Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 00.0000/ACCESS.2022.DOI

Analysis of Security Challenges in Cloud-Based SCADA Systems: A Survey

FATIMAH F. ALSHEHRY, ARWA M. WALI

Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, Jeddah, Saudi Arabia (e-mail: fdhaferalshehry@stu.kau.edu.sa; amwali@kau.edu.sa)

Corresponding author: Arwa M. Wali (e-mail: amwali@kau.edu.sa).

ABSTRACT Supervisory control and data acquisition (SCADA) systems allow industrial organizations to control and monitor real-time data and industrial processes. Moving SCADA systems to the cloud environments can improve the performance of traditional SCADA systems by enhancing features such as storage capacity, reliability and availability, security measures, as well as reducing technical and industrial costs. However, cloud cyberattacks are rapidly increasing, posing a major challenge to such type of systems. In addition, these cyberattacks still remains scattered across many research, and much of published research on cloud-based SCADA systems has been focused on narrow sets of attacks. Thus, this research provides a survey and an analysis of the most common cybersecurity attacks and challenges that cloud-based SCADA systems might experience. It also conducts a security risk assessment of the analyzed attacks. Finally, it proposes the existing suitable detection and prevention techniques to mitigate the impact of cyberattacks on such critical control systems.

INDEX TERMS cloud security, cloud-based SCADA systems, cyberattacks, risk assessment

I. INTRODUCTION

SUPERVISORY control and data acquisition (SCADA) systems are considered a type of industrial control systems that allows users to monitor and control industrial processes locally or remotely through sensors and actuators [1]. SCADA systems allow industrial organizations to operate critical infrastructure by controlling and monitoring real-time data and processes of various sectors, such as electric generation, oil, gas, and manufacturing plant systems. SCADA systems have evolved from stand-alone platforms and infrastructures with proprietary communication mechanisms and protocols into Internet-based SCADA, with full integration to corporate information technology (IT) networks and adoption of different Internet protocols, such as Transmission Control Protocol/Internet Protocol (TCP/IP) [2].

As complex industrial operations demand advanced efficient environments, the idea of moving SCADA systems into the cloud has been proposed. The cloud is a collection of interconnected computers consisting of distributed systems that present computing resources based on a service-level agreements (SLA) established between customers and service providers [3]. Cloud-based SCADA systems can improve the performance of traditional SCADA systems by enhancing features such as quality of service (QoS) for computing environments, reliability, flexibility, availability, efficiency, and proper configuration, maintenance, and reduction of technical and industrial costs.

Mirjana, S. et al. [1] provided an overview of the main scenarios regarding the migration of SCADA systems to the cloud, with a special attention paid to the cyber security factors such as authentication, access control, intrusion detection, and privacy. However, real-time data transmission over the Internet, and remote access features of the new SCADA systems have made these systems more susceptible to various cyberattacks and have initiated many security holes for potential attackers, who can exploit the systems vulnerabilities to inject worms, spyware, and viruses.

In addition, many cybersecurity challenges of cloud-based SCADA have not been addressed in the literature. For example, the data communication and industrial protocols, Modbus and DNP3, are byte-oriented, and are usually used with traditional SCADA systems for remote execution of commands on control devices. When used in IP networks extended to the Internet, these protocols lack protection and can be vulnerable to corruption and cyberattacks [2]. Moreover, traditional IT mechanisms cannot meet the proper requirements of dealing with the huge amount of data from cloud-based SCADA systems of industrial organizations.

Therefore, control and safety operations are subject to delay, data loss, and lack of reliability, security, and privacy [1].

A. RESEARCH AIM AND CONTRIBUTIONS

The aim of this research is to provide an in-depth analysis of risk challenges, threats and vulnerabilities, that might affect cloud-based SCADA systems to gain a better insight into the negative impact of these challenges on the security of such systems.

The main contributions of this research are:

- Analyze various cybersecurity threats and challenges of cloud-based SCADA systems.
- Provide a security risk assessment for cyberattacks of cloud-based SCADA systems.
- Propose a security solution in terms of detection and prevention techniques that can minimize the negative impact of cybersecurity threats on these systems.

B. RESEARCH QUESTIONS

This research addresses the following questions (RQs),

- *RQ1:* What are the challenges and threats that negatively impact the security of cloud-based SCADA systems?
- *RQ2:* What are the proper prevention techniques to minimize the effects of these threats on such critical systems?

This paper consists of eight sections, including this introduction, and is organized as follows: Section II provides a background of SCADA systems, including both traditional SCADA and cloud-based SCADA systems; Section III explains the survey methodology used for the research; Section IV reviews the related work on the main SCADA security challenges in both traditional and cloud-based systems; Section V presents a thematic analysis of the cloud-based SCADA systems security challenges; Section VI provides security risk assessment for the main cyberattacks affecting the security of these systems; Section VII proposes security solutions in the literature for the cloud-based SCADA systems, as well as providing the proper detection and prevention techniques that can be applied to such systems. The paper concludes with the discussion, limitations, and recommendations for future work in Section VIII.

II. BACKGROUND

In this section, we will provide the background of the SCADA systems that includes the architecture of both traditional and cloud-based SCADA systems, as well as the evolution of such systems.

A. TRADITIONAL SCADA SYSTEMS ARCHITECTURE

SCADA systems architecture can be divided into three main parts; 1) hardware architecture, 2) software architecture, and 3) SCADA systems communication protocols. as the following,

1) Hardware Architecture

The hardware architecture of SCADA systems consists of five layers as presented in Fig. 1: Fieldbus network layer (layer 0), controller network layer (layer 1), supervisory network layer (layer 2), operational traffic over demilitarized zone Layer (layer 3), and corporate network layer (layer 4). Layer 0 represents the direct interaction between the physical devices and industrial hardware components via the fieldbus. The signals generated from the field devices are processed by controllers in layer 1, in which they produce the appropriate commands for these devices. The controllers in layer 1, which includes Remote Terminal Units (RTUs), programmable logic controllers (PLCs), and intelligent electronic devices (IEDs), are responsible of performing local control of actuators and sensor monitoring. The resulting processes are analyzed at the control center in layer 2. This control center is responsible for; collecting and analyzing generated information from field sites, presenting the generated information on the human machine interface (HMI) consoles, and performing actions based on the events that are detected. Moreover, the control center is responsible for generating general alarms and reports. The connection between the control center and field sites is performed using a communication subsystem that allows remote access to field sites for the purpose of diagnostic and failure repair. Furthermore, the communication subsystem connects the control center with SCADA partner plants [1]. Layer 2 also contains a supervisory network that connects the SCADA master terminal unit (MTU) server, historian server, engineering workstations, HMI server and consoles, as well as communication devices such as routers, switches, and modems. The application servers, historian server, and domain controller are located in layer 3 which represents a demilitarized zone (DMZ). Finally, layer 4 represents a corporate IT network, which is connected to the Internet [1].

2) Software Architecture

The software architecture (Fig. 2) is divided into three main sections: 1) SCADA client application, 2) SCADA server application, and 3) SCADA development environment. The client application consists of a HMI, trending, alarm display, log display, active controls, and third-party applications. The server application section, on the other hand, consists of a) servers that are responsible for the acquisition and handling of data, as well as used for multitasking and real-time databases, and b) software programs that are responsible for trending, diagnostic data, and managing information such as scheduled maintenance procedures, logistic information, and detailed schematics for a particular sensor or machine. Finally, the development environment section consists of a graphic editor, library, project editor, driver toolkit, and export and import procedures [4].

3) SCADA system communication protocols

Communication protocols are defined as a set of regulations for data transmission and exchange through communication

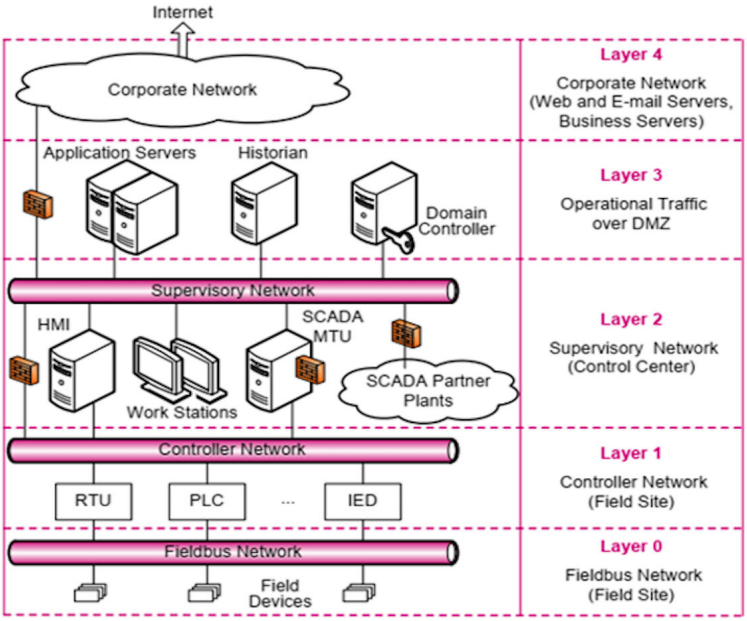

FIGURE 1. SCADA system hardware architecture [1]

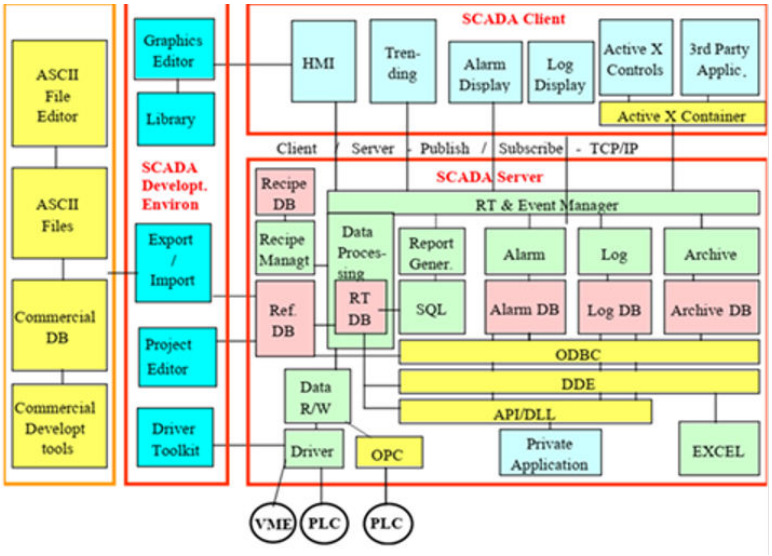

FIGURE 2. SCADA system software architecture [4]

links. SCADA system communication protocols are responsible for the interaction between MTUs and RTUs. There are six communication protocols in SCADA systems [5]:

1) Modbus: This is a transmission protocol and is mainly responsible for the interaction between MTU and RTUs. However, Modbus lacks encryption and authentication controls.
2) Distributed Network Protocol (DNP3): This is responsible for obtaining an openly standard-based interoperability between the MTU and RTUs. Unlike Modbus, DNP3 supports both encryption and authentication protocols.
3) Electro-Technical Commission 60870-5 (IEC 60870-5) is used for tele-control in electrical engineering and power systems. When applying the IEC 60870-5 protocol to a SCADA system, it is responsible for managing and controlling power utility devices. However, the IEC 60870-5 protocol supports authentication controls but does not support authentication controls.
4) Foundation Fieldbus: This is used to provide real-time control between device-to-device and device-to-host systems. Similar to the Modbus protocol, the Foundation Fieldbus protocol does not support encryption or authentication controls.

5) Process Field Bus (Profibus): This is responsible for process control and discrete manufacturing. Similar to the DNP3 protocol, Profibus protocol supports encryption and authentication controls.
6) Electro-Technical Commission 61850 (IEC 61850) is used in electrical substations for communications between intelligent electronic devices. Similar to the IEC 60870-5 protocol, the IEC 61850 protocol supports authentication controls but does not support authentication controls.

B. CLOUD-BASED SCADA SYSTEMS ARCHITECTURE

The migration of SCADA systems into the cloud can be achieved using a public cloud infrastructure, or a private/hybrid cloud infrastructure as the following [1]:

1) Public Cloud Infrastructure

This infrastructure means that the execution of SCADA applications is performed on the premises of the company or organization. The conversion units, e.g. RTUs, PLC, and IEDs are directly connected to the control center and transfer data to the cloud, where they can be stored and distributed. Moreover, as presented in Fig. 3, the public cloud infrastructure provides isolation for the control functions of SCADA applications in the controller network, while allowing cloud-connected SCADA applications to perform remote access, process visualization, and send and receive reports.

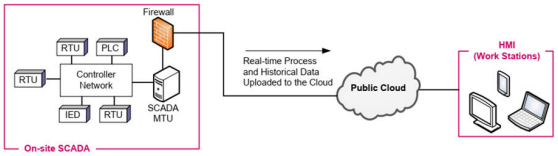

FIGURE 3. Public cloud infrastructure [1]

2) Private/Hybrid Cloud Infrastructure

, This infrastructure means that the execution of SCADA applications is performed entirely in the cloud, while the application is connected remotely to the control center. Furthermore, as shown in Fig. 4, conversion units are connected via Wide Area Networks (WANs) links to SCADA applications and control commands executions are performed in the cloud. Thus, private or hybrid cloud infrastructure implementations are suitable for distributed SCADA applications.

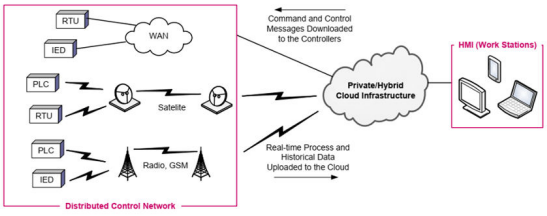

FIGURE 4. Private or hybrid cloud infrastructure [1]

C. THE EVOLUTION OF SCADA SYSTEM

SCADA systems are divided into four types In terms of evolution [5]:

1) First generation-Monolithic SCADA systems: This type of system uses minicomputers for computing operations, and was designed to work in an isolated environment. Main components of SCADA systems, e.g. MTU and RTU, communicate through WANs, as shown in Fig. 5, using proprietary communication protocols. However, the limitations of these protocols are that they only allow scanning, control, and data exchange functionalities between the MTU and RTU. An example of a monolithic SCADA systems is the PDP-11 series that was developed by Digital Equipment Corporation.

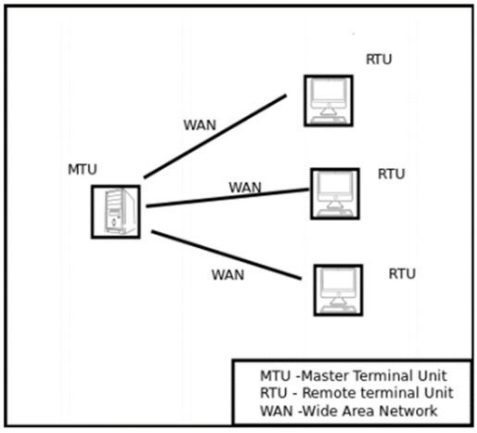

FIGURE 5. Monolithic SCADA systems [5]

2) Second generation-Distributed SCADA systems: this type of system consists of a number of systems, such as: communication processors, operator interfaces, and database servers. Distributed SCADA systems use small range networks such as Local Area Networks (LANs) to inter-connect and distribute computational operations as shown in Fig. 6. Similar to monolithic SCADA systems, distributed SCADA systems perform their operations using proprietary hardware devices, software, and network protocols.

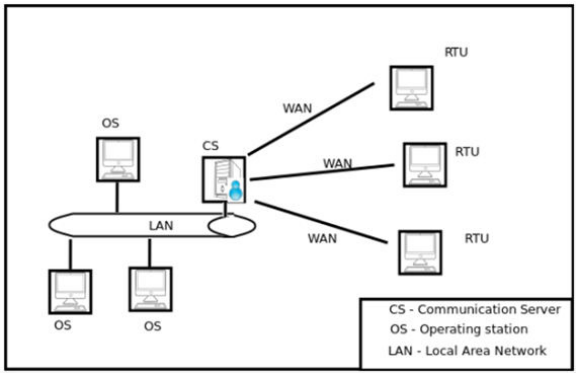

FIGURE 6. Distributed SCADA system [5]

3) Third generation-Networked SCADA systems: this type of system, also known as modern SCADA systems, is closely related to distributed SCADA systems, except that the networked SCADA systems use open communication protocols and standards rather than proprietary ones. The use of open communication protocols results in a successful distribution of MTU functions across WANs, as shown in Fig. 7. Moreover, this improvement in communication protocols enhances the connection between the MTU and RTU, and prevents crucial incidents in the systems.

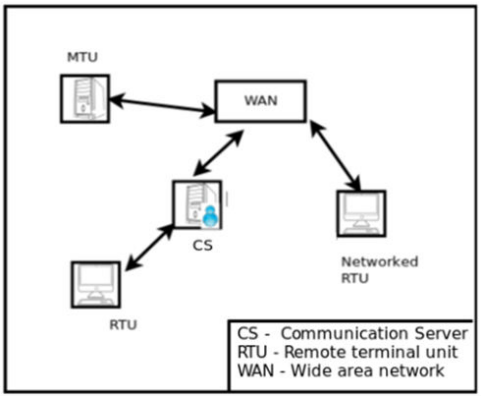

FIGURE 7. Networked SCADA systems [5]

4) Fourth generation -Internet of Things (IoT) SCADA systems: In this type of system, all data are collected and controlled using open communication standards and is stored in the cloud services. An example of an IoT SCADA systems is Industry 4.0, which includes distributed cognitive computing, cyber-physical systems (CPS), IoT, and cloud computing as shown in Fig. 8. IoT SCADA systems take the advantages of both the traditional SCADA systems and general IoT systems. These two systems share a few characteristics such as e.g., data access, manipulation, and visualization. However, general IoT systems differ in terms of interoperability, scalability, and the capability for big data analysis.

III. RESEARCH METHODOLOGY

In this section, we present the main methodologies used in this survey research. These methodologies include the primary research methodology, analysis of vulnerabilities and cyberattacks against cloud-based SCADA systems, risk assessment, and defining the detection and prevention techniques methodologies.

In general, this research is conducted by collecting information regarding the security challenges and threats that compromise the security of cloud-based SCADA systems, and providing proper prevention techniques to minimize the effect of these issues. To achieve this, relevant articles were collected using different search keywords such as: "cloud-based SCADA system", "security of cloud-based SCADA systems", "cyberattacks against cloud-based SCADA systems", âĂIJIntrusion Detection System (IDS) and Intrusion Prevention System (IPS) in SCADA systemâĂİ, âĂIJsecurity of SCADA systemsâĂİ, âĂIJsecurity of cloud computingâĂİ, and âĂIJsecurity of cloud-based SCADA systemâĂİ Moreover, these keywords are used in search for scientific papers from different scientific databases such as: "Google scholar", "researchgate", and "Institute of Electrical and Electronics Engineers (IEEE)". Afterwards, a thematic analysis is performed on the collected information to obtain insight into common patterns and themes of vulnerabilities and cyberattacks on the cloud-based SCADA systems. Next, a security risk assessment was conducted on a cloud-based SCADA system to identify the assets of the system, prioritize risks, and suggest security controls. Finally, a selection of appropriate detection and prevention techniques is proposed to control and reduce the effects of the analyzed cyberattacks. The different methodologies used are explained in the following subsections.

A. ANALYSIS METHODOLOGY

The analysis of security challenges in cloud-based SCADA systems was performed as a thematic analysis where various articles, from 2016 to 2021, regarding the security of cloud-based SCADA systems, were reviewed to observe cyberattack patterns on cloud-based SCADA systems. Cyberattack patterns were observed using an inductive generalization approach, which is a sort of defensible inference that we employ to move from the specific to the general. This approach was applied to the chosen articles in order to identify every cyberattack that would affect the security of cloud-based SCADA systems and to build patterns based on the findings. After cyberattacks patterns were identified, themes were generated by grouping similar patterns together and labeled based on the occurrence of cyberattacks.

B. SECURITY RISK ASSESSMENT METHODOLOGY

This security risk assessment will be performed based on the previous analysis of cyber attacks against cloud-based SCADA systems. A separate security risk assessment was conducted for each attack. The risk assessment of each attack

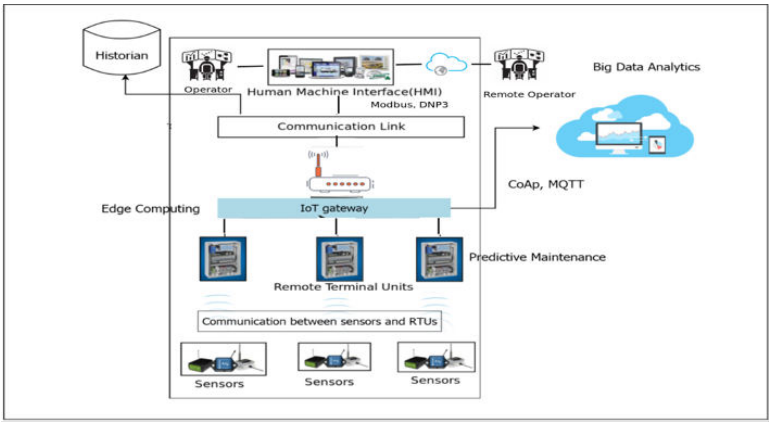

FIGURE 8. Internet of Things (IoT) SCADA systems [5]

involved the following: identification of affected assets, type of the attack, whether it is unauthorized access, human error, or natural disaster, etc. It also includes the type of vulnerability that caused the attack and the likelihoods and the impact of the attack. Finally, the selection of the likelihoods and impact was justified for each security risk assessment.

C. DEFINING DETECTION AND PREVENTION METHODOLOGY

The proposed detection and prevention methods are performed by first, reviewing multiple articles regarding the security solutions of cloud computing, in general, and cloud-based SCADA systems, in particular, then, selecting and discussing the most suitable solutions that are recommended to be applied to cloud-based SCADA systems for cyberattacks detection and prevention.

IV. RELATED WORK

In this section, the related literature regarding the challenges faced by SCADA systems is addressed from two perspectives: traditional and cloud-based systems.

A. TRADITIONAL SCADA SYSTEMS CHALLENGES

The main challenge of traditional SCADA systems is the confrontation with various attacks introduced in the literature. In this section, we start with a general attacks classification of traditional SCADA systems, then we focus our discussion on five main attacks, discussed in many scientific studie, which includes software attacks, hardware attacks, firmware attacks, communication and protocol-specific attacks, and control process attacks.

1) General Attacks Classifications

Maglaras et al. [6] defined attacks against SCADA systems as the attacks on back-end IoT devices and classified them into four main categories: 1) key-based attacks, 2) data-based attacks, 3) impersonation-based attacks, and 4) physical-based attacks. This classification of attacks was performed using two main criteria: 1) based on the state of the attack, whether it is passive or active, and 2) based on the place of the attack, whether it happened internally or externally.

Different classifications for the traditional SCADA systems have been presented in the literature. While StojanoviÄĞ et al. [1] have classified attacks against traditional SCADA systems into three types: (1) hardware attacks, (2) software attacks, and (3) communication stack attacks, Pliatsios. et al. [7] proposed binary classification attacks: 1) untargeted attacks that exploit any vulnerable system in SCADA, and 2) targeted attacks that compromise specific systems in SCADA. The authors of [7] also presented an extended classification of attacks against traditional SCADA systems, which includes, (1) traditional IT-based attacks, (2) protocol-specific attacks, and (3) process control attacks. On the other hand, Ghosh et al. [8] have classified attacks on SCADA systems into three categories; 1) attacks on hardware; 2) attacks on software, and 3) attacks on network connections.

Bhamare et al. [9] provided general examples of threats and attacks that might affect industrial control systems (ICS) that are monitored and controlled by SCADA systems, such as 1) advanced persistent threats (APTs) or zero day attacks, 2) unintentional spillover of compromises of corporate networks, 3) corruption of voice and data network services, 4) cyber and physical attacks that were coordinated, 5) attacks from hacktivists, and 6) compromises or disruption of supply chain. Furthermore, Rashid. et al. [10] analyzed the most effective attacks against ICS and resulted in four types of perception errors, which play a major role in the success of these attacks: system qualities, system boundaries, observability, and controllability.

Finally, SCADA systems are affected by various vulnerabilities. These vulnerabilities are classified in [11] into five categories: policies and procedures, architecture and design, configuration and maintenance, physical and software development, and communication and networking. Four other categories were presented in [12]; security policy, communication protocols, architectural and hardware, and software vulnerabilities. The authors in [11] also discussed five factors that might affect the vulnerabilities of traditional SCADA

systems, which are: human errors, lack of resources for physical devices, proprietary protocols, unsecure legacy systems, and accidents caused by negligence and equipment failure.

2) Software Attacks

Software attacks against SCADA systems are the primary attacks that can be identified as cyber-kinetic, which are complex, life-threatening, and physically damaging attacks [13]. Cyber-kinetics can be performed using various types of techniques such as; malware injection, command/response injections, phishing, spear phishing, Denial of Service (DoS) attacks, SQL injection attacks, man-in-the-middle (MITM) attacks, and APTs [1]. However, traditional SCADA systems defense approaches are unable to manage these latest attack methodologies, especially MITM and DoS, as they can easily avoid different detection techniques [14].

Bhamare et al. [9] identified other types of software threats that mainly affect the ICS, which are monitored and controlled by traditional SCADA systems. These include, APTs, and distributed DoS (DDoS) attacks. McLaughlin et al. [15] have defined software attacks as software layer vulnerabilities that may range from coding errors to failure in the implementation of access control mechanisms. While Rodofile et al. [16] identified software attacks on SCADA systems as configuration-based attacks such as fake master, manipulation injection, application attacker, malicious "Bring You Own" device, and configuration file attacks, Demertzis and Iliadis [17] defined software attacks as an exploitation of weaknesses and vulnerabilities by attackers to successfully gain access to systems; they and also proposed possible attacks against the power system of SCADA, which include remote tripping command injection, relay setting change, and data injection.

Tariq et al. [18] addressed different types of software attacks on the critical infrastructure of traditional SCADA systems. These attacks include trojan horses, stuxnet worm infections, the slammer worms, flame malware, dragonfly malware, DDoS, and MITM attacks. In addition, the authors addressed attacks on the social level of traditional SCADA systems, such as social engineering, inside intruders, and phishing attacks. Furthemore, Irmak and Erkek [19] identified software cyberattacks as vulnerabilities in source code design and implementation, buffer overflow, SQL injections, cross-site-scripting (XSS), and poor management of patch applications.

Chromik et al. [20] presented power grid cyberattacks of SCADA systems that include; 1) damage; loss of IT assets using attacks that alter the data of the systems, 2) nefarious activities; abuse of IT assets using attacks that purposely interfere with the information system, e.g., DoS, and 3) eavesdropping, interception, and hijacking attacks that allow undesired communication between an intruder and the system device; e.g., MITM.

Software attacks have been handled from other perspectives; for example, Cherdantseva et al. [21] identified software attacks as cyber security challenges and vulnerabilities that might affect SCADA systems in terms of patching and human factors. Patching may introduce new unknown vulnerabilities or ultimately break the systems, especially those that require running operations for 24 hours for 7 days a week. On the other hand, human factors may introduce human errors, resulting in unintended attacks, as well as social engineering that results in internal and external intended attacks.

Finally, Rubio et al. [22] classified the software threats that might affect SCADA systems into four types: 1) availability threats, including subtraction of devices, DDoS attacks, path attacks, and exhaustion of node resources; 2) integrity threats, including incorrect configuration, malware injection, false data injection, spoofing, and manipulation of routing information; 3) confidentiality threats, including sensitive information theft and passive traffic analysis; and 4) authentication threats, including privilege escalation, social engineering, deficient control access, and impersonation of nodes.

3) Hardware Attacks

Hardware of SCADA systems is connected to components from around the world as well as to many third-party libraries, which allows complex interactions to occur within the systems. SCADA systems vendors, in general, are not unaware of SCADA hardware exploitable threats such as backdoors attacks. Moreover, wireless devices that provide data to traditional SCADA systems lack adequate protection techniques because of their very low power requirements. This provides an easy entry point for the intruders into the systems [14].

McLaughlin et. al [15] defined hardware attacks on SCADA systems as hardware layer vulnerabilities, which include the injection of trojans and causing loss of reliability and security. With these vulnerabilities, unauthorized users can modify firmware, and reverse engineer logic using Joint Test Action Group (JTAG) ports, as well as malicious USB drives can change DNS settings, causing redirection in communications or damaging the circuit board.

In addition, cyberattacks on the hardware of SCADA systems might occur by injecting malware into the firmware of the programmable logic controller (PLC) and compromising the security of the controller [19], outages when system devices lose electricity and disconnect either by a switch or a damage on purpose, or by deliberate physical attacks using a controlling network [20].

4) Software and Hardware and Firmware Attacks

McLaughlin et al. [15] proposed attacks, such as sophisticated malware, which are mainly built to target both the software and hardware of ICS in traditional SCADA systems. Web Graphics Library (WebGL) is an example of such attacks, which allows access to Graphics Processing Unit (GPU) hardware using least-privileged remote parties, causing an exposure of GPU memory contents from previous workloads. Another type of traditional SCADA systems attacks, called firmware attacks, was also addressed in [15].

These attacks are performed by intruders to exploit the vulnerabilities of the firmware, such as wireless access points and recloser controller firmware, and abnormally affect the ICS process. These malicious firmware can be distributed from the central system in an Advanced Metering Infrastructure (AMI) to smart meters and launch DoS to corrupt ICS operations.

5) Communication and Protocol-Specific Attacks

In general, SCADA systems protocols have no encryption, which makes it difficult to design secure connections and communication systems [14]. To attack protocols and communications on SCADA systems, attackers mainly try to analyze and discover vulnerabilities in network processes [17]. There are various types of such attacks defined in the literature, for example, MITM attacks using the Address Resolution Protocol (ARP) poisoning, domain name service (DNS) poisoning, Network Time Protocol (NTP) spoofing, protocol data modification, protocol rule exploitation [16], unnecessary ports and services, communication channel vulnerabilities, and vulnerabilities of communication protocols, including lack of certification, lack of authority, lack of encryption, and DoS [19].

Finally, there are attacks designed specifically for network protocols of SCADA systems, such as network layer vulnerabilities that are targeting, firewalls, modems, fieldbus, communication systems and routers, remote access points, and protocols and control networks [15]. Other attacks affect the SCADA system network in general, such as, loss of availability, loss of integrity, loss of confidentiality, repudiation, and lack of authentication in the distributed network protocol [8].

6) Control Process Attacks

Control process attacks on SCADA systems were described by McLaughlin et al. [15] as process layer vulnerabilities, which includes injecting incorrect information to affect the performance of the controlled process, modifying runtime process variables or the control logic, and corrupting the process state. Therefore, control process attacks can be defined on SCADA systems, in general, as attackers take control of the systems [17].

Rodofile et al. [16] discussed different examples of control process attacks on SCADA systems, such as a modification attack on ladder logic, function attack on ladder logic, replay automation, connection hijacking, and feedback deception attacks. On the other hand, Lin et al. [23] presented other control-related attacks on SCADA systems, such as feedback-control loops attacks, compromises on the physical infrastructure of power grids, as well as proposed new attack, in which intruders modified control fields in network packets that are exchanged between SCADA systems and power substations.

B. CLOUD-BASED SCADA SYSTEMS CHALLENGES

In contrast to traditional SCADA systems, we address general challenges and issues for the cloud infrastructure and services, then focus on cloud-based SCADA systems attacks in terms of software and insider attacks, as the two main categories discussed by many researchers.

1) General Attacks Classifications

The four main factors that make cloud-based SCADA systems more vulnerable to various attacks than traditional SCADA systems are as follows [1]: 1) sharing an infrastructure with unknown outside users causes various threats for such systems, 2) attackers can compromise the entire industrial control system using the vulnerable network connection between the SCADA system and the cloud, and 3) authentication and encryption are not supported in some SCADA protocols, such as: Modbus and DNP3, and 4) using security solutions that are not proprietary designed for SCADA systems.

Connecting SCADA systems to the cloud increases cyberattacks. For example, local devices in cloud-based SCADA systems may lose connection to remote components resulting in delays in the production processes, data loss, and propagating errors on other SCADA system components. The components of cloud-based SCADA systems do not follow the same security framework as the traditional ones. Therefore, the operational performance is inconsistent [9]. The migration of SCADA-based critical infrastructure to a cloud computing environment will result in major obstacles as proposed by Tariq et al. [18], which include strict security requirements, low latency, and integration with high availability services.

Network security and shared network connections are the major security issues when migrating traditional SCADA systems to cloud computing. These issues occur as a result of a change in computational environments in which the traditional SCADA system shifts from private hardware to a shared public cloud infrastructure [24]. Alakbarov and Hashimov [25] claimed that cloud-based SCADA systems are exposed to the same cybersecurity risks as other cloud-based systems. These issues include limited visibility in network operations, malware, compliance, data loss, and inadequate due diligence.

Nazir et al. [14] also presented general security challenges for cloud-based SCADA systems, including: 1) closed networks open to the public, 2) risks of shared infrastructure, 3) communication links exposed to cyberattacks, 4) unprotected virtual machines, 5) the unavailability of cloud infrastructure, and 6) insider attacks by an employee of the cloud provider. On the other hand, Ulltveit-Moe et al. [26] described the main challenges that might affect information sharing in the Industrial Internet of Things (IIoT) scenario which includes: 1) the security issues of industrial automation and analysis devices; 2) many industrial sensors that run real-time processes have limited software security mechanisms; and 3) some industrial device manufacturers fail to add proper

backdoors capabilities to manage and update these devices.

Other security challenges of also discussed in [27] such as, 1) systems vulnerability for attacks targeting their Internet connection, due to the aggregation and analysis of a huge amount of data in order to enhance the operation of on-primes low-performance operational technology (OT) devices, 2) DDoS attacks, which affect the production processes, and 3) attacks on production process actors. Finally, according to Cerullo et al. [28], the most relevant threats to cloud-based SCADA systems are data breach, account or service traffic hijacking, DoS, shared technology vulnerabilities, and malicious insiders.

2) Software Attacks

APTs, lack of data integrity, MITM attacks, replay attacks, and DoS attacks are, in general, the main software attacks against cloud-based SCADA systems [29]. Other software threats include, 1) availability threats, e.g. DDoS attacks and service theft, 2) integrity threats, e.g. incorrect configuration and malware injection, and 3) confidentiality threats, e.g. sensitive information theft, node status exposure, and infrastructure information exposure [22].

IIoT is specifically the most affected components by the software security challenges of cloud-based SCADA systems. These challenges negatively cause configuration or software errors in the operating system, software, or the third-party software of IIoT devices. They also cause errors in the communication channel and vulnerabilities in the internal network devices, the external individual service providers, and in the cloud service providers.

3) Insider Attacks

According to Bhamare et al. [9], SCADA system managers often are responsible for the loss of data privacy due to their limited security controls over data, and other cloud users may exploit the vulnerabilities in the local security control and cause data breach. Some users of cloud-based SCADA systems fail to recognize additional security processes and configurations. Other users lack of responsibility for cloud-based SCADA systems or do not trust the security offerings by cloud service providers, which leads to major cyber security risks incidents [30].

Shen et al. [31] presented a major security flaw in cloud-based SCADA systems, which is the lack of a trusted identity authentication mechanism. With the increasing number of devices connected to cloud-based SCADA systems, access points that lack effective authentication mechanisms are increasing as well, resulting in a variety of security issues, such as the occupation of enterprises networks and resources, virus injections, exposure of the enterprise secrets, illegal access, and intrusions to the enterprise system.

One of the main threats of IIoT, defined by Ulltveit-Moe et al. [26], is an insider threat that can be performed by employees or IIoT vendors who have authorization to access or control sensors in the networks. Finally, the absence of efficient user authentication and authorization [18], privilege escalation, social engineering, and deficient control access [22] are also considered major security threats and risks for cloud-based SCADA systems [12].

V. ANALYSIS OF SECURITY CHALLENGES IN CLOUD-BASED SCADA SYSTEMS

This section presents a thematic analysis of both vulnerabilities and cyberattacks against cloud-based SCADA systems.

A. VULNERABILITIES ANALYSIS

IoT technologies, such as cloud computing, are the most suitable solutions for improving SCADA systems. The scope of the IoT concept can be identified as any devices connected to the Internet. In general, any device that has an IP address can connect to the Internet and be subjected to nearly all cyberattacks that might occur in an IP-based environment. Hence, due to the lack of security measures in classical SCADA systems, the migration of such systems into the cloud opens the door to potential security risks.

The thematic analysis of cyberattacks against cloud-based SCADA systems revealed four common factors that make cloud-based SCADA systems more vulnerable to cyberattacks: 1) connectivity of SCADA systems and cloud service, 2) shared infrastructure, 3) malicious insiders, and 4) the security of SCADA protocols.

The classical SCADA system was developed as a closed system with no Internet connection as a protection mechanism. When the SCADA system is moved to the cloud, it becomes exposed to complex network environments, which introduce our first vulnerability, the connectivity between the SCADA systems and cloud services; security threats will increase once the SCADA system is required to connect to public cloud services.

The risks of sharing infrastructure arise from the possibility of sharing the hardware infrastructure with other businesses. Therefore, the same physical server may be shared with other competitors, either other companies or other users. Sharing resources will result in many consequences that will affect cloud-based SCADA systems in their critical and real-time applications.

Malicious insiders are considered the most devastating threat to any system, especially critical systems that are responsible for industrial operations, such as SCADA systems. Malicious insiders can be any former employees, system administrators, or cloud services providers. Various security threats can be caused by malicious insiders, including unauthorized access, data breaches, and unauthorized control of SCADA system industrial sensors.

Another factor that makes cloud-based SCADA systems vulnerable is the lack of authentication and encryption mechanisms. As a result of weak authentication and encryption, communication protocols such as Modbus will allow intruders easy access to private credentials such as IP addresses, and usernames and passwords while utilizing the cloud. Moreover, the lack of security in the International Electrotechnical Commission (IEC) 61850 standard communica-

tion protocols, which used for intelligent electronic devices at electrical substations, makes the vulnerabilities of SCADA systems exploited more often.

Table 1 provides the above four factors with their different vulnerability impacts on the cloud-based SCADA systems, as indicated by various studies in the literature (Section IV-B) between 2016 and 2021.

B. CYBER-ATTACKS ANALYSIS

Based on a review of cyberattacks against cloud-based SCADA systems mentioned in the literature, we found that the three common cyberattacks that might affect the security of cloud-based SCADA systems are, 1) DoS attacks, 2) MITM attacks, and 3) APTs or zero day attacks. The impact of these attacks is as follows,

1) *DoS Attacks:* The purpose of this type of attack is to make a service inaccessible to the intended users. DoS attacks can be launched using two methods, 1) flooding the targeted system with traffic, and 2) sending data that triggers a crash in the targeted system. DoS attacks do not damage significant assets. Otherwise, vendors must deal with the money and handling time.
2) *MITM Attacks:* can be performed when an attacker positions himself in communication between the cloud user and cloud application using two methods: spoofing attack or sniffing attack. In a spoofing attack, the intruder impersonates other cloud users to gain access to cloud-based SCADA systems and bypass security control systems or steal data. On the other hand, a sniffing attack is performed when an intruder intercepts and monitors data packets on a cloud-based SCADA system network to capture sensitive information such as passwords and credentials.
3) *APTs or Zero Day Attacks:* APTs can be established when an intruder or group of intruders gains unauthorized access to the system's network to mine highly sensitive data. APTs are typically performed when the intruder exploits zero-day vulnerabilities in the system. Zero-day vulnerabilities arise shortly after the development of a system or software and can be exploited immediately without being detected or patched, which eventually will leads to a successful attack.

Table 2 provides an analysis of the three cyberattacks above with their various causes, impacts, and severity according to various research articles (Section IV) between 2016 and 2021.

VI. SECURITY RISK ASSESSMENT OF CYBER ATTACKS ON CLOUD-BASED SCADA SYSTEMS

Security risk assessment is defined as the process of identifying and prioritizing the valuable assets of an organization and estimating the risks of cyberattacks that may affect the identified assets. The goal of performing security risk assessment for cloud-based SCADA systems is to keep cloud service providers and SCADA managers informed about the identified risks and to help them when making decisions about the proper responses.

Based on the method used for security risk assessment of cyberattacks on cloud-based SCADA systems, the likelihood estimation and the attacks impact were performed using the following risk levels:

1) High: security measures must be taken urgently.
2) Medium: security measures must be taken at a reasonable time.
3) Low: managers are allowed to decide whether to accept the risk or mitigate.

Fig. 9 presents the affected asset, the likelihood estimation, the vulnerability that caused the attack, and the impact of the three cyberattacks, DoS, MITM, and APTs/Zero Day indicated in the previous section.

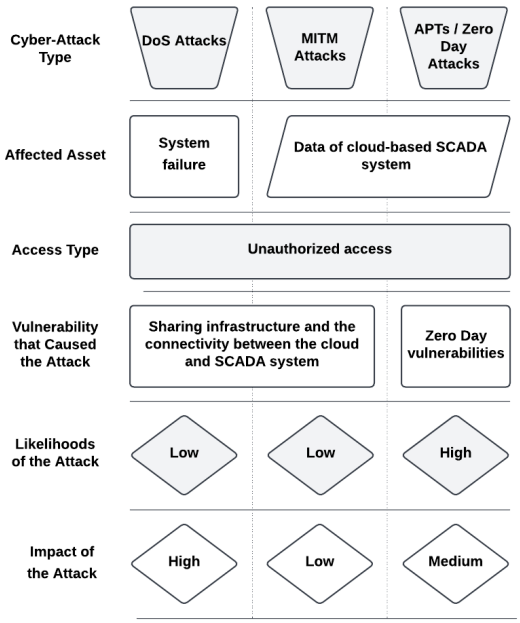

FIGURE 9. The risk assessment of three cyberattacks, DoS, MITM, and APTs/Zero Day

Based on Fig. 9 above, the likelihood of both DoS and MITM attacks is low because there is no clear history in the articles regarding whether the attack had affected cloud-based SCADA systems or not. However, the impact of the DoS attacks is high because three out of seven authors agreed on the severity of these attacks. However, the impact of the MITM attacks is low because none of the authors referred to the severity of the attack. While the likelihood of APTs/zero-day attacks is high based on two of three articles that mentioned an incident of APTs attacks e.g., Stuxnet, the impact of these attacks is medium based on one of three articles that mentioned the severity of the attacks.

VII. CLOUD-BASED SCADA SYSTEMS SECURITY

In this section, we review the proposed security solutions in the literature for the cloud-based SCADA systems and then

TABLE 1. Common factors and their impact on cloud-based SCADA systems based on articles between the years of 2016 and 2021

Factors	Vulnerability Impact	Article Reference	Authors, Year
Connectivity between SCADA system and cloud service	Increasing risks that will affect cloud-based SCADA systems security	[1]	Stojanović et al., 2019
	The dependence on cloud communication will make the SCADA system more open to outsiders	[29]	Sajid et al., 2016
	Security threats will increase due to the required connectivity to the public cloud	[32]	Yi et al., 2017
	Communication over public cloud will expose SCADA system to cyberattacks	[14]	Nazir et al., 2020
	The reliance on cloud communication can expose SCADA to Denial-of-Service Attacks and Man-in-The-Middle Attacks	[5]	Yadav et al., 2021
	The loss of connection will lead to delay of processes and loss of data	[9]	Bhamare et al., 2020
Malicious Insiders	Threats associated with external individuals and cloud service providers	[29]	Sajid et al., 2016
	The loss of access to SCADA system resources can be caused either by employees of cloud providers with malicious intent or done by innocent mistake	[14]	Nazir et al., 2020
	Employees and vendors of the cloud may have authorized access and/or control sensors on the network which will lead to various security risks	[26]	Ulltveit-Moe et al., 2016
	Malicious administrators of the Cloud Provider (CP) or any other user with privileged access to resources will be a consistent threat to the system	[28]	Cerullo et al., 2016
	Abusing the system flaws by other remote cloud users	[9]	Bhamare et al.,2020
Shared Infrastructure	Sharing the infrastructure with outside parties will expose the system to command/response injections such as DoS attacks and MITM attacks	[1]	Stojanović et al., 2019
	Vendors of the cloud do not provide any guarantees that SCADA resources would not be shared with other businesses. which will result in potential threats to the system	[14]	Nazir et al., 2020
	Security risks will arise with the multi-tenancy feature of cloud technologies	[28]	Cerullo et al., 2016
SCADA system protocols	SCADA-specific application layer protocols such as Modbus and DNP3 do not support encryption and authentication controls which will have a negative impact on cloud-based SCADA systems security	[1]	Stojanović et al., 2019
	SCADA systems use Modbus/TCP, IEC 40, DNP3 for automation and control. However, these protocols lack protection and will expose control and automation operations to cyberattacks	[29]	Sajid et al., 2016
	The security risks in the traditional SCADA system will be carried forward due to absence of protection controls in Modbus/TCP, IEC 40, and DNP3	[5]	Yadav et al., 2021

provide a proper detection and prevention techniques that can be applied to such systems.

A. SECURITY SOLUTIONS

StojanoviÄĞ et al. [1] provided security solutions when migrating SCADA systems to public, private, and hybrid cloud infrastructures. Security solutions in public cloud infrastructure are as follows: First, the security of input/output information depends on how the SCADA systems will be isolated in the controller network; thus, when using public cloud infrastructure, push technology should be used to move data to the cloud rather than pull it from the cloud. By this way, the open network ports on the controller network are minimized and the SCADA system is not exposed to the Internet. Second, the security of shared storage and computational resources will be achieved if the cloud service provider (CSP) is aware of the ability of computational resources to manage various applications on the cloud, including resource allocation, network access, service levels, and fault-tolerance strategies. Third, the security of shared physical infrastructure includes the security of cloud infrastructure locations, which provides secure communication links to connect the cloud infrastructure to the communications infrastructure. This enhances the ability to examine and analyze the locations that will serve SCADA applications.

When choosing the CSP and examining the capabilities of the offered cloud services, the main criteria to be followed are: 1) the security of user access, and collective isolation of information that was generated from different applications; 2) when the CSP experience changes, the level of user control must be determined; 3) data encryption must be applied; 4) software patches must be distributed automatically; 5) reports must be provided to satisfy the business needs; 6) continuous near real-time monitoring of the security mechanismâĂŹs efficiency must be conducte; 7) log file management capabilities must be developed to detect intrusions and generate

TABLE 2. Analysis of cyberattacks on cloud-based SCADA systems based on articles between 2016 and 2021

Attack type	Article Reference	Authors, Year	Attack's cause	Attack's Impact	Attack's Severity
DoS Attacks	[1]	Stojanović et al., 2019	Sharing infrastructure	N/A	Severe
	[29]	Sajid et al., 2016	N/A	Unavailability of the service	N/A
	[14]	Nazir et al., 2020	N/A	System collapsing	N/A
	[27]	Molle et al., 2019	Vulnerable Internet connection in SCADA systems	Prevents data acquisition and data analytics from being available to users	N/A
	[28]	Cerullo et al., 2016	N/A	Target the availability of SCADA systems	Severe
	[5]	Yadav et al., 2021	Communication links between SCADA systems and cloud services	Altering of SCADA system information network and opening backdoors	N/A
	[22]	Rubio et al., 2019	Vulnerabilities in hypervisors	The service become unavailable to its intended users	Severe
MITM Attacks	[1]	Stojanović et al., 2019	Sharing infrastructure	N/A	N/A
	[29]	Sajid et al., 2016	N/A	Gain unauthorized access to the system using spoofing attacks and monitor activities using sniffing attacks	N/A
	[5]	Yadav et al., 2021	Communication links between SCADA systems and cloud service	Attackers can spoof or sniff information on the network of SCADA systems	N/A
APTs / Zero day Attacks	[29]	Sajid et al., 2016	Zero-day Attacks	Stealing data of cloud-based SCADA systems	N/A
	[26]	Ulltveit-Moe et al., 2016	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	Severe
	[22]	Rubio et al., 2019	Network zero-day vulnerabilities	Attackers can execute remote operations using previously launched malware	N/A

responses; 8) constant analysis of incidents, suspicious activities, and anomalies must be conducted; 9) immediate actions must be taken in case of vulnerability identification; and 10) reliable customer services must be provided. While the main security solution in a private cloud infrastructure is to apply a defense-in-depth strategy, which is an architecture of security multilayer mechanisms that minimize the impact of failure in one layer rather than the others, the main security solution in a hybrid cloud infrastructure is a suggestion to use secure virtual private networks (VPN) to control the infrastructure [1].

Finally, Sajid et al. [29] suggested a set of best practices to secure cloud-based SCADA systems, such as network segregation, log analysis, network traffic analysis, using tools to detect regular malicious activities, applying regular vulnerability testing, continuous monitoring and analysis, performing file integrity monitoring, analyzing of memory dumps, updating and patching continuously, and applying proxy solutions.

B. DETECTION AND PREVENTION TECHNIQUES IN CLOUD COMPUTING

According to Alam et al. [33], the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) are essential components for defending cloud computing systems from critical threats and cyberattacks. Generally, an IDS can be defined as a technique to detect malicious activities, where as an IPS can be defined as a technique to prevent and block malicious activities, and both are considered as defensive measures. Both IDS and IPS can be used in cloud-based SCADA systems; however, the mechanisms of these techniques in traditional network environments are different from those in environments. In a traditional network, network professionals conduct an IDS to process raw network traffic directly in the network layer. However, the cloud environment is limited and entirely administered by cloud service providers, making it difficult for network professionals to conduct an IDS. Therefore, an IDS on the cloud depends entirely on the cloud service provider and not on the users.

Alam et al. [33] presented several cloud security solutions, including cloud-based IDSs and IPSs. Common IDSs and IPSs for cloud computing are the Host-based Intrusion

Detection System (HIDS)/Host-based Intrusion Prevention System (HIPS), and Network-based Intrusion Detection System (NIDS)/ Network Prevention System (NIDS), which described as follows:

1) Host-based Intrusion Detection System (HIDS) / Host-based Intrusion Prevention System (HIPS) This type of IDS/IPS monitors, analyzes, and prevents anomalies in collected data from host machines. The collected data are usually gathered from the file systems, databases, and network analysis of a computing system. When anomalies are detected, an alarm is triggered as a prevention technique.
2) Network-based Intrusion Detection System (NIDS)/ Network-based Intrusion Prevention system (NIPS) This type of IDS/IPS monitors and detects malicious traffic in the network; it searches all network packets for malicious patterns. If an attack occurs, the NIDS/NIPS notifies administrators or bans the source of IP from accessing the network based on the severity of the attack.

As presented in the previous section, DoS, MITM, and APTs/zero day attacks mainly target the network infrastructure of the cloud-based SCADA systems. Therefore, NIDS/NIPS can be considered more suitable for defending such systems against various cyberattacks than HIDS/HIPS techniques.

VIII. DISCUSSION AND CONCLUSION

This research proposed a survey and an analysis of both vulnerabilities and cyberattacks affecting the security of cloud-based SCADA systems, as well as conducting separate security risk assessments for each cyberattack. Consequently, moving the traditional SCADA system into the cloud environment, a complex network structure, was the main reason for the vulnerability of SCADA systems. The analysis of cyberattacks against cloud-based SCADA systems showed that Denial of Service (DoS) attacks are the most damaging attacks because SCADA systems depend on real-time industrial operations and high availability. On the other hand, the security risk assessments of cyberattacks showed that APTs / zero day attacks are most likely to occur due to the instant occurrence of zero-day vulnerabilities. Thus, the results of this research answered the *RQ1: What are the challenges and threats that will have a negative impact on the security of cloud-based SCADA systems?* by indicating that sharing infrastructures and DoS attacks are threats that have a negative impact on such systems.

To answer the *RQ2: What is the proper prevention techniques to minimize the effect of these threats on such critical systems?*, this research has also suggested proper Intrusion Detection Systems (IDSs) and Intrusion Prevention Systems (IPSs) techniques to protect the security of cloud-based SCADA systems, which are network-based IDS/IPS (NIDS/NIPS) that are considered suitable security solutions for detecting and preventing cyberattacks as well as minimizing the threats to such critical systems, as most common attacks are network-based attacks, e.g., DoS, MITM, and APTs/Zero Day attacks.

However, the lack of previous articles specifically dedicated to the security of cloud-based SCADA systems and the limited access to these articles have a noticeable effect on the results of this research. Finally, it is essential to proceed with the work on the security of cloud-based SCADA systems to prevent incidents and catastrophic events from happening in the future. Future research should focus on the importance of conducting more advanced security risk assessments for cloud-based SCADA systems as well as the importance of conducting proper testbeds to confirm security solutions for cloud-based SCADA systems.

.

ACKNOWLEDGMENT

The authors would like to thank Dr. Asma Cherif from for her suggestions on the research, valuable comments, and insightful feedback.

REFERENCES

[1] M. D. Stojanović, S. V. Boštjančič-Rakas, and J. D. Marković-Petrović, "Scada systems in the cloud and fog environments: Migration scenarios and security issues," *Facta universitatis-series: Electronics and Energetics*, vol. 32, no. 3, pp. 345–358, 2019.

[2] N. Cai, J. Wang, and X. Yu, "Scada system security: Complexity, history and new developments," in *2008 6th IEEE International Conference on Industrial Informatics*. IEEE, 2008, pp. 569–574.

[3] M. F. Mushtaq, U. Akram, I. Khan, S. N. Khan, A. Shahzad, and A. Ullah, "Cloud computing environment and security challenges: A review," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 10, 2017.

[4] A. Daneels and W. Salter, "What is scada?" 1999.

[5] G. Yadav and K. Paul, "Architecture and security of scada systems: A review," *International Journal of Critical Infrastructure Protection*, vol. 34, p. 100433, 2021.

[6] L. Maglaras, M. Ferrag, A. Derhab, M. Mukherjee, H. Janicke, and S. Rallis, "Threats, countermeasures and attribution of cyber attacks on critical infrastructures," *EAI Endorsed Transactions on Security and Safety*, vol. 5, no. 16, p. e1, 2018.

[7] D. Pliatsios, P. Sarigiannidis, T. Lagkas, and A. G. Sarigiannidis, "A survey on scada systems: secure protocols, incidents, threats and tactics," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1942–1976, 2020.

[8] S. Ghosh and S. Sampalli, "A survey of security in scada networks: Current issues and future challenges," *IEEE Access*, vol. 7, pp. 135 812–135 831, 2019.

[9] D. Bhamare, M. Zolanvari, A. Erbad, R. Jain, K. Khan, and N. Meskin, "Cybersecurity for industrial control systems: A survey," *computers & security*, vol. 89, p. 101677, 2020.

[10] A. Rashid, J. Gardiner, B. Green, and B. Craggs, "Everything is awesome! or is it? cyber security risks in critical infrastructure," in *International Conference on Critical Information Infrastructures Security*. Springer, 2019, pp. 3–17.

[11] S. V. B. Rakas, M. D. Stojanović, and J. D. Marković-Petrović, "A review of research work on network-based scada intrusion detection systems," *IEEE Access*, vol. 8, pp. 93 083–93 108, 2020.

[12] P. Zeng and P. Zhou, "Intrusion detection in scada system: a survey," in *Intelligent Computing and Internet of Things*. Springer, 2018, pp. 342–351.

[13] D. Resul and M. Z. Gündüz, "Analysis of cyber-attacks in iot-based critical infrastructures," *International Journal of Information Security Science*, vol. 8, no. 4, pp. 122–133, 2020.

[14] S. Nazir, S. Patel, and D. Patel, "Cloud-based autonomic computing framework for securing scada systems," in *Innovations, algorithms, and applications in cognitive informatics and natural intelligence*. IGI Global, 2020, pp. 276–297.

[15] S. McLaughlin, C. Konstantinou, X. Wang, L. Davi, A.-R. Sadeghi, M. Maniatakos, and R. Karri, "The cybersecurity landscape in industrial control systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1039–1057, 2016.
[16] N. R. Rodofile, K. Radke, and E. Foo, "Extending the cyber-attack landscape for scada-based critical infrastructure," *International Journal of Critical Infrastructure Protection*, vol. 25, pp. 14–35, 2019.
[17] K. Demertzis and L. Iliadis, "A computational intelligence system identifying cyber-attacks on smart energy grids," in *Modern Discrete Mathematics and Analysis*. Springer, 2018, pp. 97–116.
[18] N. Tariq, M. Asim, and F. A. Khan, "Securing scada-based critical infrastructures: Challenges and open issues," *Procedia computer science*, vol. 155, pp. 612–617, 2019.
[19] E. Irmak and İ. Erkek, "An overview of cyber-attack vectors on scada systems," in *2018 6th international symposium on digital forensic and security (ISDFS)*. IEEE, 2018, pp. 1–5.
[20] J. J. Chromik, A. Remke, and B. R. Haverkort, "Improving scada security of a local process with a power grid model," in *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, 2016, pp. 114–123.
[21] Y. Cherdantseva, P. Burnap, A. Blyth, P. Eden, K. Jones, H. Soulsby, and K. Stoddart, "A review of cyber security risk assessment methods for scada systems," *Computers & security*, vol. 56, pp. 1–27, 2016.
[22] J. E. Rubio, C. Alcaraz, R. Roman, and J. Lopez, "Current cyber-defense trends in industrial control systems," *Computers & Security*, vol. 87, p. 101561, 2019.
[23] H. Lin, A. Slagell, Z. T. Kalbarczyk, P. W. Sauer, and R. K. Iyer, "Runtime semantic security analysis to detect and mitigate control-related attacks in power grids," *IEEE Transactions on Smart Grid*, vol. 9, no. 1, pp. 163–178, 2016.
[24] P. Church, H. Mueller, C. Ryan, S. V. Gogouvitis, A. Goscinski, H. Haitof, and Z. Tari, "Scada systems in the cloud," in *Handbook of Big Data Technologies*. Springer, 2017, pp. 691–718.
[25] R. Alakbarov and M. Hashimov, "Migration issues of scada systems to the cloud computing environment (review)," *SOCAR Proceedings*, pp. 155–164, 09 2020.
[26] N. Ulltveit-Moe, H. Nergaard, L. Erdödi, T. Gjøsæter, E. Kolstad, and P. Berg, "Secure information sharing in an industrial internet of things," *arXiv preprint arXiv:1601.04301*, 2016.
[27] M. Molle, U. Raithel, D. Kraemer, N. Graß, M. Söllner, and A. Aßmuth, "Security of cloud services with low-performance devices in critical infrastructures," *CLOUD COMPUTING 2019*, p. 98, 2019.
[28] G. Cerullo, G. Mazzeo, G. Papale, L. Sgaglione, and R. Cristaldi, "A secure cloud-based scada application: The use case of a water supply network." in *SoMeT*, 2016, pp. 291–301.
[29] A. Sajid, H. Abbas, and K. Saleem, "Cloud-assisted iot-based scada systems security: A review of the state of the art and future challenges," *IEEE Access*, vol. 4, pp. 1375–1384, 2016.
[30] S. Zhang, X. Luo, and E. Litvinov, "Serverless computing for cloud-based power grid emergency generation dispatch," *International Journal of Electrical Power & Energy Systems*, vol. 124, p. 106366, 2021.
[31] J. Shen, J. Xu, K. Cai, and Y. Ji, "Access point authentication scheme of scada system based on cloud computing technology," in *Journal of Physics: Conference Series*, vol. 1748, no. 2. IOP Publishing, 2021, p. 022010.
[32] M. Yi, H. Mueller, L. Yu, and J. Chuan, "Benchmarking cloud-based scada system," in *2017 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*. IEEE, 2017, pp. 122–129.
[33] S. Alam, M. Shuaib, and A. Samad, "A collaborative study of intrusion detection and prevention techniques in cloud computing," in *International Conference on Innovative Computing and Communications*. Springer, 2019, pp. 231–240.

FATIMAH F. ALSHEHRY received the B.S. degree in Computer Science from King Khalid University, Abha, Saudi Arabia, and the executive M.S. in cyber security from King Abdulaziz University, Jeddah, Saudi Arabia, in 2018 and 2022, respectively. Her research interests include cloud security, critical infrastructures, information security, and security threats analysis.

ARWA M. WALI received the M.S. degree in Information Systems, and the and Ph.D. degree in Computer Science from New Jersey Institute of Technology (NJIT), Newark, New Jersey, USA, in 2011 and 2018, respectively. She is currently an Assistant Professor at the Information Systems Department, Faculty of Computing and Information Technology (FCIT), King Abdulaziz University, Jeddah, Saudi Arabia. Her research interests include data mining, machine learning, indexing and compression, fingerprinting, and information security.