Cyber Security for Smart Grid: Vulnerabilities, Attacks, and Solution

Shreyash More, Suraj Hajari, Mahshooq Abdul Majeed, Neeraj Kumar Singh, and Vasundhara Mahajan

Abstract The smart grid (SG) is an emerging technology. To overcome the limitations of traditional power grid systems, it is an optimistic alternative. Smart grid includes green energy resources and enhances the reliability of power generation, transmission, as well as distribution. This transformation involves a bidirectional communication network that monitors the power flow and stores the data at each level. Moreover, as numerous information data and communication devices are involved in the smart grid, it is a prime target for cyber attacks. Targeting the smart grid can lead to disclosure of private data, supply chain failures, and it can also lead to blackouts. Therefore, cyber security becomes a major concern of all power companies around the world. This paper talks about the basic overview of SG, its security objectives, followed by the existing vulnerabilities in the SG network, attack types, some major attacks on the power grid, and highlight some recent solutions.

Keywords Smart grid (SG) · Vulnerabilities · Cyber security · Smart grid security

1 Introduction

The SG is an electrical network, which can smartly combine the action of all the components that are connected to the system. In SG, power flow is bidirectional, which means utility to consumer and consumer to the utility if a surplus is available at the consumer's end [1]. According to the National Institute of Standards and Technology (NIST), SG is described as an integration of traditional grid and Information and Communication Technology (ICT) [2]. NIST described the SG as follows:

S. More · S. Hajari · M. A. Majeed · N. K. Singh · V. Mahajan (✉)
Department of Electrical Engineering. SVNIT, Surat, India
e-mail: vmahajan@eed.svnit.ac.in

S. More
e-mail: p20ps019@eed.svnit.ac.in

S. Hajari
e-mail: p20ps020@eed.svnit.ac.in

V. Mahajan et al. (eds.), *Sustainable Technology and Advanced Computing in Electrical Engineering*, Lecture Notes in Electrical Engineering 939,
https://doi.org/10.1007/978-981-19-4364-5_60

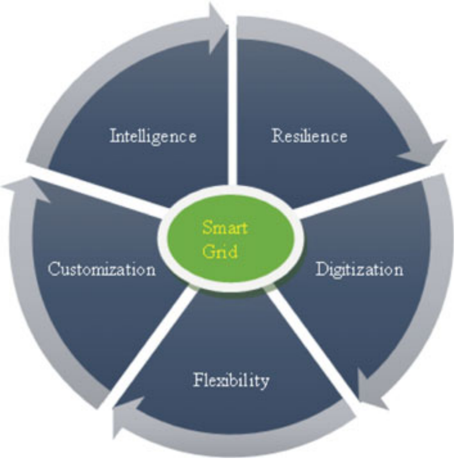
- Provide reliable and quality power.
- Increased capacity and enhanced efficiency.
- Strengthen resiliency to disturbance and self-healing in nature.
- Self-operating and automated maintenance.
- Use renewable energy sources effectively and utilize distributed energy sources.
- Reduced oil consumption.
- Adapt plug-in electric vehicles.
- Minimize requirements of backup.
- Increase consumer choice.
- Decreased greenhouse gas emissions.

SG technology enriches the traditional power grid with enhanced capabilities, which introduces more complexity and vulnerabilities to several attacks [3–7]. The attacker targets these vulnerabilities and gets access to the system. This compromises the integrity and confidentiality of system data and, as a result, makes the system unreachable.

SG is an emerging technology; hence, very less data is available related to security ruptures. Hence, identifying security threats to the system is a very complex and tough job. Also, relatively less practical knowledge about cyber attacks and their influence on the network is available. Cyber security professionals are trying to learn the concept and develop algorithms and devices to protect the network and for mitigation of attacks [77–80]. However, physical safety and attacks are well known to the persons and workers of the grid deployment. Any natural accidents like earthquakes or hurricanes that affect the grid physically are very random, but cyber attacks are not. Cyber attacks depend on the attackers, their motives, interests, and capabilities. Apart from this, the above-mentioned aspects change with time. This makes cyber security a huge challenge that becomes very necessary to be solved.

This paper presents a survey that shows the vulnerabilities present in the SG, attacks that might happen, and highlights some of the existing solutions to overcome them. The remaining paper is categorized as given. Section 2 presents the features of the SG followed by the conceptual model based on NIST and key subsystems of the SG. Section 3 explains the security objectives as well as the requirements for a SG. Section 4 describes the core vulnerabilities of the SG system in detail. Section 5 highlights the possible threats to the SG system and its categories. Section 6 discusses the major attacks that happened on the power grid. Section 7 points out the human factor in the SG. Section 8 discusses the solutions that overcome the challenges of the SG security system. Section 9 concludes this paper.

Fig. 1 Smart grid's features



2 Smart Grid Technology

2.1 Smart Grid's Features

The SG provides some advantages over the traditional grid, given as increasing grid resilience, intelligence, digitization, customization, and flexibility [9] as shown in Fig. 1. Resilience specifies the capability of a given system to resist unexpected events and recover rapidly thereafter [8]. Intelligence means inheritance to intelligent technology. Digitization indicates the digital platform that makes the system faster and reliable too. Customization indicates that the system needs to be client-tailored. And the last is flexibility, which means the SG needs to be adaptable, compatible as well as expandable. Nowadays, grid resilience has become an essential feature, especially when power interruption can greatly impact financially. As SG involved the renewable energy resources and energy storage system, it assures reliable power supply by providing corrective capabilities when a failure occurs.

2.2 Smart Grid Model

NIST classifies the SG into seven domains, given as generation, transmission system, distribution network, electricity market, provider, customer, and operations [10]. All these seven domains involve players and applications. The player includes devices, programs, and systems, whereas applications are functions accomplished by the player in the above given domain [11]. Figure 2 shows the conceptual SG model.

Generation Domain: In a bulk generation domain, players are the generators. Generation is the first step in order to deliver electricity to end users. Energy resources

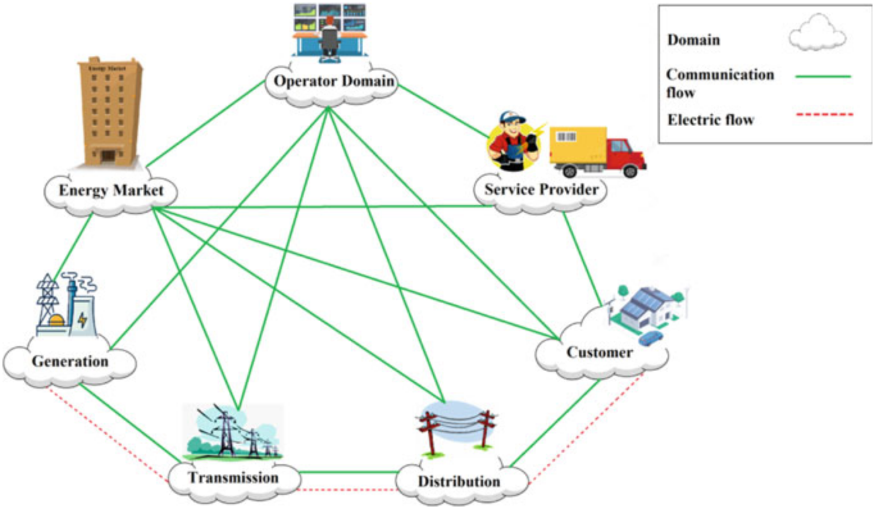


Fig. 2 Conceptual model of SG based on NIST

like coal, water, solar radiation, wind, and nuclear fission are used to generate electricity.

Transmission Domain: In the transmission domain, the generated energy is transmitted over a long distance from the generation to the distribution domain. For control and monitoring the transmission domain, SCADA is used.

Distribution Domain: In the distribution domain, actors are the distributors of electricity. This domain contains different structures like radial, parallel, ring, etc. Energy storage and generation can also integrate with this domain. The domain is electrically connected to the transmission domain and has communication flow with the market, transmission, customer, and operator domains.

Market Domain: In this domain, the players in the electricity market are service operators and end users. The market domain maintains the balance between electricity demand and supply. In order to fulfill the demand, the market domain communicates with the bulk generation domain.

Service Provider Domain: The organization is the main actor in the service provider domain which provides services to both utilities and consumers. The services managed by the organization include billing, use of energy, and customer accounts. This domain interacts with the operator domain for system control and situational awareness. It also communicates with the market and customers to grow smart services, like allowing interaction between both, power generation at consumer premises, etc.

Customer Domain: The end user is the main player in this domain. These are categorized as: residential, commercial, and industrial. In addition to consuming power, SG gives provision to this domain to generate power (by using solar PV, EV, etc.), store it (batteries, etc.) and also control the usage.

Operator Domain: In the operator domain, actors are managers who control the electricity flow between the domains. The objective of the domain is to maintain efficiency as well as optimal operation in transmission and distribution. It also applies energy management system (EMS) in the transmission system, whereas in distribution it uses distribution management system (DMS).

2.3 Key Subsystem in Smart Grid

Advanced Metering Infrastructure (AMI): AMI is a system that combines several technologies which measures, collects, and analyzes the energy use. It enables bidirectional communication between utility and users. It has three parts: a smart meter, an AMI head end, and a communication network [50]. Smart meters are integrated meters which consist of memory and microprocessors that are used to monitor and collect energy use as well as communicate data in real time to the utility's AMI head end. The AMI head-end is the server of AMI which contains the meter data management system (MDMS) [12]. Many communication protocols like Zigbee and Z-wave [50] are used for communication between MDMS and smart meters.

Supervisory Control and Data Acquisition (SCADA): It is a system that monitors, regulates, and measures the electrical power grid. The SCADA system contains three components: The RTU, i.e., remote terminal units, a central master terminal unit (MTU) and the human–machine interface (HMI) system [13]. RTU is used to interface field devices with the SCADA system. RTU is governed by the MTU system. The HMI is a graphical interface for the operators present at the SCADA system.

Plug-in Hybrid Electric Vehicle (PHEV): PHEVs offer the ability to minimize emissions, transportation costs, and dependency on fossil fuels. In addition to this, it can also provide support to distributed energy resources (DER) in SG [14]. During the peak periods, PHEVs can be used to supply the grid, and in off-peak periods they can be charged, thus it improves the reliability and efficiency of the grid.

3 Smart Grid Security Objectives and Requirements

In SG, there is mainly the exchange of operational data and information data. The operational data is instantaneous voltage (V) and current (I) values, relay status, circuit breaker status, fault location, transformer tap changer, and capacitor banks [15]. Information data includes consumer's information and emails, power consumption bills, etc. [15–17]. A high level of security is needed for operational data to secure SG against vulnerable attacks which compromise reliable supply.

3.1 The Security Objectives of Smart Grid

Availability: Availability is one of the most important objectives of the SG. It guarantees reliable and punctual entry to data. The power delivery could be affected by the loss of availability. The attacks which target availability are considered Denial of Service attacks (DoS). A DoS attack makes resources unavailable due to which legitimate users may unable to access the data. For example, if availability is compromised, then information flow in the network will be interrupted and control over the system will not possible. So, the security of the communication channel is necessary.

Integrity: It refers to the detection or prevention of modification of system information by an unauthorized person. Due to loss of integrity, illegitimate users can modify the sensor values, which may affect the power management. For example, attackers purposely modify the original information in the SG communication system, which results in wrong system decisions. The protection of customer's data and operational network data is needed.

Confidentiality: It refers to protecting personal privacy and safety from unauthorized access. If not, then data can be compromised. For example, smart meters are full of user data and they can be used as a tool by the attacker for future attacks. Hence, the protection of the smart meter data is also very important.

3.2 The Security Requirements of Smart Grid

Authentication: Verifying the true identities of communicating parties. It is very important to authenticate humans and machines. Due to any weakness in it, it may lead the attacker to gain access to information. For example, the implementation of strong authentication is needed such that only authenticated persons are able to communicate.

Authorization: Issuing permission and allowing access to the system, there are large numbers of devices and users in SG that need authorization of appropriate governance for resources as well as information. If the defense mechanism for authorization is weak, then the attacker will get easy access control to plan an attack on the system.

Non-Repudiation: It promises that tasks done by the user cannot be denied later. If integrity is compromised, then it will affect non-repudiation too. It is most important regarding regulatory requirements. The violation of it will have legal and commercial consequences.

4 Security Challenges and Vulnerable Links in the Smart Grid System

As stated earlier, SG is a fusion of the traditional grid and ICT. It improves the capabilities of the conventional network. It also adds complexity to the power network, making it vulnerable. It might make a passage for attackers to attack the network. As a result, compromise the data and broke the security objectives of SG, i.e., confidentiality and integrity. The next paragraphs highlight vulnerable links in the SG [22–27].

In a smart grid, ICT acts as a central nervous system. Generation, transmission, and distribution are the sectors of the grid, and data associated with them is foremost important. Besides, while considering the end user, ensuring customer's privacy is an important aspect, and it should be well preserved and protected. There are many challenges regarding customer's information privacy as all data is collected by smart meters in the SG. If hackers get access to the meters, then it will be available to the hacker. This data includes information about the time of availability of consumers at home. Also, it is possible to extract information about daily activities like at what time they are sleeping or which household gadgets they use. Criminals can utilize this information to commit crimes, and marketers can also utilize data for marketing. Hence, it is very important to secure both transfer and storage process to avoid leakage [27].

SG comprises abundant devices which monitor the power supply and network conditions [28]. Smart meters and AMI communication infrastructure are the best suitable example. Managing these multiple devices is an intricate task. Hence, the attacker will get wide area access points to attack.

The interconnection between the ICT and distribution domains extends the security threats. For example, smart meters are installed inside the consumer's premises, buildings, etc. These meters not have any direct control over the operators. Hence, they might interfere as it has already happened with old electromechanical meters. Additionally, once the attacker gets an entry in the smart meter, they may get access to the AMI network and use it as a medium to send malware [29]. Protection of such devices located at faraway is again a major task.

The IT components present in a grid have a limited life, hence their up-gradation is needed. If they continue to work in the older version, then it acts as the weakest point for the attack, and it also introduces connection issues [22].

There are different teams working in different domains of SG, incompatibility and any miscommunication among them will give the wrong command. And, it might act as a vulnerable point in the system [21].

SG has a very intricate infrastructure, and it needs to collaborate with more and more stakeholders to get a better result out of it. There are a huge number of actors involved: consumers, power producers, retailers, EV-related businesses, etc. The coordination between all these stakeholders along with each of its own organizational processes, priorities, requirements, and standards, is very difficult. The authorized person might attack the system and will be difficult to identify. Many of the standards used in SG were never made by considering the security threats. These standards are currently used for the control and communication of all three domains of the grid, i.e., generation, transmission, and distribution. They might be helpless against cyber attacks such as denial of service (DoS), spoofing, etc. However, new standards are now developed for the application of SG, and these are designed by considering security principles like cryptography, encryption, etc. But, controlling cryptographic material for a large number of devices is a tough task.

The supply chain is the most vulnerable area of the SG. The supply chain present in the SG consists of many embedded software, control systems, sensors, microchips, SCADA systems, operating systems, etc. The supply chain might be invaded at some steps by the attacker. The attacker changes the electronic circuitry of the devices or could substitute a dummy part. They could add logic bombs, malware, etc. All these backdoors could be used by enemy states or terrorists to execute their plans. They might use the logic bombs to cause terrible harm. So, the supply chain security, well-regulated manufacturing process of electronic devices used in the chain is very important. Table 1 summaries common challenges on smart grid.

5 Possible Threats and Their Categories

The attacker first identifies the vulnerabilities, which could be anyone from the previous section or any other, and plans the attack against the network for its own intentions. The attackers could be categorized based on their intentions of the attack and listed in Sect. 5.1 [30], Further, Sect. 5.2 highlights some of the attacks that can be performed on the smart grid system by attackers. The attacker follows the steps given in Sect. 5.3 to execute the plan of any attack.

5.1 Types of Attackers

Non-malicious hackers: These attackers consider the security network as a puzzle and try to break the system with their technical skills.

Customers: As SG is a very beneficial technology, many customers are accepting it. As a result, SG connectivity increased. But, the system does not know the intentions of a user, so some might not be trustworthy. Some users will not adhere to the agreement and policies. Users may try to compromise the smart meter to reduce the bill amount by interfering with the meter reading.

Subversive Hackers: These types of attackers are subversive in nature. They target the power grid, try to interrupt the supply, and so the entire area can suffer from blackouts. They could break the system and get access to crucial information. Terrorists, bombers, arsonists, etc., can be considered under this category.

Employee: A person who is unhappy with the service provider or with the customers, or may be an untrained employee.

Table 1 Common challenges on smart grid

Challenge	Asset/target	Effects	Measures
Privacy [18]	Data and information, generation, transmission, distribution related data, customer data-consumption pattern, sleeping time, appliances used, billing information	Misuse of data, for ex- by terrorists for destruction, by criminals to commit crimes, by marketers for marketing and etc.	Privacy impact assessment (PIA), Encryption-Decryption for data flow, authentication, digital certificate, etc. [20]
Increased access point [19]	Electronic devices including smart meters, AMI, monitoring and control devices, data and information	Attacker can use it for blackouts, supply interruption, damage the grid, etc.	Cloud computing security, routine service, in depth strategies of security system, etc. [20]
Physical security [20]	Remotely installed devices like smart meters, etc.	Financial loss, data and information can be compromised and attacker can get control over the grid and etc.	Strong authorization, protect access credentials, etc. [20]
Frequent updating of component [21]	IT components	Acting as a weakest point and can be attacked easily, etc.	Routine up-gradation [21]
Dissimilarity among teams [21]	Communication links	Wrong decisions, incorrect command or action, etc.	Effective and efficient communication standards, etc. [21]
Stakeholders [20]	Data and information control mechanisms	Data misuse, reliability compromised, etc.	Strong authentication and authorization, etc. [20]
Communication protocols [20]	Communication links	Service unavailable, etc.	Cryptography for end to end encryption– decryption and authentication, efficient and effective implementation of keys, certificates needed for the cryptography, etc. [20]
Supply chain [20]	SCADA system, operating system, control system, microchips, electronic devices, etc.	Blackouts, operation, control and monitoring system compromised, serious physical damages to the grids, etc.	Well controlled and duly regulated design, manufacturing, components assembly and administration of electrical components, etc. [20]

Competitor: These types of attackers are also called rivals. They try to target the grid for their personal profit, or they trying to end the competition in the market.

5.2 Types of Attacks

Using Malware: Malware is malicious software designed with the main intention to harm the services. An attacker can use malware to gain access and collect critical data. It could also be used for data modification or for eradicating sensitive information [31].

Illegal Access: It is also called an unauthorized access. It can manipulate systems settings and operations.

Replay: In order to create an unauthorized effect, an intruder may send an identical message or false message multiple times. This may create an unnecessary burden on the receiver. This burden may cause communication to falloff.

Denial of Service attack: This type of attack is used by the attacker to make the system unavailable for the users [32].

Traffic Analysis: In this type of attack, the attacker attacks the system to get an idea about the routing structure and to analyze the traffic in the network. In such attacks, an attacker may gain sensitive data like energy usage, smart grid structure, price, etc.

5.3 Attack Formats

Firstly, the attacker identifies the target; in this case, it is smart grid. Then he/she follows the below steps,

Reconnaissance: The term refers to the practice of gathering and collecting information about the target. It is also continuously used by cyber security experts to find out cyber threats and to prevent them. In this step, the system confidentiality can be compromised.

Scanning: In this step, attacker tries to find out the weakest link in the system or the vulnerability of the system. It can compromise the confidentiality of the system.

Exploitation: Here, attacker executes his plan of action and tries to get full control of the system and compromise the data. Confidentiality, integrity, and availability will be compromised during this step.

Future Access: After execution of the attack, the attacker installs an undetectable and cloaked program that could be used in the future for the attack. In this confidentiality, integrity, and availability can be compromised.

Table 2 shows the comparison between some of the most general types of attack and illustrates their respective effects on the smart meter and related economical impact [33]. The availability attacks are the most serious because they have the most detrimental impact on smart meters, and the remaining three types of attacks have

Table 2 Types of attacks and their impacts

Attack	Objective violation	Smart meter systems delay	Financial impact	Smart meter communication blockade duration	Counter measure
DoS	Availability	Mild	Moderate	Extreme	Strong authorization, trolling techniques, honey-pot models
Radio frequency jamming	Availability	Extreme	Mild	Extreme	Use anti-jamming technologies
Replay attacks	Availability	Extreme	Mild	Extreme	Time stamping
False data injection attack (FDIA)	Integrity	Extreme	Mild	Mild	Use encryption-decryption techniques
Unauthorized access	Confidentiality	Extreme	Mild	Mild	Use virus or spyware protection programs, protect password and login credentials

serious economical effects. The availability attack class, replay attacks, and radio frequency jamming, having severe financial impacts and smart meter communication blockade. However, DoS is also a good choice of weapon for producing a delay in smart meters [33].

6 Major Cyber Attacks on the Power Grid

Table 3 shows, some major cyber attacks against power utilities and the grid over the past decade [35–47]. Note that there have been numerous attacks, either not detected or not announced in the public domain for security reasons. For example, in 2012 there were nearly 200 cyber attacks detected and nearly half of these attacks targeted a power grid. Now attacks on the power grid are becoming more frequent. According to ESET security researchers, Industroyer malware was used to attack Kiev in December 2016 to be the biggest threat to industrial control systems [43]. Malware such as Industroyer is very dangerous as it permits attackers to carry out huge industrial sabotage as well as it allows them access to control power utility networks. As a result, they can control the commands given to the equipment like switches, circuit breakers, and relays, and interrupt the electricity flow at anytime and cause blackouts [46].

Table 3 Major cyber attacks on the power grid

Year	Cyber attack	Cause	Discussion
Jan. 2003	Nuclear power plant was infected with MS SQL worm in Ohio	Entry of malicious code through a secondary pathway into the control network	On 25 January 2003, Davis Besse nuclear power plant's private computer network was infected by '*slammer*' Microsoft SQL worm. As a result, network site overloaded by traffic, which makes safety and monitoring system not accessible and temporary failure of process computer [35]
Feb. 2011	Brazilian power plant management system	By an infected machine	The power plant was contaminated by the worm called "*Conficker*". It affects the management system of the plant make it stop. And hence unable to displace data [36]
June 2011	Petrobras, Brazilian energy company website hacked	It is a DDoS attack, multiple infected computers targeted the website with useless requests and make them out of action	Based on anarchic intentions, LulzSec, a hacking group, attacks the website of the biggest energy producer of Latin America, Petrobras. The attack has made total shutdown of the site [37]
2012	Power utility of German	DoS attack with a botnet involves thousands of requests was sent to a server each second to make a system inoperable	German power utility specialized in renewable energy was hit by a DoS attack and make its Internet communications systems offline [38]
2013–14	Attack against 1000 + energy companies from 84 countries	Hackers had infected the websites with malicious software, which were visited by the targeted individuals often. The targeted individuals visited the site and unknowingly downloaded the software	Dragonfly, a hacker group, used a Havex, a type of Trojan, and take control over the 1000+ energy firms from 84 countries which include Germany, Spain, US, etc. Their target maybe industrial sabotage [39, 40]

(continued)

Table 3 (continued)

Year	Cyber attack	Cause	Discussion
Dec. 2015	Against Ukrainian regional power companies	The hackers sent an email to employees, attached with malware, which allows them to get login credentials and shut down substations	Hacker team, sandworm, by using black energy malware took control over the control actions of many regional power stations of Ukraine, around 225 k people suffered from blackouts [41, 42]
Dec. 2016	Attack on the capital of Ukraine	Industroyer malware, designed for power grid attack	The attacker cut the power supply for 1/5th of Kiev, the capital of Ukraine for one hour. This attack is considered to have been a large-scale test [43]
2017	Electricity distribution board, West Bengal, India	Ransomware	WannaCry ransomware infected around 4 billing departments of West Bengal, India, that cater to around 800 k houses. As a result, electricity bill payment operations were interrupted for the day. The attacker asked for the ransome to restore the system [44]
2017	Petrochemical power plant, Saudi Arabia	Computer system compromised	The power plant was hit by a cyber strike. The strike was planned to destroy the data and make the plant offline. According to the expert the attack was designed for sabotage and an explosion trigger [45]
2017	Attack many western energy companies	Phishing mails, Trojanized software, etc.	Dragonfly 2.0, a Russian hacking group, attacked many western energy firms, enter into networks of around 20 + firms, also get operation control in the US and Turkey, and also aimed to sabotage operational systems at energy facilities [46]

(continued)

Table 3 (continued)

Year	Cyber attack	Cause	Discussion
2019	Power grid cyber attack in western US	Distributed Denial of Service (DDoS) attack	Communication lines between the power control center and power generation sites interrupted resulted in communication loss and system and firewall of the system were restarting and again becomes offline [47]

7 Human Factor in Cyber Security

The human factor is considered by many security experts as the weakest link in cyber security. It is because many individuals are easily trapped in phishing and equivalent attacks. These attacks are utilized to get access credentials of the system. This has earlier happened in Ukraine. The hackers had sent emails to the concerned individuals. The malware carrying links were attached to the emails. After opening the links, hackers obtained the credentials which allowed them to get access to the systems control and operations parameters. It caused a power cut in regional distribution utilities [41]. The security method named 'multifactor authentication' is one of the methods which mainly concentrates on the human factor. The method needs two or more than two credentials, i.e., biometric, password, or security key to verify the identity of an individual who is trying to access the network, and this is all needed prior to access [49]. On that account, the combination of all, something you know, something you have, and something unique you have, like a password, token, and biometrics, makes you a recognized user for that network.

8 Solution to Smart Grid Security

8.1 Three Phase Strategy

The author in [6] suggested that security can only be achieved by combining many strategies into a worldwide plan, rather than by relying on a single solution. They also propose a cyber security strategy consisting of three phases, given as, pre-attack, under attack, and post-attack, as shown in Fig. 3.

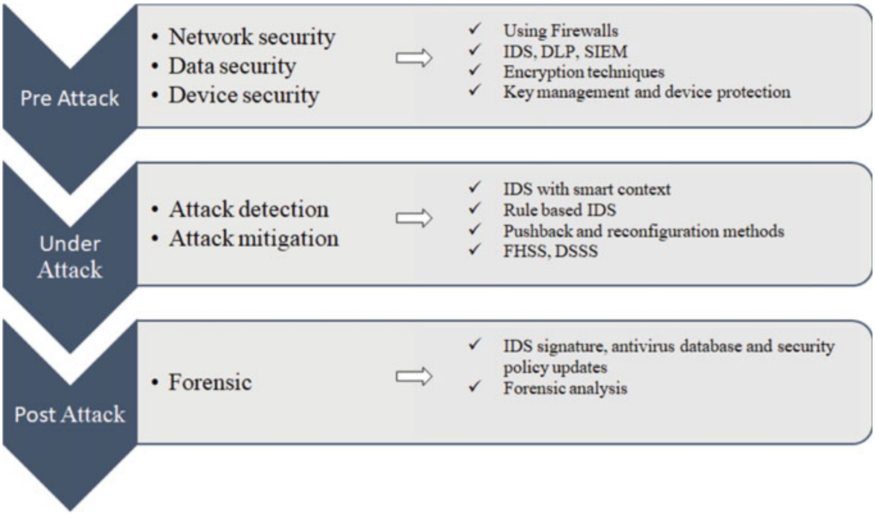


Fig. 3 Smart grid security solutions

8.1.1 Pre-attack

In the first stage, before the attack, it is recommended to use various solutions (like network, data, and device security, etc.) to improve the security of SG and be ready for any possible attack. Security countermeasures are generally classified into three main categories as given below,

Network security: The network is a very important part of the smart grid. The security of the network is necessary and if it is not, then the whole system becomes vulnerable. It is suggested to use a firewall additionally with the other examining and monitoring techniques to secure SG [8]. Based on some policies and rules, the firewall is designed to permit or decline network connections. But, more advanced or unknown attacks can break the firewall. Therefore, technologies like security information and event management systems (SIEM), intrusion detection system (IDS), and data loss prevention (DLP) should be used along with firewalls. SIEM is a system that collects and compiles information from all devices that are present in a network [50]. This gathered data will then be processed and analyzed by the central server, so it can identify any threats or destructive activity in the network [8]. To detect any malicious activity in the network, an IDS system is used. To prevent any data theft or loss of information, a DLP system is used [51].

Data security: To protect users' data, secure communication, and authenticate users, cryptography methods and algorithms are used to encrypt the data [56–58]. There are two types of encryption, namely: symmetric key encryption and asymmetric key encryption. Symmetric key encryption requires lower computing capabilities regardless of key size. However, asymmetric key encryption requires more computing capabilities for long key size (better security).

Authentication is an important identification process in SG to terminate an attack that targets data integrity. Certain requirements have to be met for authentication, like tolerance to faults and attacks, high efficiency, and multicast support. Multicast has many applications in SG, which include monitoring, protection, generation, and distribution. For example, if an IED monitoring the feeder senses any abnormality like high current or high voltage, then it will issue a trip command to CB. Under such conditions, unicasting the same time-crucial tripping signal to every circuit breaker will inescapably lead to a huge delay and may damage the power equipment. To avoid this, multicasting is the most systematic method to multicast time-crucial signals to all correlated breakers belonging to the corresponding multicast category. Multicast authentication can be done through secret information asymmetry, time asymmetry, or hybrid asymmetry [59].

Key management plays an important role in encryption and authentication in order to safeguard the SG. Public key infrastructure (PKI) is a technology that attaches public keys to individual users' identities through a certificate authority (CA). Before starting any communication, the PKI mechanism ensures security by cross-checking the real identity of the user by getting a certificate from a certificate authority (CA). There are four steps that are utilized in symmetric key management, namely: generation of key, distribution of key, key storage, and key update. The benefit of it over public key infrastructure is its speed and effectiveness for a large amount of data.

Device Security: In the secure supply chain of SG, the protection of devices is the third critical component. In order to assure the security of end devices in SG, various security technologies are recommended, like data loss prevention, antivirus, and intrusion detection systems [8]. These tools perform checks on all components of SG to verify that the configuration of each device is uptodate, particularly current configuration files and device firmware. Since SG components are extremely interconnected, any deficiency in a device can put the whole system at risk.

8.1.2 Under Attack

Generally, there are two tasks in this step: detection and mitigation of the attack. For example, denial of service (DoS) is the most frequent attack in SG. The main goal of this attack is to make the system not work as expected. DoS attacks must be detected in the SG to take proper countermeasures. Some recent DoS identification methods are [53]:

Using signal strength: In this method, wireless devices are used to detect signal strength. By measuring the strength of a signal, a device can decide if it is under a jamming attack or it is receiving legitimate data. In a jamming attack, the attacker chooses to send a continuously amplified signal to jam the channel or send a noise-like signal. A detector must detect these types of signals [54].

Using measurement of sensing time: Carrier sense multiple access (CSMA) is a commonly used multiple access technique. In this case, by sensing the channel, the transmitter confirms that it is free before sending the data. The sensing time will be large in the case of a jamming attack, and the channel will not be free. Each time before transmitting the data transmitter records the sensing time. If sensing time is larger than the threshold value, then the transmitter will reveal it as a DoS attack [55].

Detection using transmission failure: This method keeps the record of transmission failure. A jamming attack can cause failure in data transmission or can corrupt the transmitted packets. It is declared as a jamming attack if the count of failures crosses the threshold value [55].

Using signature: Attack signatures are generally built using known attack patterns. Some doubtful actions are compared with signature, and if it matches, then it is considered as a DoS attack [53].

After confirming the DoS attack, the smart grid should take proper measures as soon as possible to minimize the outage period and to safeguard nodes. In the SG, countermeasures to mitigate DoS attacks are generally implemented in two layers: physical and network layer. The mitigation methods for the network layer are given below [60].

Pushback: After confirming the attack, properties of the attack like the pattern or IP address are sent back to the upstream router, and then all the traffic that matches the attack properties is blocked by the router [53].

Rate limiting: Once the detector determines that a certain user is executing the DoS attack, the router will limit the user's data rate. Thus, the effectiveness of the attack is reduces. One drawback of this method is the high false detection rate. Under such instances, if the user is legitimate, then they can make a complaint to increase the data speed.

Reconfiguration: This is accomplished by modifying the network's topology to make available more resources to the victim or isolate an attack. Since reconfiguration is costlier, it is rarely used.

Filtering: A suspicious packet's source IP is checked through the detector's blacklist by the router. If a match is found, packets are quickly filtered to create a path for legitimate packets to pass.

Cleaning center: Basically, it is a combination of reconfiguration and filtering. Once the attack has been confirmed on a node, the traffic is redirected to the "cleaning center". It is a node present in the network which is capable of filtering suspicious packets [54].

Physical layer mitigation: Frequency jamming is the usual form of DoS attack at the physical layer level. Some algorithms used to mitigate such attacks are: Direct sequence spread spectrum (DSSS), frequency hopping spread spectrum (FHSS), and chirp spread spectrum (CSS).

8.1.3 Post Attack

The post-attack phase is critical when the attack is not detected. After the attack, it is necessary to identify the entities affected or compromised in the attack. After that, the anti-virus database, IDS signature, and security policies need to be updated by learning from the attack, so that the SG will be able to withstand similar upcoming attacks. Forensic analysis is the main methodology used after the attack. SG forensic collects, analyzes, and intercepts the data to recognize the entities involved in the incident. Forensic studies can also be used to identify and resolve physical and network vulnerabilities in SG to predict potential attacks. Additionally, SG forensic studies play a crucial role in the inspection of cybercrimes like cyber terrorism, hacking, and digital spying, violating users' privacy, viruses, modifying SG data, state property, and secret [52].

8.2 Blockchain Technology

Blockchain is the technology in which each block contains the data, timestamp, index, hash, and previous hash [61]. These blocks form a chain in which newly generated blocks are continuously added at regular intervals [62]. In recent years, researchers have been trying to integrate blockchain technology into the security of the smart grid [63]. The features like decentralization, scalability, immutability, resiliency, smart contracts, transparency, and auditability, etc. make it a hopeful alternative to ensure the security and privacy of the smart grid [62]. There are mainly three types of blockchain variants being studied: public, consortium, and private blockchain. As a large number of nodes are present in the public blockchain, it is not possible to interfere with the public blockchain [64]. And practically, in the case of private and consortium blockchain, the nodes are authorized and well protected [65].

The author in [66] discussed cyber security technologies like firewalls with an intrusion detection system for network security, IDS for device security, and authentication and encryption for data security. But due to the real-time performance and continuous functioning requirements of the smart communication network, these techniques are hardly integrated into the network [67]. In SG, the communication network is centralized which makes it more prone to single-point failure [68]. To overcome this, blockchain provides peer-to-peer (P2P) data transfer and decentralized replication of data storage on multiple devices, which avoids single-point failure and ensures high availability [69]. In a blockchain-based smart grid system due to features like distributed data validation, verification, and storage, the data is immutable [63]. Hence, data confidentiality, integrity, and availability of the smart grid can be protected. Further, accountability/non-repudiation attacks are nearly impossible in blockchain-based smart grids, due to the high auditability of technology. The authentication and authorization level of blockchain-based AMI is increased because of asymmetric cryptography. This can secure the electricity data integrity and privacy of customers [70]. Data integrity attacks like FDIA, consumption data tampering, altering power trading transactions, customer's data compromised, get access to IEDs control, etc. [71] are major threats to the smart grid. Many papers like [8, 50, 72] give firewall-based methods as countermeasures against these attacks. However, due to the low computational power of ICT devices, these techniques are slow and vulnerable to cyber attacks [73]. The blockchain has been proven to be an efficient and best alternative to FDIA [74]. Further, to ensure the immutability of data, protection of cyber attacks against data collection and transfer, researchers in [69, 74–76] introduced some solutions. The article [63] discussed blockchain-based platforms, services, and applications for the cyber security of the smart grid and concluded that it is a propitious solution for the cyber security of the smart grid.

9 Conclusion

SG is a new and growing technology. The advanced features of the SG will give plentiful advantages to the customers. However, the system has to face some huge challenges, so security is a big concern. Currently, the implementation of security cautions against the cyber attacks in SG is very trending among industrialists, researchers as well as government firms. The paper introduced the SG concepts, point out core vulnerabilities, discussed the types of attacks, types of attackers and their intentions, tabular analysis of some major cyber attacks in the last two decades, and reviewed existing security solutions and integration of blockchain in SG. Blockchain comes out as a promising solution for the cyber security of the SG.

Smart grid has a complex network; hence, spotting all the possible sensitive areas is necessary to secure them from the attacks. In order to have a better future and popularity for the smart grid, it should be free from the security gaps and drawbacks. The SG has to be future resistance, which means, if there will be any attacks in the future, then it should be able to get through it. The SG is now in the earlier stage, so it is easier to implement things now instead of running without considering the security problems. The paper concludes brief conceptual understanding of the security of SG, necessity, and objectives.

It is now critical to raise cyber security awareness among SG's human interface platform. If the SG system is totally secure but the peoples are not aware of the security concept, threats, and how it works, then the security system is of no use. For example, Dec 2015 attack against Ukraine companies [41, 42], 2017 attack on western countries [46], are due to less awareness of cyber security.

The SG's total prevention is not realistic. Instead, it should be ready for the attacks, able to detect them quickly and be prepared as possible to respond.

References

1. Wang W, Lu Z (2016) Cyber security in the smart grid: survey and challenges. Comput Netw 57(7):1344–1371
2. Gopstein A, Nguyen C, O'Fallon C, Hastings N, and Wollman D (2021) NIST framework and roadmap for smart grid interoperability standards, release 4.0. Department of Commerce. National Institute of Standards and Technology
3. Farhangi H (2010) The path of the smart grid. IEEE Power Energy Mag 8(1):18–28. [Online]. Available http://ieeexplore.ieee.org/document/5357331/

4. Konstantinou C, Mohanty SP (2020) Cybersecurity for the smart grid. Computer 53(5):10–12. https://doi.org/10.1109/MC.2020.2975901
5. Faquir D et al (2021) Cybersecurity in smart grids, challenges and solutions. AIMS Electron Electr Eng 5(1):24–37
6. Liang X, Gao K, Zheng X, Zhao T (2013), A study on cyber security of smart grid on public networks. IEEE Green Technol
7. Essaaidi M et al (2015) An overview of smart grid cyber-security state of the art study. In: 3rd international renewable and sustainable energy conference (IRSEC), pp 1–7
8. Knapp ED, Samani R (2013) Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure. Syngress, Elsevier Amsterdam
9. Li F, Qiao W, Sun H et al (2010) Smart transmission grid: vision and framework. IEEE Trans Smart Grid 1(2):168–177. (Article ID 5535240)
10. Panda DK, Das S (2021) Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. J Cleaner Prod 301:126877
11. N. Framework, Roadmap for smart grid interoperability standards, release 2.0. NIST Special Publication, 1108
12. Ghosal A, Conti M (2019) Key management systems for smart grid advanced metering infrastructure: a survey. In: IEEE communications surveys and tutorials, vol 21, no 3, pp 2831–2848, thirdquarter 2019. https://doi.org/10.1109/COMST.2019.2907650
13. Pliatsios D, Sarigiannidis P, Lagkas T, Sarigiannidis AG (2020) A survey on SCADA systems: secure protocols, incidents, threats and tactics. IEEE Commun Surv Tutorials 22(3):1942–1976. https://doi.org/10.1109/COMST.2020.2987688 (thirdquarter 2020)
14. Bilal M, Rizwan M (2020) Electric vehicles in a smart grid: a comprehensive survey on optimal location of charging station. IET Smart Grid 3(3):267–279
15. Naidua H, Thanushkodib K (2010) Recent trends in SCADA power distribution automation systems. J Sci Ind Res 45(3):205–218
16. Liu Y (2012) Wireless sensor network applications in smart grid: recent trends and challenges. Int J Distrib Sens Netw 492819-1–492819-8
17. Panel SGI (2010) Guidelines for smart grid cyber security: vol. 1, smart grid cyber security strategy, architecture, and high-level requirements, and vol. 2, privacy and the smart grid, National Institute of Standards and Technology (NIST). Interagency Rep, vol 7628
18. Khurana H, Hadley M, Ning L, Frincke DA (2010) Smart grid security issues. IEEE Secur Priv 7(I):81–85
19. Line MB, Tondel IA, Jaatun MG (2011) Cyber security challenges in smart grids. In: Presented at the 2nd IEEE PES international conference and exhibition, innovative smart grid technologies (ISGT Europe), Manchester
20. European Network and Information Security Agency (ENISA). Smart Grid Security, Annex II. Security aspects of the smart grid [online]. Available https://bit.ly/3xU3xnv
21. Yadav SA, Kumar SR, Sharma S, Singh A (2016) A review of possibilities and solutions of cyber attacks in smart grids. In: 2016 international conference on innovation and challenges in cyber security (ICICCS-INBUSH), pp 60–63. https://doi.org/10.1109/ICICCS.2016.7542359
22. Clements S, Kirkham H (2010) Cyber-security considerations for the smart grid. IEEE Power and Energy Society General Meeting 2010:1–5
23. Ericsson GN (2010) Cyber security and power system communication—essential parts of a smart grid infrastructure. IEEE Trans Power Del 25:1501–1507
24. Mo Y, Kim T-J, Brancik K, Dickinson D, Lee H, Perrig A, Sinopoli B (2012) Cyber-physical security of a smart grid infrastructure. Proc IEEE 100(1):195–209
25. Baig ZA, Amoudi A-R An analysis of smart grid attacks and countermeasures. J Commun 8(8):473–479
26. Ustun TS, Hussain SMS (2019) A review of cybersecurity issues in smartgrid communication networks. In: 2019 international conference on power electronics, control and automation (ICPECA). IEEE
27. Lisovich MA, Mulligan DK, Wicker SB (2010) Inferring personal information from demand-response systems. IEEE Secur Priv 11–20

28. Chang YH (2010) Cyber security of a smart grid: vulnerability assessment. s.l. http://www.ece.nus.edu.sg/stfpage/elejp/FYP/CYH09.pdf
29. McDaniel P, McLaughlin S (2009) Security and privacy challenges in the smart grid. IEEE Secur Priv 7(3):75–77
30. Flick T, Morehouse J (2010) Securing the smart grid: next generation power grid security. Syngress, Elsevier
31. Li X, Liang X, Lu R, Shen X, Lin X, Zhu H (2012) Securing smart grid: cyber attacks, countermeasures, and challenges. IEEE Commun Mag 50(8):38–45
32. Huseinović A et al (2020) A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access 8:177,447–177,470
33. Tellbach D, Li Y-F (2018) Cyber-attacks on smart meters in household nanogrid: modeling, simulation and analysis. Energies 11(2):316
34. Engebretson P (2013) The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier
35. Poulsen K (2006) Slammer worm crashed Ohio nuke plant net. The Register, 20 Aug 2003 [online]. Available https://www.theregister.com/2003/08/20/slammer_worm_crash-ed_ohio_nuke/
36. McMillan R (2011) A power plant hack that anybody could use. COMPUTERWORLD, 5 Aug 2011 [online]. Available https://www.computerworld.com/article/2509910/a-power-plant-hack-that-anybody-could-use.html?page=2
37. Rapoza K, Lulzsec attacks Brazil Gov, Petrobras. Forbes 22 June 2011 [online]. Available https://www.forbes.com/sites/kenrapoza/2011/06/22/lulzsec-attacks-brazil-gov-petrobras/?sh=7e4f0dc71cab
38. Neslen A (2012) European renewable power grid rocked by cyber-attack. EURACTIV, 10 Dec 2012 [online]. Available https://www.euractiv.com/section/energy/news/european-renewable-power-grid-rocked-by-cyber-attack/
39. Finkle J (2014) U.S. Government asks firms to check networks after. 'Energetic Bear' attacks. Reuters, 2 July 2014 [online] Availablehttps://reut.rs/3xSvTyy
40. Symantec (2014) Dragonfly: cyberespionage attacks against energy suppliers. Symantec Security Response Version 1.21, 7 July 2014 [online] Available https://docs.broadcom.com/doc/dragonfly_threat_against_western_energy_suppliers
41. Schwartz MJ (2016) More phishing attacks target Ukraine energy sector. Information Security Media Group, 22 Jan 2016 [online]. Available https://www.bankinfosecurity.com/phishing-attacks-again-target-ukraine-energy-sector-a-8822
42. Zetter K (2017) The ukrainian power grid was hacked again. Motherboard, 10 Jan 2017 [online]. Available https://www.vice.com/en/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report
43. Cherepanov A (2017) Industroyer: biggest malware threat to critical infrastructure since Stuxnet. ESET, 12 June 2017 [online]. Available www.eset.com/int/industroyer
44. Correpondent HT (2017) WannaCry ransomware attack hits computers in West Bengal and Kerala. Hindustan Times, 15 May 2017 [online]. Available https://bit.ly/2VVR7OD
45. Perlroth N, Krauss C (2018) A cyber attack in Saudi Arabia failed to cause carnage, but the next attempt could be deadly. Independent [online]. Available https://www.independent.co.uk/news/long_reads/cyber-warfare-saudi-arabia-petrochemical-security-america-a8258636.html
46. Greenberg A (2017) Hackers gain direct access to US power grid controls. Wired [online]. Available https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/
47. Kass DH (2019) DOE: cyber event hit power grid in three U.S. States, No Outage Reported, MSSP Alert, 7 May 2019 [online]. Available https://www.msspalert.com/cybersecurity-news/cyberattacks-us-energy-grid/
48. Greenberg A (2017) Hackers gain direct access to US power grid controls. Wired [online]. Available www.wired.com/story/hackersgain-switch-flipping-access-to-us-power-systems
49. TechTarget (2018) Network, Multifactor Authentication [online]. Available https://searchsecurity.techtarget.com/definition/multifactorauthentication-MFA

50. Faisal MA, Aung Z, Williams JR, Sanchez A (2015) Data-stream based intrusion detection system for advanced metering infrastructure in smart grid: a feasibility study. IEEE Syst J 9(1):31–44
51. Zhang Y, Wang L, Sun W, Green RC II, Alam M (2011) Distributed intrusion detection system in a multi-layer network architecture of smart grids. IEEE Trans Smart Grid 2(4):796–808
52. Erol-Kantarci M, Mouftah HT (2013) Smart grid forensic science: applications, challenges, and open issues. IEEE Commun Mag 51(1):68–74
53. Abliz M (2011, March) Internet denial of service attacks and defense mechanisms. Department of. Computer Science, University of Pittsburgh, Pittsburgh, PA, USA, Tech. Rep. TR-11-178 [Online]. Available https://people.cs.pitt.edu/mehmud/docs/abliz11-TR-11-178.pdf
54. Lin D (2013, April 2013) Network intrusion detection and mitigation against denial of service attack. WPE-U Report, University of Pennsylvania
55. Xu W, Trappe W, Zhang Y, Wood T (2005) The feasibility of launching and detecting jamming attacks in wireless networks. In: Presented at the 6th ACM international symposium on mobile ad hoc networking and computing
56. Peng T, Leckie C, Ramamohanarao K (2007) Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Comput Surv 39(1):3
57. Zargar ST, Joshi J, Tipper D (2013) A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks. IEEE Commun Surv Tutorials 15(4):2046–2069
58. Masdari M, Jalali M (2016) A survey and taxonomy of DoS attacks in cloud computing. Secur Commun Netw 9(16): 3724–3751. [Online]. Available https://onlinelibrary.Wiley.com/doi/abs/https://doi.org/10.1002/sec.1539
59. Challal Y, Bettahar H, Bouabdallah A (2004) A taxonomy of multicast data origin authentication: issues and solutions. IEEE Commun Surv Tutorials 34–57
60. Molsa J (2005) Mitigating denial of service attacks: a tutorial. J Comput Secur 13(6):807–837
61. Tufail S, Parvez I, Batool S, Sarwat A (2021) A survey on cybersecurity challenges, detection and mitigation techniques for the smart grid. Engergies 14:5894
62. Mollah MB, Zhao J, Niyato D, Zhang X (2021) Blockchain for future smart grid: a comprehensive survey. IEEE Internet of Things J 8(1)
63. Zhaung P, Zamir T, Liang H (2021) Blockchain for cybersecurity in smart grid: a comprehensive survey. IEEE Trans Ind Inf 17(1)
64. Wang W et al (2019) A survey on consensus mechanisms and mining strategy management in blockchain networks. IEEE Access 7:22328–22370
65. Hamida EB, Brousmiche KL, Levard H, Thea E (2017, July) Blockchain for enterprise: overview, opportunities and challenges. In: Proceedings of ICWMC, pp 83–88
66. Mrabet ZE, Kaabouch N, Ghazi HE, ElGhazi H (2018) Cybersecurity in smart grid: survey and challenges. Comput Electr Eng 67(1):469–482
67. Yan Y, Qian Y, Sharif H, Tipper D (2012) A survey on cyber security for smart grid communications. IEEE Commun Surv Tutorials 14(4):998–1010
68. Bani-Ahmed A, Rashidi M, Nasiri A, Hosseini H (2019) Reliability analysis of a decentralized microgrid control architecture. IEEE Trans Smart Grid 10(4):3910–3918
69. Winter TMGL (2018) The advantages and challenges of the blockchain for smart grids. MS thesis, TU Delft University of Technology, Delft, Netherlands
70. Lazaroiu GC (2018) Blockchain and smart metering towards sustainable prosumers. In: Proceedings of IEEE international symposium on power electronics, electrical drives, automation and motion, pp 550–555
71. Hao J, Piechocki RJ, Kaleshi D, Chin WH, Fan Z (2015) Sparse malicious false data injection attacks and defense mechanisms in smart grids. IEEE Trans Ind Informat 11(5):1198–1209
72. Grammatikis PR, Sarigiannidis P, Liatifs T (2018, October) An overview of the firewall systems in the smart grid praradigm. In: 2018, GIIS, pp 1–4
73. Tan S, Song W, Member S, Stewart M, Yang J, Tong L (2018) Online data integrity attacks against real-time electrical market in smart grid. IEEE Trans Smart Grid 9(1):313–322
74. Kurtm MN, Yilmaz Y, Wang X (2019) Secure distributed dynamic state estimation in wide-area smart grids. CoRR 1(1):1902–1918

75. Wang S, Ouyang L, Yuan Y, Ni X, Han X, Wang F (2019) Blockchain enabled smart contracts: architecture, applications, and future trends. IEEE Trans Syst Man Cybern Syst 49(11):2266–2277
76. Wang S, Taha AF, Wang J (2018) Blockchain assisted crowdsourced energy systems. In: Proceedings of IEEE power energy society general meeting, pp. 167–172
77. Singh NK, Mahajan V (2019) Smart grid: cyber attack identification and recovery approach. In: 2019 2nd international conference on innovations in electronics, signal processing and communication (IESC), 2019, pp 1–5. https://doi.org/10.1109/IESPC.2019.8902401
78. Abdul Majeed M, Kumar Singh N, Tak L, Mahajan V (2021) Detection of stealthy cyber intrusion in smart electric grid using advanced state estimation. In: 2021 11th international conference on cloud computing, data science & engineering (Confluence), pp 660–665. https://doi.org/10.1109/Confluence51648.2021.9377067
79. Singh NK, Mahajan V (2021) End-user privacy protection scheme from cyber intrusion in smart grid advanced metering infrastructure. Int J Crit Infrastruct Prot 100410
80. Gupta PK, Singh NK, Mahajan V (2020) Monitoring of cyber intrusion in wireless smart grid network using weight reduction technique. In: 2020 international conference on electrical and electronics engineering (ICE3), pp 136–139. https://doi.org/10.1109/ICE348803.2020.9122981