SCADA systems.

Table 4. "SCADA system protocols" vulnerability impacts on cloud-based SCADA systems based on articles between the years of 2016 and 2024.

Vulnerability Impact	Article Reference	Authors, Year
SCADA systems use Modbus/TCP, IEC 61850, and DNP3 for automation and control. However, these protocols lack protection and expose control and automation operations to cyberattacks.	[15]	Sajid et al., 2016
SCADA-specific application layer protocols such as Modbus and DNP3 do not support encryption and authentication controls, negatively impacting the security of cloud-based SCADA systems.	[4]	Stojanović et al., 2019
The security risks in the traditional SCADA system propagate due to the absence of protection controls in Modbus/TCP, IEC 40, and DNP3.	[2]	Yadav et al., 2021

5. Cyberattacks of Cloud-Based SCADA Systems

Previous studies that address cyberattacks on cloud-based SCADA systems are addressed either broadly [13,14,28] or by classifying them based on specific criteria such as passive or active, internal or external [16], and targets of attacks [4,17,18]. Since the most common classification criterion by many researchers is the target of the attack or the system part affected or exploited, we adopt this criterion in our survey and expand the existing classification into five attack types: hardware, software, communication and protocol-specific, control process, and insider. Software attacks are further categorized into ICS-related, vulnerabilities-based, or cloud-specific. We survey and discuss these attacks in the subsequent subsections.

5.1. Hardware Attacks

Hardware in cloud-based SCADA systems is interconnected with diverse global components and various third-party libraries, enabling complex interactions within the systems. The primary hardware elements include the control center and controller units, such as RTUs, PLCs, and intelligent electronic devices.

The control center gathers and analyzes data from field sites, displays these data on HMI consoles, and acts based on detected events. The controller units' control functions collect data and relay them to the cloud for storage and distribution. Additional system components encompass the MTU server, application servers, Historian server, engineering workstations, HMI server, and consoles, along with communication devices like routers, switches, and modems [4].

In general, vendors of SCADA systems are aware of hardware security threats, such as backdoor attacks. Moreover, wireless devices that supply data to traditional SCADA systems lack robust protection due to their minimal power requirements, presenting an accessible vector for system intrusions [25].

McLaughlin et al. [29] identified hardware attacks in cloud infrastructure as vulnerabilities at the hardware layer, including Trojan injections and compromising reliability and security. These vulnerabilities allow for the unauthorized modification of firmware, reverse engineering of logic through Joint Test Action Group ports, and circuit board damage through manipulated universal serial bus drives that can alter domain name system (DNS) settings, leading to communication redirects.

Another sophisticated hardware attack was described in [30] that targets both ICS software and hardware. This attack employs Web Graphics Library malware to infiltrate graphics processing unit (GPU) hardware through least-privileged remote parties, potentially exposing content from GPU memory past workloads. This attack can propagate from the central system to other devices and be leveraged to initiate DoS attacks, disrupting ICS operations.

In addition, SCADA system hardware may be targeted by malware injected into the firmware of PLCs, thus compromising controller security. In addition, unauthorized access to SCADA systems' physical locations can lead to substantial operational disruptions, including tampering with critical threshold settings [31]. Hardware attacks could also result from device power loss due to switches, intentional damage, or physical attacks on the control network [32].

5.2. Software Attacks

SCADA software encompasses all applications used to operate SCADA systems, responsible for managing information, controlling and monitoring procedures, data diagnostics and maintenance, as well as client/server and third-party development environments [33]. Software attacks on SCADA systems are a primary concern, identified as cyber-kinetic attacks, which are complex and can threaten life and cause physical damage [34]. These cyber-kinetic attacks can be executed using various techniques such as malware injection, command/response injections, phishing, spear phishing, DoS attacks, SQL injection attacks, MITM attacks, and APTs [4]. Within cloud-based SCADA systems, software attacks can be categorized as ICS-related, vulnerabilities-based, or cloud-specific. These three attack types are briefly reviewed in the sections that follow.

5.2.1. ICS Attacks

In their work, Bhamare et al. [13] provided examples of general attacks that could impact ICSs overseen by SCADA systems, including (1) APT attacks, (2) DDoS attacks, (3) corruption of voice and data network services, (4) combined cyber and physical assaults, (5) hacktivist-initiated attacks, and (6) supply chain compromises or disruptions.

Green et al. [35] investigated several high-profile attack scenarios against ICSs and critical infrastructures, such as MITM incidents, control request injections, replay attacks on the RTU, and pin control manipulations. Moreover, the authors in [28] noted that perception errors significantly contributed to the success of these attacks. These perception errors are associated with four dimensions: system qualities, system boundaries, observability, and controllability.

Tariq et al. [7] discussed various software attacks affecting the critical infrastructure of SCADA systems, including Trojan horse viruses, Stuxnet worm outbreaks, Slammer worms, Flame malware, Dragonfly malware, DDoS, and MITM attacks. In addition, they examined social-level attacks, such as social engineering, insider threats, and phishing schemes. In a related study, Chromik et al. [32] outlined cyberattacks on power grid SCADA systems, detailing (1) the damage or loss of IT assets due to attacks that manipulate system data; (2) malicious activities such as the abuse of IT assets with intentional interference in the information systems (e.g., DoS); and (3) eavesdropping, interception, and hijacking, which facilitate unauthorized communications with system devices (e.g., MITM).

5.2.2. Vulnerabilities-Based Attacks

McLaughlin et al. [29] characterized software attacks as vulnerabilities at the software layer, ranging from coding errors to the improper implementation of access control mechanisms. Conversely, Irmak and Erkek [31] described software attacks as stemming from flaws in source code design and implementation, including issues such as buffer overflow, SQL injections, cross-site scripting (XSS), and inadequate patch management.

Similarly, Demertzis and Iliadis [36] described software attacks as the exploitation of weaknesses by attackers to gain unauthorized access to systems. They also listed specific attacks targeting the power system of SCADA, such as remote tripping command injection, changes to relay settings, and data injection attacks. Rodofile et al. [37] categorized software attacks on SCADA systems as those based on configuration manipulations, including fake master station attacks, the manipulation of injection commands, attacks from malicious "Bring Your Own Device" scenarios, and attacks targeting configuration files.

Cherdantseva et al. [38] examined software attacks from various perspectives, recognizing them as cybersecurity challenges and vulnerabilities potentially impacting SCADA systems, particularly concerning patching and human factors. They noted that patching can inadvertently introduce new vulnerabilities or disrupt systems, particularly those needing continuous operation 24/7. In addition, human factors can lead to errors, causing unintentional attacks, and social engineering, which may result in both deliberate internal and external attacks.

5.2.3. Cloud-Specific Attacks

In general, software attacks against cloud-based SCADA systems primarily include APTs, compromised data integrity, MITM attacks, replay attacks, and DoS attacks [15]. According to Rubio et al. [39], these software attacks are classified into four categories: (1) availability threats, encompassing device subtraction, DDoS attacks, service theft, path attacks, and depletion of node resources; (2) integrity threats involving incorrect configuration, malware injection, false data injection, spoofing, and the manipulation of routing information; (3) confidentiality threats, which cover theft of sensitive information, passive traffic analysis, exposure of node status, and infrastructure information exposure; and (4) authentication threats, including privilege escalation, social engineering, inadequate access control, and node impersonation.

The IIoT, characterized by the integration of cyber and physical systems that facilitate the exchange of various data types and sensitive information, enabling smart applications and services to operate accurately in real time, is particularly vulnerable to these software security challenges in cloud-based SCADA systems. These challenges can lead to configuration or software errors in the operating systems and third-party software of IIoT devices, as well as in the communication channels. They also contribute to vulnerabilities in internal network devices, external individual service providers, and cloud service providers [15].

Ulltveit-Moe et al. [27] characterized the attacks that are based on zero-day vulnerabilities as the most perilous, noting their ability to evade detection by anti-malware software. These attacks pose a significant risk, as millions of IoT devices could be instantly compromised if an unknown software flaw emerges in their systems. In general, the integration of IoT into SCADA systems introduces complexities in ensuring the security of the interconnected devices and may attract some vendors whose products violate security communication protocols [40].

Similarly, Nazir et al. [25] reported that the convenience of accessing cloud-based systems from any location worldwide also makes them vulnerable to attacks from malicious actors. Types of attacks, such as DoS, DDoS, and MITM, have become increasingly sophisticated, eluding traditional detection methods. Furthermore, the defense strategies of traditional SCADA systems are often inadequate in handling these evolved attacks.

5.3. Communication and Protocol-Specific Attacks

Communication protocols are sets of rules for data transmission and exchange via communication links. SCADA system communication protocols facilitate interactions between MTUs and RTUs [2]. Typically, the SCADA system protocols do not incorporate encryption, which poses challenges in designing secure connections and communication systems [25].

The most widely used protocols in SCADA systems include Modbus and DNP3. These byte-oriented protocols are commonly employed in industrial systems to remotely execute commands on control devices. However, when integrated into IP networks extended to the

Internet, these protocols become susceptible to cyberattacks and corruption due to their lack of protective measures [3].

Attackers targeting SCADA system protocols and communications primarily focus on identifying and exploiting vulnerabilities in network processes [36]. The literature identifies various attack types, such as MITM attacks via address resolution protocol poisoning, DNS poisoning, network time protocol spoofing, modification of protocol data, exploitation of protocol rules [37], as well as targeting unnecessary ports and services, communication channel vulnerabilities, and flaws in communication protocols. These flaws include the absence of certification, authority, encryption, and vulnerability to DoS attacks [31].

Finally, there are attacks designed specifically for the network protocols of SCADA systems. These include attacks on network layer protocols targeting elements such as firewalls, modems, fieldbus systems, communication systems, routers, remote access points, and protocols and control networks [29]. Other attacks affect the SCADA system network in general and cause a loss of availability, integrity, and confidentiality, along with issues of repudiation and a lack of authentication in distributed network protocols [18].

5.4. Control Process Attacks

McLaughlin et al. [29] categorized control process attacks on SCADA systems as process layer vulnerabilities. These include injecting incorrect information to impair the performance of the controlled process, altering runtime process variables or control logic, and corrupting the process state. Consequently, control process attacks in SCADA systems generally involve attackers gaining control of these systems [36].

Rodofile et al. [37] highlighted various examples of control process attacks on SCADA systems. These encompass modification attacks on ladder logic, function attacks on ladder logic, replay automation, connection hijacking, and feedback deception attacks. Similarly, Lin et al. [41] identified different control-related attacks on SCADA systems, such as assaults on feedback–control loops and the physical infrastructure of power grids. They also introduced a novel attack wherein intruders alter control fields in network packets exchanged between SCADA systems and power substations.

As a result, control and safety operations in cloud-based SCADA systems face challenges like delays; data loss; and compromised reliability, security, and privacy [4].

5.5. Insider Attacks

According to Bhamare et al. [13], SCADA system managers often bear responsibility for data privacy loss due to their limited security controls. Other cloud users might exploit vulnerabilities in these local security controls, leading to data breaches. Some users of cloud-based SCADA systems fail to acknowledge the need for additional security processes and configurations, demonstrate a lack of responsibility, or distrust the security measures offered by cloud service providers. This leads to significant cybersecurity risk incidents [42].

Ulltveit-Moe et al. [27] reported that one of the primary threats in IIoT is the insider threat, which can be executed by employees or IIoT vendors authorized to access or control network sensors. Insiders might commit intentional or unintentional errors, potentially causing significant damage due to their knowledge of the system. Moreover, cloud provider employees, having full data access, might misuse it for malicious purposes like espionage or subversion. This might also happen because of a simple or unintended error, inadvertently causing a loss of access to SCADA resources [25].

Finally, the lack of efficient user authentication and authorization [7], along with privilege escalation, social engineering, inadequate control access [39], and knowledgeable insiders, who can control systems without connected networks or introduce malware [43], are also major security threats and risks for cloud-based SCADA systems.

6. Cyberattack Tactics

Based on the cyberattack classifications in Section 5, it is evident that the three most prevalent and typical tactics potentially compromising cloud-based SCADA system secu-

rity are DoS, MITM, and APT attacks. DoS attacks aim to render a service unavailable to its legitimate users. This is achieved by inundating the targeted system with excessive traffic until it becomes unresponsive or crashes, thereby denying access to authorized users [44]. These attacks can be performed in multiple ways such as DoS or DDoS. Although DoS attacks do not directly harm significant assets, they can incur financial losses and time expenditures for a company during periods when their services and resources are unavailable.

Attackers carry out MITM attacks by positioning themselves in the communication flow between cloud users and cloud applications. They achieve this through either spoofing or sniffing attacks. In spoofing attacks, the intruder masquerades as other cloud users, gaining access to cloud-based SCADA systems. This allows them to circumvent security controls or steal data. Sniffing attacks involve intruders intercepting and monitoring data packets within a cloud-based SCADA system network. This enables them to capture sensitive information, such as passwords and credentials [15].

APTs occur when an intruder, or a group of intruders, gains unauthorized access to a system's network with the intent of mining highly sensitive data. APTs typically exploit zero-day vulnerabilities, which are security holes in software that are unknown to the vendor. These vulnerabilities are present shortly after the development of a system or software and can be immediately exploited without detection or patching, leading to successful attacks [45].

These three attacks are network-based and represent unauthorized access to cloud-based SCADA systems. They can lead to system failures and the manipulation of data and messages within the systems. A common vulnerability in cloud-based systems that leads to susceptibility to DoS and MITM attacks is the sharing of infrastructure. For APTs, the primary vulnerability is zero-day vulnerabilities.

Table 5 summarizes the various causes and impacts of these three cyberattacks, as outlined in various research articles presented in Section 5.

Table 5. Common cyberattack tactics and their various causes and impacts on cloud-based SCADA systems based on articles between 2016 and 2024.

Attack Type	Authors, Year, Reference	Attack's Cause	Attack's Impact
DoS Attacks	Cerullo et al., 2016, [26]	Not mentioned	Target the availability of SCADA systems
	Sajid et al., 2016, [15]	Not mentioned	Unavailability of the service
	Molle et al., 2019, [46]	Vulnerable Internet connection in SCADA systems	Prevents data acquisition and data analytics from being available to users
	Rubio et al., 2019, [39]	Vulnerabilities in hypervisors	The service becomes unavailable to its registered users
	Stojanović et al., 2019, [4]	Sharing infrastructure	Not mentioned
	Nazir et al., 2020, [15]	Not mentioned	System collapsing
	Yadav et al., 2021, [2]	Communication links between SCADA systems and cloud services	Altering of SCADA system information network and opening back doors
MITM Attacks	Sajid et al., 2016, [15]	Not mentioned	Gain unauthorized access to the system using spoofing attacks and monitor activities using sniffing attacks
	Stojanović et al., 2019, [4]	Sharing infrastructure	Not mentioned
	Yadav et al., 2021, [2]	Communication links between SCADA systems and cloud service	Attackers can spoof or sniff information on the network of the SCADA systems

Table 5. *Cont.*

Attack Type	Authors, Year, Reference	Attack's Cause	Attack's Impact
APTs Attacks	Sajid et al., 2016, [15]	Zero-day attacks	Stealing data of cloud-based SCADA systems
	Ulltveit-Moe et al., 2016, [27]	Zero-day vulnerabilities that are not patched on time	Anti-malware cannot detect zero-day attacks, which can initiate many software errors that will make several SCADA devices instantly vulnerable
	Rubio et al., 2019, [39]	Network zero-day vulnerabilities	Attackers can execute remote operations using previously launched malware

7. Cloud-Based SCADA Systems Security

There are various security solutions proposed in the literature, some of which are designed for cloud computing in general while others are specifically for cloud-based SCADA systems. Stojanović et al. [4] introduced security solutions tailored to the cloud infrastructure utilized in SCADA systems, covering public, private, or hybrid models. For public cloud infrastructures, one solution involves using push technology instead of pull technology to move data into the cloud. This approach reduces open network ports on the controller network, thereby lessening the SCADA system's exposure to the Internet. Another strategy focuses on securing cloud infrastructure locations and the services provided by the cloud service provider, including user access security, information privacy, user control levels, log file management for intrusion detection and response, and data encryption. In contrast, the primary security solution for private cloud infrastructure involves employing a defense-in-depth strategy. This multi-layer security architecture aims to minimize the impact of any single layer's failure and includes measures like smart access control, firewalls, intrusion detection and prevention systems, anti-virus software, and more. Moreover, the main recommended security solution for hybrid cloud infrastructure is using secure virtual private networks to manage the infrastructure.

Sajid et al. [15] proposed a series of optimal methods to secure cloud-based SCADA systems. These include segregating networks, analyzing logs, examining network traffic, employing tools for the regular detection of malicious activities, conducting routine vulnerability testing, implementing continuous monitoring and analysis, executing file integrity monitoring, scrutinizing memory dumps, consistently updating and patching, and using proxy solutions.

In order to guarantee secure operations, Nechibvute and Mafukidze [40] suggested the design of the software architecture to protect various IoT devices from intrusions, the deployment of industrial-grade network devices, and the application of fault-tolerant systems capable of withstanding various cybersecurity threats. The authors recommended the development and standardization of security protocols and architectures tailored to the SCADA and IIoT ecosystem.

In [47], the authors presented a new access control approach to enhance security in cloud-based SCADA systems integrated with IoT technologies. The approach is based on Ciphertext Policy Attribute-Based Encryption (CP-ABE) to provide fine-grained access control over data stored in the cloud by considering both static and dynamic user attributes. The security framework is designed to mitigate unauthorized data access, data leakage, and hiding the access policy to ensure data confidentiality. The approach employs fog servers to verify users' dynamic attributes and offload computational tasks from end-users, which in turn reduces the computational cost, making the system more scalable and efficient.

In [23], the authors introduced the SCADA honeypots, specifically a low-interaction honeypot called Conpot, to detect potential malicious activities within SCADA networks. Besides network segmentation, access controls, and intrusion detection systems, organizations can employ honeypots to address the risks of Operational Technology (OT) (e.g., PLCs,

RTUs, HMIs, etc.) attacks in cloud and IoT-based systems. Employing honeypots, or decoy systems designed to attract attackers away from actual assets, enables the gathering of valuable information on attack patterns. An analysis of honeypot data aids in understanding OT attack dynamics and enhancing security mechanisms. Specifically, SCADA honeypots allow security administrators to identify system vulnerabilities by simulating attacker targets within a controlled environment and monitoring attacker behaviors. This can reveal new attack techniques and methods and allow one to improve SCADA system security by patching vulnerabilities and implementing stronger security measures. However, honeypots should be deployed securely to minimize potential threats of attracting more attention from attackers.

Alam et al. [48] discussed various cloud security solutions, such as cloud-based intrusion detection systems (IDSs) and intrusion prevention systems (IPSs). Key types of IDSs and IPSs for cloud computing include the host-based intrusion detection system (HIDS)/host-based intrusion prevention system (HIPS) and the network-based intrusion detection system (NIDS)/network intrusion prevention system (NIPS). The HIDS/HIPS function by monitoring, analyzing, and preventing anomalies in data collected from host machines. These data typically come from file systems, databases, and analyses of network computing systems. When anomalies are detected, an alarm is set off as a preventive measure. The NIDS/NIPS, in contrast, monitor and detect malicious traffic in the network by examining all network packets for malicious patterns. In the event of an attack, the NIDS/NIPS alert administrators or block the IP source from accessing the network, depending on the attack's severity.

As discussed earlier, DoS, MITM, and APT attacks primarily target the network infrastructure of cloud-based SCADA systems. Thus, the NIDS/NIPS is arguably more effective in protecting these systems against various cyberattacks compared to HIDS/HIPS techniques.

Figure 4 summarizes the main security solutions linked to the different cyberattacks on cloud-based SCADA systems, as presented in Sections 5 and 6.

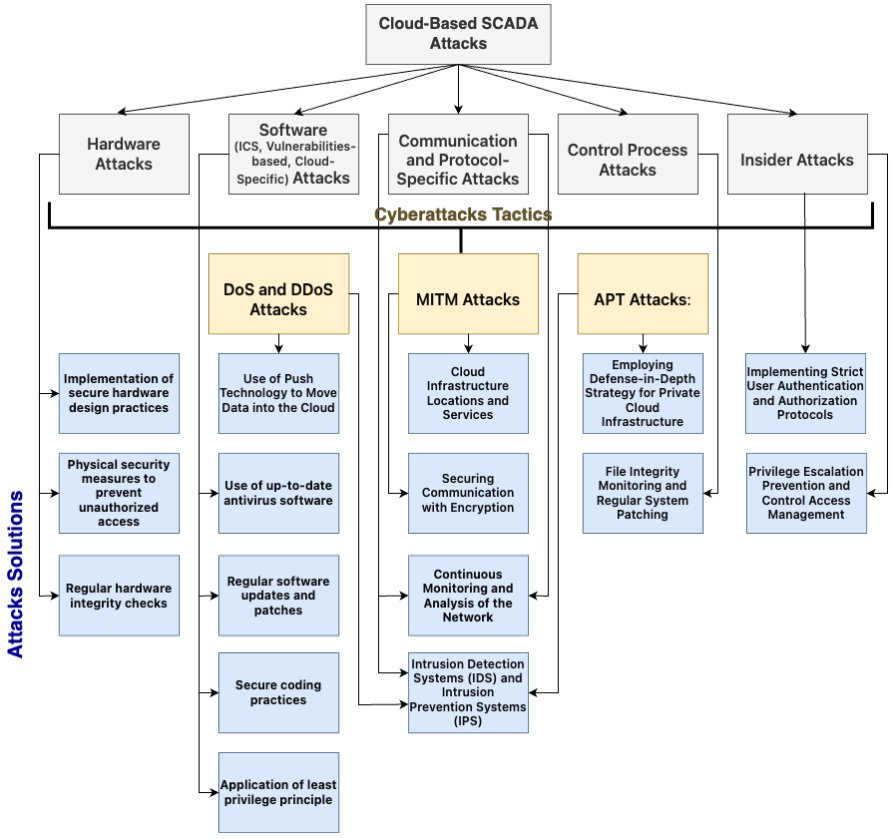

Figure 4. Summary of security solutions linked with the primary attacks they are mitigating.

8. Discussion and Conclusions

This study examined vulnerabilities and cyberattacks impacting the security of cloud-based SCADA systems. Four primary areas of vulnerability were identified: connectivity between SCADA systems and cloud services, shared infrastructure, the presence of malicious insiders, and the security robustness of SCADA protocols. Additionally, this study categorized cyberattacks into five groups: hardware, software, communication and protocol-specific, control process, and insider attacks. It found that DoS, MITM, and APTs pose the most significant threats to these systems due to their reliance on shared infrastructures, real-time industrial operations, and high availability. This research also reviewed several security solutions to mitigate these threats. Given that the most prevalent attacks are network-based (such as DoS, MITM, and APTs), this study suggests that network-based IDSs/IPSs (the NIDS/NIPS) are effective security measures for detecting and preventing cyberattacks, thereby safeguarding cloud-based SCADA systems.

While our study covered different vulnerabilities, attacks, and security mechanisms, various threats and attacks remain uncovered by current solutions, such as sophisticated malware (e.g., ransomware and spyware) that can adapt and mutate to avoid detection, and the insufficient security (e.g., default passwords or unencrypted communications) in IoT devices, making them soft targets for attackers. Additionally, reliance on cloud vendors for security exposes SCADA systems to risk if the vendors fail to implement stringent security measures or if they themselves are compromised. Furthermore, as cloud-based SCADA systems often rely on components and services from multiple providers, they are susceptible to supply chain attacks (e.g., compromised software updates). Complex supply chain attacks occurring upstream can impact SCADA systems downstream, and such risks may not always be considered in current security models. Additionally, weaponized PLCs pose a significant threat in cloud systems, where malware can be inserted into PLCs to alter their functioning or to use them as entry points for infiltrating SCADA systems.

One of the most significant emerging threats to cloud-based systems is the concept of adversarial artificial intelligence (AI) [49], where machine learning models are manipulated either to deceive security systems or to execute attacks on SCADA systems. For instance, an APT group might use a machine learning model to analyze patterns in the SCADA system's network traffic or identify regular maintenance periods and data transfer intervals. This model can be trained to mimic normal network traffic patterns, generate traffic that blends with regular maintenance data, and avoid detection while mapping out the network. Machine learning models can also learn the operational patterns of the SCADA system, including load balancing, substation switch cycles, and transformer settings, thereby gaining control over several PLCs and subtly altering transformer loads to create imbalances. The attackers schedule these changes to occur simultaneously during peak usage hours to maximize impact. The sudden, unexpected load change can cause a cascade failure across the grid, leading to power loss. In such cases, engineers may struggle to identify the cause of the outages, resulting in extended recovery times. The AI-driven approach not only enables the initial infiltration but also allows the attackers to learn and adapt to the system's behavior, making the attack highly effective and challenging to mitigate or detect by security tools.

To address the previously uncovered threats and attacks, various important steps should be considered by organizations adopting cloud-based SCADA system infrastructures. For example:

- Implementing real-time security monitoring systems that can adapt to new and evolving threats, which can, in turn, reduce the window of opportunity for attackers.
- Having a robust incident response plan that can be quickly and effectively enacted in the event of a security breach.
- Performing regular, comprehensive security audits, including vulnerability scanning and penetration testing, to uncover potential security gaps.
- Developing robust security frameworks for IoT devices integrated into SCADA systems to ensure these devices do not become entry points for attackers.

- Enhancing the security of the supply chain by working closely with vendors and partners to ensure they adhere to high-security standards.
- Improving awareness and training among the workforce to prevent security breaches due to human error or insider threats, and
- Engaging in collaborations for threat intelligence sharing, which can aid in the quicker identification and response to new threats.

Furthermore, employing AI and machine learning algorithms can predict attacks on SCADA systems and enhance the detection of sophisticated and previously unknown attack patterns. These algorithms can also detect anomalous behavior that might indicate a PLC has been compromised. To safeguard against AI-driven attacks and weaponized PLCs, system administrators and security teams should consider techniques such as a combination of hardware and software integrity checks, AI-driven behavior analysis, and establishing a secure development lifecycle for PLC software. Adapting regulations and standards to mandate secure coding practices and AI audit trails is crucial to prevent malicious AI activities. Regular patching of known and potential vulnerabilities is also essential, especially in a cloud environment where threats can escalate quickly.

Finally, the security of cloud-based SCADA systems is a crucial issue that needs more dedicated research. Addressing the security challenges of these systems is vital to prevent future incidents and catastrophic events. Future research should explore several unexplored types of threats. This includes quantum-based attacks, where traditional encryption methods may become obsolete. Researchers must dedicate efforts to quantum-resistant cryptographic techniques to secure cloud-based SCADA systems against future threats. In addition to quantum threats, supply chain security needs researchers' attention, including developing frameworks to assess the security posture of third-party vendors and mechanisms to detect compromised software or hardware components. Despite technological advancements, human factors and insider threats remain critical vulnerabilities. Research into sophisticated access control, behavioral analytics, and insider threat detection mechanisms could offer significant security enhancements. Future research should also emphasize advanced security risk assessments and the importance of conducting proper testbeds to validate security solutions for these systems. Additionally, implementing advanced AI-driven security measures and considering security as an integral component of system design are critical for cloud-based SCADA systems. By focusing on these areas, future research can address the evolving landscape of threats facing cloud-based SCADA systems and contribute to developing more resilient security solutions.

Author Contributions: Conceptualization, A.W. and F.A.; methodology, F.A.; validation, A.W.; formal analysis, A.W. and F.A.; investigation, A.W.; resources, A.W. and F.A.; writing—original draft preparation, F.A.; writing—review and editing, A.W.; visualization, A.W.; supervision, A.W.; project administration, A.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data were contained in the main text.

Acknowledgments: The authors would like to thank Asma Cherif for her suggestions on the research, valuable comments, and insightful feedback. The following AI-assisted tool was used in this paper: chatGPT 4. It was only used for checking that there is no grammatical or structural errors in the manuscript.

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

References

1. Morsey, C. *Supervisory Control and Data Acquisition (SCADA) Systems and Cyber-Security: Best Practices to Secure Critical Infrastructure*; Robert Morris University: Pittsburgh, PA, USA, 2017.
2. Yadav, G.; Paul, K. Architecture and security of SCADA systems: A review. *Int. J. Crit. Infrastruct. Prot.* **2021**, *34*, 100433. [CrossRef]
3. Cai, N.; Wang, J.; Yu, X. SCADA system security: Complexity, history and new developments. In Proceedings of the 2008 6th IEEE International Conference on Industrial Informatics, Daejeon, Republic of Korea, 13–16 July 2008; pp. 569–574.

4. Stojanović, M.D.; Boštjančič-Rakas, S.V.; Marković-Petrović, J.D. SCADA systems in the cloud and fog environments: Migration scenarios and security issues. *Facta Univ.-Ser. Electron. Energetics* **2019**, *32*, 345–358. [CrossRef]
5. Buyya, R.; Yeo, C.S.; Venugopal, S. Market-oriented cloud computing: Vision, hype, and reality for delivering it services as computing utilities. In Proceedings of the 2008 10th IEEE International Conference on High Performance Computing and Communications, Dalian, China, 25–27 September 2008; pp. 5–13.
6. Mushtaq, M.F.; Akram, U.; Khan, I.; Khan, S.N.; Shahzad, A.; Ullah, A. Cloud computing environment and security challenges: A review. *Int. J. Adv. Comput. Sci. Appl.* **2017**, *8*, 183–195.
7. Tariq, N.; Asim, M.; Khan, F.A. Securing SCADA-based critical infrastructures: Challenges and open issues. *Procedia Comput. Sci.* **2019**, *155*, 612–617. [CrossRef]
8. Church, P.; Mueller, H.; Ryan, C.; Gogouvitis, S.V.; Goscinski, A.; Haitof, H.; Tari, Z. SCADA systems in the Cloud. In *Handbook of Big Data Technologies*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 691–718.
9. El Mrabet, Z.; Kaabouch, N.; El Ghazi, H.; El Ghazi, H. Cyber-security in smart grid: Survey and challenges. *Comput. Electr. Eng.* **2018**, *67*, 469–482. [CrossRef]
10. Church, P.; Mueller, H.; Ryan, C.; Gogouvitis, S.V.; Goscinski, A.; Haitof, H.; Tari, Z. Moving SCADA systems to IaaS clouds. In Proceedings of the 2015 IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity), Chengdu, China, 19–21 December 2015; pp. 908–914.
11. Wilhoit, K. *SCADA in the Cloud*; Trend Micro: Cupertino, CA, USA, 2013; p. 5.
12. Yi, M.; Mueller, H.; Yu, L.; Chuan, J. Benchmarking cloud-based SCADA system. In Proceedings of the 2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), Hong Kong, China, 11–14 December 2017; pp. 122–129.
13. Bhamare, D.; Zolanvari, M.; Erbad, A.; Jain, R.; Khan, K.; Meskin, N. Cybersecurity for industrial control systems: A survey. *Comput. Secur.* **2020**, *89*, 101677. [CrossRef]
14. Alakbarov, R.; Hashimov, M. Development of Security Mechanisms in Cloud Based SCADA Systems. In Proceedings of the 2023 5th International Conference on Problems of Cybernetics and Informatics (PCI), Baku, Azerbaijan, 28–30 August 2023; pp. 1–4.
15. Sajid, A.; Abbas, H.; Saleem, K. Cloud-assisted IoT-based SCADA systems security: A review of the state of the art and future challenges. *IEEE Access* **2016**, *4*, 1375–1384. [CrossRef]
16. Maglaras, L.; Ferrag, M.; Derhab, A.; Mukherjee, M.; Janicke, H.; Rallis, S. Threats, countermeasures and attribution of cyber attacks on critical infrastructures. *EAI Endorsed Trans. Secur. Saf.* **2018**, *5*, e1. [CrossRef]
17. Pliatsios, D.; Sarigiannidis, P.; Lagkas, T.; Sarigiannidis, A.G. A survey on SCADA systems: Secure protocols, incidents, threats and tactics. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1942–1976. [CrossRef]
18. Ghosh, S.; Sampalli, S. A survey of security in SCADA networks: Current issues and future challenges. *IEEE Access* **2019**, *7*, 135812–135831. [CrossRef]
19. Combs, L. Cloud computing for SCADA. *Control Eng.* **2011**, *58*, 22–26.
20. Byers, C. Fog Computing for Industrial Automation. 2018. Available online: https://www.controleng.com/articles/fog-computing-for-industrial-automation/ (accessed on 1 March 2024).
21. Nugent, E. How Cloud and Fog Computing will Advance SCADA Systems. *Manuf. Autom.* **2017**, *32*, 22–24.
22. Howard, P. A Security Checklist for SCADA Systems in the Cloud. 2015. Available online: https://www.route-fifty.com/infrastructure/2015/06/a-security-checklist-for-scada-systems-in-the-cloud/287164/ (accessed on 15 April 2022).
23. Mesbah, M.; Elsayed, M.S.; Jurcut, A.D.; Azer, M. Analysis of ICS and SCADA Systems Attacks Using Honeypots. *Future Internet* **2023**, *15*, 241. [CrossRef]
24. Rakas, S.V.B.; Stojanović, M.D.; Marković-Petrović, J.D. A review of research work on network-based scada intrusion detection systems. *IEEE Access* **2020**, *8*, 93083–93108. [CrossRef]
25. Nazir, S.; Patel, S.; Patel, D. Cloud-based autonomic computing framework for securing SCADA systems. In *Innovations, Algorithms, and Applications in Cognitive Informatics and Natural Intelligence*; IGI Global: Hershey, PA, USA, 2020; pp. 276–297.
26. Cerullo, G.; Mazzeo, G.; Papale, G.; Sgaglione, L.; Cristaldi, R. A Secure Cloud-Based SCADA Application: The Use Case of a Water Supply Network. In Proceedings of the International Conference on New Trends in Intelligent Software Methodology Tools and Techniques (SoMeT 16), Larnaca, Cyprus, 12–14 September 2016; pp. 291–301.
27. Ulltveit-Moe, N.; Nergaard, H.; Erdödi, L.; Gjøsæter, T.; Kolstad, E.; Berg, P. Secure information sharing in an industrial Internet of Things. *arXiv* **2016**, arXiv:1601.04301.
28. Rashid, A.; Gardiner, J.; Green, B.; Craggs, B. Everything is awesome! Or is it? Cyber security risks in critical infrastructure. In Proceedings of the International Conference on Critical Information Infrastructures Security, Linköping, Sweden, 23–25 September 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 3–17.
29. McLaughlin, S.; Konstantinou, C.; Wang, X.; Davi, L.; Sadeghi, A.R.; Maniatakos, M.; Karri, R. The cybersecurity landscape in industrial control systems. *Proc. IEEE* **2016**, *104*, 1039–1057. [CrossRef]
30. Common Vulnerabilities and Exposures, "CVE-2011-2367". SUSE. Available online: https://www.suse.com/ko-kr/security/cve/CVE-2011-2367.html (accessed on 30 February 2022).
31. Irmak, E.; Erkek, İ. An overview of cyber-attack vectors on SCADA systems. In Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, Turkey, 22–25 March 2018; pp. 1–5.
32. Chromik, J.J.; Remke, A.; Haverkort, B.R. Improving SCADA security of a local process with a power grid model. In Proceedings of the 4th International Symposium for ICS & SCADA Cyber Security Research, Belfast, UK, 23–25 August 2016; pp. 114–123.

33. Daneels, A.; Salter, W. What is SCADA? In Proceedings of the International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy, 4–8 October 1999.
34. Resul, D.; Gündüz, M.Z. Analysis of cyber-attacks in IoT-based critical infrastructures. *Int. J. Inf. Secur. Sci.* **2020**, *8*, 122–133.
35. Green, B.; Krotofil, M.; Abbasi, A. On the significance of process comprehension for conducting targeted ICS attacks. In Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy, Dallas, TX, USA, 3 November 2017; pp. 57–67.
36. Demertzis, K.; Iliadis, L. A computational intelligence system identifying cyber-attacks on smart energy grids. In *Modern Discrete Mathematics and Analysis*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 97–116.
37. Rodofile, N.R.; Radke, K.; Foo, E. Extending the cyber-attack landscape for SCADA-based critical infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2019**, *25*, 14–35. [CrossRef]
38. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A review of cyber security risk assessment methods for SCADA systems. *Comput. Secur.* **2016**, *56*, 1–27. [CrossRef]
39. Rubio, J.E.; Alcaraz, C.; Roman, R.; Lopez, J. Current cyber-defense trends in industrial control systems. *Comput. Secur.* **2019**, *87*, 101561. [CrossRef]
40. Nechibvute, A.; Mafukidze, H. Integration of scada and industrial iot: Opportunities and challenges. *IETE Tech. Rev.* **2023**, 1–14. [CrossRef]
41. Lin, H.; Slagell, A.; Kalbarczyk, Z.T.; Sauer, P.W.; Iyer, R.K. Runtime semantic security analysis to detect and mitigate control-related attacks in power grids. *IEEE Trans. Smart Grid* **2016**, *9*, 163–178. [CrossRef]
42. Zhang, S.; Luo, X.; Litvinov, E. Serverless computing for cloud-based power grid emergency generation dispatch. *Int. J. Electr. Power Energy Syst.* **2021**, *124*, 106366. [CrossRef]
43. Zeng, P.; Zhou, P. Intrusion detection in scada system: A survey. In *Intelligent Computing and Internet of Things*; Springer: Berlin/Heidelberg, Germany, 2018; pp. 342–351.
44. Davis, C.; Tate, J.; Okhravi, H.; Grier, C.; Overbye, T.; Nicol, D. SCADA cyber security testbed development. In Proceedings of the 2006 38th North American Power Symposium, Carbondale, IL, USA, 17–19 September 2006; pp. 483–488.
45. Bere, M.; Muyingi, H. Initial investigation of industrial control system (ICS) security using artificial immune system (AIS). In Proceedings of the 2015 International Conference on Emerging Trends in Networks and Computer Communications (ETNCC), Windhoek, Namibia, 17–20 May 2015; pp. 79–84.
46. Molle, M.; Raithel, U.; Kraemer, D.; Graß, N.; Söllner, M.; Aßmuth, A. Security of cloud services with low-performance devices in critical infrastructures. In Proceedings of the Cloud Computing 2019, The Tenth International Conference on Cloud Computing, GRIDs, and Virtualization, Venice, Italy, 5–9 May 2019; p. 98.
47. Routray, K.; Bera, P. Context-Aware Attribute Based Access Control for Cloud-based SCADA Systems. In Proceedings of the 1st Workshop on Enhanced Network Techniques and Technologies for the Industrial IoT to Cloud Continuum, New York, NY, USA, 10 September 2023; pp. 35–40.
48. Alam, S.; Shuaib, M.; Samad, A. A collaborative study of intrusion detection and prevention techniques in cloud computing. In Proceedings of the International Conference on Innovative Computing and Communications, New Delhi, India, 5–6 May 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 231–240.
49. Anthi, E.; Williams, L.; Rhode, M.; Burnap, P.; Wedgbury, A. Adversarial attacks on machine learning cybersecurity defences in industrial control systems. *J. Inf. Secur. Appl.* **2021**, *58*, 102717. [CrossRef]