IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 21, 2016, accepted March 25, 2016, date of publication March 31, 2016, date of current version April 21, 2016.

Digital Object Identifier 10.1109/ACCESS.2016.2549047

Cloud-Assisted IoT-Based SCADA Systems Security: A Review of the State of the Art and Future Challenges

ANAM SAJID[1], HAIDER ABBAS[2,3], AND KASHIF SALEEM[3]

[1]Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Islamabad 44000, Pakistan
[2]National University of Sciences and Technology, Islamabad 44000, Pakistan
[3]Center of Excellence in Information Assurance, King Saud University, Riyadh 11653, Saudi Arabia

Corresponding author: H. Abbas (haiderabbas-mcs@nust.edu.pk)

This work was supported by the National Plan of Science, Technology and Innovation, King Abdulaziz City for Science and Technology, Saudi Arabia, under Grant 12-INF2817-02.

Industrial scale needs:
* Stability
* Fault tolerance
* Flexibility

ABSTRACT Industrial systems always prefer to reduce their operational expenses. To support such reductions, they need solutions that are capable of providing stability, fault tolerance, and flexibility. One such solution for industrial systems is cyber physical system (CPS) integration with the Internet of Things (IoT) utilizing cloud computing services. These CPSs can be considered as smart industrial systems, with their most prevalent applications in smart transportation, smart grids, smart medical and eHealthcare systems, and many more. These industrial CPSs mostly utilize supervisory control and data acquisition (SCADA) systems to control and monitor their critical infrastructure (CI). For example, WebSCADA is an application used for smart medical technologies, making improved patient monitoring and more timely decisions possible. The focus of the study presented in this paper is to highlight the security challenges that the industrial SCADA systems face in an IoT-cloud environment. Classical SCADA systems are already lacking in proper security measures; however, with the integration of complex new architectures for the future Internet based on the concepts of IoT, cloud computing, mobile wireless sensor networks, and so on, there are large issues at stakes in the security and deployment of these classical systems. Therefore, the integration of these future Internet concepts needs more research effort. This paper, along with highlighting the security challenges of these CI's, also provides the existing best practices and recommendations for improving and maintaining security. Finally, this paper briefly describes future research directions to secure these critical CPSs and help the research community in identifying the research gaps in this regard.

INDEX TERMS APT, industrial control system, Internet of Things (IoT), NIST, PRECYSE, supervisory control and data acquisition system, SOA.

Benefits of IoT-cloud architecture in smart industrial scale CPSs: cost reduction, improved uptime, increase in redundancy and flexibility.

I. INTRODUCTION

Industries are always concerned with reducing their operational costs and related expenses. Therefore, companies are constantly searching for solutions that improve their systems' stability, fault tolerance, flexibility, and cost efficiency. By adopting such solutions, the complexity and interactivity of communications within the industrial systems is expected to expand. One such solution to fulfil the current needs of industrial systems is the concept of IoT, which involves cloud computing. The IoT-cloud combination offers the advantage of integrating CPSs such as SCADA systems. This integration leads to the concept of "smart" industrial systems [1].

The advent of the IoT-cloud combination has brought multiple benefits to the information technology (IT) industry that includes embedded security, cost reductions, improved uptime, and an increase in redundancy and flexibility. Critical infrastructures (CI) are also being integrated with the IoT-cloud services. IoT-cloud appears to exactly meet the uptime, flexibility, cost, and redundancy requirements of these systems in a reasonable way. We can describe CPSs as smart systems encompassing both physical and computational components that are seamlessly integrated and interact closely to sense changing states in the real world. CPS applications include—but are not limited to—smart transportation, smart medical technologies, smart electric grids,

What are Cyber Physical Systems?

air traffic control, and so on. Under the IoT architecture it is not easy to clearly differentiate between Wireless Sensor Networks (WSN), machine-to-machine technologies, and CPSs. However, the study in [2] makes an effort to provide a general CPS model to show the overlapping concepts involved in these systems, as shown in Fig. 1.

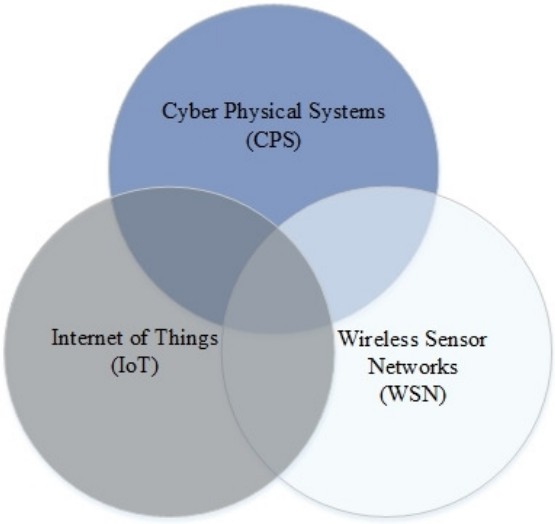


FIGURE 1. The cyber physical system model [2].

What are SCADA systems?

At a supervisory level, the major responsibility of SCADA systems is to monitor a system's processes and apply the appropriate controls accordingly. SCADA systems are basically CPSs used in industries. These systems include a wide number of application sectors, as presented in Fig. 2, and currently a lot of research has been conducted in this regard [3]–[9]. For example, one application is in the healthcare sector [10]–[12]. SCADA systems that provide medical solutions enable doctors and associated healthcare team members to monitor and control a patient's state of health in a cost effective and efficient manner. One such solution

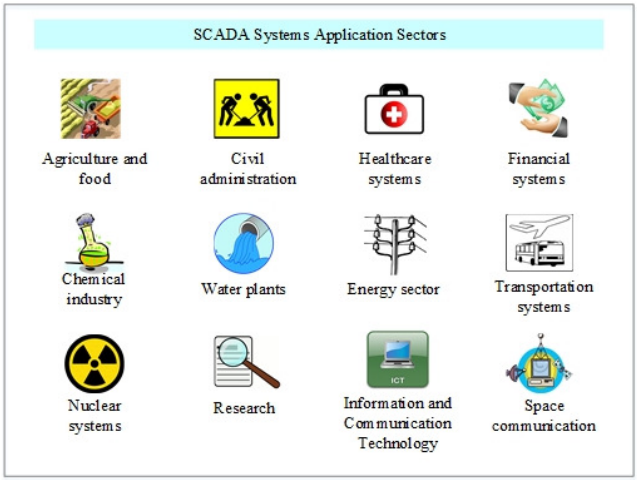


FIGURE 2. SCADA systems application sectors.

present in the industry is WebSCADA [13], which provides multiple benefits that include anywhere/anytime accessibility to the system through a secure web browser connection. WebSCADA is a scalable and flexible system that can easily integrate with new project features, easy maintenance, and is customizable for other industrial applications such as oil, manufacturing, gas utilities, security monitoring, and so on.

The future Internet is considered as a new concept for classical SCADA systems that have already been in operation for many years. We are aware that, with time, new technologies replace old technologies, but unfortunately, these existing SCADA systems are being retrofitted to combine the capabilities of both the old and the new technologies. Due to this overlapping use of both technologies, the security of SCADA systems is at risk. Hence, we can say that the integration of industrial business systems and the IoT-cloud concept has made the integrated SCADA systems more vulnerable compared with classical SCADA systems. In general, SCADA systems architecture contains a Human Machine Interface (HMI), hardware, software, Remote Terminal Units (RTUs), a supervisory station, sensors and actuators [14]. The general architecture of SCADA systems in an IoT-cloud environment is illustrated in Fig. 3.

Problem 1

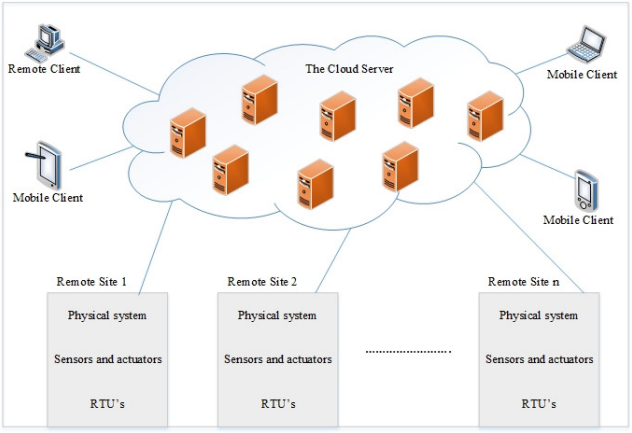


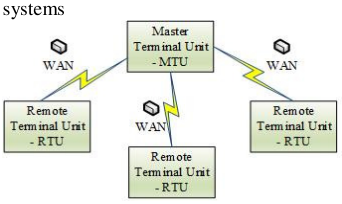
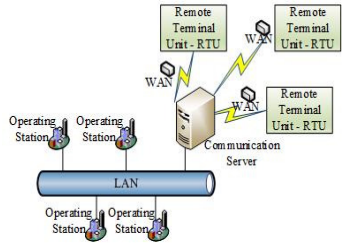
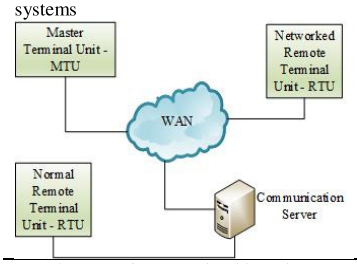
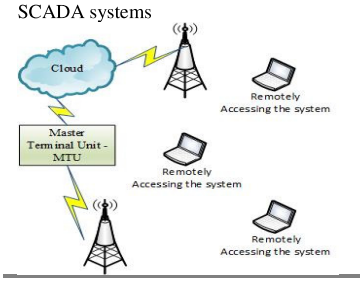
FIGURE 3. The general architecture of SCADA systems in an IoT-cloud environment.

Standard protocols and wired communications were used when SCADA systems first came into existence and were solely aimed at monitoring and controlling system processes. However, when these systems were exposed to the IoT environment, which involves cloud computing and complex network environments, they became more vulnerable to cyberthreats and attacks. Table 1 describes the journey of SCADA systems from first generation to the IoT-based SCADA systems being used now.

Problem 1 Extended

The remainder of this paper is divided as follows. Section II presents the challenges of IoT-cloud based SCADA systems by identifying their major vulnerabilities and threats. Based on these identifications, Section III describes the current efforts to secure industrial SCADA systems in IoT-cloud environments. Section IV provides a number of

TABLE 1. The evolution of SCADA systems.

General Representation of SCADA Systems Generations	Main Features
First generation monolithic SCADA systems 	Mainframe systems were responsible for computing These systems were not interlinked These systems used proprietary software's Wide Area Networks (WAN's) were used only for communicating with RTUs Today's WAN Protocols were not known to these systems
Second generation distributed SCADA systems 	These systems utilized Local Area Networks (LAN's) technology System miniaturization made the distributed SCADA systems tiny and less expensive in comparison to the previous generation systems Distributed systems increased the performance of SCADA systems in terms of redundancy, processing power and reliability Protocols used for LAN's were mostly proprietary
Third generation networked SCADA systems 	The major difference is that this generation of SCADA systems used open source instead of proprietary systems Eliminated the limitations of proprietary systems by using off-the-shelf systems Utilized Internet Protocol (IP) for communications
Fourth generation IoT-cloud based SCADA systems 	The current generation of SCADA systems utilizes IoT technology and commercial cloud-computing services IoT-cloud based SCADA systems are easy to maintain and integrate Increased data accessibility, cost efficiency, flexibility, optimization, availability and scalability

Benefits of IoT-cloud based SCADA systems:
* cost efficiency
* flexibility
* optimization
* data accessibility
* availability
* scalability

recommendations and best practices being proposed to secure these systems. Section V describes a wide range of future research options for securing the industrial SCADA systems in an IoT-cloud environment, and Section VI concludes the paper.

II. CHALLENGES TO SECURE SCADA SYSTEMS IN IoT-CLOUD ENVIRONMENTS

The Siberian Pipeline Explosion happened in 1982 and is considered to be the first cybersecurity incident in the history of SCADA systems. In this explosion, an attacker exploited a system vulnerability using a virus called a Trojan horse. In 2000, a former worker hacked into the Maroochy Shire water plant control system, flooding the hotel grounds with raw sewage [15]. In 2010, Iran's nuclear system was disrupted by the Stuxnet worm [16]. In 2011, another form of Stuxnet was discovered and given the name Duqu. Most recently, the Flame worm [17] brought devastation to Industrial Control Systems (ICS) and to SCADA systems.

A detailed literature review and analysis of the major attacks on SCADA systems can help focus attention on the reasons why these critical infrastructures are so vulnerable. Particularly in cases where these systems are integrated with the IoT and cloud based environments, they are far more exposed to such vulnerabilities. A number of vulnerabilities exist in these environments that could possibly implant malware in SCADA systems, some of which are listed below [1], [18], [19]:

1. System commands and information can be modified, sniffed, lost, or spoofed during communication because the reliance on cloud communication makes the SCADA systems more open.
2. The network connections between SCADA systems and the cloud potentially open backdoors to the ICS, which can then be exploited by attackers.
3. SCADA systems integrated into the cloud have all the same risks as typical cloud infrastructure.
4. Data on the cloud is separated only internally because the same cloud can be accessed by other clients.
5. SCADA systems applications running on the cloud can be easily searched and abused by attackers.
6. For control and automation SCADA systems use Modbus/TCP, IEC 40, and DNP3, but some of these protocols lack protection.
7. SCADA systems use commercial off-the-shelf solutions instead of proprietary solutions.
8. SCADA systems lack proper security controls.
9. Unnecessary services and default factory settings lead to configuration errors in the IoT device operating systems.
10. Memory corruption and weakness in validating input data causes software errors in IoT device operating systems.
11. Third party software used for IoT devices can lead to configuration errors such as parameter tempering and lack of encryption.
12. Cloud and external individual service providers have security vulnerabilities of their own.

The vulnerabilities mentioned above form the basis for why CIs are exposed to threats that have a negative impact on the performance of these systems. A general statistical representation of the threats to SCADA systems before their exposure to the IoT-cloud environment is shown in Fig. 4. Insider threats are considered to be the most prominent type of attacks on IoT-based SCADA systems [19]. Based on the current literature, a few threats to the SCADA systems in IoT-cloud environments are defined below:

1) *Advanced Persistent Threats (APTs):* APTs are network attacks in which an unauthorized person attempts

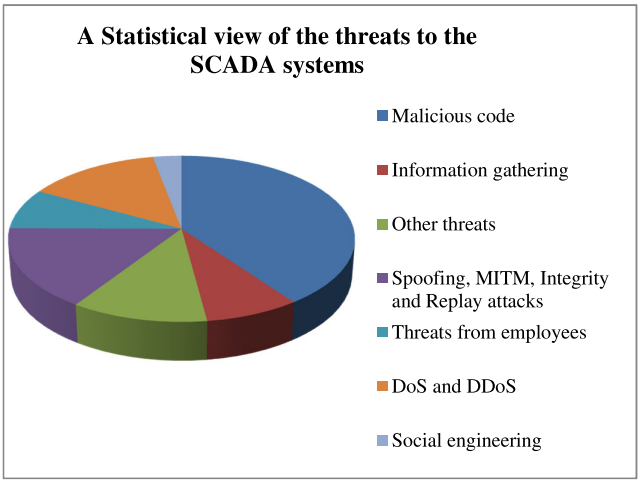


FIGURE 4. A statistical view of the threats to the SCADA systems [24].

to gain access to the system using zero-day attacks with the intention of stealing data rather than causing damage to it [20].

2) *Lack of Data Integrity:* Data integrity is lost when the original data are destroyed, and this could happen through any means such as physical tampering or interception.
3) *Man-in-the-Middle (MITM) Attacks:* Two attacks that can easily be launched as a result of a man-in-the-middle attack are spoofing attacks and sniffing attacks. In a spoofing attack, a program or person masquerades as another program or person to gain illegitimate access to the system or the network. In a sniffing attack, the intruder monitors all the messages being passed and all the activities performed by the system [21].
4) *Replay Attacks:* Replay attacks are a type of network attack in which a valid message containing some valid data is repeated again and again; in some cases, the message may repeat itself. These attacks affect the performance of SCADA systems and can be serious threats when a replay attack delays messages sent to physical devices [22].
5) *Denial of Service (DoS) Attacks:* The purpose of a DoS attack is to make a service unavailable for the intended user. Such attacks can be performed in multiple ways such as DoS or DDoS. At the simplest level, these attacks overload computer resources such that the machine is unable to perform its intended tasks [23].

III. EFFORTS TO SECURE SCADA SYSTEMS

To protect the SCADA systems from the above mentioned threats, many efforts have been made in terms of security frameworks, protection mechanisms and assurance approaches. The following section summarizes these efforts by first focusing on the efforts to secure SCADA systems outside of the IoT-cloud environment and then within the IoT-cloud environment.

A. SCADA SYSTEMS SECURITY IN GENERAL

The following general security considerations apply to SCADA systems:

1) *Policy Management:* Cyber security is considered a threat because if an intruder somehow gains access to a SCADA system then the intruder most probably also gains control over everything within the system. The threats increase enormously when these systems are connected to the Internet. For example, protecting SCADA systems against Internet connectivity was not even considered a possible vulnerability when power systems were first developed. Because people often have little awareness of the methods for securing CIs, cyberattacks are increasing. To assess power system vulnerabilities, an attack tree model was used by Watts [25]. The author argues that good password policies make the system access points strong and make it difficult for an intruder to guess a password to access the systems. A drawback of this methodology is that attack trees do not capture the penetration sequence of attack leaves. Cagalaban *et al.* [21] present a fault detection algorithm to find the vulnerabilities in SCADA system software. The authors of [21] used a test-bed architecture and the Modbus protocol. The purpose of an attacker can be easily identified by this methodology. The results reveal that SCADA systems software strength increases when these systems follow proper rules for authentication and authorization.
2) *Data Integrity:* To mitigate Denial of Service (DoS) attacks, Davis *et al.* [23] adopted a test-bed architecture using RINSE, which also assesses vulnerabilities faced by power systems. Three attack scenarios are considered. In the first scenario, there is no attack and systems perform normally; in the second scenario, the DoS attack is introduced; and the last scenario applies filters such that the effects of a DoS attack can be measured. A drawback of this methodology is that it focuses only on the software level; hence, hardware is not taken into consideration. Giani *et al.* [26], presented a test-bed architecture in which system availability and integrity are compromised by introducing multiple attacks. The major goal of this study was to measure the impact that such attacks have on SCADA systems. Davis *et al.* [23] proposed a few models to investigate attacks, determine their effects, and identify mitigation strategies. Cárdenas *et al.* [27] presented a methodology that detects such attacks by monitoring and analyzing the physical system under observation. As recommended by [27], attack-resilient algorithms are required to make the systems able to survive intentional attacks such as Stuxnet.
3) *Weak Communication:* According to Wang [22], the communication links of SCADA systems can be attacked easily because they do not typically provide encryption and authentication mechanisms. The American Gas Association (AGA) has played a vital

role in securing SCADA system communications and introduced the concept of cryptography within these systems' communication. Secure SCADA (sSCADA), a plugin device, is presented in [22] as Part 1 of the AGA's cryptographic standard, with two vulnerabilities that lead to man-in-the-middle and replay attacks. To address these vulnerabilities, the authors propose four channels of communication, each fulfilling different security services. The job of an attacker is made easy by the use of a weak protocol. The communication protocols used in SCADA systems are responsible for communicating messages over the entire industry network. Many protocols are used including DNP3, PROFIBUS, Ethernet/IP, etc., but based on the system requirements a particular protocol is selected for communication. The devices that were considered as trusted were connected to the SCADA systems network long before security issues were taken into consideration. Use of the new Internet-based technologies established untrusted connections. Hence, we can say that the built-in vulnerability of the communication protocols makes the systems weak. Igure and Williams [28] described three challenges that must be considered to improve SCADA system networks, as follows:

- SCADA systems security within the network can be improved by utilizing intrusion detection systems and keeping firewalls up to date, thereby keeping the system's activities under constant supervision.
- SCADA systems security management can be improved by performing regular risk assessments and improving the clarity of security plans and their implementations.
- Access control for SCADA systems can be improved as well. The first step in securing any system is to prevent the system from being accessed by unauthorized entities. Although this can be achieved by improving authorization password and smart cards, those are not the ultimate solution.

Securing weak communication protocols requires:
* Firewall
* Intrusion detection systems
* Encryption techniques

To assess and analyze the Modbus communication protocol's vulnerability and risks, Byres *et al.* [29] used an attack tree model, revealing that the Modbus protocol is weak and lacks basic security requirements such as integrity, confidentiality and authentication. They recommended [29] using firewalls, Intrusion Detection Systems (IDSs) and encryption techniques for secure communications.

To secure the communication channels of SCADA systems, Patel and Sanyal [30] presented some solutions based on IP-Sec and SSL/TLS. The strengths and weakness of both presented solutions are also described in detail. On the network layer IP-Sec is presently capable of providing protection to each application responsible for carrying out communication tasks between two hosts. IP-Sec can secure the IP traffic, prevent DoS attacks, and is also able to stop any arbitrary communication packet from entering the TCP layer. Over TCP/IP, communications between (Remote Terminal Unit) RTUs and (Master Terminal Units) MTUs are secured by SSL/TLS, which is an efficient and fast solution and at the same time provides protection against man-in-the-middle and replay attacks. However, IP-Sec is also a complex and less scalable solution that is unable to provide nonrepudiation and authentication [30]. In addition, IP-Sec encrypts all the traffic. Similarly, SSL/TLS is considered to be an expensive solution with known vulnerabilities and is also unable to provide nonrepudiation. Although both IP-Sec and SSL have their drawbacks, the clients need determine which solution to use. Security in IP-based SCADA systems is addressed in detail in [31].

In another approach to securing the communication channels of SCADA systems, two middleware methods are described by Khelil *et al.* [32]. In the first method, the aim of the authors is to maintain data integrity and availability based on peer-to -peer protection by maintaining more than one copy of data. This data access technique can protect SCADA systems from router crashes as well as from data modifications. However, this approach is considered to be intrusive and requires modifications to be made on existing networks. In the second method, data availability is approached by using GridStat middleware. To ensure data availability, this methodology adds some new components to the architecture that require no changes to the original components: it follows a nonintrusive approach.

B. SCADA SYSTEM SECURITY IN AN IoT-CLOUD ENVIRONMENT

1) DATA INTEGRITY AND PRIVACY

Antonini *et al.* [33] addressed security challenges to SCADA systems, and Baker *et al.* [34] presented a security oriented cloud platform for Service Oriented Architecture (SOA) based SCADA systems. The main idea of this proposal is to deliver an innovative solution to integrate cloud platforms into SOA based SCADA systems. It also focuses on the enhancement of security and integrity concerns for these systems. Smart Grid systems are used in the proposed approach through a real-world scenario. This paper directs readers' attention toward building a secure cloud platform that supports the use of SOA based SCADA systems. Another threat stems from APTs, which are focused on networks. In this type of attack, an unauthorized person manages to enter a network and then tries to steal data from the system. The focus of this attack is not to cause damage but rather to stay undetected as long as possible, steal data and then leave, all the while keeping the attacker's identity hidden. Bere and Muyingi [20] addressed these types of threats and claim that APTs use zero-day vulnerabilities to steal data from systems.

What are zero-day vulnerabilities?

2) DATA LOGGING

Security risks related to data logging are also a challenge in IoT-based SCADA systems because of the presence of the cloud [19]. Compared to localized logging, keeping track of cloud-based system logs is difficult.

3) OWNERSHIP

Use of third party cloud services in IoT-based SCADA systems takes ownership privileges from the SCADA systems organization and puts them under the control of the Cloud Service Provider (CSP) [43]. Hence, we can say that these systems have lack of control.

4) AUTHENTICATION AND ENCRYPTION

Problem 1 Extended

There is a lack of authentication and encryption mechanisms for IoT-based SCADA systems. If these systems use weak communication protocols such as Modbus [29] while utilizing the cloud, an attacker can easily gain access to IP addresses, usernames, and other private credentials, as the result of weak authentication and encryption. Modern cyber security attacks have also taken over ICS, as described in [33], in which the vulnerabilities of SCADA systems are exploited more often because the International Electrotechnical Commission (IEC) 61850 standard itself lacks security. According to the authors [33], SCADA systems networks still face key management issues.

5) WEB APPLICATIONS IN THE CLOUD

Web applications are frequently used in these systems. Based on the literature [1], [2], [13]–[43], web applications have their own security needs that are currently not addressed by IoT-cloud based SCADA systems.

6) RISK MANAGEMENT

Ongoing research on SCADA systems is presented by Nicholson *et al.* [36], who emphasize that the threats and risks to SCADA systems are not completely addressed because of their integration with corporate networks, making them more vulnerable to cyberattacks. Identification of risk mitigation techniques is a positive contribution from [36]. Research challenges faced by SCADA systems in risk assessment are outlined in [37] and [38].

7) EMBEDDED DEVICE PROTECTION IN INDUSTRIAL IoTs

Because classical IT systems differ from CPS such as SCADA systems, existing concepts of information security cannot be adopted. To defend against the privacy and security risks, the Industrial IoT requires a cyber security concept capable of addressing such risks at all possible levels of abstraction. Some solutions for protecting the embedded devices at the core of industrial IoT-based SCADA systems are shown in the Table 2.

The major difference between SCADA systems and Distributed Control Systems (DCSs) is that they differ in size: SCADA systems are restricted to large areas while DCSs are restricted to smaller areas. Originally, SCADA systems were developed as isolated systems, but that is no longer true due to the usage of commercial off the shelf solutions and widely expanded networked environments such as the IoT-based SCADA systems. There is a need to develop a more secure solution that considers the security requirements and constraints faced by these systems. Although some security improvement actions have been implemented since 2010 to protect these systems against major attacks, still, they remain vulnerable to intrusions, data modifications, denial of service attacks, threats from legitimate users, and many more security-related threats. IoT-based SCADA systems are vulnerable to network attacks as well. The differences between IoT-based SCADA system security in particular and IT systems security in general must be clearly understood because this understanding can help in developing more efficient and secure solutions that focus on IoT-based SCADA systems security.

TABLE 2. Security architectures for industrial IoTs.

Security Architectures	Brief Description and Analysis
Intel and ARM architectures	These are widely used in mobile devices such as tablets and smartphones; however, they are prohibitively expensive for embedded systems designed specifically for well-defined focused tasks that must be low power and low cost.
SMART—Secure and Minimal Architecture for (Establishing a Dynamic) Root of Trust)	SMART protects the integrity of only one embedded task with read-only memory; it does not provide a code change option after deployment.
SPM (Self Protecting Modules)	SPM provides task isolation that is hardware enforced and uninterruptable because the memory layouts of the tasks are fixed.
SANCUS—Low-cost trustworthy extensible networked devices with a zero-software trusted computing base	SANCUS is an extension to SPM that manages cryptographic secrets for tasks, but it also inherits the limitations of SPM.
TrustLite—A security architecture for tiny embedded devices	Concepts of SPM and SMART are generalized by TrustLite and support task interruptions as well. A requirement of TrustLite is that all the software components must be loaded and task isolation of tasks must be configured at boot time.

IV. RECOMMENDATIONS AND BEST PRACTICES FOR SECURING IoT-CLOUD BASED SCADA SYSTEMS

SCADA systems in IoT-cloud environment are not like regular IT systems; we cannot assume that by simply using some strong password policies, updated antivirus protection, firewalls, or frequent patching will solve the problems (as they would for simpler IT systems). Therefore, countermeasures are required that directly address the security needs of SCADA systems in IoT-cloud environments. Recently, the Internet Engineering Task Force (IETF) has been working on a new draft that focuses on security considerations for Industrial IoT (IIoT) in IP-based environments. This draft standard also provides an overview on the present state of the art (as of 2013) and emphasizes that future connections are moving towards an all-IP solution. The current draft standard defines five security profiles: IoT devices for home use, IoT devices with no security requirements, IoT devices for industrial usage, IoT devices for managed home use, and IoT devices for advanced industrial usage. When considering the future for secure and flexible industrial IoT networks, this draft

identifies that Datagram Transport Layer Security (DTLS) will form the basic building block for these systems. However, the draft argues that there is a need to introduce more interconnectivity among the multiple layers of security in the IoT and cloud based industrial systems.

Similarly, the methodology named ''Prevention, Protection and REaction to CYber attackS to critical infrastructurEs'' (PRECYSE) is a security methodology intended to improve by design the reliability, resilience and security of Information and Communication Technology (ICT) that supports CI's such as CPS, SCADA, IIoT, and so on. PRECYSE is built on research standards already in existence and has a special focus on relevant security, policy, privacy, ethical and legal issues for CIs. The major goals of PRECYSE for CIs such as SCADA systems [39] are as follows:

- Investigating privacy and ethical issues.
- Improving resilience through a security architecture.
- Providing tools for preventing and protecting against cyberattacks on SCADA systems and controlling the reaction to such attacks.
- Presenting a methodology for identifying assets and their associated vulnerabilities and threats.
- Deploying prototypes at two sites, one in the transport sector and the other in the energy sector.

Some basic principles can be considered for protecting Industrial IoT and IIoT-cloud based SCADA systems, as shown in Fig. 5. These principles have the objective of protecting vulnerable infrastructure by surrounding these systems with a combination of security tools based on currently available good practices. Following is a brief overview of few such good practices that helps in improving the security of IoT and cloud based SCADA systems, keeping in view the guidelines of NIST SP 800-53 [40], NIST SP 800-53, Revision 4 [41], NIST SP 800-82, Revision 2 [42], and other literature reviewed in the reference section.

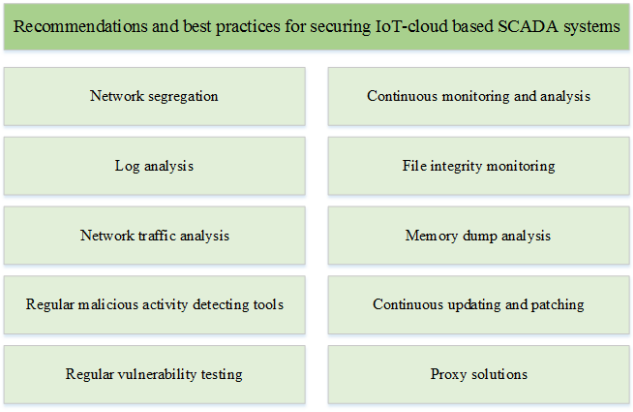


FIGURE 5. Best practices for securing IoT-cloud based SCADA systems.

1) NETWORK SEGREGATION

An approach to segregate networks introduces security tools that surround each network and as a result effectively segregate and monitor network activities, preventing policy violations.

2) CONTINUOUS MONITORING AND ANALYSIS

The computers involved in SCADA systems are performing critical tasks that often make the computer systems complex. Due to the increased frequency of attacks, there is a need to continuously monitor and analyze the activities these computer systems perform.

3) LOG ANALYSIS

Activity logs are kept by nearly all computer software and devices including operating systems, network devices, applications and other intelligent programmable devices. These logs play a vital role in troubleshooting, compliance checking, forensic analysis and intrusion detections. Tracking via these logs can identify and help control many attacks. Such log analysis is typically supported by host-based IDS.

4) FILE INTEGRITY MONITORING

File integrity analysis is used to validate the integrity of some software and operating systems. The cryptographic checksum method is the most frequently used verification method. Harmful files (black lists) and allowed files (white lists) can be easily identified using checksum verification methods. Checksum methods are also supported by host-based IDS.

5) NETWORK TRAFFIC ANALYSIS

Malicious activities can sometimes be detected though network monitoring by performing network packet analysis. Malicious activities can also be detected based on behavioral or pattern analysis. For sophisticated malware, where the information is hidden inside covert channels, network analysis can detect only the number of network packets or the destination for that packet; hence, other techniques are required to detect malicious behaviors within covert channels.

6) MEMORY DUMP ANALYSIS

Both known and unknown malicious activity present within the memory of an operating system can be detected by memory dump analysis. Using advanced technologies, a volatility framework can analyze multiple types of memory dumps. This type of analysis makes it easy to detect system libraries and hidden processes, which also helps in detecting the sophisticated attacks and intrusions.

7) UPDATING AND PATCHING REGULARLY

Third-party software is used by IoT-cloud SCADA systems, and keeping this software continuously up to date is a challenge. Unknown errors in such software can trigger the possibility of arbitrary code execution by attackers. Monitoring the current security news and following the best approaches for updating and patching this critical infrastructure software is a requirement.

8) TESTING VULNERABILITY REGULARLY

To a large extent, the design of a system determines its security level. Unknown errors in cloud systems are easily discovered by continuous monitoring and vulnerability testing. These tests can be applied to either the whole system or to

particular system components, but should be performed at regular intervals because new threats are revealed through analysis over time.

9) PROXY SOLUTIONS

To increase the security of these systems, proxy solutions are used to build a fine layer of protection around vulnerable or legacy solutions. Proxy solutions can perform filtering and inspections, implement access control, and limit the range of instructions sent to the network or to devices. When a supplier needs access to the critical network this protection can be removed for the subset of data required; for example, a Demilitarized Zone (DMZ) can be used as a trusted process.

10) TOOLS FOR DETECTING MALICIOUS ACTIVITY

In addition to all the practices mentioned above, it is a requirement to regularly use intrusion detection and prevention systems, antivirus software, and so on, and to keep these up to date, ensuring that attack patterns are kept current in the database to help in improving the security of these systems.

V. FUTURE RESEARCH DIRECTIONS IN SECURING IoT-CLOUD BASED SCADA SYSTEMS

To secure CPSs in the future, more research needs to be performed. Because the concepts related to the future Internet such as IoTs and cloud computing, specifically, are at an early stage of deployment in industrial SCADA systems, more focus is required on preventing cyberattacks on industrial SCADA systems. A few research directions for securing IIoT-based CPSs [43] are briefly explained below and presented in Fig. 6.

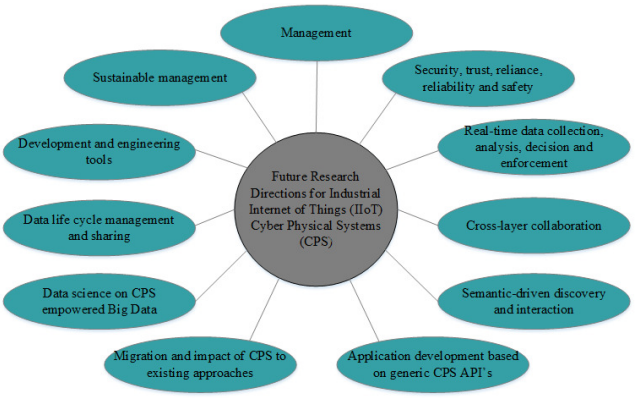


FIGURE 6. Future research directions for securing CPS.

1) MANAGEMENT

There is a need to develop new methods capable of managing complex and large-scale systems because thousands of IoT devices will be active in such industrial settings, including smart industries, smart cities, and so forth.

2) SECURITY

The CPSs are responsible for controlling real-world infrastructures and, thus, have a real-world impact on them. Failure to secure these critical infrastructures can have devastating impacts. There is a need to answer questions such as: ''To what extent will future CIs be vulnerable?'' and ''To what level can we ensure that they are trustworthy, resilient and reliable?''

3) REAL-TIME DATA HANDLING

CPSs such as IIoT, which are primarily based on supervising and controlling data acquisitions, need to collect and analyze the data in real time and make business decisions; these systems cannot afford delays. For such decision making, classical CPSs utilize local decision loops, but with the cloud and IoT, they are becoming more dependent on external services. Therefore, aspects of timely interaction need to be revisited.

4) CROSS-LAYER COLLABORATIONS

The effectiveness of these systems depends on collaboration among the involved platforms that are responsible for delivering services in a service-based infrastructure. However, these complex collaborations possess multiple requirements from both the business and technical worlds that are based on specific application scenarios. To make the CPS ecosystem flourish, people need assurance that these complex collaborations can deliver services efficiently and effectively—but providing that assurance is not an easy task and needs more research.

5) APPLICATION DEVELOPMENT

To build complex services and behaviors for critical CPSs the underlying core API functionalities must be standardized. API consolidation can be applied as a short term solution until new solutions are developed that work through semantically driven interactions.

6) MIGRATION OF CPSs AND THE IMPACT ON EXISTING APPROACHES

The large-scale impact of CPSs needs to be carefully assessed and investigated; however, this is a challenging task. It is expected that CPSs will replace the classical approaches gradually in the future. Therefore, new strategies are required to migrate these classical systems to CPS.

7) SUSTAINABLE MANAGEMENT

Cloud-based CPSs promise to provide more efficient and optimized usage of global resources. Therefore, sustainable strategies for managing the business and information structures are required—e.g., energy-driven management. There is a need to understand and implement new solutions with respect to a greater context such as applications that apply at smart citywide scales, cross-enterprise scales, etc. To effectively integrate such solutions in large-scale CPSs, new approaches and tools are needed.

8) ENGINEERING AND DEVELOPMENT TOOLS

Within complex environments, there is a need for new engineering and development tools that can help ease the complexity of service creation in CPS ecosystems.

9) SHARING AND MANAGEMENT OF DATA LIFECYCLE

The first step in the data lifecycle involves acquiring data from the cyber physical world; however, the second step is sharing these data and managing them because building sophisticated services is a challenge. This challenge becomes ever more complex now that the security and privacy of these data must also be ensured in cloud environments. The entire topic needs more research and new and innovative solutions.

10) DATA SCIENCE

Massive CPS infrastructures integrated with the cloud will acquire enormous amounts of data. The term for such data volumes is ''Big Data''. It is possible to analyze big data in the cloud to deliver new insights on industrial processes, which can result in the ability to better identify optimized solutions and enterprise operations. Approaches based on data science and big data are expected to have a positive impact on the way in which CPS infrastructures are designed and operated.

VI. CONCLUSIONS

The objective of this study was to highlight some important facts about industrial SCADA systems with an emphasis on threats, vulnerabilities, management and the current practices being followed. CPSs such as SCADA systems are widely used. The objective of IoT-based SCADA systems is to increase their flexibility, cost efficiency, optimization capability, availability and scalability of such systems. For this purpose, industrial SCADA systems utilize the benefits of IoT and cloud computing. However, these benefits are accompanied by numerous critical risks. Major security risks related to the industrial SCADA systems in the cloud may vary from one scenario to another. In such environments, the nature of data is such that it must be stored on server/s for backup or sharing purposes, and these server/s are mostly managed by a third party. This third party management means that these servers are likely to contain large numbers of clients and their confidential information. The result is that the privacy of data on these cloud servers cannot be guaranteed, as the data may or may not be shared with other clients. Therefore, such security breaches must be considered before integrating industrial SCADA systems with IoT-cloud environments. The purpose of this paper was to highlight the unique importance of critical industrial SCADA systems from the perspective of IoT and cloud computing. The efforts being made to secure these systems within the future Internet environment were described and discussed extensively. After performing this study, it can be concluded that several of the vulnerabilities described in this paper are particularly relevant to industrial IoT based SCADA systems, and it is extremely important to note that each specific IoT device is a separate entity and will typically possess an attack surface of its own. Therefore, there is a clear need to perform more research on securing these systems because attacks not only have the potential for devastating effects to both industrial machines and to individuals associated with them but also are expected to become even more critical in the future.

REFERENCES

[1] T. Lojka and I. Zolotová, ''Improvement of human-plant interactivity via industrial cloud-based supervisory control and data acquisition system,'' *Advances in Production Management Systems. Innovative and Knowledge-Based Production Management in a Global-Local World* (IFIP Advances in Information and Communication Technology). Berlin, Germany: Springer, 2014, pp. 83–90.

[2] C.-R. Rad, O. Hancu, I.-A. Takacs, and G. Olteanu, ''Smart monitoring of potato crop: A cyber-physical system architecture model in the field of precision agriculture,'' *Agricult. Agricult. Sci. Procedia*, vol. 6, pp. 73–79, Sep. 2015, doi: 10.1016/j.aaspro.2015.08.041.

[3] G. Fortino, A. Guerrieri, and W. Russo, ''Agent-oriented smart objects development,'' in *Proc. IEEE 16th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, May 2012, pp. 907–912.

[4] W. Wei, X. Fan, H. Song, X. Fan, and J. Yang, ''Imperfect information dynamic stackelberg game based resource allocation using hidden Markov for cloud computing,'' *IEEE Trans. Services Comput.*, vol. PP, no. 99, p. 1, Feb. 2016, doi: 10.1109/TSC.2016.2528246.

[5] I. Butun, M. Erol-Kantarci, B. Kantarci, and H. Song, ''Cloud-centric multi-level authentication as a service for secure public safety device networks,'' *IEEE Commun. Mag.*, vol. 54, no. 4, 2016.

[6] H. Song, Q. Du, P. Ren, W. Li, and A. Mehmood, ''Cloud computing for transportation cyber-physical systems,'' in *Cyber-Physical Systems: A Computational Perspective*, vol. 15, L. M. Patnaik, Ed. Boca Raton, FL, USA: CRC Press, 2015, pp. 351–369.

[7] Y. Sun, H. Song, A. J. Jara, and R. Bie, ''Internet of Things and big data analytics for smart and connected communities,'' *IEEE Access*, vol. 4, pp. 766–773, Mar. 2016, doi: 10.1109/ACCESS.2016.2529723.

[8] H. Abbas, M. Q. Mahmoodzadeh, F. A. Khan, and M. Pasha, ''Identifying an OpenID anti-phishing scheme for cyberspace,'' *Secur. Commun. Netw.*, vol. 9, no. 6, pp. 481–491, 2014.

[9] H. Abbas, C. Magnusson, L. Yngstrom, and A. Hemani, ''Addressing dynamic issues in information security management,'' *Inf. Manage. Comput. Secur.*, vol. 19, no. 1, pp. 5–24, 2011.

[10] K. Saleem, A. Derhab, J. Al-Muhtadi, and B. Shahzad, ''Human-oriented design of secure machine-to-machine communication system for e-healthcare society,'' *Comput. Human Behavior*, vol. 51, pp. 977–985, Oct. 2015.

[11] H. Khattak, H. Abbas, A. Naeem, K. Saleem, and W. Iqbal, ''Security concerns of cloud-based healthcare systems: A perspective of moving from single-cloud to a multi-cloud infrastructure,'' in *Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom)*, 2015, pp. 50–56.

[12] B. M. C. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, ''Mobile-health: A review of current state in 2015,'' *J. Biomed. Inform.*, vol. 56, pp. 265–272, Aug. 2015.

[13] (2016). *WebSCADA, Web SCADA, Automation Systems, Process Control, Historian, Event Alarm, SCADA Solution*, accessed on Feb. 5, 2016. [Online]. Available: http://www.webscada.com/SCADA/SolMedSys.aspx

[14] R. J. Robles and M.-K. Choi, ''Assessment of the vulnerabilities of SCADA, control systems and critical infrastructure systems,'' *Int. J. Grid Distrib. Comput.*, vol. 2, no. 2, pp. 27–34, 2009.

[15] S. Mustard, ''Security of distributed control systems: The concern increases,'' *J. Comput. Control Eng.*, vol. 16, no. 6, pp. 19–25, Dec. 2005.

[16] J. P. Farwell and R. Rohozinski, ''Stuxnet and the future of cyber war,'' *Survival*, vol. 53, no. 1, pp. 23–40, 2011.

[17] *'Flame' Spyware Infiltrating Iranian Computers*, CNN, Atlanta, GA, USA, 2012.

[18] J. D. Fernandez and A. E. Fernandez, ''SCADA systems: Vulnerabilities and remediation,'' *J. Comput. Sci. Colleges Arch.*, vol. 20, no. 4, pp. 160–168, Apr. 2005.

[19] N. Ulltveit-Moe, H. Nergaard, L. Erdödi, T. Gjøsæter, E. Kolstad, and P. Berg. (2016). ''Secure information sharing in an industrial Internet of Things.'' [Online]. Available: http://arxiv.org/abs/1601.04301

[20] M. Bere and H. Muyingi, ''Initial investigation of industrial control system (ICS) security using artificial immune system (AIS),'' in *Proc. Int. Conf. Emerg. Trends Netw. Comput. Commun. (ETNCC)*, 2015, pp. 79–84.

[21] G. Cagalaban, T. Kim, and S. Kim, ''Improving SCADA control systems security with software vulnerability analysis,'' in *Proc. 12th WSEAS Int. Conf. Autom. Control, Modeling Simulation*, 2008, pp. 409–414.

[22] Y. Wang, ''sSCADA: Securing SCADA infrastructure communications,'' *Int. J. Commun. Netw. Distrib. Syst.*, vol. 6, no. 1, pp. 59–78, 2012.

[23] C. M. Davis, J. E. Tate, H. Okhravl, C. Grier, T. J. Overbye, and D. Nicol, "SCADA cyber security testbed development," in *Proc. 38th North Amer. Power Symp.*, Sep. 2006, pp. 483–488.
[24] H. M. N. Al Hamadi, C. Y. Yeun, and M. J. Zemerly, "A novel security scheme for the smart grid and SCADA networks," *Wireless Pers. Commun.*, vol. 73, no. 4, pp. 1547–1559, 2013.
[25] D. Watts, "Security & vulnerability in electric power systems ," in *Proc. 35th North Amer. Power Symp.*, Rolla, MO, USA, Oct. 2003, pp. 559–566.
[26] A. Giani, G. Karsai, T. Roosta, A. Shah, B. Sinopoli, and J. Wiley, "A testbed for secure and robust SCADA systems," in *Proc. 14th IEEE Real-Time Embedded Technol. Appl. Symp.*, 2008, pp. 1–4.
[27] A. A. Cárdenas, S. Amin, Z.-S. Lin, Y.-L. Huang, C.-Y. Huang, and S. Sastry, "Attacks against process control systems: Risk assessment, detection, and response," in *Proc. 6th ACM Symp. Inf., Comput. Commun. Secur. (ASIACCS)*, 2011, pp. 355–366.
[28] V. M. Igure and R. D. Williams, "Security and SCADA protocols," in *Proc. 5th Int. Topical Meeting Nuclear Plant Instrum. Controls, Human Mach. Interface (NPIC HMIT)*, 2006, pp. 560–567.
[29] E. Byres, M. Franz, and D. Miller, "The use of attack trees in assessing vulnerabilities in SCADA systems," in *Proc. IEEE Int. Infrastruct. Survivability Workshop (IISW)*, Lisbon, Portugal, Dec. 2004.
[30] S. Patel and P. Sanyal, "Securing SCADA systems," *Inf. Manage. Comput. Secur.*, vol. 16, no. 4, pp. 398–414, 2008.
[31] H. Kim, "Security and vulnerability of SCADA systems over IP-based wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 2012, Oct. 2012, Art. no. 268478, doi: 10.1155/2012/268478.
[32] A. Khelil, D. Germanus, and N. Suri, "Protection of SCADA communication channels," in *Critical Infrastructure Protection*, J. Lopez, R. Setola, and S. D. Wolthusen, Eds. Berlin, Germany: Springer, 2012, pp. 177–196.
[33] A. Antonini, A. Barenghi, G. Pelosi, and S. Zonouz, "Security challenges in building automation and SCADA," in *Proc. Int. Carnahan Conf. Secur. Technol. (ICCST)*, 2014, pp. 1–6.
[34] T. Baker, M. Mackay, A. Shaheed, and B. Aldawsari, "Security-oriented cloud platform for SOA-based SCADA," in *Proc. 15th IEEE/ACM Int. Symp. Cluster, Cloud Grid Comput.*, May 2015, pp. 961–970.
[35] R. Tawde, A. Nivangune, and M. Sankhe, "Cyber security in smart grid SCADA automation systems," in *Proc. Int. Conf. Innov. Inf., Embedded Commun. Syst. (ICIIECS)*, Mar. 2015, pp. 1–5.
[36] A. Nicholson, S. Webber, S. Dyer, T. Patel, and H. Janicke, "SCADA security in the light of cyber-warfare," *Comput. Secur.*, vol. 31, no. 4, pp. 418–436, 2012.
[37] Y. Cherdantseva *et al.*, "A review of cyber security risk assessment methods for SCADA systems," *Comput. Secur.*, vol. 56, pp. 1–27, Feb. 2015.
[38] W. Knowles, D. Prince, D. Hutchison, J. F. P. Disso, and K. Jones, "A survey of cyber security management in industrial control systems," *Int. J. Crit. Infrastruct. Protect.*, vol. 9, pp. 52–80, Jun. 2015.
[39] (2016). *European Commission: CORDIS: Projects & Results Service: Periodic Report Summary 1—PRECYSE (Prevention, Protection and Reaction to Cyber Attacks to Critical Infrastructures)*, accessed on Feb. 3, 2016. [Online]. Available: http://cordis.europa.eu/result/rcn/149966_en.html
[40] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," Ph.D. dissertation, Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, 2012.
[41] *Security and Privacy Controls for Federal Information Systems and Organizations*, NIST Special Pub. 800-53 Revision 4, National Institute of Standards and Technology, 2013.
[42] *Guide to Industrial Control Systems (ICS) Security*, Nat. Inst. Standards Technol. (NIST), USA, 2015.
[43] S. Karnouskos, A. W. Colombo, and T. Bangemann, "Trends and challenges for cloud-based industrial cyber-physical systems," *Industrial Cloud-Based Cyber-Physical Systems*. 2014, pp. 231–240.

ANAM SAJID received the B.S. degree in software engineering and the M.S. degree in computer science with a minor in information security from the Shaheed Zulfikar Ali Bhutto Institute of Science and Technology, Pakistan, in 2011 and 2014, respectively. Her research interests include cloud computing, Internet of Things, Internet of Everything, healthcare data privacy and security, supervisory control and data acquisition system security, malware analysis, critical infrastructures, social networking, computer forensics, and big data analysis.

HAIDER ABBAS received the M.S. degree in engineering and management of information systems and the Ph.D. degree in information security from the KTH Royal Institute of Technology, Sweden, in 2006 and 2010, respectively. He has received several research grants for ICT related projects from various research funding authorities and working on scientific projects in U.S., EU, Saudi Arabia, and Pakistan. His professional services include—but are not limited to—Guest Editorships, Industry Consultations, a Workshops Chair, a Technical Program Committee Member, an Invited/Keynote Speaker, and a Reviewer for several international journals and conferences. He has authored over 50 scientific research articles in prestigious international journals and conferences. He is a Research Fellow/Assistant Professor with the Centre of Excellence in Information Assurance, King Saud University, Saudi Arabia. He is also associated with the National University of Sciences and Technology, Pakistan, as an Assistant Professor, and Security Masons, Sweden, as a Chief Executive Officer. He is the Principal Advisor for several graduate and doctoral students with King Saud University, Saudi Arabia, and the National University of Sciences and Technology, Pakistan.

KASHIF SALEEM received the B.Sc. degree in computer science from Allama Iqbal Open University, Islamabad, Pakistan, in 2002, the Post Graduate Diploma degree in computer technology and communication from Government College University, Lahore, Pakistan, in 2004, and the M.E. degree in electrical (electronics and telecommunication) engineering and the Ph.D. degree in electrical engineering from University Technology Malaysia, in 2007 and 2011, respectively. He is currently with the Center of Excellence in Information Assurance, King Saud University, as an Assistant Professor. His research interests include ubiquitous computing, mobile computing, intelligent autonomous systems, information security, and biological inspired optimization algorithms.