Electronics and Electrical Engineering

http://www.aimspress.com/journal/ElectronEng

AIMS Electronics and Electrical Engineering, 5(1): 24–37.
DOI: 10.3934/electreng.2021002
Received: 16 October 2020
Accepted: 27 November 2020
Published: 12 January 2021

Review

Cybersecurity in smart grids, challenges and solutions

Dharmesh Faquir[1], **Nestoras Chouliaras**[2], **Vlachou Sofia**[2], **Kalopoulou Olga**[2] **and Leandros Maglaras** [1,2,*]

[1] School of Computer Science and Informatics, De Montfort University, The Gateway, Leicester, LE1 9BH, UK

[2] Department of Informatics and Computer Engineering, University of West Attica, Greece

* **Correspondence:** Email: leandros.maglaras@dmu.ac.uk.

Abstract: Smart Grid technology will revolutionize modern industries providing powerful solutions to increase the efficiency of traditional Electric Grids. Smart Grid is an energy supply network that uses digital communications technology. The increasing load and consumption demands increase electricity complications, for instance, the demand has increased, along with problems like blackouts, overloads, and voltage sags as well as current electrical network growing critical carbon emissions and foremost dealing with cyber-attacks. However, the Smart Grid technology originates with vulnerabilities and complications especially for securing information which is the most vital concern. This article analyzes the threats and potential solutions of smart grids based on the Internet of Things. We focus on the types of cyber attacks and provide in-depth information The cyber security status of the smart grid.

Keywords: smart grid; security; privacy; electric grids; digital technology; cyber-attack; information; electrical network

1. Introduction

The Smart Grid technology is about to revolutionize the modern industries with powerful solutions that evolve the efficiency of traditional Electric Grids. The Smart Grid is an energy supply network that uses digital communications technology. According to the in [1], “the increasing load and consumption demands increase electricity complications” for instance, the demand has increased, and the problems originate with blackouts, overloads, and voltage sags as well as the current electrical network growing critical carbon emissions and foremost dealing with the cyber-attack. The United States is taking along up to forty percent (40%) of power system carbon dioxide emissions all nationwide which is harming the environment.

The demand for power supply has increased vividly whether it is domestic or commercial regions, because of progression in new emerging technologies which uses the machine, appliances, and devices greater than before. For these reasons, the power requirement has elevated dramatically. The traditional Grid system is insufficient to deliver the services up to standards, whereas the Smart Grid is the next generation power system that will substantiate the power for the manufacturing industries.

The Smart Grid with the integration of advanced technologies such as communication and advance computing power is anticipated to offer enhancement in efficiency, reliability, and availability [2]. Furthermore, the Smart Grid provides infrastructure which is integrated with two-way communication and electricity flows. The Smart Grid is an organized technology where its inheritance the legacy power generation techniques which use natural gas, fossil fuel, coal as well as uses renewable sources of energy, such as wind turbines and solar power. The Smart Grid is known to provide well-organized power distribution and consumption to a network of smart devices, transformer sand machines. Satisfactory, to achieve these goals it uses two-way communication whereas the legacy grid system uses one-way communication. The Smart Grid provides quick and enhanced services for the customers, with a reduced amount of response time delay where the energy crisis can be achieved by implemented efficiently. However, the Smart Grid technology comes with vulnerabilities and complications with the biggest difficulty being to secure the information that is the most vital asset. The reasons are that the Smart Grid system will frequently exchange information as there could be sensitive information resides.

Cyber Security in Smart Grid has a critical operation because numerous devices individually commercial and domestic will be connected via a series of networks to communicate and delivering the security to the networks with various techniques [3]. These issues are challenging which will be based on a literature review where numerous security solutions are evaluated and analyzed to help provide resolve solutions to complex security problems.

2. Smart Grid technology

The potential vulnerabilities of Smart Grid technology and its information networking are associated with information security. There are many types of research being conducted to provide potential solutions to security problems related to Smart Grids (See Figure 1).

Figure 1. Smart Grid technology.

2.1. Fundamental networking architecture of Smart Grids

The architecture for Smart Grid essentially needs a highly-distributed and hierarchical network system, [1]. The authors suggested that the architectural framework and implementation standards of Smart Grid are still being monitored and analyzed by many researchers. Both academic researchers [4, 5, 6], industrial researchers [7] and government sectors are still investigating this area. However, the researchers have delivered various designs for the Grid architecture and still, every design is based on the reference model of which is suggested by the U.S. National Institute of Standards and Technology (NIST). In general we can see that a smart grid incorporates two types of communication: Home Area Network (HAN) and Wide Area. A wide area network (WAN) is a telecommunications network that extends over a large geographical area for the primary purpose of computer networking. Wide area networks are often established with leased telecommunication circuits. The WAN can communicate using WiMAX, 3G/GSM/LTE, or fiber optics. The smart meter acts as a gateway between the in-house devices and the external parties to provide the needed information (see Figure 2).

Furthermore, according to NIST's conceptual model [8] the Smart Grid consists of several "domains" and these conceptual models provide resourceful information by analyzing the "use cases, identify interfaces for which interoperability standards are needed, and to facilitate the development of a cyber-security strategy" according to U.S. National Institute of Standards and Technology (NIST). The NIST's logical domains consist of Bulk Generation, Transmission, Distribution, Customer, Markets, Service Provider, and Operations. According to [9] authors suggested that the Bulk Generation, Transmission, Distribution and Customer domains are the features that two-way power and information flow whereas, the last three feature collects the information and manages the power in the Smart Grid.

Moreover, another survey paper [9], provides information related to the networking architecture of Smart Grids and the authors defining the simple network architecture by how the network is distributed in a hierarchical network system as it influences to work for communication. The research presented by the authors about the simple network architecture provides important information about it features. For instance, the authors have provided information about the changes in Performance Metric, Traffic Model, Timing Requirement, Communication Model, and Protocol Stack.

Figure 2. Smart Meters help balance the power consumption in the Grid Smart.

A part of these conducted researches are very significant, as a result of offering the information about insignificant differences between the common traditional networking concepts and modification effected in smart grid networks, they offer needed modifications to methods and designs for providing efficient solutions. However, the authors in [9] have provided an insufficient solution for providing network security in Smart Grid networks. The reason for this is because the architecture of Smart Grids is different than traditional IT architecture.

- **Traffic Modelling:** Traffic modeling has the resemblance properties of Internet (WWW) traffic, on the other hand, these properties of internet traffic will not be relevant for the Smart Grid, because the Smart Grid network will use the regular traffic flow (periodic traffic) for the purpose of constant monitoring. However, according to the authors' research, the Smart Grid uses Ad-Hoc networks for creating regular traffic flow (periodic traffic). Ad-Hoc network is challenging when establishing a reliable periodic traffic flow. The reason it is challenging because the periodic traffic flow requires a dependable, secure connection and essentially it requires stable network topology as well as complex network protocols for using the techniques such as a three-way-handshake and encryption mechanism. However, the Ad-hoc network was used in an emergency as it is initially designed for creating a rapid network. Although, the authors lack in providing information about the traffic modeling where it does not reflect on the properties of ad-hock networks.
- **Performance Metrics:** Performance Metrics in Smart Grid are different from the basic Internet functionality as they provide data services such as web surfing and music downloading. The Smart Grid network is different from than Internet because it is substantial, and it uses the power communication networks for"dependable, secure, and real-time message delivery and non-real-time monitoring and management" (Wang W. X., 2011)which is a vital part of Performance Metric. Likewise, power communication requires latency as it is important than the throughput in power systems. Another important of Performance Metric is that it uses the power communication protocol where it related to delay-oriented design. By emphasizing the authors' research on Performance Metric, it provides security aspects over speed which is the essential and valuable solution when dealing with the power communication protocol. However, it may require a higher-cost for maintaining and securing the network.
- **Communication Model:** The Communication Model is the essential and required feature for the Smart Grid as it uses two-way communication whereas the Communication Model in the legacy power grid it uses the one-way communication. However, according to the authors' research, it said that "Smart Grids communication model has top-down and bottom-up approach" (Wang W. X., 2011). By emphasizing this, it is an effective and efficient communication model, because the Communication Model is well-established within the Smart Grid.
- **Timing requirement:** Most IP traffic over the Internet requires to support voice-over-IP and multimedia services which may have delay-sensitive traffic. However, the Smart Grid has a wide range of features where the requirement for sending messages will delay the information from milliseconds to minutes. As for the result, the Smart Grid has considerably stricter timing requirements for message delivery than the Internet.
- **Protocol Stack:** The Internet is generally designed using the IP protocol version 4 (IPv4) for networking. According to NIST (Arnold, 2010), the Smart Grid will use the IP protocol version 6 (IPv6) for the main network-layer protocol. The IP protocol version 6 (IPv6) is the most advanced protocol, as it can improve the security benefits of this protocol. However, the authors

(Wang W. X., 2011) only talked about the network-layer protocol whereas it lacks information security protocols of different layers of the OSI Model because it is important when dealing with cybersecurity in Smart Grid.

The information provided by the authors about the networking architecture of Smart Grids is beneficial. The reason is that most research papers lack in providing this information. Although, the research only discusses the information on cyber-attacks in detail. This information essential and relevant but providing the information about the architecture of a Smart Grid, provides an understanding of how the attacks can be minimized and performed in the actual real-world.

3. Security risks, breaches and solutions

Due to the heterogeneous communication architecture of smart grids, it is quite a challenge to design sophisticated and robust security mechanisms that can be easily deployed to protect communications among different layers of the smart grid-infrastructure [10, 11]. The traditional electrical power grid is currently evolving into the smart grid. A smart grid integrates the traditional electrical power grid with information and communication technologies (ICT) [12]. Such integration empowers the electrical utility providers and consumers to improve the efficiency and the availability of the power system while constantly monitoring, controlling, and managing the demands of customers [13].

Several main security objectives must be incorporated in the smart grid system:

- Availability of uninterrupted power supply according to user requirements,
- Integrity of communicated information
- Confidentiality of user's data. We must emphasize the grid's main vulnerabilities, the various attackers and the types of attacks they can conduct and needed security solutions.
- Preventive analysis, reactive security using intrusions response and mitigation is insufficient for critical CPS and like smart grids. Unlike traditional IT systems, where the impact of an attack in a critical infrastructure can be devastating in terms of damages and consequences. Thus, it is required to proactively identify the potential threads in order o reduce the attack surface for a smart grid and avoid the detrimental consequences.
- Automating the security analysis for large and hybrid systems like smart grids. The smart grid security guidelines developed by NIST are highly detailed.
- Dynamic measures for security, is the ability to provide security and Resiliency to smart grids by introducing agility to the system properties

In this section the security risks in Smart Grid will be reviewed as well as discussions on some possible attacks on Smart Grids and possible security solutions.

3.1. Common security risks in Smart Grids

These suggestions are possible common threats that may be effective threats for Smart Grids. There are many risks that Smart Grids can potentially obtain, and these could not only affect the organizations but will also affect regular customers. These risks possibly pose significant threats to individuals' privacy, such as sensitive information about customers, maybe at risk of getting information stolen or terminating the business for good. These risks are not just posed at using the internet but also affect customers at home while adversaries could possibly collect personal information.

- **Phishing:** Phishing could be the first step of putting customers and organizations at risk, as it is very easy to execute the process. The hackers could use the information from customers where customers, not accordingly discarding the bills or payment receipt and with this information the hacker would use social engineering, to get crucial information about the organization, in this case, the information about the power supplier. On the other hand, inside the organization, the employee may possibly face other risks, such as fake emails or messages that look genuine emails where the employee, may enter personal information that could lead to getting hacked. These posed risks probably affect a Smart Grid customer, when giving the information to unknown sources and not knowing the consequences of these risks may affect customers mentally and financially. However, when dealing with security measures against phishing attacks it is an important concern.
- **Denial-of-Service:** TThe Denial-of-Service (DoS) is a strategic attack and any attacks against availability then it's part of the DoS- attack. Regarding the Smart Grid, the leading services for Smart Grids are available which means that the Smart Grid has a chance of getting a Denial-of-Service attack. The Smart Grid's connectivity connection must need to be secure and reliable. The reason for connectivity connection must be reliable and secure because the Smart Grid distributes the connection to countless devices in a larger area using the distributed architecture systems. If (Dos) attack occurs on the Smart Grid, then it will suffer immense loss. The Denial-of-Service attack will occur its impact on jamming the channel and it is a common way to attack the physical layer and Data-link layer of OSI-Model. The hackers may possibly modify the MAC address and use the hacker's tool such as "Tsunami Backdoor" to gain backdoor access into the network which can help the hackers to flood computers with standard network requests. Furthermore, the OSI-Model has some security protocol in Network and Transport layer such as the TCP, SSL, and IPv6 but still the protocols are vulnerable when it originates from Smart Grid network architecture. However, the (DoS) attack will be mainly executed in the Application layer of OSI-Model because the Application layer enables to send and receive data whereas, regarding the Smart Grid, if (DoS) attack occurs then it can stop the communication system respond to various devices.
- **Malware spreading:** The major risk the Smart Grid can be faced by Malware spreading which is the major concern. The attackers can develop malware that can be speared into infecting the organization servers as well as infecting the devices. By using the Malware spreading, the attacker can manipulate the functions of devices or the systems which will allow the attackers to gain access for collecting sensitive information.
- **Eavesdropping and traffic analysis:** Eavesdropping and traffic analysis are types of spoofing attacks. the attacker can gain sensitive information by monitoring network traffic. The Smart Grid will be facing this risk because of the large network it contains, the Smart Grid includes many network nodes and it is hard to maintain the devices connected to the larger network. The Smart Grid poses the biggest risk of data getting stolen which is the major concern in securing the data from the whole word.

In [9] authors provide detailed information on cyber-attack which are related to the OSI-Model along with accurate information related to "Network Security Threats in the Smart Grid". Correspondingly, the information in this survey paper gives solutions and precautions on how to tackle the risks in Smart Grid. The authors discuss and clarify the risks in-depth and give important information related to Smart Grid. Table 1 shows the smart grid cyber-attacks in smart grid according to CIA triage [14].

Table 1. Cyber attacks against smart grids according to the CIA.

CIA	Attack
Confidentiality [15]	Social Engineering, Eavesdropping, Traffic Analysis, Unauthorized Access, Password Pilfering, MITM, Sniffing, Replay, Masquerading, Data Injection
Integrity [16]	Tampering, Replay, Wormhole, False Data Injection, Spoofing, Data Modification, MITM, Time Synchronization, Masquerading, Load-Drop
Availability [17]	Jamming, Wormhole, Denial of Service, LDos, Buffer Overflow, Teardrop, Smurf, Puppet, Time Synchronization, Masquerading, MITM, Spoofing

3.2. Security breaches

The Smart Grid technology composite of using the network and communication technologies, it provides various benefits while offering the energy. However, smart grids can be vulnerable to common threats that are related to computer networks. There are numerous securities breaches, and these are discussed in different papers which provide information on the impact of some major cyber-attacks and also provided the solutions for mitigating these in the future, these breaches are discussed below.

3.3. Trojanhorse malware BlackEnergy

A cyber-attack outbreak took place during a civil war context on 25th December 2015. An electrical power station in Ukraine's Ivano-Frankivsk city was targeted for a cyber-attack which affected colossal impact on eighty thousand (80,000) people at risk by putting them in the dark whereas one million, four hundred thousand (1.4 million) people were affected.

The cyber-attack was done using the spear-phishing email and a Trojan horse malware which known as the "BlackEnergy". This powerful virus was capable of deleting the data, destroy hard drives, and able to take control of infected computers. The cyber-attack accelerated further, as the attacker launched a coordinated Denial-of-service attack (DoS attack)on the company's utility equipment, crippling the support phone number that manages the power station. As a result, the users were not able to contact the breakdown because of the (DoS attack). This situation developed enormously and critically because the cyber-attack not just stole the information, but it has also destabilized a country's critical infrastructure. The situation probably the most devastating incident because with no electricity many people have suffered from harsh cold weather conditions.

However, according to the authors in [18], it's not fully guaranteed that the protection against "BlackEnergy" can be dealt with but on the other hand, following the precaution can help minimize the risks which provide the solutions and safeguarding against the future cyber-attack. These solutions can be accomplished with updating anti-virus signatures, antimalware, and firewall configurations as well as updating the systems and application of security patches to prevent already known vulnerability attacks. The updated firewall can be used for blocking the incoming connection ports, but the firewall is not effective in the circumstance of spear-phishing emails. The authors in [18] suggested that the Sandboxes can provide protection while "testing/executing unverified applications/documents". Conversely, by emphasizing the authors [18] research on solution strategies, it does not fully mention tangible solutions for the larger organisations because it's some typical solutions for home use.

However, on the other hand, an online critical from "search security TechTarget" gives defence solution against "BlackEnergy" attack, the author in [19] has provided a concrete solution for defending the attack against the "BlackEnergy" threat. The author suggested that it requires wider measures and not just protecting against the original Windows-based malware, it also requires to protect against the "new target platforms for Cisco routers and MIPS- and ARM-based systems" and essential it requires to cover all defences for the Linux systems, by ensuring the integration platforms into current security controls. For example, the security configurations and difficult patch management.

The author in [19] also suggested that the defence also requires basic appropriate "information security hygiene" it means that the software must be updated with the latest patches, it also requires using the secure configurations, it also acquires to use the strong passwords, multifactor authentication and mainly it also needs to be secure the basic security such as monitoring networks and logs. The solutions offered are tangible and supportive which can be useful for larger organisation as well as it can be helpful for everyday use system.

3.4. Stuxnet

A malicious computer worm, known as the Stuxnet, targeted the Supervisory Control and Data Acquisition (SCADA). The Stuxnet was first uncovered in 2010. However, it has been developed in since at least 2005 (Denning, 2012). The Stuxnet was rumoured to have been created by the intelligence agencies of the United States and Israel. The Stuxnet malicious computer worm is able to manipulate Programmable Logic Controllers(PLCs) and it is the responsible controlling electromechanically processes of machines, the Stuxnet computer worm also uses the Microsoft Windows operating system and networks. The overwhelming computer worm Stuxnet mange to infiltrated inside Iran's Nuclear Power Plant control system which was able to manipulate the (PLCs) which controls the centrifuges and separates nuclear material by triggering them to spin faster in resolves to tear the equipment apart. The impact of Stuxnet computer worm causes the dedicated equipment to increase the rotation speed and quickly started destabilising the nuclear fuel.

The Stuxnet does not harm computers but when it infects the computers, it runs a check to see if the computer is connected to specific models of programmable logic controllers (PLCs) manufactured by Siemens. The purpose of using the Stuxnet computer worm was as a tool by the U.S. and Israeli governments to terminate the Iranian program to develop nuclear weapons.

However, when illustrating the impact of the Stuxnet computer worm attacking on Iran's Nuclear Power plant, it just shows how fatal a computer security breach can be impactful. The Stuxnet cyber-attack highlights the headlines which shows how virtual attacks on computers causes huge impact on the world. Author in [20] discussed the impact of Stuxnet caused a cyber-attack on cyber-defence. The author also provides important information about the attack which also revealed that it is a type of cyber warfare.

By emphasising the author's research, it illustrated how lethal the impact of cyber-attack caused during the time of that period. The author conducted research thoroughly and systematically that the information about the cyber-attack was written in steps of hierarchy, starting from "Cyber Weapons continuing through State-Level Cyber Conflict up till Cyber Warfare and Cyber-Terrorism". However, the author did not provide deep solutions such as preventing and countermeasures for future cyber-attack. On other hand, online blogs provide several solutions precisely that could help to prevent future cyber-attacks.

3.5. WannaCry Ransomware

A devastating programme WannaCry Ransomware caused a global cyber-attack on well-known organisations, including Renault, FedEx and crashed thousands of regular users' computers. The WannaCry Ransomware was lunched on 12th of May 2017.

The WannaCry Ransomware program infected more than 200,000 computers - demanding a ransom to unlock the victim's files. The hackers demanded cryptocurrency bitcoins worth three hundred dollars ($300) to be sent to a specific address to decrypt the whole system and if victims didn't pay in time given then whole system files being permanently deleted. According to the attack has caused the biggest impact by hacking the NHS hospital computers and more than nineteen thousand (19,000) appointments were cancelled and the WannaCry Ransomware have put many lives on jeopardy. The total cost of restoring the NHS's IT system consists of fines worth of twenty million pounds (£20m) and further seventy-two million pounds (£72m) on ensuring to cleaning-up and upgrading the IT systems.

The Ransomware attack was spread using various methods which include out-dated systems without up-to-date security patches on Microsoft as well as phishing emails. The investigation carried on by the United State, the United Kingdom and Australia formally declared that the attack was blamed on elite North Korean hackers. By emphasising this lethal cyber-attack, it has caused a devastating threat to human lives as the computers used in the hospital are used for operations which put huge risk on the line when saving human life.

Providing sophisticated solutions for preventing WannaCry ransomware attacks is important. The organisation network administrator must disable the "SMBv1 on Windows servers by running this PowerShell cmdlet command", the user has to remove the Windows Feature using the PowerShell command prompt, latest Microsoft Patch must be updated from the official website, adding rules on antivirus protection to prevent the creation of ".wnry file extensions", the TCP port 139 and 455 must be blocked as in only allows inbound Internet connections, training and educating staff about the threat. The author has provided bold solutions and step-by-step guild for preventing against the WannaCry Ransomware cyber-attack which can be helpful to combat a future cyber-attack.

3.6. Proposed security solutions for Smart Grids

Practically some security risks ideally need security solution to protect against vulnerabilities and regarding network security in Smart Grids, the networks are the most vulnerable against threats and risks [21]. The threats and risks are the biggest obstacles to maintain the network and system. The attacker can target different networks layers of the OSI-Model. In this section, the proposed solutions that are suggested to counter a cyber-attack are discussed.

- **Encryption:** Encryption is the process of taking some information (your data) and scrambling it so that it can't be read. When you connect to the internet using a VPN your connection is what becomes encrypted, which means that if cybercriminals were to intercept the stream of your data, all they would get is gibberish code. You can consider encryption a form of secret code. The way your data is scrambled is called a cypher, and there is a key (or logic) that allows you to decipher the message. The highest encryption standard available is known as AES (Advanced Encryption

Standard) 256-bit and is used by the most recommended VPN providers. What does 256-bit mean? It's the size of the cipher used in the encryption. The bigger it is, the more possibilities there are, and the harder it is to guess the key. In the case of 256-bit encryption, there are more combinations than there are stars in the universe. In fact, this level of encryption is so secure it's used by banks and governments worldwide to ensure the security of their data.

- **Authentication:** Maintaining authentication and control access are the main concern where the identity should be verified via strong authentication mechanisms according to the authors [22]. In order to implement the authentication, an "implicit deny policy" possibly valuable when accessing the network, as well as using the policy to grant access permissions to only explicit users. By using the policy, it offers security solutions for the organization and using the implicit deny policy it can be beneficial because the individual users will have different permission which grants individual users' specific permissions where the Manager can see all the additional data related to projects whereas the staff has limited access of data. By giving explicit access to individuals within the organization, as it can help reduce the risk of getting hacked as well as it can easily be identified the user who accessed the network. Furthermore, the use of authentication can be implemented using SSL protocols. However, the protocols may be exposed to cyber-attack such as Denial-of-service attacks. The Smart Grid network requires higher-bandwidth to communicate which also means that the Cryptography techniques can be used for authentication. Maintaining Cryptography techniques will increase the cost although they provide an excellent authentication mechanism. It is best practice to use the Control system and IT security engineers to work together and equally to secure the smart grid network.
- **Malware Protection:** The Smart Grid requires Malware Protection because the Embedded system and the General-purpose systems which are connected to the Smart Grid needed to be secured and protected from cyber-attacks. The Embedded system requires a manufactures key which can be used to secure the product for software validation. The main reason that Embedded System is secure it is because the Embedded systems are only exposed to run the software which is supplied by the manufacturer and it requires manufacture key to validate the software, whereas the General-purpose systems support third-party software such as antivirus software it will constantly update the antivirus software.

  By providing the solutions, it is possible that the manufacture's software must be genuine, and the organization must require to adopt risk management to mitigate the risks if using third-party software. Another solution for using the manufactures key is to verify that the software is genuine, and it has not been copied without authorization. Using the antivirus software for malware protection may put some layers of protection and primary methods for identifying risks. However, the antivirus must be up to date with a new patch, and foremost the attacker must not find a way to bypass the antivirus software as threats can become vulnerable to malware via phishing attacks.

  The effective approach will be appropriate to use in the Smart Grid is using the Network Intrusion Prevention System (NIPS), for controlling access to a network as well as it can protect from various cyber-attack. Furthermore, the (NIPS) is designed to monitor intrusion data and take action to prevent an attack from developing. Another approach that can be used for Smart Grid is by using the Network Intrusion Detection System (NIDS) where the (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats [23].

- **Network Security:** The Virtual Private Network (VPN) provides additional security while using the public network, such as the Internet. The (VPN) uses a variety of security methods such as encryption and protecting any data transmitted across the network as the data may be at risk when using the public network infrastructure. Virtual Privet Networks (VPN) are also used communication because it provides a secure path for communication. There are two types of (VPN) available and these are beneficial for the organization and regular users.
- **Remote access VPN:** The Remote access VPN uses a public network such as the internet to provide access to organizations' private network. The users will use mobile devices or desktop using the VPN gateway for access after providing authentication. The authentication can validate the access if credentials are correct and then gains access to resources stored on the virtual network. These resources only available for the organization's users and it includes business applications and documents. The Remote access VPN can help users to access their work anywhere if they are connected to a VPN gateway.
- **IDS & IPS:** Network Intrusion Prevention System (IPS) and Network Intrusion Detection System (IDS) technologies. What is an Intrusion Prevention System An intrusion prevention system (IPS) is a form of network security that works to detect and prevent identified threats [24]. Intrusion prevention systems continuously monitor your network, looking for possible malicious incidents and capturing information about them. The IPS reports these events to system administrators and takes preventative action, such as closing access points and configuring firewalls to prevent future attacks. IPS solutions can also be used to identify issues with corporate security policies, deterring employees and network guests from violating the rules these policies contain.

  IPS solutions come across intrusion detection systems (IDS). The main difference between IPS and IDS is the action they take when a potential incident has been detected. Intrusion prevention systems control access to an IT network and protect it from abuse and attack [25]. These systems are designed to monitor intrusion data and take the necessary action to prevent an attack from developing. Intrusion detection systems are not designed to block attacks and will simply monitor the network and send alerts to systems administrators if a potential threat is detected. IDSs can be based on Semi-supervised learning, reinforcement learning, active learning or DL solutions [26]. According to [27], data mining, a term that is used to describe knowledge discovery, can be used as a basis in order to implement and deploy IDSs with higher accuracy and robust behaviour as compared to traditional IDSs that are based only on specific rules. The idea behind smart security mechanisms is to produce a model that either learns the normal operation of the system or creates patterns for every abnormal situation, e.g. Denial of Service Attack (DoS), Man in the Middle Attack (MITM) etc. Based on this knowledge the detection mechanism is able to detect attacks in real time. The downside of using ML techniques to perform classifications is the possibility of adversaries trying to circumvent the classifiers causing misclassification [28], performing adversarial attacks.

  IPS solutions offer proactive prevention against some of today's most notorious network exploits. When deployed correctly, an IPS prevents severe damage from being caused by malicious or unwanted packets and brute force attacks. Next-Generation Firewall provides advanced intrusion prevention and detection for any network.
- **Site-to-site VPN:** Site-to-site VPN is similar to the Remote access VPN. However, it generally connects the entire network in one location, but the networks are located somewhere else as this is

useful for a larger organization which provides access or share the recourses securely to multiple branches in various location for the organizations' partner or client business.

- **Risk and Maturity Asssements:** Conducting efficient cybersecurity risk assessments and implementing mitigations in large complex networks and facilities where full security audits cannot be implemented due to time and capacity limitation led to a number of smart solutions recently. In [29] authors propose a cyber defense triage process that can help spot areas of priority where the impact of attacks is greatest and thus the application of security solutions to these areas is more urgent. Risk assessment is only one of the numerous controls that can be assessed when conducting a maturity assessment, as proposed in [30], where again security gaps and weak points can be revealed and mitigated accordingly.

4. Conclusions

Smart Grids are better than traditional legacy power grids in terms of competency and productivity as the Smart Grids are environmentally friendly, it uses a lot of renewable sources of energy and foremost it is more secure than the traditional power grid. Furthermore, the research suggested possible benefits and vulnerability against the Smart Grid. The benefits of using a Smart Grid in the overall perspective, it will provide a wider range of security with having various techniques and techniques to overcome some of the cyber-attack issues. However, while conducting the research, the various paper has suggested the security benefits and vulnerability related Smart Grids, almost every research paper suggested that threatening weakness for Smart Grids would be the Denial-of-Service attack. Since Smart Grids are the construction of the network and attacking the network would cripple the Smart Grid. Although, the Smart Grid will protect the Availability of the service with multiple layers of security an optimal solution for the security aspects would be using the Virtual Private Network (VPN) for more secure communication.

Moreover, concluding this research, self-awareness related to cyber-attack in Smart Grids is important. The user should be aware of the risks related to the Smart Grid and mitigate them by doing various risk assessments and case studies to provide a further solution in protecting the Smart Grid against different types of cyber-attack. Additionally, the research addressed possible challenges related to the Smart Grid. The Smart Grids challenges are that various devices connected over vast geographical area networks. The biggest challenge to secure these devices over larger infrastructure. Blockchain technology could help resolve security issues by providing a shared and encrypted ledger that is immutable to changes made by malicious nodes or attackers. It can also be utilized to verify identities and authorize access by storing and recording transactions in the immutable ledger and make data exchanges between distributed gadgets smooth and cost-efficient. In conclusion, the computer network protocols need to be modified according to the current posture of communication as well as providing sophisticated encryption methods and to offer security countermeasures. Therefore, it will provide defense against evolved cyber-attacks.

Conflict of interest

Authors declare no conflict of interest.

References

1. Liu J, Xiao Y, Li S, et al. (2012) Cyber security and privacy issues in smart grids. *IEEE Commun Surv Tut* 14: 981–997.
2. Dileep G (2020) A survey on smart grid technologies and applications. *Renew Energ* 146: 2589–2625.
3. Maglaras LA, Kim KH, Janicke H, et al. (2018) Cyber security of critical infrastructures. *Ict Express* 4: 42–45.
4. Ferrag MA, Maglaras LA, Janicke H, et al. (2018) A systematic review of data protection and privacy preservation schemes for smart grid communications. *Sustain Cities Soc* 38: 806–835.
5. Clark A, Pavlovski CJ (2010) Wireless networks for the smart energy grid: application aware networks. *Proceedings of the International MultiConference of Engineers and Computer Scientists* 2: 98.
6. Wei C (2010) A conceptual framework for smart grid. *2010 Asia-Pacific Power and Energy Engineering Conference*, 1–4.
7. Metke AR, Ekl RL (2010) Smart grid security technology. *2010 Innovative Smart Grid Technologies (ISGT)*, 1–7.
8. Greer C, Wollman DA, Prochaska DE, et al. (2014) *Nist framework and roadmap for smart grid interoperability standards, release 3.0*, No. Special Publication (NIST SP)-1108r3.
9. Wang W, Xu Y, Khanna M (2011) A survey on the communication architectures in smart grid. *Comput Netw* 55: 3604–3629.
10. El Mrabet Z, Kaabouch N, El Ghazi H, et al. (2018) Cyber-security in smart grid: Survey and challenges. *Comput Electr Eng* 67: 469–482.
11. Al-Shaer E, Rahman MA (2016) Security and resiliency analytics for smart grids. *Advances in Information Security*.
12. Kimani K, Oduol V, Langat K (2019) Cyber security challenges for iot-based smart grid networks. *Int J Crit Infr Prot* 25: 36–49.
13. Khurana H, Hadley M, Lu N, et al. (2010) Smart-grid security issues. *IEEE Secur Priv* 8: 81–85.
14. Gunduz MZ, Das R (2020) Cyber-security on smart grid: Threats and potential solutions. *Comput Netw* 169: 107094.
15. Lopez C, Sargolzaei A, Santana H, et al. (2015) Smart grid cyber security: An overview of threats and countermeasures. *Journal of Energy and Power Engineering* 9: 632–647.
16. Procopiou A, Komninos N (2015) Current and future threats framework in smart grid domain. *2015 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, 1852–1857.
17. Sanjab A, Saad W, Guvenc I, et al. (2016) Smart grid security: Threats, challenges, and solutions. *arXiv preprint arXiv:1606.06992*.

18. Khan R, Maynard P, McLaughlin K, et al. (2016) Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid. *4th International Symposium for ICS & SCADA Cyber Security Research 2016 4*, 53–63.

19. Lewis N (2015) What's the best defense against blackenergy malware? Available from: `https://searchsecurity.techtarget.com/answer/Whats-the-best-defense-against-BlackEnergy-malware`.

20. Denning DE (2012) Stuxnet: What has changed? *Future Internet* 4: 672–687.

21. Li X, Liang X, Lu R, et al. (2012) Securing smart grid: cyber attacks, countermeasures, and challenges. *IEEE Commun Mag* 50: 38–45.

22. Aloul F, Al-Ali A, Al-Dalky R, et al. (2012) Smart grid security: Threats, vulnerabilities and solutions. *International Journal of Smart Grid and Clean Energy* 1: 1–6.

23. Maglaras LA, Jiang J (2014) Ocsvm model combined with k-means recursive clustering for intrusion detection in scada systems. *10th International conference on heterogeneous networking for quality, reliability, security and robustness*, 133–134.

24. Sutherland BR (2020) Securing smart grids with machine learning. *Joule* 4: 521–522.

25. Maglaras LA, Jiang J (2014) A real time ocsvm intrusion detection module with low overhead for scada systems. *International Journal of Advanced Research in Artificial Intelligence (IJARAI)* 3.

26. Ferrag MA, Maglaras L, Moschoyiannis S, et al. (2020) Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *J Inf Secur Appl* 50: 102419.

27. Dewa Z, Maglaras LA (2016) Data mining and intrusion detection systems. *International Journal of Advanced Computer Science and Applications* 7: 62–71.

28. Martins N, Cruz JM, Cruz T, et al. (2020) Adversarial machine learning applied to intrusion and malware scenarios: a systematic review. *IEEE Access* 8: 35403–35419.

29. Cook A, Janicke H, Smith R, et al. (2017) The industrial control system cyber defence triage process. *Comput Secur* 70: 467–481.

30. Drivas G, Chatzopoulou A, Maglaras L, et al. (2020) A nis directive compliant cybersecurity maturity assessment framework. *arXiv preprint arXiv:2004.10411*.