IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 7, 2019, accepted June 8, 2019, date of publication July 2, 2019, date of current version October 1, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2926441

A Survey of Security in SCADA Networks: Current Issues and Future Challenges

SAGARIKA GHOSH, (Student Member, IEEE), AND SRINIVAS SAMPALLI, (Member, IEEE)
Emerging Wireless Technologies Laboratory, Faculty of Computer Science, Dalhousie University, Halifax, NS B3H 1W5, Canada

Corresponding author: Srinivas Sampalli (srini@cs.dal.ca)

This work was supported in part by the Natural Sciences and Engineering Research Council (NSERC) and industry partners Cistel Technology Inc. and Technologie Sanstream through a Collaborative Research Grant.

ABSTRACT Supervisory Control and Data Acquisition (SCADA) systems are used for monitoring industrial devices. However, their security faces the threat of being compromised due to the increasing use of open access networks. The primary objective of this survey paper is to provide a comparative study of the on-going security research in SCADA systems. The paper provides a classification of attacks based on security requirements and network protocol layers. To secure the communication between nodes of SCADA networks, various security standards have been developed by different organizations. We conduct a study of the security standards developed for SCADA networks along with their vulnerabilities. Researchers have proposed various security schemes to overcome the weaknesses of SCADA standards. The paper organizes security schemes based on current standards, detection, and prevention of attacks. It also addresses the future challenges that SCADA networks may face, in particular, from quantum attacks. Furthermore, it outlines directions for further research in the field.

INDEX TERMS Asymmetric cryptography, intrusion detection system, key management protocol, n-ary tree, symmetric cryptography, SCADA networks.

I. INTRODUCTION

SCADA systems are used as control systems for monitoring industrial processes such as oil mining, electric grids, traffic control systems, water treatment plants, space stations and nuclear systems. Modern SCADA systems have been exposed to a range of cyber attacks since they use open access networks to leverage efficiency. Failure to secure SCADA systems can be catastrophic [1]. For example, a malicious user can take control of the power supply to a city, shut down the water supply system, or cause the malfunction of a nuclear reactor.

Modern SCADA systems have a number of added features which increase the system complexities and are thus difficult to maintain. Some of the added features include control logic, communication protocols, user interfaces, and security. For example, many organizations do not tolerate data delay or data loss. Added features like firewall function and anti-virus software processes can lead to delayed delivery of data [2]. The systems must operate continuously and in tight timing [3]. Moreover, the communications are vulnerable to various threats. In the past few years, the number of cyber-attacks, in general, is rising and has been affecting power station, water, gas, and nuclear control systems. The pattern of cyber-attacks has also evolved beyond the simple attacks such as Denial of Service or Man-in-the-Middle [3].

In December 2015, due to a successful cyber-attack on SCADA, nearly 250,000 people were left without power for hours in Ukraine. After a year, another similar attack hit the country. This attack was launched by using spear phishing emails and is still in practice against industrial organizations. According to the U.S. Department of Justice, there was an attack on a small dam in Rye Brook, New York in 2013. The hackers gained access to the core command-and-control system by using a cellular modem. Although the breach occurred in 2013, it remained unreported until 2016. Furthermore, according to a FBI and Homeland Security joint report [4], there have been cyber-attacks on nuclear power plants throughout the U.S., in which the control systems were targeted. The main motive and severity of the attacks are not known, but the method used for the attack was spear phishing.

SCADA networks also comprise of resource-constrained devices such as Remote Terminal Units and Programming Logic Units, and these devices require lightweight ciphers.

The associate editor coordinating the review of this manuscript and approving it for publication was Chin-Feng Lai.

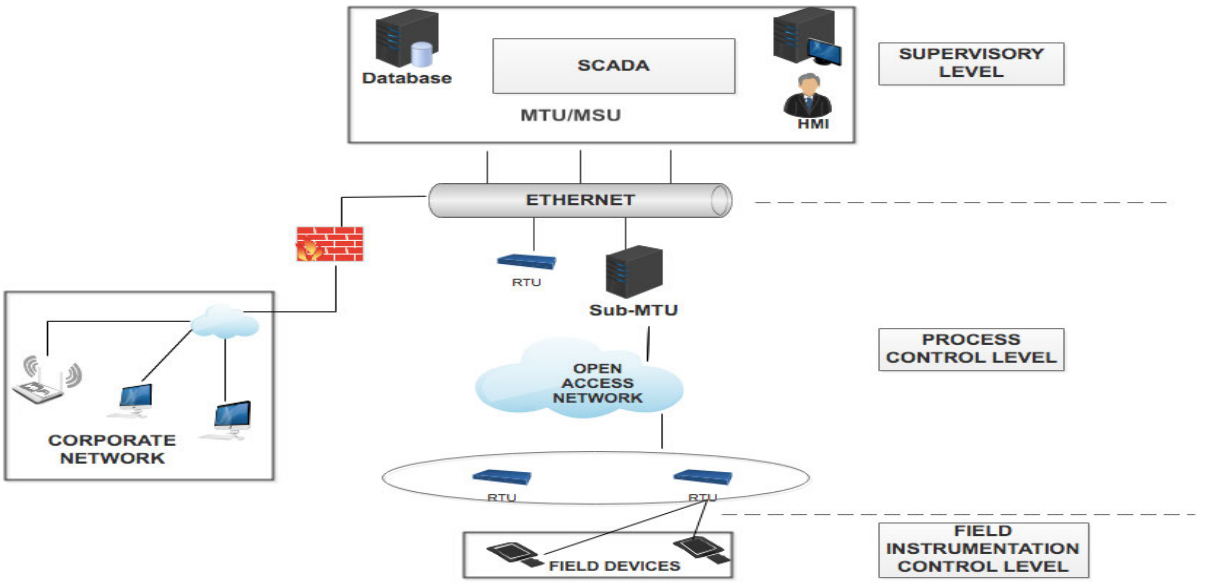

FIGURE 1. SCADA network communication architecture.

Traditional intrusion detection systems (IDSs) are now unable to protect from new threats [5]. Robust security schemes involving machine learning to detect intrusions and encryption algorithms are essential to ensure a secure encrypted communication between nodes in SCADA networks. These threats and attacks have motivated researchers and organizations to develop new robust and secure techniques for SCADA networks.

Although there are several survey papers on security threats, key management schemes, and intrusion detection systems in SCADA networks [6]–[8], the reviews do not provide a comprehensive comparison of the various schemes. The work by Sajid *et al.* [9] is an excellent survey on the security and challenges of the SCADA systems. However, the paper does not provide a comparison of all the security protocols and standards for SCADA systems. Motivated by this, our paper is an extension of the survey provided by Sajid *et al.* [9]. It gives a review of the SCADA communication structure and the recent threats faced by them. It then provides a classification and comparative study of the existing security protocols used and proposed to date. Based on the analysis, it also provides the limitations of each of the standards and protocols.

A. CONTRIBUTION OF THE SURVEY

The main contribution in this survey is to provide researchers and organizations with a report that discusses and analyzes the schemes and efforts proposed to secure the SCADA networks. It also gives a comparative study of the existing standards and schemes. Furthermore, it identifies a new threat based on quantum computing faced by SCADA networks.

B. ORGANIZATION OF THE SURVEY

Section II and Section III describe the SCADA communication structure and threats faced by such systems. Section IV describes the attacks on SCADA networks. Section V discusses the threat posed by quantum computing. Section VI gives a thorough study of on-going SCADA security schemes. Section VII discusses the primary factors used for comparison of all the schemes. Section VIII gives a critical analysis of the schemes used to secure the SCADA networks, and Section IX provides concluding remarks.

II. SCADA COMMUNICATION ARCHITECTURE

SCADA systems consist of several entities organized in a hierarchical structure [5]. They are used in monitoring various kinds of infrastructure and industries. They comprise the integration of data acquisition systems, data transmission systems and Human-Machine Interface (HMI) [5]. The HMI is a user interface that connects a person to a device. It is mainly used to visualize data, and monitor production time, machine inputs and outputs. Figure 1 illustrates a generic SCADA network communication architecture [10]–[12]. The HMI is a software interface while the hardware components are as follows [11], [12].

- Master Station Unit or Master Terminal Unit (MSU/MTU) is the control center of a SCADA network.
- Sub-MSU or Sub-MTU acts as a sub-control center. However, it is not needed in some cases. The MSU can connect to the remote station units directly.
- Remote Station Units are Remote Terminal Unit (RTU), Intelligent End Device (IED) and Programmable Logic Controller (PLC). They are used to monitor sensors and actuators to collect data values.

A communication link is shared between the MSU and Remote Station Units. Various types of communication links may be used, such as wired ethernet, WiFi or satellite link.

SCADA system architectures have four typical architectural styles [13]:

- **Monolithic:** In 1970s, control units or MTUs were hard-wired to RTUs.
- **Distributed:** In 1980s to 1990s, MTUs and RTUs communicated using communication protocols and servers. However, they did not allow Internet connection.
- **Networked:** In 2000s, SCADA architecture started using external networks like the Internet.
- **Web-based SCADA:** Currently, users can access SCADA systems using web browsers and mobile devices.

The evolution of SCADA has led to increased complexities. Some of the features responsible for this are the following [2], [13].

- Addition of new components such as computers, operating stations, communication servers and other types of resources.
- Increase in amount of data exchange between units with increase in the number of components.
- Increase in the amount of interactions between system components.
- Usage of firewalls and antivirus software that consequently slows down the processing power of the system and leads to delay in data transfer to other units.

Thus, as the size of the SCADA architecture and added features increase, the complexity of the SCADA architecture also increases. This makes managing large amount of data more difficult leading to loss of data availability. Furthermore, it makes the SCADA architecture susceptible to cyber-threats [2], [13].

III. SECURITY THREATS FACED BY SCADA NETWORKS

Like any other system or network, a SCADA network faces the following threats [1], [12].

- Loss of availability can cause power outages and can have a negative impact on the efficiency of power supply. This condition may have a cascading effect in the physical domain. Thus, achieving availability as a security goal should be one of the primary objectives of a SCADA network.
- Loss of integrity is a scenario when the attacker modifies the data, and thus, the receiver receives the changed data. This type of scenario is achievable by launching a Man-in-the-Middle attack, which can further result in malware injection and IP spoofing.
- Loss of confidentiality can be achieved by eavesdropping on a channel. It leads to the loss of privacy and stealing of data as private data is exposed.
- Repudiation is where the sender denies they have sent the data at that time.
- Slowloris, GoldenEye for operating system Kali Linux.
- And, another tool named Low Orbit Ion Cannon (LOIC) [28]
- Lack of authentication in the Distributed Network Protocol 3.0 (DNP 3) used in SCADA systems which can lead to an impersonation attack [14].

IV. ATTACKS ON SCADA NETWORKS

The usage of Internet connectivity, cloud computing, wireless communications, and social engineering on SCADA networks have made its architecture vulnerable [1]. One of the main reasons for the vulnerabilities in SCADA is the lack of strong encryption and real-time monitoring.

Attacks can occur at all layers from the supervisory level to the field instrumentation level [15]. The most common attacks are outlined in Table 1A and 1B [15]–[19].

They can also be categorized based on attacks on hardware, software, and network connection [15].

- *Attack on hardware:* This is a scenario where the hacker gets unauthenticated access to the units and tampers with them or their functions. The primary challenge in securing hardware is access control. For example, the doorknob-rattling attack [15] as explained in Table 1.
- *Attack on software:* The SCADA system utilizes a variety of software to enhance its efficiency by fulfilling the functional demands. However, due to poor implementation, it is vulnerable to SQL injection, trojan horse and buffer overflow. These are a few examples of attack on software [15].
- *Attack on network connection:* The attack on communication stack can be on the network layer, transport layer, and the application layer. Figure 2 gives a classification of attacks based on the layers of the Open Systems Interconnection (OSI) model and maps them to the violation of security goals, namely, confidentiality, integrity, availability, and non-repudiation [15].

V. POSSIBLE ATTACK USING QUANTUM COMPUTING

A. QUANTUM COMPUTER

Traditional computers are the digital electronic computers which encode information in bits, where each bit can be 0 or 1. They execute algorithms on bits using simple digital logic operations such as AND, OR, and NOT [33]. Instead, quantum computers encode information in qubits which are generated using atoms as digital bits [34]. The value of qubits is based on the rules of modern physics: superposition and entanglement principle. According to the superposition principle, each qubit can represent 0 or 1 or both at the same time. Entanglement occurs when two superposed qubits are allied with each other [34], [35]. Therefore, the number of qubits is directly proportional to the number of states held by the set of qubits [35], [36]. These two principles make quantum computing way faster than traditional computing.

A quantum algorithm was proposed to solve a binary maze problem [37]. Each line has one input and two outputs. The quantum algorithm attempted all the paths at the same time, and therefore, it solved the problem at extreme speed. Whereas, solving the maze problem was hard for a traditional computer since the size of the problem was doubling each time. For example, a 1000 step binary maze has 2^{1000} outcomes, and this took more time in the case of traditional approach [37].

TABLE 1. A. Standard attacks on SCADA networks.

Attacks	*Description of the attack*	*How can the attack be launched?*	*Few Tools that can be used to launch the attack*
Eavesdrop	It can be of two types: Passive eavesdropping and Active eavesdropping[20] .	The communication network can be wired or wireless. By accessing the network between the MTU and sub-MTUs or RTUs, the invader can install eavesdropping equipment in the network [21].	Wireshark, tcpdump and, dsniff [22].
Man-in-the-Middle (MiM)	This occurs when the attacker is in between two units and fetches the private information. The most common MiM attacks are the following [20]: Session Hijacking network server, IP Spoofing and Replay attack.	In MiM attack, the intruder monitors the traffic and injects abnormal data during the transmission and sends it to the receiver [21]. In case of a successful session hijacking and IP spoofing, it takes over the session and maintains the connection. The spoofing helps the attacker to go undetected [23].	Ettercap, SSLStrip and, Evilgrade [24].
Masquerade	The attacker uses a fake identity to pretend to be a legitimate user and steals information from the system or the network.	By launching IP Spoofing and a brute force password attack, they can use stolen passwords and logins to gain unauthorized access [21].	Ettercap, Arpspoof and Brutus[24].
Virus and worms	A malware is a malicious software or a program that corrupts the data stored in the computer. They can also lead to Distributed Denial of Service attack. Virus and worms are types of malware [25].	The intruder can send a file containing malicious code to the MTU after launching MiM or masquerade attack. For example, the virus or worm can spread through sending e-mail attachments, web link and peer-to-peer file sharing networks [25].	Any malicious code which is self-replicable and attached to .exe file in the device [25].
Trojan Horse	This is a type of malicious program disguised as a harmless file. However, unlike a virus, a trojan horse is not self-replicable. Therefore, hackers use social engineering tactics to transfer this type of virus [26].	After launching IP Spoofing or social engineering, the intruder can inject innocent looking malicious and executable code and send it as a web link or a free download to the target system. Thus, the hacker can gain access and hack the control systems [26].	Social engineering. For example, web links offering free software download.
Denial of Service (DoS)	This is a type of attack where a legitimate user is denied access to a resource. It attacks the availability requirement of a network [27].	An infected RTU by virus or worm can send random IP packets to the MTU and thus consume network bandwidth. It further leads to resource starvation.	• Slowloris, GoldenEye for operating system Kali Linux. • And, another tool named Low Orbit Ion Cannon (LOIC) [28]

D-wave, a quantum computing company, launched its first commercial quantum computer named D-Wave One in 2011, which is being used by National Aeronautics and Space Administration (NASA) for in-depth space exploration. By 2013, they increased the number of qubits and released the D-Wave Two system. Google is also planning to use a quantum computer for big data mining [35].

TABLE 1. B. Standard attacks on SCADA networks.

Attacks	*Description of the attack*	*How can the attack be launched?*	*Few Tools that can be used to launch the attack*
Fragmentation	Fragmentation attack is a type of DoS leading to unavailability of resource [29][30].	It involves sending of over-sized datagrams. In this type of attack, the sizes of the sent datagrams are greater than network's maximum transmission unit [30].	Tools used to launch DoS attack can be used for Fragmentation attack.
Cinderella	The objective of this type of attack is to expire the security software license.	The hacker disguises their ID as a legitimate user and gains access to system by using a brute-force attack. Then the internal network clock is changed to expire the security software prematurely, thus increasing the network vulnerability [31]. Attackers can use the tools that are used to launch masquerade and brute-force attack.	For example, Ettercap for masquerade [32]. Ncrack, Hydra and Hashcat for brute-force attack [32].
Doorknob rattling	The type of attack when the failed attempts of a brute-force remains hidden from the detection system of the network [15].	At first the attacker will launch masquerade attack. Then, they try to attempt a random combination of username and passwords repeatedly on different devices to gain access. So, this leads to a few failed attempts. If the failed attempts are going undetected, this kind of attack can be successful [15].	• Ettercap for masquerade [32]. • Ncrack, Hydra and Medusa for brute-force attack [32].

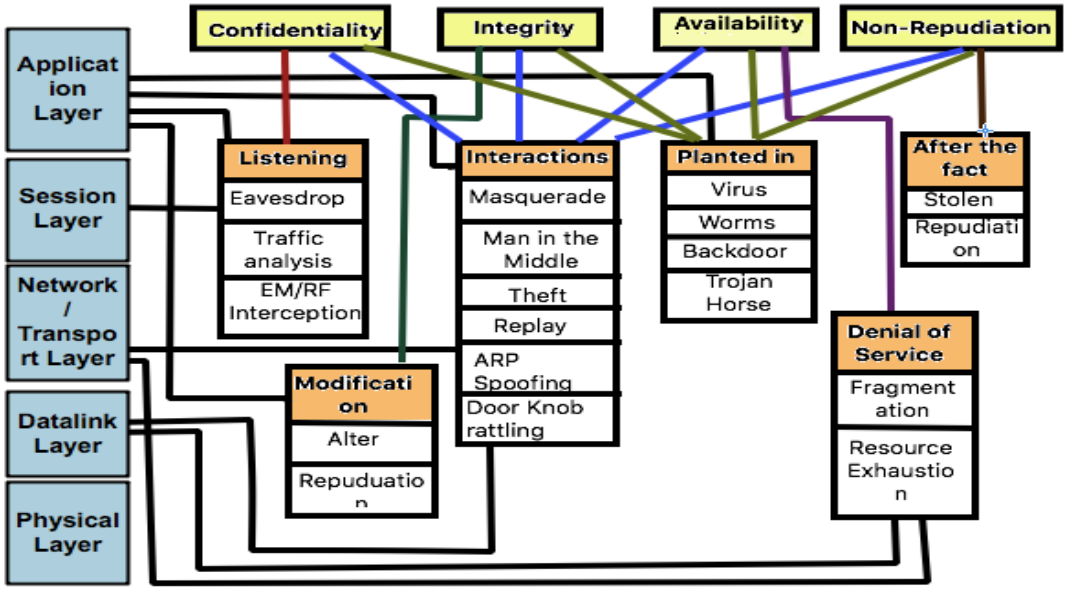

FIGURE 2. Classification of SCADA attacks in terms of security requirements and OSI layers.

B. BRUTE FORCE ATTACK BY USING A QUANTUM COMPUTER

The capacity and speed of quantum computer for solving mathematical problems make them a threat to traditional security schemes. All the encryption schemes are derived from mathematical logic. Cracking these schemes may be possible for quantum computers [38], [39]. One such problem is Elliptic curve cryptography (ECC or ECDSA).

TABLE 2. Steps in Shor's Algorithm.

Section 1: CLASSICAL PART	
Step 1:	Select a random positive integer m such that m<n. Then, calculate gcd(m,b) using the Euclidean algorithm. If gcd is not equal to 1, a non-trivial factor is obtained. Thus, the algorithm ends. Otherwise, go to Step 2.
Section 2: QUANTUM PART	
Step 2:	Calculate the period P of the sequence: x mod n, x^2 mod n, x^3 mod n, …
Step 3:	If p is odd, return to step 1. If p is even, go to step 4.
Step 4:	$\left(m^{p/2}-1\right)^2 = m^p - 1 = 0 \; mod \; n$, since p is even. If $m^{p/2} + 1 = 0 \; mod \; n$, then return to step 1. Else, go to step 5.
Step 5	Calculate $result = gcd\left(m^{p/2}-1, n\right)$ using the Euclidean algorithm.

Using Shor's algorithm, a quantum computer can launch a brute force attack and crack ECC in a brief time [39].

Shor's algorithm is a quantum algorithm for factorizing a number [40]. It implies that any public key cryptography can be easily cracked. The algorithm has two sections as follows [41]. Table 2 shows the steps.

- The classical computer can compute Section 1 in Table 2. It reduces the factoring problem to an order finding problem using the Euclidean algorithm. The Euclidean algorithm is a fast scheme to calculate the greatest common divisor (gcd) of two integers [42].
- Section 2 is the quantum part which used order finding algorithm. It finds the period of the function using the Quantum Fourier Transform (QFT).

In step 2, to calculate the period of the function based on the series, Quantum Fourier Transform (QFT) is used. Using QFT increases the speed of the algorithm by evaluating the function at all points simultaneously [41]. The QFT is a linear operator when applied to any state of qubit transforms it into another state. In other words, it is applied to the vector of amplitudes of a quantum state. [43] For example, if QFT operates on a quantum state X, then it transforms it into a quantum state Y.

$$X : |x> = \sum_{i=0}^{N-1} x_i |i>$$

$$Y : |y> = \sum_{i=0}^{N-1} y_i |i>$$

The QFT refers to (1).

$$y_{k=1/\sqrt{N}} \sum_{j=0}^{N-1} x_j \omega_n^{jk}, \quad k = 0, 1, 2, 3, ..., N-1 \qquad (1)$$

where,

$\omega_n = e^{\frac{2\pi i}{N}}$ and is a primitive N^{th} root of unity, N is the length of vectors such that $N := 2^n$ [43].

Existing security standards and schemes are based on traditional cryptography such as Advanced Encryption System (AES), Elliptic-curve cryptography (ECC), and Secure Hash Algorithm (SHA). Therefore, they are vulnerable to quantum attacks. The transformation of quantum computing from theory to practice in the recent past has not only brought with its potential advantages but also increasing threats [38], [39].

VI. EXISTING SCADA SECURITY SCHEMES

An attack on a SCADA system may have many adverse effects. Due to this reason, organizations and researchers have been putting much effort into developing standards, protocols, and security schemes. The existing security schemes can be categorized based on: current standards, detection of SCADA attacks, and prevention of SCADA attacks.

Classification 1: Current standards can be divided into two categories: Standard Providing Guidelines and Standards acting as crypto-suites. These standards are used in practice depending on the particular industry's requirements. However, the mechanisms of thwarting attacks in the standards are either not clearly discussed or, are not strongly secure.

Thus, to add more security in the existing standards for SCADA, many researchers have proposed novel schemes. In this paper, the academic effort has been further classified into two following categories:

Classification 2: Detection of SCADA attacks consists of all the proposed intrusion detection systems for SCADA networks. The main objective is to overcome the lack of availability that is one of the security requirements.

Classification 3: Prevention of SCADA attacks consists of all the key management protocols proposed to secure the communication between the units.

A. CURRENT STANDARDS

Throughout the world, over 10 countries have proposed more than 40 standards and protocols. The available standards are described as follows [44], [45]. Few of the standards provide guidelines to secure an infrastructure from physical and cyber-attacks. Furthermore, the remaining standards include a major part that acts as a crypto-suite. In this paper, they are categorized into two: 1) Security guidelines-based Standards and 2) Crypto-suites based Standards.

1) SECURITY GUIDELINES BASED STANDARDS

a: IEEE 1402

Institute of Electrical and Electronics Engineers (IEEE) 1402-2000 is an IEEE Guide for Electric Power Substation

Physical and Electronic Security. The Power Engineering Society/Substations of IEEE sponsors the standard. It discusses security issues caused by human intrusion at power supply substations along with methods and schemes to mitigate physical and electronic intrusions [46].

In the guide, the intrusions are classified into four main categories: pedestrian, vehicular, projectile, and electronic intrusion [45], [46]. The paper also categorizes the security methods used at power control substations [45], [46].

The computer security systems include using passwords, dial-back verification, selective access, virus scans, and encryption. The guide also explains the substation security plan and categorizes it into three questions: Why is the plan required? Who may monitor the plan? What security methods are needed? According to the guide, these are the main criteria on which the security plan should be executed [45], [46].

IEEE 1402 does not solely focus on the information security. Rather, it gives a broad and general guideline for physical as well as cyber security.

b: ISO 17799 – "INFORMATION TECHNOLOGY – CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT"

The International Organization for Standardization (ISO) published ISO 17799 in December 2000. The ISO 17799 is an international guideline for monitoring information security management of any organization [45]. The standard refers to information as an asset that is valuable to industry. The main objective of the standard is to protect the asset by preserving confidentiality, integrity and availability [47].

ISO 17799 provides a structured guideline to control security and perform security risk assessment. It provides the following benefits [47].

- Organizational Security
- Asset Classification
- Personnel security
- Physical and environmental security
- Network management that involves media handling, backup schedules and logging.
- Access control
- Maintenance of cryptographic controls and system integrity.

ISO 17799 is the one standard that is dedicated to Information Security Management. However, ISO 17799 does not provide any evaluation methodology of a security scheme. It also does not deal with the requirements of functional and security components in an organization. ISO 15408 was developed in 2004 to alleviate some of these issues.

c: ISO 15408 – "COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION"

ISO developed the ''Common Criteria got Information Technology Security Evaluation'' in January 2004 [45]. The criteria are used to evaluate various functional classes as listed as follows [48].

- Audit
- Communication
- Cryptographic support
- User data protection
- Identification and authentication
- Security Management
- Privacy
- Security functions protection
- Resource Utilization
- Access
- Trusted path/channels

It has three sections. ISO 15408-1 provides the introduction and general model. ISO 15408-2 provides the functional security components, and ISO 15408-3 discusses the security assurance components [45].

However, the report does not focus on the utilization of cryptographic designs in communication and control applications [45]. Furthermore, it does not uniquely focus on the need of physical security in SCADA structure.

d: NERC SECURITY GUIDELINES – "SECURITY GUIDELINES FOR THE ELECTRICITY SECTOR: PHYSICAL SECURITY"

On June 14, 2002, North American Electric Reliability Council (NERC) releases a version 1.0 of NERC Security Guidelines discusses physical and cyber security along with the general practices for protecting the power supply infrastructure systems [45].

The general guideline focuses on the need of the physical security to maintain the integrity and availability of electric power systems, for example, promoting and deploying the security standards and procedures, periodic evaluation of the security measures, monitoring and reporting threats to the operating section, and quick recovery of the delivery services if damaged [49].

The report also guides to follow a strategy 'Protection in Depth'. The objective of this strategy is to delay the progress of an attacker. This buys time to the organization to defend and recover against the attack [49].

However, the security guidelines focus mainly on physical security. In 2003, NERC produced a report that deals with cyber security parameters.

e: NERC 1200 – "URGENT ACTION STANDARD 1200 – CYBER SECURITY" AND NERC 1300 – "CYBER SECURITY"

NERC developed a temporary standard named ''Urgent Action Standard 1200'' for setting a set of security requirements for the energy industry infrastructure. NERC adopted this standard on August 13th, 2003 for a one-year period and later, it extended the standard till August 2006 [45].

NERC developed NERC 1300 to replace NERC 1200 by addressing the security requirements and recommendations mentioned in NERC 1200 [45], [50]. NERC 1300 focuses on both physical and cyber security. The report has a section that implies that a responsible industry should follow the System Security Management to prevent any malicious

TABLE 3. Concerns addressed in API 1164.

API 1164	*Concerns /Areas Addressed*
First edition	Access control
	Secure communication
	Classification of data distributed
	Physical complications for example disaster recovery
	Operating systems
	Network Designs
	Management systems
	Field devices configuration and local access

cyber activity. The Management section mainly involves the following security measures [50]:

- Account and Strong Password management.
- Using security patch manager to check security updates.
- Using anti-virus monthly.
- Performing vulnerability assessment at least annually.
- Preserving and auditing system logs quarterly.
- Using operating status monitoring tools.
- Back-up of information on computer systems.
- Disabling unused ports.

NERC 1200 and NERC 1300 are security guidelines for the energy industry infrastructure. They do not provide security features for the oil and pipeline infrastructure. Therefore, the American Petroleum Institute developed a standard that provides security guidelines for control systems of oil and pipeline systems.

f: API 1164 – "SCADA SECURITY"

API 1164 has three editions. The first edition was released in September 2004. It specifies guidance to secure the SCADA system used in the oil and pipeline infrastructures [45], [51]. It addresses the following issues mentioned in Table 3 [45].

The second edition is the API – ''Security Guidance for the Petroleum Industry.'' Oil and gas infrastructures utilize this standard to prevent terrorist attacks [45].

The American Petroleum Institute and the National Petrochemical and Refiners Association mutually developed the third edition named API- ''Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries''. It is utilized for evaluating various kinds of threats, vulnerabilities, and aftereffects of terrorist attacks [45].

The above-discussed standards are general guidelines to protect the infrastructure of an organization. They do not involve any in-depth discussion of cryptographic algorithms or any technical methodology to detect or protect from any attack. However, the following standards use crypto-suites.

2) CRYPTO-SUITE STANDARDS

a: IEC 62210 – "DATA AND COMMUNICATION SECURITY"

In 1999, IEC 62210 was developed by the International Electrotechnical Commission (IEC) as the report of IEC TC 57 AHWG06. Later, AHGW06 was systemized into Working Group (WG) 15 upon Data and Communications Security. Later, it was published in 2003. The IEC TC57 WG15 developed the cybersecurity standards for power control system communications [45].

The working group report describes the security process for the power control systems which involves the corporate security policy, network security protocol, and the end to end application security. The security scheme was also utilized for encrypting communication in the network [45].

AHWG06 issued the report recommending establishing the following tasks [45]:

- Consequence analysis combined with ISO 15408
- Attention to the application layer
- Address key management
- Address end-to-end security

However, the above recommended tasks were challenging to resolve at that time [45]. Therefore, the following standard was developed as an extension of IEC 62210.

b: IEC 62351 – "DATA AND COMMUNICATION SECURITY"

International Electrotechnical Commission (IEC) developed IEC 62351 to address the deficiency in IEC 62210. The standard is classified into as shown in Table 4 [45], [52]:

Using TLS security, IEC 62351 provides defense mechanisms against various attacks including spoofing, message replay attack and to some extent Denial-of-Service (DoS) attacks. However, it involves simple encryption schemes.

Immediately after the 9/11 attack, the American Gas Association (AGA) decided to improve the security mechanism which can protect SCADA communication from malicious users. The primary purpose of the standard was to develop a security scheme which can provide security as well as save time and computation cost [44].

c: AGA-12 – "CRYPTOGRAPHIC PROTECTION FOR SCADA COMMUNICATIONS GENERAL RECOMMENDATIONS"

Traditional security protocols used in SCADA systems such as IEC 60870, DNP3, IEC 61850 and Modbus lack proper security services [14]. However, the new protocol AGA-12 provides security features to the SCADA systems. It uses cryptographic suites to secure the wireless communication between field devices and the MTUs [14], [45]. The steps in AGA-12 is described in Table 5 [44].

AGA-12 provides confidentiality, integrity and authentication. However, it fails to provide availability. It does not defend against DoS attacks. Furthermore, AGA-12 uses RSA as the key management protocol which has been cracked recently [53].

Furthermore, the current standards including IEC 62210, IEC 62351 and AGA-12 fail to provide two main security requirements, namely, defense against DoS attacks and a strong key exchange protocol.

The aforesaid studies have research gaps that fail to address availability and secured communication channel. Therefore,

TABLE 4. Classification of IEC 62351.

Sections	*Schemes used*
Security for profiles including TCP/IP	It uses Transport Layer Security (TLS) for secure transactions over the internet. It provides confidentiality, integrity, and authentication.
Security for profiles including MMS	For Transport Layer which includes layer 1 to layer 4 of the OSI Reference Model, Transport Layer Security is used. The report describes a set of protocols, how to use them, and the requirements for Application Layer which includes layer 5 to layer 7 of the OSI Reference Model.
Security for derivatives (DNP 3.0)	For network versions which run over TCP/IP, the standard uses TLS encryption. For the serial version, it uses an authentication mechanism named Hashed Message Authentication Code (HMAC).
Security for IEC 61850 peer-to-peer profiles	For client/server, the standard utilizes TLS and MMS. For Generic Object-Oriented Substation Events (GOOSE), it uses analog and digital multicast.

researchers have proposed schemes to overcome these limitations in SCADA networks.

In this paper, the proposed schemes are categorized based on limitations addressed.

- Detection of SCADA attacks: It involves the security schemes addressing the availability issue in the SCADA networks. Most of the schemes are based on machine learning algorithms.
- Prevention of SCADA attacks: The discussed schemes address the key exchange and management issue in SCADA networks.

B. DETECTION OF SCADA ATTACKS

Traditional standards and Intrusion Detection Systems (IDSs) such as firewalls used in SCADA are not strong enough to cope up with emerging attacks [5]. To increase the immunity in SCADA, machine learning algorithms, such as Naïve Bayes, Random Forest, C4.5 decision tree algorithm, Support Vector Machine, etc. are used to detect intrusion in the network [54].

1) RULE-BASED INTRUSION DETECTION SYSTEM FOR SCADA NETWORKS

The proposed IDS uses a rule-based in-depth protocol analysis along with a Deep Packet Inspection (DPI) method. The model establishes a new set of intrusion recognition rules. The rule-based scheme contains two sub-schemes; namely, signature-based detection and model-based detection [55]. Signature-based detection utilizes a blacklist approach and is used for detecting a more significant amount of false spontaneous messages, unauthorized commands between nodes, and buffer-overflow. The model-based detection builds a model based on an in-depth analysis of the protocol. The created models portray the expected behavior of the protocol. It uses protocols and traffic pattern to generate the expected behavior [55]. It can detect known attacks as well as its source. Using the proposed IDS along with IEC/104 protocol, unknown attacks may be diagnosed in the SCADA network [55]. However, the proposed rule-based IDSs do not ensure the detection of novel or unidentified intrusions that pass through traditional IDS in open access networks.

2) NETWORK ANOMALY DETECTION FOR M-CONNECTED SCADA NETWORKS

Usually, IDSs and security schemes are for SCADA systems using open access networks. However, there is no intrusion detection mechanism for closed and isolated SCADA networks. This kind of SCADA architecture is referred to as an 'm-connected' SCADA network [56].

The model uses a dynamic detection for detecting intrusions with a packet logger and packet sniffer followed by a pattern matching algorithm. It generates new rules and stores them in a database. It further uses new rules for the next round [56]. The proposed scheme is based on rule-based intrusion detection and further research is needed for accurate implementation [56]. Furthermore, the scheme does not guarantee detection of unidentified attacks.

3) L_P - NORMS IN ONE-CLASS CLASSIFICATION FOR INTRUSION DETECTION IN SCADA SYSTEMS

In 2014, an intrusion detection system was proposed to detect abnormal activity in the network that is not detected by the traditional IDS or firewalls. It uses a machine learning based on the one-class classification algorithm for live detection of unnoticed cyberattacks [5].

The paper analyses two approaches: the support vector data description (SVDD), and the kernel method [5]. It uses kernel principle as non-linear methods to detect patterns, and interdependencies within the real-world data. SVDD maps the data to the subspace which is optimized for one-class classification. The paper concludes that the proposed method showed the highest error detection and the lowest false alarm rates after conducting tests on a real dataset with several cyber-attacks [5].

TABLE 5. Steps in the AGA-12 standard.

Steps	*Sub – Step(s)*	*Description*
Perform system security audit	• System-wide network audit must be done. • Following the audit, risk assessment is required. • Security goals must be set.	During risk assessment, cost-benefit analysis is done. When benefits outweigh the cost, the AGA-12 is implemented in the SCADA network.
Agreement of Hardware and Software Modules to be used	• Guidelines are provided for testing of hardware and software modules. • The guidelines must also provide the cryptographic process agreement.	The algorithms which are accepted and permitted by National Institute of Standards and Technology (NIST), AGA 12 are as follows. • Advanced Encryption System (AES) Encryption with a key length of minimum 124 bits. • Rivest-Shamir-Adleman (RSA) with a key length of minimum 1024 bit. • Elliptic Curve Digital Signature Algorithm (ECDSA) with a key length of minimum 160 bits. • Secure Hash Algorithm (SHA-1).
Performing a post-deployment security audit	• Implement AGA-12 • Post Implementation audit	After implementation, it involves a detailed audit throughout the network. If any security threat is detected, the necessary compliance level should be approached.

4) ONE-CLASS SUPPORT VECTOR MACHINE (OCSVM)

In 2014, Maglaras and Jiang [57] developed a One-Class Support Vector Machine model for detecting new attacks in the SCADA network. The proposed model addresses the following issues:

- The research community has developed many IDS algorithms for SCADA networks. Most of them are rule-based algorithms which make them incapable of detecting any new intrusions. In a real-time application, when any new anomaly is present, it fails to predict the behavior of the system [57].
- Other algorithms such as K-nearest neighbor (KNN), Hidden Markov models, and Support Vector Machines are used for detecting intrusion. However, they require learning of expected anomaly. Thus, these schemes may be sensitive to noise present in the training dataset [57].
- Negative selection algorithms can fail in the case of real-time application because of enormous diversity in real time data [57].

The proposed IDS is an algorithm to detect anomaly without any labeled data for training. Network traces train the OCSVM model without the use of open access networks. These features help the proposed IDS to perform in real time. Table 6 outlines the steps in the detection process [57].

However, the OCSVM model does not manage false positive results.

TABLE 6. Steps to detect intrusion using OCSVM.

Step	*Description*
Step 1	Data analysis.
Step 2	Attributes in the network traces are extracted. The attributes, rate. and packet size, are used to train the model.
Step 3	Integration of OCSVM Module.
Step 3.1	The network traces data, and the extracted attributes are used to train and generate the model.
Step 3.2	The model is tested for real-time anomaly detection.
Step 3.3	The detected anomalies are classified based on the severities.
Step 3.4	The main correlator is alarmed regarding the detected anomalies.

5) OCSVM MODEL COMBINED WITH K-MEANS RECURSIVE CLUSTERING FOR INTRUSION DETECTION IN SCADA SYSTEMS

One-class classifiers suffer from false positives and overfitting. False positive is a scenario when the IDS detects abnormal behavior but there is no intrusion in real. Overfitting is a case when the model begins to learn the details and errors in the training data. These two factors decline the performance of the model on the new data [58].

To address these two issues, Maglaras and Jiang [58] developed an intrusion detection model to detect the malicious network traffic in SCADA. The model includes the One-Class Support Vector Machine (OCSVM) with Radial Basis Function (RBF) kernel and recursive k-means clustering [58]. OCSVM is an extension of support vector machines and is used to detect the outliers in the data. The k-means clustering algorithm is used to cluster the outliers and sort them with two clusters. OCSVM obtains two values, namely, maximum and minimum negative value [58]. The cluster which is near to minimum negative value represents severe alerts, and therefore, the cluster is used as input when there is recalling of k-means clustering. This step is repeated till the after-k means clustered are in a single cluster. After the completion of K-OCSVM phase, the model distributes the severe alerts among the nodes in the SCADA structure [58].

6) A HYBRID MODEL FOR ANOMALY-BASED INTRUSION DETECTION IN SCADA NETWORKS

Usually, intrusion detection systems when deployed in real time lead to high computational and time costs. These two factors affect the performance of a SCADA network [16].

In 2017, anomaly-based intrusion detection was developed using a feature selection model after removing redundant data. Irrelevant data can affect the efficiency of SCADA systems. This proposed scheme is time-saving, has low computational complexity and has 99.5% accuracy of detecting specific-attack labeled [9]. At first, the J48 classifier is used to train the dataset and then, to develop the model, Bayes Net classifier is utilized. The proposed model is tested on a database with three types of labeling as follows [9].

- Case 1: binary-labeled
- Case 2: categorized-labeled
- Case 3: specific attack labeled

The above-mentioned scheme focuses on the availability limitation in the SCADA networks. The schemes propose novel IDSs that detect any abnormal network behavior, which can lead to DoS attacks. However, the scheme fails to secure the communication channel. The following section on the prevention of SCADA attacks focuses on securing the communication channel with novel key exchange and management schemes in SCADA networks.

C. PREVENTION OF SCADA ATTACKS

The existing standards use vulnerable key management protocols that do provide a strong secure communication channel.

Encryption and key management are crucial in communication between nodes in a SCADA architecture. Key management schemes developed for SCADA can be categorized into two, namely, centralized key distribution and decentralized key distribution [6]. They can also be categorized into symmetric key cryptography, asymmetric key cryptography, and hybrid key cryptography [7]. In this paper, another classification concerning self-healing property is added.

1) SYMMETRIC KEY CRYPTOGRAPHY

a: SCADA KEY ESTABLISHMENT(SKE)

SKE categorizes SCADA communication into Controller - Subordinate (C-S) which uses symmetric key cryptography and Peer to Peer (P-P) which uses public key cryptography. The controller is the sub-MTU or sub-MSU, and the subordinate is the RTU. Peer-to-peer communication is between two sub-MTUSs or two RTUs [6].

For C-S communication, SKE uses four kinds of keys: Long-Term key, General Seed Key (GSK), General Key (GK) and Session Key (SK). The Long-Term Key (LTK) is manually distributed between the controller and subordinate [59]. The controller stores the GSK and is used by Cryptographic Authority (CA) to produce GK. By using two keys, GSK and LTK, the GK is generated and is then shared between the controller and the subordinate. While transmitting GK, it is encrypted by LTK. The session key is generated by using GK, sender's identity and TVP (Time-Varying Parameters). TVP field involves timestamp and a sequence number [6], [59].

For peer-to-peer communication, SKE uses four different keys: Cryptographic Authority Public Key (CAPK), Public key Signature Key (PKSK), Common Key (CK) and Session Key (SK). The CAPK is shared among sub-MTUs while the PKSK is shared among the sub-MTUS, MTU and Cryptographic Authority (CA). The common key is generated by following a key exchange algorithm. The methodology to generate session key is the same as that of C-S communication. The session key is used to encrypt the messages transmitted [6], [59].

However, the RTU to RTU communication is not directly allowed. Since the communications are treated differently in different conditions, it increases the overall overhead and complexity. Furthermore, the long-term keys are managed manually [6], [59].

b: SCADA KEY MANAGEMENT ARCHITECTURE (SKMA)

In comparison to SKE, the implementation of SKMA architecture is more simplified. The architecture establishes the key exchange protocol among the Key Distribution Center (KDC), and any two nodes. The long-term keys are accumulated only on the required nodes and on the KDC which is the third party. The design uses three main keys [12], [59]:

- Long-Term Node-KDC key is used to yield keys for communication and is manually shared between a node and the KDC.
- Long-Term Node- Node key is distributed between the nodes that require to communicate with each other.
- Session Key is used for encrypting the information transmitted from one node to another. Once the key establishment is completed, the session key is generated by using pseudorandom number function, nonce-key and a timestamp [12].

The SKMA scheme does not use GSK. The key exchange in SKMA only happens when a new node joins the SCADA network [12].

Nevertheless, the SKMA does not provide the following security features [59].

- SCADA systems mostly use broadcast communication. However, the SKMA cannot provide such a mechanism.

This protocol does not provide any confidentiality and integrity.

c: LOGICAL KEY HIERARCHY (LKH)

To address one of the issues, the LKH protocol was developed. LKH protocol provides secure broadcast communication [6] [7]. It is based on an architecture of the logical tree of keys [12]. It maps all the nodes of the SCADA network as the leaves of a structure tree. Each node stocks the entire symmetric keys from the root to its leaf. When a node leaves or joins, the node keys from its leaf to the root is updated so that the security of the network is preserved [12]. For example, Figure 3 [12] explains the mechanism when a node joins the network.

d: ADVANCED KEY-MANAGEMENT ARCHITECTURE (ASKMA)

To enhance the efficiency of SKMA and LKH, the ASKMA was proposed [6]. It provides both message broadcasting and secure communication. It also keeps a minimal load on the resource-constrained nodes [6], [12].

In ASKMA, the LKH protocol is used by Choi *et al.* [12] for message broadcasting in 2009. The nodes of the SCADA networks such as RTUs, sub-MTUs, and the MTU are organized in two tree structure: binary tree and n-ary tree. The MTU to sub-MTU follows a binary tree structure whereas the sub-MTUs to RTUs follows n-ary tree structure [6].

The ASKMA protocol evenly spreads the computations to the sub-MTUs and MTUs which are high power nodes and keeps a minimal load on the low power nodes like RTUs. Therefore, the nodes are arranged logically in a tree structure, n-ary or binary tree, depending on their computational power [12].

When a new node is added to the SCADA network, the ASKMA follows a Join Protocol. Any key received by a new RTU must be independent of any existing keys in the nodes of the tree. It preserves backward confidentiality. When a new node joins the tree, the KDC updates all the keys from its leaf to the root on the freshly joined RTU's path. It uses a hash function for renewing the keys. The Join Protocol has the following steps [12].

Step 1: The KDC renews all $K_{i,j}$ to $K^{/}_{i,j}$ where $K^{/}_{i,j} = H(K_{i,j})$.

Step 2: In case the RTUs have keys belonging to $K_{i,j}$, each RTU updates their key $K_{i,j}$ to $K^{/}_{i,j}$.

Step 3: With K_m, the KDC encrypts all $K^{/}_{i,j}$ and transmits the encrypted information to the newly joined RTU which is N_m.

When a node leaves the SCADA network, the ASKMA follows a Leave Protocol. Similar to the Join Protocol, all the keys throughout the key path updated with new keys [12]. However, the leaving node N_m should not be able to use the updated keys. This makes the Leave Protocol a little more complicated than Join Protocol. The following are the steps of Leave Protocol [12].

Step 1: The KDC removes the RTU which is parting.

Step 2: It then updates the remaining keys by executing a key generation algorithm such that the leaving RTU does not know the updated key. Consequently, the departed RTU is unable to compute the new keys.

Step 3: Each RTU updates its keys by using the hash function.

Step 4: If the RTUs are unaware of their sibling keys, KDC encrypts the new keys and sends them to those RTUs.

Step 5: The departed node knows all the ancestor keys of the sibling RTUs. Therefore, the KDC encrypts all the updated keys with sub-MTU's private key and transmits to the sub-MTU. The sub-MTU encrypts the received keys with the child RTU's key and then sends it to each child RTU.

ASKMA supports broadcast and multicast communication. However, it does not offer efficient multicast communication. To solve this issue, ASKMA+ was proposed [6]. By reducing the number of stored keys, it provides efficient multicast and broadcast mechanism [6]. However, ASKMA and ASKMA+ do not address the availability issue in SCADA [6].

2) HYBRID KEY CRYPTOGRAPHY

a: HYBRID KEY MANAGEMENT ARCHITECTURE(HKMA)

To satisfy the availability requirement, Choi *et al.* [60] proposed a Hybrid Key Management Architecture (HKMA) which supports a replace scheme [60]. The scheme includes an operation of the replace protocol in case of compromised or broken main device. It uses a public key cryptosystem in MTU to sub-MTU communication which has high performance, and symmetric key cryptosystem in sub-MTU to RTU which has low performance. Thus, it reduces the number of keys to be stored in the MTU [60].

b: ADVANCE HYBRID KEY MANAGEMENT ARCHITECTURE(AHSKMA)

Rezai *et al.* [6], [61] proposed a scheme based on hybrid key management architecture to tackle the availability issue in SCADA networks and to increase the performance and security of HKMA. It follows ECC for MTU to sub-MTU communication. Since RTUs have limited computational resources, symmetric cryptography is used for sub-MTU to its RTUs communication. This scheme makes the architecture suitable for the environments with resource constrained devices and supports unicast, multicast and broadcast communications [61]. Figure 4 shows the mechanism of the protocol.

The Iolus [62] Framework is used while connecting the MTU and RTUs. The MTUs act as the Group Security Control (GSC) and the sub-MTUs act as the group security intermediary (GSI). The architecture consists of four

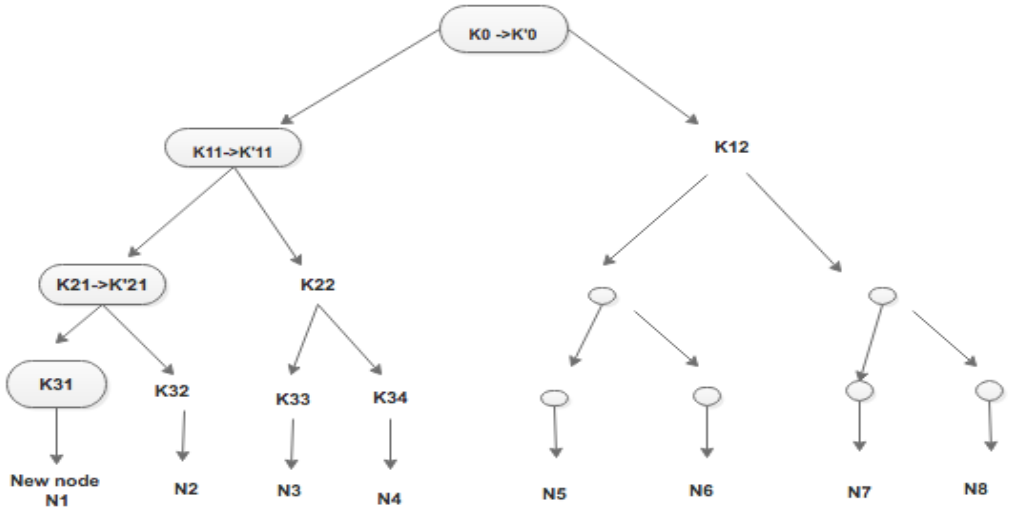

FIGURE 3. Update Mechanism of LKH protocol when a new node joins.

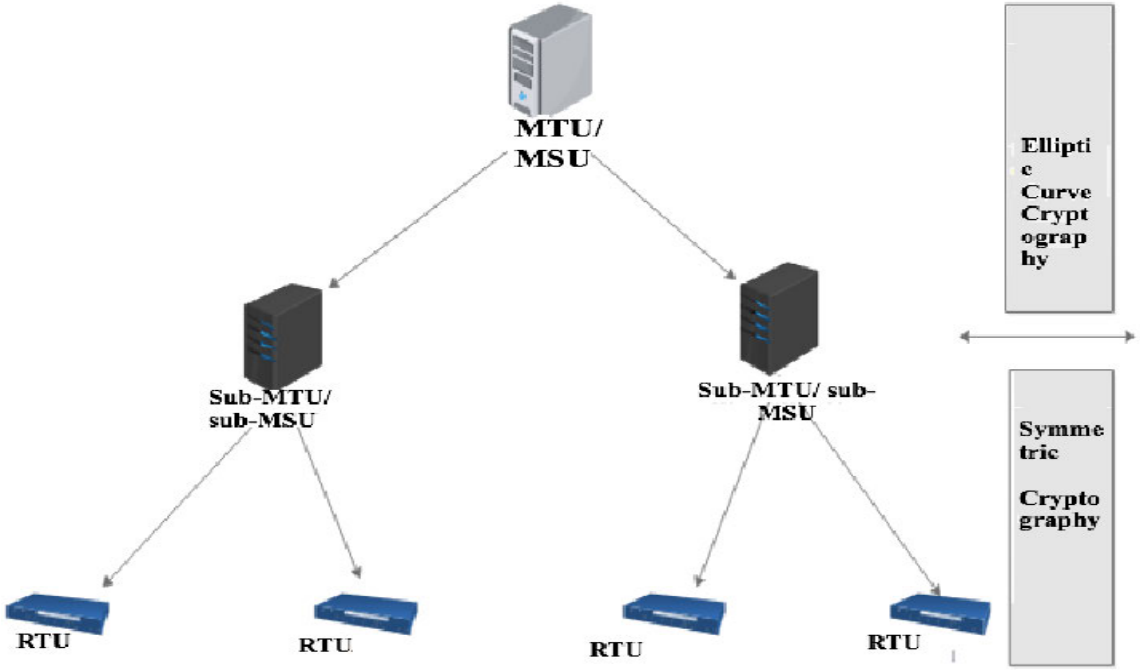

FIGURE 4. Mechanism of AHSKMA.

phases: Setup phase, Join Phase, Leave Phase and Replace phase [61].

a. **Setup Phase:** In the first phase, the group key is generated by the MTU and is shared with RTUs and IEDs.
b. **Join Phase:** Similar to LKH and AHSKMA, the MTU updates all the keys of the remaining nodes in the SCADA network as soon as a new node joins.
c. **Leave Phase:** This phase is also similar to the leave protocol of the AHSKMA.
d. **Replace Phase:** In case the MTU is damaged, it

is replaced by its backup device. Each MTU and sub-MTU has a backup device. While backing up the broken device, the Join phase and the Leave phase are performed concurrently.

The Replace Phase resolves the availability issue in SCADA networks. In this scheme, the session is produced using a hash function, a key, and TVP with a sequence number and timestamp [61]. So, HSKMA also guarantees the freshness of key along with availability.

Both HKMA and AHSKMA provides replace scheme to satisfy the availability requirement, but the affected devices stop working during the replacement. To solve this issue, LiSH+ was proposed [6], [63].

3) SELF-HEALING GROUP KEY DISTRIBUTION

a: LIMITED SELF-HEALING KEY DISTRIBUTION (LISH+)

LiSH+ is an efficient group key management scheme which utilizes a self-healing procedure having collusion resistance

capability and effective revocation [63]. The scheme involves five phases: initialization, rekeying, self-healing mechanism, the addition of new nodes, and reinitialization. It uses a bivariate polynomial to lower the storage burden from RTUs [63]. It also uses intrusion detection system to detect compromised and eliminate users. These features provided helps LiSH+ to enhance the security of SCADA networks [63].

However, the LiSH+ focuses on only two requirements: availability, and efficiency [63]. It does not focus on the authentication mechanism.

4) ASYMMETRIC KEY CRYPTOGRAPHY

a: ID-BASED KEY MANAGEMENT ARCHITECTURE

Lim [64] proposes an ID-based key management architecture (ID-KMA) based on pairing algorithm based on elliptic curves. The architecture addresses the issues of the public key cryptography with a digital signature. It involves fast and efficient session key establishment along with session key recovery protocol. It removes the concept of the digital certificate which minimizes the overhead.

The architecture involves the role of three units of SCADA: Key Management System (KMS), MTU and RTUs. The KMS is linked with the MTU, and the MTU is connected to the RTUs. The KMS communicates with RTUs through MTU [64].

The ID-based Key Management architecture uses four main keys [64] as described in Figure 5.

- **Emergency Key (EK):** This is a symmetric key stored in every component in the architecture: KMS, MTU, and RTUs. In case if the private key of each unit or master key of KMS gets compromised due to malicious attacks, the EK is used for key recovery or system restoration. Therefore, EK should be kept in a secure area.
- **Long Term Key (LTK):** It is an ID-based public and private keys of each node.
- **Update Key (UK):** It is a symmetric key distributed among the MTU and its RTUs. It is used to share the session key.
- **Session Key (SK):** The session key is shared among MTU and the RTUs. It is also shared between the RTUs. The SK is used to encrypt the communication.

The ID-based key management protocol is composed of four phases [64].

- **EK setup:** The EK is stored in each component of the architecture in advance.
- **Initialization:** The initialization has two stages. In the first stage, the KMS produces system parameters (SP) which are public and generates MTU's and RTU's LTK. The SK and LTK are encrypted with EK. The KMS shares the encrypted SP and LTK with the MTU. In the second stage, the KMS distributes a UK and LTK to each component so that the MTU can share an SK with RTUs. The first stage is LTK distribution and the second stage is the UK distribution.
- **RTU-RTU session key establishment**: This phase focuses on the secure communication between the RTUs with the usage of session key (SK) and initially shared update key (UK).
- **MTU-RTU session key establishment:** The session key is distributed among MTU and RTU to have a secure communication. The MTU sends a session key request to the RTU.
- **RTU-MTU session key establishment**: Similarly, the session key is established between MTU and RTU. The RTU sends a session key request to the MTU.

All the afore-mentioned key management protocols are based on traditional cryptography schemes which are vulnerable to quantum attacks [38]. Furthermore, public key algorithms tend to increase the computational and time cost [65].

Therefore, the following scheme named as Nth Degree Truncated Polynomial Ring (NTRU) is proposed to defend against quantum attacks.

b: NTRU CRYPTOGRAPHIC ALGORITHM FOR SCADA NETWORKS

The key management scheme is based on a faster and light-weight public key algorithm named NTRU cryptography [65]. The cryptographic algorithms in IEC62351 and AGA-12 have performance issues when apples to SCADA network security. They are time and power consuming [65], [66].

Due to various security and performance complexities of SCADA systems [66], [67] [6], NTRU was developed. It is a public key scheme based on lattice-based cryptography [68], [69]. The security of the cryptography depends on a hard problem known as Short Vector Problem [65], [68]. The encryption and decryption use polynomial operations which makes the system faster [65]. Therefore, it has better processing speed than traditional schemes and is suitable for real-time requirements of SCADA security [70].

The NTRU algorithm is also known as post-quantum cryptography and has been resistant to quantum attacks [65]. The scheme has two sub-algorithms, namely, NTRU Encrypt which is used for encryption, and NTRU Sign which is used for generating a digital signature. The scheme comprises of three phases [65]:

- **Key Generation and Certificate Creation phase:** In this phase, public and the private key of the RTU and its digital certificate is generated. For this, it uses a public key infrastructure. In this phase, other than RTU, two components play their roles. One, Local Key Store (LKS) and another, Certificate Authority (CA). The phase has the following steps [65].
  Step 1: The RTU generates a public key and private key using key generation algorithm. The algorithm uses algebraic structures of certain polynomial rings and is based on the Short Vector Problem. It then stores the generated key pair in the LKS.
  Step 2: The RTU then sends a request containing its public key to CA for generating a digital certificate. The CA in return creates a digital certificate and directs it to the RTU.

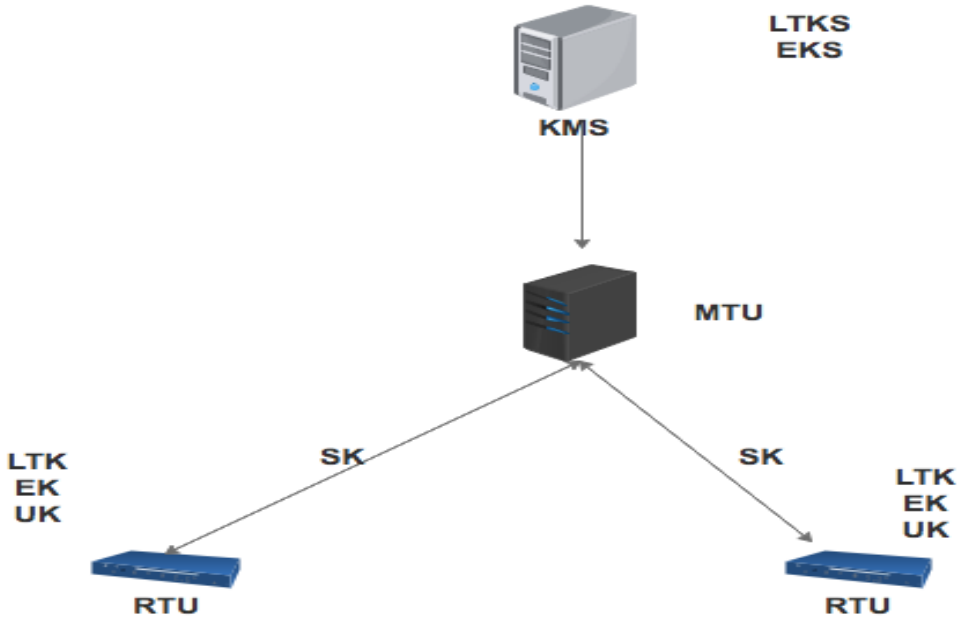

FIGURE 5. Architecture of ID-KMA.

- **NTRU Encryption:** In this phase, the RTU uses the receiver's public key, generated by the CA, to encrypt the messages. The messages are converted to a ring of truncated polynomials modulo. The receiver then decrypts the cipher using its private key.
- **NTRU based authentication:** In this phase, it is verified that the encoded message, which is in the state of a truncated polynomial ring, is validated. This phase uses a procedure built on a non-keyed hash function to ensure the integrity and authenticity of the message. The scheme creates a message digest by using the hash function. The message digest is then digitally signed by using the RTU's private key. Thus, it generates the digital signature. Therefore, the RTU sends the encrypted message and its digital signature to the receiver. The receiver uses its own NTRU private key to decode the message and generates the message digest (MD1) following the same procedure. The digital signature is then decrypted using the RTU's public key. The receiver gets the expected message digest (MD2). It then verifies whether MD1 and MD2 are equal or not. If they match, the signature is verified [65].

Even though NTRU is not yet vulnerable to quantum threats, a quantum computer can crack the algorithm using brute-force [71]. There are further challenges in post-quantum cryptography as follows [72].

- Need to improve the efficiency of the algorithm.
- Need to build confidence in the scheme.
- Need to improve the usability of the algorithm.

The existing standards have research gaps that have been addressed by the above-discussed security schemes. However, all the schemes are based on arithmetic operations. The emergence of quantum computers is proven to be beneficial as well as precarious to the cyber world. By launching a brute-force attack using Shor's or Grover's algorithms, these schemes can be broken. Therefore, there is a research gap in securing the SCADA networks from quantum attacks.

TABLE 7. Classification of current Standards.

Guideline based Standards	Crypto-suites based standards
IEEE 1402	IEC 62210
ISO 17799	IEC 62351
ISO 15408	AGA-12
NERC Security Guidelines	
NERC 1200	
NERC 1300	
API 1164	

VII. PRIMARY FACTORS USED FOR COMPARATIVE STUDY

The comparative analysis in this paper is based on the primary factors in each category. In case of current standards, the current standards are categorized into two classes as shown in Table 7. In this scenario, the primary factors used for comparison are as follows:

- Information Security Policy is a set of security rules governed by an industry that is imposed on the users of its system [73].
- Vulnerability and risk assessment are the processes where the weaknesses in a system are detected, analyzed and prioritized by the organization. The analyzed results are used to recommend security requirements in the system [74].
- Information security infrastructure is a set of security rules to protect only critical fundament such as airports,

TABLE 8. Comparative analysis of current standards used in SCADA systems.

CURRENT STANDARDS			*Organizational Security*	
Standards	*Information security policy*	*Vulnerability and risk assessment*	*Information security Infrastructure*	*Security of third-party access*
AGA 12	Yes	Yes	Yes	Yes
API 1164	Yes	No	No	Yes
ISO 17799	Yes	No	Yes	Yes
NSERC Security Guideline	Yes	Yes	Yes	Yes
NERC 1200	Yes	No	Yes	No
NERC 1300	Yes	Yes	Yes	Yes
IEC 62210	Yes	No	Yes	Yes
IEC 62351	Yes	No	No	No
IEEE 1402	Yes	No	Yes	No
ISO 15408	Yes	Yes	Yes	No

TABLE 9. Comparative analysis of crypto-suite based SCADA standards.

Crypto-suite based Standards	**Presence of Key Management scheme**		**Strength of Encryption**		**Sustaining Security Requirements**		
	Strong	Weak	Strong	Weak	Confidentiality	Integrity	Availability
IEC 62210	No		Yes, weak		Yes	Yes	No
IEC 62351	Yes, weaker than AGA-12		Yes, weaker than AGA-12		Yes	Yes	Yes
AGA-12	Yes, weak		Yes, weak		Yes	Yes	No

nuclear power plants and traffic control systems. It is similar to the Information Security Policy [73].

- Third Party access or Outsourcing is giving access to service providers, vendors and contractors that can lead to credential theft and data risk management. To overcome these security concerns, the organizations extend the security policy. For example, the third party can be given access to a separate domain from the internal network, by using firewalls [75].

Furthermore, the crypto-suites standards are compared based on the following factors.

- Presence of Key Management Protocol in the standard and the strength of the protocol.
- Presence of Strong Encryption and strength of the encryption algorithm used in the standard.
- Sustaining security requirements refers to the existence of confidentiality, integrity and availability in the security scheme of the standard.

The strength of the key management and encryption scheme depends on the resources and time utilized to crack the scheme.

In case of detection of SCADA attacks, the primary factors are as follows:

- Known Attack Detection is the scenario where any traffic is categorized as an attack if the features of that particular traffic fall under the domain of attacks stored in the IDS database.
- New Attack Detection is the scenario where any traffic with unique behavior will be detected.
- Open Access networks are the public networks where the connected devices are exposed to each other. The public networks are vulnerable to various cyber threats. The private networks that provides access to the legitimate user.
- False positive is the situation where the IDS can detect the false alarms. False positives are the consequences where an activity is classified as abnormal even if its behavior is normal.

In case of prevention of SCADA attacks, the primary factors used for critical analysis are as following:

- The efficiency of the encryption scheme depends on the amount of computation resources utilized by

TABLE 10. Comparative analysis of detection schemes of SCADA attacks.

Detection of SCADA attacks	*Known Attack Detection*	*New Attack Detection*	For Open access networks	Distinguish false positives
Rule-based	Yes	No	Yes	No
IDS for m-connected SCADA networks	Yes	No	No	No
l_p – norms in One-Class Classification	Yes	Yes	Yes	No
OCSVM	Yes	Yes	Yes	No
OCSVM with K-means	Yes	Yes	Yes	Yes
Hybrid model	Yes	No	Yes	No

TABLE 11. Comparative analysis of prevention schemes of SCADA attacks.

Prevent SCADA attacks	Cost	Confidentiality	Integrity	Non-repudiation	Availability	Authenticate	Broadcast Interaction	Self-Heal	Prone to QC attack
SKE	High	Yes	No	No	No	No	No	No	Yes
SKMA	Low	Yes	No	No	No	No	No	No	Yes
LKH	High	Yes	No	No	No	No	Yes	No	Yes
ASKMA	Low	Yes	No	No	No	No	Yes	No	Yes
HKMA	Low	Yes	No	No	Yes	No	Yes	No	Yes
AHSKMA	Low	Yes	No	No	Yes	No	Yes	No	Yes
LiSH+	Low	Yes	No	No	Yes	No	Yes	Yes	Yes
ID-based KMP	Low	Yes	No	Yes	No	Yes	Yes	No	Yes
NTRU	Low	Yes	Yes	Yes	No	Yes	Yes	No	No

the algorithm. Therefore, an algorithm with high overhead or cost is less efficient and vice versa.

- Confidentiality is the secured privacy of the data.
- Integrity is when the data remains intact and unmodified.
- Authentication is a security property focusing on verifying and validating the identity of the user in the network.
- Availability is the scenario where the server is always accessible to the client.
- Non-repudiation is when the sender cannot deny that the data has not been sent by him at a particular time.
- Broadcast communication is the one-to-many communication case in a network.
- Self-healing is the case the users of an attacked network can recover their lost session keys to secure the data communication.
- Vulnerability to quantum attack refers to the absence of security measures to protect a system from quantum attack.

VIII. CRITIQUE

We now present a critical analysis of the schemes developed for SCADA network security. The schemes are classified into three categories: current standards, detection, and prevention of SCADA attacks. The paper analyzes the schemes in each category. Moreover, all the schemes are compared with each other. The tables below show the comparison between the protocols.

Table 8 shows that AGA-12 is the best among all the standards providing cryptographic protection to the SCADA systems. However, AES relies on ECDSA, AES, RSA, and SHA which leads to high computational and time cost.

It also does not involve an intrusion detection system and a strong key management protocol.

Table 9 provides the comparison of all the crypto-suite based standards and AGA-12 is by far the best standard. However, unlike IEC 62351, it does not provide defense against DoS attacks. Thus, the scheme has lack of availability property.

In all the standards, the key management protocols and encryption scheme used are weak and vulnerable to quantum attacks.

Table 10 compares all the intrusion detection system proposed for SCADA network security. In this category, OCSVM with K-means emerged as the best detection scheme for SCADA systems using open access networks. However, it is unclear whether it will be efficient when used for closed access networks.

Table 11 compares all the proposed key management protocols for SCADA networks. NTRU is the best scheme among the proposed schemes. It satisfies the main security requirements: confidentiality, integrity, and authentication. The scheme is not yet vulnerable to attacks from quantum computers. However, a quantum computer may able to crack the NTRU algorithm in the future.

IX. CONCLUSION

The paper provides a study of the SCADA communication architecture along with its threats and attacks. It discusses and classifies the frequent attacks on SCADA networks, and potential attack by a quantum computer. Furthermore, it lists all current standards used by organizations standards and provides the security threats of each standard. The two main security threats are lack of defense against Denial of Service attack and, using weak key exchange protocol. To address these two security requirements, researchers offered various novel security schemes. The paper classifies these schemes based on the addressed issue of the current standards. Thus, the schemes are categorized into detection of attacks on SCADA networks, and prevention of the attacks. It further explores and compares all the protocols that fall under each main category. It also addresses the security concerns and requirements that a SCADA security scheme needs to approach in future. Thus, the article gives a foundation to provide a course for further researches and assist an organization to decide on a suitable standard and scheme.

ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable feedback and comments, which have substantially improved the quality of the paper.

REFERENCES

[1] D.-J. Kang, J.-J. Lee, S.-J. Kim, and J.-H. Park, "Analysis on cyber threats to SCADA systems," in *Proc. Transmiss. Distrib. Conf. Expo., Asia–Pacific*, Oct. 2009, pp. 1–4.

[2] *Managing SCADA Complexity-Minimizing Risk: Balancing System Growth Against Destabilizing Uncertainty*, Trihedral Eng. Ltd., Bedford, NS, Canada, 2016.

[3] S. Nazir, S. Patel, and D. Patel, "Autonomic computing meets SCADA security," in *Proc. IEEE 16th Int. Conf. Cogn. Inform. Cogn. Comput. (ICCI CC)*, Jul. 2017, pp. 498–502.

[4] Department of Homeland Security and The Federal Bureau of Investigation, "Russian government cyber activity targeting energy and other critical infrastructure sectors," Tech. Rep. TA18-074A, Mar. 2018, pp. 1–18.

[5] P. Nader, P. Honeine, and P. Beauseroy, "LP-norms in one-class classification for intrusion detection in SCADA systems," *IEEE Trans. Ind. Informat.*, vol. 10, no. 4, pp. 2308–2317, Apr. 2014.

[6] A. Rezai, P. Keshavarzi, and Z. Moravej, "Key management issue in SCADA networks: A review," *Eng. Sci. Technol., Int. J.*, vol. 20, no. 1, pp. 354–363, 2017.

[7] R. J. Robles, M. Balitanas, R. Caytiles, Y. Gelogo, and T.-H. Kim, "Comparison of encryption schemes as used in communication between SCADA components," in *Proc. Int. Conf. Ubiquitous Comput. Multimedia Appl. (UCMA)*, Apr. 2011, pp. 115–118.

[8] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, "Machine learning for reliable network attack detection in SCADA systems," in *Proc. IEEE 17th Int. Conf. Trust, Secur. Privacy Comput. Commun./IEEE 12th Int. Conf. Big Data Sci. Eng.*, Aug. 2018, pp. 633–638.

[9] 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.

[10] M. Endi, Y. Z. Elhalwagy, and A. Hashad, "Three-layer PLC/SCADA system architecture in process automation and data monitoring," in *Proc. 2nd Int. Conf. Comput. Automat. Eng. (ICCAE)*, vol. 2, Feb. 2010, pp. 774–779.

[11] H. Saputra and Z. Zhao, "Long term key management architecture for SCADA systems," in *Proc. IEEE 4th World Forum Internet Hings (WF-IoT)*, Feb. 2018, pp. 314–319.

[12] D. Choi, H. Kim, D. Won, and S. Kim, "Advanced key-management architecture for secure SCADA communications," *IEEE Trans. Power Del.*, vol. 24, no. 3, pp. 1154–1163, Jul. 2009.

[13] H. A. Abbas, "Future SCADA challenges and the promising solution: The agent-based SCADA," *Int. J. Crit. Infrastruct.*, vol. 10, nos. 3–4, p. 307, 2014.

[14] *SCADAPack E Security Technical Reference*, Control Microsyst., Ottawa, ON, Canada, 2013.

[15] B. Zhu, A. Joseph, and S. Sastry, "A taxonomy of cyber attacks on SCADA systems," in *Proc. 4th Int. Conf. Internet Things Int. Conf. Cyber, Phys. Social Comput. (iThings/CPSCom)*, Oct. 2011, pp. 380–388.

[16] I. Ullah and Q. H. Mahmoud, "A hybrid model for anomaly-based intrusion detection in SCADA networks," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Dec. 2017, pp. 2160–2167.

[17] E. Irmak and I. Erkek, "An overview of cyber-attack vectors on SCADA systems," in *Proc. 6th Int. Symp. Digit. Forensic Secur.*, Mar. 2018, pp. 1–5.

[18] K. Holl. (2003). SANS Security Essentials GSEC Practical Assignment Version 1.4b OSI Defense in Depth to Increase Application Security. GIAC Certifications. Accessed: Oct. 21, 2018. [Online]. Available: https://www.giac.org/paper/gsec/2868/osi-defense-in-depth-increase-application-security/104841

[19] H. Hilal and A. Nangim, "Network security analysis SCADA system automation on industrial process," in *Proc. Int. Conf. Broadband Commun., Wireless Sensors Powering (BCWSP)*, Nov. 2017, pp. 1–6.

[20] J. Melnick. (2018). Top 10 Most Common Types of Cyber Attacks. Netwrix Blog. Accessed: Apr. 6, 2019. [Online]. Available: https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/

[21] Y. Zhang, Y. Xiang, and L. Wang, "Reliability analysis of power grids with cyber vulnerability in SCADA system," in *Proc. IEEE PES Gen. Meeting|Conf. Expo.*, Jul. 2014, pp. 1–5.

[22] Tutorialspoint. *Ethical Hacking Sniffing Tools*. Accessed: Apr. 6, 2019. [Online]. Available: https://www.tutorialspoint.com/ethical_hacking/ethical_hacking_sniffing_tools.htm

[23] Grey Campus. *Session Hijacking Process|Ethical Hacking*. Accessed: Apr. 6, 2019. [Online]. Available: https://www.greycampus.com/opencampus/ethical-hacking/session-hijacking-process

[24] Hacking Like a Pro. (2015). *11 Offensive Security Tools for SysAdmins*. Accessed: Apr. 6, 2019. [Online]. Available: https://hackinglikeapro.blogspot.com/2015/06/11-offensive-security-tools.html

[25] Kaspersky Lab. *Computer Viruses vs. Network Worms|Kaspersky Lab US*. Accessed: Apr. 6, 2019. [Online]. Available: https://usa.kaspersky.com/resource-center/threats/computer-viruses-vs-worms
[26] M. Rouse. (2018). What is Trojan Horse (Computing)?—Definition From WhatIs.com. TechTarget. Accessed: Apr. 7, 2019. [Online]. Available: https://searchsecurity.techtarget.com/definition/Trojan-horse
[27] R. Kalluri, L. Mahendra, R. K. S. Kumar, and G. L. G. Prasad, "Simulation and impact analysis of denial-of-service attacks on power SCADA," in *Proc. Nat. Power Syst. Conf. (NPSC)*, Dec. 2016, pp. 1–5
[28] A. Sharma. (2017). *Top 10 PowerFull DoS/DDoS Attacking Tools for Linux, Windows & AMP; Android—TheHackerStuff*. Accessed: Apr. 7, 2019. [Online]. Available: https://thehackerstuff.com/top10-powerfull-ddos-tools-linux-windows/
[29] J. Anderson. (2001). *An Analysis of Fragmentation Attacks*. Accessed: Oct. 21, 2018. [Online]. Available: http://www.ouah.org/fragma.html
[30] N. Sayegh, A. Chehab, I. H. Elhajj, and A. Kayssi, "Internal security attacks on SCADA systems," in *Proc. 3rd Int. Conf. Commun. Inf. Technol. (ICCIT)*, Jun. 2013, pp. 22–27.
[31] A. Luis, *Cybersecurity Lexicon*, vol. 158. Berkeley, CA, USA: Springer, 2016, pp. 1–199.
[32] INFOSEC. (2019). *Popular Tools for Brute-force Attacks [Updated for 2019]*. Accessed: Apr. 7, 2019. [Online]. Available: https://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref
[33] L. Chang. (2017). How Secure is Today's Encryption Against Quantum Computers? BetaNews. Accessed: Oct. 21, 2018. [Online]. Available: https://betanews.com/2017/10/13/current-encryption-vs-quantum-computers/
[34] P. K. Amiri, "Quantum computers," *IEEE Potentials*, vol. 21, no. 5, pp. 6–9, Dec. 2002.
[35] X. Zhang, Z. Y. Dong, Z. Wan, C. Xiao, and F. Luo, "Quantum cryptography based cyber-physical security technology for smart grids," in *Proc. 10th Int. Conf. Adv. Power Syst. Control, Operation Manage. (APSCOM)*, Nov. 2017, pp. 1–6.
[36] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," in *Proc. Int. Conf. IoT Appl. (ICIOT)*, May 2017, pp. 1–4.
[37] N. Kumar and D. Goswami, "Quantum algorithm to solve a maze: Converting the maze problem into a search problem," 2013, *arXiv:1312.4116*. [Online]. Available: https://arxiv.org/abs/1312.4116
[38] S. Castellanos. (Sep. 13, 2017). *Nascent Quantum Computing Poses Threat to Cybersecurity—CIO Journal.—WSJ*. Accessed: Oct. 21, 2018. [Online]. Available: https://blogs.wsj.com/cio/2017/09/13/nascent-quantum-computing-poses-threat-to-cybersecurity/
[39] R. Dennis. Quantum Computers are the Most Powerful Tech Threat to Cryptocurrency. ICO ALERT. Accessed: Oct. 21, 2018. [Online]. Available: https://blog.icoalert.com/quantum-computers-are-the-most-powerful-tech-threat-cryptocurrency-will-face-9b271e76edda
[40] Quantiki. (2015). *Shor's Factoring Algorithm*. Accessed: Nov. 5, 2018. [Online]. Available: https://www.quantiki.org/wiki/shors-factoring-algorithm
[41] S. Blanda. (Apr. 2014). *Shor's Algorithm—Breaking RSA Encryption—AMS Grad Blog*. Accessed: Jul. 3, 2019. [Online]. Available: https://blogs.ams.org/mathgradblog/2014/04/30/shors-algorithm-breaking-rsa-encryption/
[42] B. Lynn. Number Theory—Euclid's Algorithm. Standford University. Accessed: Nov. 5, 2018. [Online]. Available: https://crypto.stanford.edu/pbc/notes/numbertheory/euclid.html
[43] F. X. Lin, "Shor's algorithm and the quantum Fourier transform," McGill Univ., Montreal, QC, Canada, Tech. Rep. 12-13/nt/ Fangxi-Lin.pdf, 2014. [Online]. Available: http://www.math.mcgill.ca/darmon/courses/12-13/nt/projects/Fangxi-Lin.pdf
[44] B. Parvez, J. Ali, U. Ahmed, and M. Farhan, "Framework for implementation of AGA 12 for secured SCADA operation in oil and gas industry," in *Proc. 2nd Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2015, pp. 1281–1284.
[45] R. E. Carlson, E. D. Jeffery, S. A. Shamsuddin, and R. P. Evans, "A summary of control system security standards activities in the energy sector," Nat. Scada Test Bed, U.S. Dept. Energy Office Electr. Del. Energy Rel., Oct. 2005, pp. 1–13.
[46] *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE Standard 1402-2000, 2000.
[47] T. Carlson, "Information security management: Understanding ISO 17799," Lucent Technol., 2001.
[48] *ISO 15408 Compliance, IS Decisions*. Accessed: Oct. 22, 2018. [Online]. Available: https://www.isdecisions.com/compliance/ISO-15408-compliance.htm
[49] *Security Guideline for the Electricity Sector: Physical Security*, NERC, Atlanta, GA, USA, 2012.
[50] NERC. (2004). *Standard 1300-Cyber Security*. Accessed: Oct. 22, 2018. [Online]. Available: https://www.nerc.com/pa/Stand/CyberSecurityPermanent/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf
[51] American Petroleum Institute, *Pipeline SCADA Security*, 2nd ed., API Standard 1164, Pipeline SCADA Security, Jun. 2009, pp. 1–22.
[52] R. Schlegel, S. Obermeier, and J. Schneider, "Assessing the security of IEC 62351," in *Proc. 3rd Int. Symp. ICS SCADA Cyber Secur. Res.*, Jan. 2015, pp. 11–19.
[53] A. Williams. (2019). RSA Encryption Cracked Easily (Sometimes). Hackaday. Accessed: Apr. 4, 2019. [Online]. Available: https://hackaday.com/2019/01/16/rsa-encryption-cracked-easily-sometimes/
[54] J. M. Beaver, R. C. Borges-Hink, and M. A. Buckner, "An evaluation of machine learning methods to detect malicious SCADA communications," in *Proc. 12th Int. Conf. Mach. Learn. Appl. (ICMLA)*, vol. 2, Dec. 2013, pp. 54–59, Dec. 2013.
[55] Y. Yang, K. McLaughlin, T. Littler, S. Sezer, and H. F. Wang, "Rule-based intrusion detection system for SCADA networks," in *Proc. 2nd IET Renew. Power Gener. Conf. (RPG)*, 2013, p. 1.05.
[56] S.-J. Kim, B.-H. Kim, S.-S. Yeo, and D.-E. Cho, "Network anomaly detection for M-connected SCADA networks," in *Proc. 8th Int. Conf. Broadband Wireless Comput., Commun. Appl. (BWCCA)*, Oct. 2013, pp. 351–354.
[57] L. A. Maglaras and J. Jiang, "Intrusion detection in SCADA systems using machine learning techniques," in *Proc. Sci. Inf. Conf.*, Aug. 2014, pp. 626–631.
[58] L. A. Maglaras and J. Jiang, "OCSVM model combined with K-means recursive clustering for intrusion detection in SCADA systems," in *Proc. 10th Int. Conf. Heterogeneous Netw. Qual., Rel., Secur. Robustness (QSHINE)*, vol. 1, Aug. 2014, pp. 133–134.
[59] R. Dawson, C. Boyd, E. Dawson, and J. M. G. Nieto, "SKMA: A key management architecture for SCADA systems," in *Proc. Australas. Workshops Grid Comput. E-Res.*, vol. 54, pp. 183–192, 2006.
[60] D. Choi, H. Jeong, D. Won, and S. Kim, "Hybrid key management architecture for robust SCADA systems," *J. Inf. Sci. Eng.*, vol. 29, no. 2, pp. 281–298, 2013.
[61] A. Rezai, P. Keshavarzi, and Z. Moravej, "Advance hybrid key management architecture for SCADA network security," *Secur. Commun. Netw.*, vol. 9, no. 17, pp. 4358–4368, Nov. 2016.
[62] S. Mittra, "Iolus: A framework for scalable secure multicasting," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 27, no. 4, pp. 277–288, 1997.
[63] R. Jiang, R. Lu, J. Luo, C. Lai, and X. Shen, "Efficient self-healing group key management with dynamic revocation and collusion resistance for SCADA in smart grid," *Secur. Commun. Netw.*, vol. 8, no. 6, pp. 1026–1039, 2014.
[64] Y.-H. Lim, "IKMS—An ID-based key management architecture for SCADA system," in *Proc. 7th Int. Conf. Netw. Comput.*, Sep. 2011, pp. 139–144.
[65] A. P. Premnath, J.-Y. Jo, and Y. Kim, "Application of NTRU cryptographic algorithm for SCADA security," in *Proc. 11th Int. Conf. Inf. Technol., New Gener. (ITNG)*, Apr. 2014, pp. 341–346.
[66] B. Babu, T. Ijyas, M. P., and J. Varghese, "Security issues in SCADA based industrial control systems," in *Proc. 2nd Int. Conf. Anti-Cyber Crimes (ICACC)*, Mar. 2017, pp. 47–51.
[67] G. M. Coates, K. M. Hopkinson, S. R. Graham, and S. H. Kurkowski, "A trust system architecture for SCADA network security," *IEEE Trans. Power Del.*, vol. 25, no. 1, pp. 158–169, Jan. 2010.
[68] J. Hoffstein, J. Pipher, and J. H. Silverman, "NTRU: A ring-based public key cryptosystem," in *Proc. Int. Algorithmic Number Theory Symp.* Berlin, Germany: Springer, Jun. 1998, pp. 267–288.
[69] F. B. Advised and P. C. Bachoc, *Lattice-Based Cryptography*. Bordeaux, France: Univ. of Bordeaux, 2016.
[70] N. Challa and J. Pradhan, "Performance analysis of public key cryptographic systems RSA and NTRU," *Int. J. Comput. Sci. Netw. Secur.*, vol. 7, no. 8, pp. 87–96, 2007.
[71] E. Williams. (2015). Quantum Computing Kills Encryption. Hackaday. Accessed: Oct. 22, 2018. [Online]. Available: https://hackaday.com/2015/09/29/quantum-computing-kills-encryption/

[72] D. J. Bernstain, "Introduction to post-quantum cryptography," in *Post-Quantum Cryptography*, no. 1978. Berlin, Germany: Springer, 2009, pp. 1–14.
[73] D. Kostadinov. (2018). *Key Elements of an Information Security Policy, General Security, Infosec*. Accessed: Apr. 7, 2019. [Online]. Available: https://resources.infosecinstitute.com/key-elements-information-security-policy/#gref
[74] A. Jøsang, B. AlFayyadh, T. Grandison, M. AlZomai, and J. McNamara, "Security usability principles for vulnerability analysis and risk assessment," in *Proc. 23rd Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 2007, pp. 269–278.
[75] H. Barwick. (2012). Security Threats Explained: Third Party Access—Computerworld. ComputerWorld from IDG. Accessed: Apr. 7, 2019. [Online]. Available: https://www.computerworld.com.au/article/429271/security_threats_explained_third_party_access/

SAGARIKA GHOSH received the B.Tech. degree in information technology from the Maulana Abul Kalam Azad University of Technology, West Bengal, India, in 2015. She is currently pursuing the master's degree in computer science with Dalhousie University, Halifax, NS, Canada, and will be continuing as a Ph.D. candidate with a focus on network security. She has industrial experience in the areas of database management and Web development. Her research interests include the Internet of Things, cryptography, data privacy and security, supervisory control and data acquisition system security, quantum computing, and quantum cryptography.

SRINIVAS SAMPALLI received the B.E. degree from Bangalore University and the Ph.D. degree from the Indian Institute of Science (IISc), Bengaluru, India. He is currently a Professor and a 3M National Teaching Fellow with the Faculty of Computer Science, Dalhousie University, Halifax, NS, Canada. He has led numerous industry-driven research projects on the Internet of Things, wireless security, vulnerability analysis, intrusion detection and prevention, and applications of emerging wireless technologies in healthcare. He currently supervises five Ph.D. and ten master's students in his EMerging WIreless Technologies (MYTech) Laboratory and has supervised over 120 graduate students in his career. His primary joy is in inspiring and motivating students with his teaching and research. He received the Dalhousie Faculty of Science Teaching Excellence Award, the Dalhousie Alumni Association Teaching Award, the Association of Atlantic Universities' Distinguished Teacher Award, a teaching award instituted in his name by the students within his faculty, the Atlantic Canada Section IEEE Outstanding Educator Award, and the 3M National Teaching Fellowship, Canada's most prestigious teaching acknowledgement. Since September 2016, he has been holding the honorary position of the Vice President (Canada) of the International Federation of National Teaching Fellows (IFNTF), a consortium of national teaching award winners from around the world.