International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(REVIEW ARTICLE)

Check for updates

A robust firewall security based on software defined networking for mitigating data availability attacks in smart grid AMI network

Uchechukwu Okonkwo *

College of Business, University of Louisville, Louisville Kentucky, United States.

International Journal of Science and Research Archive, 2023, 09(02), 1026–1035

Publication history: Received on 03 April 2023; revised on 22 July 2023; accepted on 25 August 2023

Article DOI: https://doi.org/10.30574/ijsra.2023.9.2.0364

Abstract

The global transition from conventional grids to smart grids is advancing rapidly, bringing with it new opportunities as well as challenges. One of the most significant challenges facing the smart grid is safeguarding it against potential cyberattacks. With millions of sensors continuously transmitting and receiving data packets across the network, managing such an extensive system presents a formidable challenge. Cyberattacks can severely compromise the confidentiality, integrity, and availability of the smart grid, undermining its core functions.

The smart grid is comprised of three primary layers, each of which is vulnerable to cyberattacks: customers accessing the network, the communication infrastructure of smart devices and sensors, and the decision-makers responsible for managing the network. In this survey, we examine the various threats and vulnerabilities that can impact the key cybersecurity elements within the smart grid and propose security measures to mitigate these risks across all three levels. Additionally, we recommend techniques to reduce the likelihood of cyberattacks and enhance the resilience of the smart grid at each layer.

Keywords: Firewall Security; Mitigating Data; Smart Grid AMI Network; Software

1. Introduction

The traditional electricity grid has evolved through modern technology into what is now known as the smart grid. A smart grid integrates a range of advanced operational and energy management techniques, including smart meters, smart appliances, production meters, renewable energy generators, smart inverters, and energy efficiency resources. These components are deployed both at the customer's premises and at the grid level. Renewable energy generators play a significant role in reducing energy costs, as electricity generated from renewable sources has no production cost. However, renewable energy is intermittent and highly dependent on factors such as temperature, humidity, wind speed and direction, and geographic location. For example, solar energy production is influenced by irradiance, cloud cover, and ambient temperature, while wind energy fluctuates based on wind speed and direction. Various forecasting techniques exist to predict wind energy, solar energy, and battery charge levels to incorporate renewable energy efficiently and reliably.

The smart grid facilitates two-way communication between the grid and sensors located in various areas. These sensors continuously transmit production data to the grid, including energy generation, consumption, voltage, frequency, and other critical information. Currently, battery-integrated grids also communicate the battery's state of charge, exposing the battery management system (BMS) to potential cyber threats. Such cyber threats could lead to overcharging or undercharging, potentially resulting in catastrophic outcomes.

* Corresponding author: Uchechukwu Okonkwo

The smart grid offers several advantages over traditional grids, including improved power quality, self-healing capabilities, cost-effective integration of renewable energy, adaptive energy generation, environmental benefits, real-time energy monitoring at the customer level, automation through artificial intelligence, remote fault detection, and automated maintenance. These benefits make the smart grid far more attractive than conventional grids. However, two primary challenges persist: cybersecurity and system complexity. These challenges are further compounded when smart grid data is hosted on the cloud.

Cybersecurity is a critical concern for the smart grid to ensure its stability and security. While physical security remains important, cybersecurity has become a vital component, not only for smart grids but for traditional grids as well. Studies have shown that even nonsmart grids are vulnerable to cyberattacks. For instance, research demonstrated that malicious software (botnets) could control power consumption in devices such as CPUs, GPUs, hard disks, and printers, destabilizing the grid if 2.5 to 9.8 million infections occur. Another study highlighted the potential impact of high-wattage IoT devices on grid stability, where attackers could manipulate these devices to cause frequency instability, line failures, and increased operational costs. Such attacks have the potential to cause widespread blackouts by artificially inflating energy demand.

As the complexity of the smart grid increases, so do the chances of faults. For example, thousands of sensors may be installed, and a malfunction in one sensor could transmit faulty data, destabilizing the entire grid despite no actual fault in the production devices. Another critical challenge is securing communication between devices and the grid. The complexity of these communication channels makes it difficult to safeguard smart grid data, leaving it vulnerable to cyberattacks that could result in physical damage to the grid.

2. Communication Architecture of Smart Grid

A communication network connects the three domains: service provider, grid, and customer. This communication occurs across a variety of different protocols and channels. The grid domain encompasses large-scale energy generation, distribution, and transmission. The smart meter connects concurrently with the consumer domain and the communication network and this combined network is known as Advanced Metering Infrastructure(AMI) network. Smart meters are assigned to send data of consumption of use, outages, and electricity prices [7]. It communicates with the consumer domain using a short-range protocol such as Zigbee, and with the customer domain via GSM, Wi-Fi, and so on. While the smart grid enables more efficient energy distribution than the traditional centralized system, it is subject to security attacks at many tiers

3. Vulnerabilities in the Smart Grid

The vulnerability of a smart grid network is the weak spot at which an attacker may enter the network and attack the system. The smart grid connects with multiple domains using different protocols, making it vulnerable to numerous cyberattacks. In this section, we explore the conditions that might increase the vulnerability of the grid to cyber intrusion. However, first, we discuss the types of cyberattacks. There are mainly two kinds of attacks: (1) passive attacks and (2) active attacks. Passive attacks are those in which no harm to the data is done, but the attacker only monitors the data, whereas the active attacks are more dangerous compared to active attacks, as the attacker modifies the data or stops the receiver from receiving the data.

The passive attacks are classified into two categories:

- Eavesdropping attack and
- Traffic analysis attacks.

The types of active attacks includes masquerade attacks, replay attack, false data attack, and denial of service attacks.

The eavesdropping attacks is when the attacker can see the data packets shared between sender and the receiver. However, the attacker does not modifies the data. Traffic analysis attack is another kind of passive attack in which the attacks continuously monitors and analyzes the traffic between the sender and the receiver. Active attacks are more harmful than the passive attacks, as the attacker has full control over the data. The replay attack is when the attacker and sender both send the data to the receiver; this confuses the receiver in differentiating between real data by sender and the data routed through the attacker. In the masquerade attack, the sender is idle, but the receiver keeps receiving data from the attacker. The false data injection attack in when the data do not come to the receiver directly from the sender instead the receiver receives the modified data from the attacker. However, both the sender and the receiver are

unaware about the modification done by the attacker. Denial of service attack is a kind of attack in which attacker does not target the sender or receiver but the data server. The attacker generates a bulk amount of irrelevant requests from the server and the server starts serving those irrelevant requests until all of its resources are exhausted. The receiver/sender requests information from the server, and due to unavailability of resources, the request from the sender/receiver is denied. The major causes that make the smart grid vulnerable to cyberattacks are as follows:

- Increased installation of intelligent electronic devices (IEDs): As the number of devices in the network rises, the number of attack sites for attackers increases as well. Even if the security of a single point is compromised, the entire network system would be impacted.
- Installation of third-party components: Third-party components that are not advised by experts increase the network's vulnerability to cyberattack. These devices may be infected with trojans, which can then infect other devices on the network.
- Inadequate personnel training: Proper training is necessary to operate any technology. When staff are not sufficiently taught, they might easily fall victim to phishing attempts.
- Using Internet protocols: Not all protocols are secure when it comes to data transmission. Certain protocols transfer data in an unencrypted format. As a result, they are easy candidates for data extraction via man in the middle attacks.
- Maintenance: While the primary goal of maintenance is to keep things functioning properly, it can become a vector for cyberattacks at times. While doing maintenance, operators often disable the security system to conduct testing. In 2015, electric power companies in eastern Europe reported one similar occurrence.

4. Cybersecurity Challenges in Grid-Connected EV Charging Stations

The integration of electric vehicle charging systems (EVCS) has added complexity to power systems and grids. In recent years, electric vehicle (EV) sales have surged, driven primarily by economic and environmental benefits. Technological advancements have significantly reduced the cost of EVs and their batteries, further supported by government incentives. Additionally, EVs contribute to reducing carbon footprints due to their independence from fossil fuels.

However, EVCSs are vulnerable to cyberattacks as they rely on both wired and wireless communication systems to interact with the smart grid. EVCS vulnerabilities can be broadly categorized into internal and external threats. Internal vulnerabilities include weak password protection, insufficient hashing algorithms, inadequate access control, unsigned firmware updates, and easy extraction of firmware—each of which could enable attackers to gain full control of the system. External vulnerabilities, such as human-machine interfaces (HMIs) allowing users to connect USB devices on-site, can be exploited to compromise EVCS configurations.

There is no universal communication standard for EVCSs, though many vendors have adopted the Open Charge Point Protocol (OCPP). Unfortunately, OCPP is susceptible to man-in-the-middle attacks. Moreover, numerous smartphone and web-based applications have been developed to assist users in locating nearby EVCSs, authenticating vehicles, and remotely managing charging and payments. These apps present additional cybersecurity risks, as malicious or cloned applications could potentially harm EVCSs.

Research on cybersecurity challenges within the onboard charging (OBC) system of EVs highlights vulnerabilities in the electric component units (ECUs), which communicate through a controller area network (CAN). Cyberattacks on OBC systems are classified into two main categories: control-based attacks and hardware-based attacks. The growing sales of EVs are closely tied to the expansion of EVCS installations, which will inevitably impact energy demand as EV adoption rises.

This study outlines the communication requirements and standards for the Internet of Electric Vehicles (IoEV). Another research effort proposed a framework for analysis, comparison, and testing of standards (FACTS) to identify cyberthreats in battery management systems (BMS).

5. Cyberattack Detection and Mitigation Techniques

Smart grids involve a wide range of stakeholders, including consumers, electric utilities, grid operators, and third-party service providers. This diversity of stakeholders makes managing smart grid data, particularly from smart meters, a complex and challenging task. To enhance the security and privacy of smart meters, a framework has been proposed that provides guidelines for integrating security and privacy across various domains. The framework categorizes security into three key areas: communication security, secure computing, and system control security.

Communication security encompasses cryptosystems, routing security, and network privacy, which can be achieved through key management systems, end-to-end encryption, and multi-hop routing. Additionally, smart meters are primarily responsible for recording energy consumption and factors such as voltage and frequency, as well as transmitting this data to the grid through secure communication channels. They also allow operators to control load switches to prevent blackouts during emergencies. The concept of high assurance smart meters (HASM) was introduced to address these needs.

In addressing cybersecurity for smart grids, various approaches have been proposed. As the complexity of the grid increases with the integration of artificial intelligence (AI), further research is being conducted to improve reliability. Some studies also indicate that the smart grid is vulnerable to human error, particularly due to social engineering attacks. In this paper, we categorize existing approaches into two main groups: non-human-centric approaches and human-centric approaches.

5.1. Machine-Learning-Based Attack Detection and Mitigation

As the transition from traditional grids to smart grids progresses, thousands of sensors are being installed within the smart grid infrastructure. These sensors continuously monitor the status of connected devices, generating vast amounts of data in the form of log files or time series data. Examples of such sensors include irradiance sensors, module temperature sensors, voltage monitors, and current monitors. The data collected by these sensors are stored on servers, which may be local or cloud-based. Before transmission to servers, the data are sometimes preprocessed. While local servers offer the highest level of data protection, they limit the potential for uncovering new patterns or gaining insights from the data. Cloud servers, on the other hand, provide greater flexibility, allowing remote access and data retrieval via GETS commands.

Recently, machine learning algorithms have demonstrated high accuracy in detecting cyber intrusions. Unlike traditional rule-based methods, machine learning relies on historical data to identify potential threats. A combination of JRipper and Adaboost has been developed to predict power system disturbances, classifying events into three categories: attack, natural disturbances, and no event. False data injection attacks (FDIA), also known as data poisoning attacks, are among the most common threats to smart grid networks. These attacks can cause significant damage to both utilities and customers by compromising data from smart meters. To detect FDIA, researchers have applied ensemble-based machine learning algorithms. When tested on the IEEE 14-bus system, these models outperformed traditional methods such as linear regression, naive Bayes, decision trees, and support vector machines (SVM), achieving a highest accuracy of 73%.

Further research has examined the impact of FDIA on AI-based smart grids using multilayer perceptron (MLP) models. Findings indicate that falsifying as little as 20% of the data can reduce the accuracy of machine learning algorithms by 15%, significantly affecting critical decision-making processes. For instance, if false data prevents the model from predicting disturbances, the grid could enter an unstable state, potentially leading to catastrophic outcomes. To address this, a conditional deep belief network model has been proposed for real-time detection of FDIA related to power theft, showing promising results on IEEE 118 and 300 bus systems when compared to artificial neural networks and SVM-based methods.

In addition to FDIA, smart grids are also vulnerable to distributed denial of service (DDoS) attacks, which target communication resources such as servers. The goal of a DDoS attack is to overwhelm the server with fake requests, rendering it unavailable for legitimate communication. A multilevel autoencoder model has been proposed to detect DDoS attacks, utilizing data from approximately 700,000 packets with 49 features, including source and destination IP addresses, ports, jitters, record time, and attack categories. The model, trained using the publicly available UNSW-NB15 dataset, outperformed other methods such as long short-term memory (LSTM), random forest, naive Bayes, decision trees, k-nearest neighbors, and LSVM.

5.2. Cloud-Based Detection and Mitigation

A study explored how cloud computing attributes can enhance security during DDoS attacks on the smart grid. Another study proposed a cloud-based firewall to prevent such attacks by simulating 250 Gbps of data to replicate a DDoS scenario, with results showing low latency using the grid's OpenFlow firewall. Additionally, an attribute-based online/offline searchable encryption scheme was introduced to secure data access for authorized users in cloud environments, specifically for smart grid applications. Researchers also proposed a secure home area network, leveraging the cloud of things, to defend against brute force, replay, capture, and other attacks. Furthermore, a security evaluation model for the smart grid was developed using a deep belief network (DBN) comprising multiple restricted Boltzmann machines (RBMs) and a backpropagation (BP) neural network. This model evaluated security risks across

five dimensions: policy and organizational risks, general technical risks, and risks associated with SaaS, PaaS, and IaaS environments.

5.3. Blockchain-Based Detection and Mitigation

Blockchain has emerged as one of the most promising technologies across various industries due to its inherent security features. It operates as a chain of blocks, each containing an index, timestamp, previous hash, current hash, and data. The security of blockchain is largely attributed to its hashing mechanism, which makes tampering with any block computationally expensive, as altering the hash of one block would require changes to all preceding blocks in the chain.

One study proposed a blockchain-based policy architecture to protect against false data injection attacks (FDIA) by enabling secure data exchange between independent system operators and sub-operating agents. This model consists of three layers: the data layer (responsible for data collection), the detection layer (for community detection), and the blockchain layer (which secures community detection and transaction records).

Another research effort introduced a blockchain-based secure message transfer method for smart meters and service providers, aiming to prevent FDIA on the smart meter side. In this approach, each transaction is initiated by the smart meters, with the service provider acting as the master node. Transaction information is shared across the network and validated periodically through auditing and broadcasting, with providers connected in a peer-to-peer (P2P) network. To add a new block, consensus verification is required, and a key is generated using the SHA-256 algorithm for each transaction. This method demonstrated the feasibility of secure data exchange within a P2P service provider network.

In addition, a decentralized security model using the lightning network and smart contracts in the blockchain ecosystem was introduced, covering registration, scheduling, authentication, and charging phases. Another study proposed an innovative framework that integrates hardware security with blockchain for grid-edge devices, providing a distributed cybersecurity solution to verify the provenance of messages to and from the devices.

5.4. Hardware-Based Security

IoT devices play a crucial role in the smart grid network, responsible for data collection, analysis, and transmission over communication channels. However, these devices must also be fortified against cyberattacks. Key hardware security challenges include physical attacks, side-channel analysis, and hardware Trojans. In a physical attack, the attacker bypasses the authentication system by exploiting system vulnerabilities identified through reverse engineering. Side-channel analysis involves predicting cryptographic keys by analyzing features such as current, voltage, and frequency profiles. Hardware Trojans refer to unauthorized modifications made to circuits to compromise functionality, reliability, or access to sensitive data. Methods to detect hardware Trojans using path delay fingerprints have been proposed to address these threats.

IoT devices, including smart meters and sensors, face significant challenges such as limited energy capacity and computational resources. Physical unclonable functions (PUFs) offer secure authentication for these resource-constrained devices without requiring cryptographic capabilities. However, the rise of machine learning has made PUF behavior increasingly predictable, with models achieving up to 95% accuracy. To counter machine-learning-based attacks, researchers developed a configurable tristate PUF (CTPUF) that uses an XOR-based mechanism to obscure the relationship between challenges and responses. This approach significantly reduces machine learning accuracy, with models such as support vector machines (SVM), artificial neural networks (ANN), and logistic regression dropping to around 60%.

Additionally, studies have highlighted the vulnerabilities of voltage-overscaling (VOS)-based authentication systems, which can also be exploited by machine learning models. To address this, a machine-learning-resistant VOS method was proposed, integrating prior challenges with cryptographic keys. This technique, known as challenge self-obfuscation structure (CSoS), reduced the accuracy of machine learning models to approximately 51.2%, providing enhanced security against such attacks.

6. Human-Centric Mitigation Approaches

This section discusses various human-centric attack detection and mitigation approaches.

6.1. Multifactor Authentication (MFA)

MFA is a critical measure for protecting data from unauthorized access by integrating two sequential authentication processes, exponentially increasing the difficulty of breaking passwords. This approach significantly reduces the likelihood of unauthorized access. Common MFA techniques include SMS token authentication, email token authentication, hardware token authentication, software token authentication, and phone authentication. After the user completes the initial authentication, they are prompted to verify their identity using one of these methods. The codes or passwords generated in the second phase are valid for a single login session.

In SMS token systems, users receive a unique 4 to 8-digit pin via text message. Similarly, email tokens are sent to a verified email address. The algorithms used to generate these random codes are beyond the scope of this discussion. Hardware tokens, considered the most secure MFA method, are often used in sectors where data security is paramount, such as banking, insurance, and healthcare. Users must physically insert the hardware token into their device to authenticate. Software tokens operate similarly to SMS tokens but deliver the one-time password through an app rather than a wireless provider, offering security comparable to hardware tokens. Phone MFA can either involve receiving a token via SMS or a voice call to verify identity.

6.2. Employee Training

As technology advances, attackers increasingly target human vulnerabilities, recognizing that employees may be the weakest link in security. Machine learning tools assist attackers in understanding employee behavior and responses in various situations. Without proper training, employees become easy targets. Social engineering attacks, second only to malware, have become a common tactic, with ransomware specifically targeting humans rather than machines. Comprehensive employee training is crucial in preventing cyberattacks, especially in smart grid networks, where human operators at control centers are key decision-makers. Proper training equips employees to recognize and avoid social engineering attacks, such as phishing or ransomware, which, if successful, can grant attackers control over the grid, leading to catastrophic consequences.

Employee training also helps mitigate insider attacks, where disgruntled employees use their access to harm the organization. Training can provide employees with guidance on how to handle workplace dissatisfaction and encourages the reporting of unusual or suspicious behavior among colleagues.

6.3. Password Strength

Strong passwords are essential in reducing the risk of integrity and confidentiality breaches. Weak passwords are particularly susceptible to password-guessing attacks, in which an attacker attempts to gain access to a system by guessing passwords, often remotely. These attacks consume network resources and bandwidth, disrupting service for legitimate users and generating large volumes of log data. The strength of a password is measured by its information entropy, expressed in bits. For example, a 32-bit password would require 2^32 attempts to crack via brute force. The stronger the password, the more difficult it becomes for attackers to guess, making it a viable defense against intrusions.

7. Customer Protection Technique

7.1. Operating System Protection

Customers are often considered one of the weakest links in the cybersecurity chain, largely because they cannot be systematically trained like employees. Therefore, it is crucial to ensure that devices such as smart meters and inverters are protected against tampering. Making these devices tamper-proof is the most effective way to prevent customers from altering the internal operating system. This not only secures the device but also helps avoid meter manipulation, which could result in significant financial losses for utility providers due to underreported usage.

7.2. Customer Notifications

Providing customers with tailored recommendations based on their current settings is another protective measure. For instance, if a customer uses a utility application on a handheld device with an outdated operating system, they become more vulnerable to attacks. Even if only one customer's security is breached, the attacker can gather enough information

to potentially target others. Ensuring customers are notified of potential risks, such as using outdated systems, helps mitigate these threats.

7.3. Software and Hardware Security

In addition to safeguarding devices from network-based attacks, customers must protect their devices physically, starting with strong passwords. Sharing personal details or passwords with friends can make customers susceptible to password-guessing attacks. In some cases, this could enable attackers to install malicious software (bots) to monitor or even take control of the device.

7.4. Protection Against Third-Party Applications

Customers should exercise caution when granting permissions to third-party applications. Many applications request more access than necessary, which could expose sensitive information. Studies show that 98.5% of users pay little to no attention to the permissions required by these applications, and 93.6% accept the terms and conditions within a minute of viewing them. This careless approach increases the risk of data breaches.

7.5. Cyberattack Reporting

Utility providers should establish a platform for customers to report suspected cyberattacks promptly. The longer the delay between an attack and its reporting, the greater the potential damage, not only to the affected customer but to others as well. A 24/7 customer support service that guides users through the necessary actions in the event of an attack is an essential solution to minimize harm.

8. Open Issues, Challenges, and Future Research Directions

Smart grids, recognized for their environmental benefits, utilize renewable energy sources and offer enhanced safety compared to traditional power grids. They also demonstrate superior efficiency and productivity. However, research indicates that smart grids are susceptible to cyberattacks. While the advantages of smart grids can mitigate cybersecurity challenges through various technologies and techniques, multiple studies highlight both their security benefits and vulnerabilities.

One significant concern is the potential for denial-of-service attacks, which could incapacitate smart grids due to their reliance on interconnected networks. To maintain service availability, smart grids must incorporate multiple security layers, such as virtual private networks (VPNs) for secure communication, intrusion prevention systems (IPS), and intrusion detection systems (IDS). Human error remains a risk for both smart and traditional grids. This risk can stem from overburdened employees, social engineering, or insider threats, particularly if employees are not adequately trained to address these vulnerabilities. Ransomware attacks, which have surged by 500% since 2018, require urgent attention due to their potential for significant financial losses and the exposure of confidential information. Although some researchers have explored the effects of ransomware on smart grid infrastructure, further investigation is necessary to understand the underlying causes and impacts.

Self-awareness regarding cyberattacks on smart grids is essential for users. To enhance protection against various cyber threats, users should engage in risk analysis and case studies to identify and mitigate potential risks associated with smart grid technology. A critical challenge faced by smart grids is the integration of diverse devices across extensive geographic networks, necessitating robust security measures for this infrastructure. Blockchain technology offers promising solutions by enabling data sharing and encryption, addressing security concerns related to malicious actors, and facilitating secure identity authentication and transaction access through a centralized database. Furthermore, it allows for efficient data transfers across distributed devices.

To stay ahead of emerging threats, it is essential to update computer network protocols to reflect current communication standards and incorporate modern encryption technologies and security countermeasures. The complexities of securing smart grid systems arise from the wide dispersion of safety requirements and objectives across vast areas. Given the importance of power infrastructure and the socioeconomic repercussions of blackouts, smart grids are particularly vulnerable to cyber terrorism.

Comprehensive cyber defense solutions are needed to protect all components of smart grid systems. These solutions should integrate a range of defense technologies, including machine learning, proactive IDS/IPS systems, wireless

controlled propagation, and robust authorization, authentication, and certification measures. Additionally, these defenses must be scalable, resilient, and adaptive, ensuring that cybersecurity measures do not compromise the operational integrity of smart grids.

9. Conclusions

Innovation inherently involves risks, and the transition from a conventional grid to a smart grid introduces additional complexities. Alongside the necessity of developing and maintaining a robust physical architecture for the smart grid, the construction, operation, and maintenance of the communication network architecture present significant challenges.

This study conducts a comprehensive analysis of the smart grid communication network, including a thorough examination of potential cyberattacks and their corresponding mitigation strategies. It is important to recognize that no attack is insignificant; even minor incidents can lead to catastrophic consequences.

To address these vulnerabilities, we propose a solution aimed at creating a resilient smart grid network by securing customers, the communication network itself, and the personnel involved in its management. We emphasize that the communication network is susceptible to cyberattacks, and the individuals who utilize or oversee it are equally vulnerable, potentially becoming easy targets if they fail to adequately manage these threats.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] FERC. Federal Energy Regulatory Commission Assessment of Demand Response & Advanced Metering; Federal Energy Regulatory Commission: Washington DC, USA, 2020. Available online: https://www.ferc.gov/industries-data/electric/power-sales-and-markets/demand-response/reports-demand-response-and.

[2] Benger, S.N.; Zhou, S.; Guan, H. A dynamic solar irradiance model for assessing solar PV power generation potential in urban areas. In Proceedings of the 2014 International Conference and Utility Exhibition on Green Energy for Sustainable Development (ICUE), Jomtien Beach, Thailand, 19–21 March 2014; pp. 1–4.

[3] Tufail, S.; Qadeer, M.A. Cloud Computing in Bioinformatics: Solution to Big Data Challenge. Int. J. Comput. Sci. Eng. 2017, 5, 232–236.

[4] Parvez, I.; Ahmed, A.; Dharmasena, S.; Tufail, S.; Sundararajan, A. Latency Critical Data Processing in Cloud for Smart Grid Applications. In Advances in Information and Communication; Arai, K., Ed.; Springer International Publishing: Cham, Switzerland, 2021; pp. 663–676.

[5] Dabrowski, A.; Ullrich, J.; Weippl, E.R. Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. In Proceedings of the 33rd Annual Computer Security Applications Conference, Orlando, FL, USA, 4–8 December 2017; Association for Computing Machinery: New York, NY, USA, 2017; pp. 303–314.

[6] Soltan, S.; Mittal, P.; Poor, H.V. BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid. In Proceedings of the 27th USENIX Security Symposium (USENIX Security 18), Baltimore, MD, USA, 15–17 August 2018; USENIX Association: Baltimore, MD, USA, 2018; pp. 15–32.

[7] Yi, P.; Zhu, T.; Zhang, Q.; Wu, Y.; Li, J. A denial of service attack in advanced metering infrastructure network. In Proceedings of the 2014 IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 10–14 June 2014; pp. 1029–1034.

[8] Bari, A.; Jiang, J.; Saad, W.; Arunita, J. Challenges in the Smart Grid Applications: An Overview. Int. J. Distrib. Sens. Netw. 2014, 2014, 1–11.

[9] Ericsson, G.N. Cyber Security and Power System Communication—Essential Parts of a Smart Grid Infrastructure. IEEE Trans. Power Deliv. 2010, 25, 1501–1507.

[10] Knapp, E.D.; Samani, R. Chapter 4—Privacy Concerns with the Smart Grid. In Applied Cyber Security and the Smart Grid; Knapp, E.D., Samani, R., Eds.; Syngress: Boston, MA, USA, 2013; pp. 87–99.

[11] McLaughlin, S.; Podkuiko, D.; McDaniel, P. Energy Theft in the Advanced Metering Infrastructure. In Critical Information Infrastructures Security; Rome, E., Bloomfield, R., Eds.; Springer: Berlin/Heidelberg, Germany, 2010; pp. 176–187.

[12] Asghar, M.R.; Dan, G.; Miorandi, D.; Chlamtac, I. Smart Meter Data Privacy: A Survey. IEEE Commun. Surv. Tutor. 2017, 19, 2820–2835.

[13] Cleveland, F.M. Cyber security issues for Advanced Metering Infrasttructure (AMI). In Proceedings of the 2008 IEEE Power and Energy Society General Meeting—Conversion and Delivery of Electrical Energy in the 21st Century, Pittsburgh, PA, USA, 20–24 July 2008; pp. 1–5.

[14] Gauci, A.; Michelin, S.; Salles, M. Addressing the challenge of cyber security maintenance through patch management. CIRED-Open Access Proc. J. 2017, 2017, 2599–2601.

[15] Kumar, R.R.; Alok, K. Adoption of electric vehicle: A literature review and prospects for sustainability. J. Clean. Prod. 2020, 253, 119911.

[16] Acharya, S.; Dvorkin, Y.; Pandžić, H.; Karri, R. Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective. IEEE Access 2020, 8, 214434–214453.

[17] Chandwani, A.; Dey, S.; Mallik, A. Cybersecurity of Onboard Charging Systems for Electric Vehicles—Review, Challenges and Countermeasures. IEEE Access 2020, 8, 226982–226998.

[18] Bayram, I.S.; Papapanagiotou, I. A survey on communication technologies and requirements for internet of electric vehicles. EURASIP J. Wirel. Commun. Netw. 2014, 2014, 223.

[19] Khalid, A.; Sundararajan, A.; Hernandez, A.; Sarwat, A. FACTS Approach to Address Cybersecurity Issues in Electric Vehicle Battery Systems. In Proceedings of the 2019 IEEE Technology & Engineering Management Conference (TEMSCON), Atlanta, GA, USA, 12–14 June 2019.

[20] Pillitteri, V.; Brewer, T. Guidelines for Smart Grid Cybersecurity, 2014-09-25; NIST Interagency/Internal Report (NISTIR); National Institute of Standards and Technology: Gaithersburg, MD, USA, 2014.

[21] Agarkar, A.; Agrawal, H. A review and vision on authentication and privacy preservation schemes in smart grid network. Secur. Priv. 2019, 2, e62.

[22] Shuaib, K.; Trabelsi, Z.; Abed-Hafez, M.; Gaouda, A.; Alahmad, M. Resiliency of Smart Power Meters to Common Security Attacks. Procedia Comput. Sci. 2015, 52, 145–152.

[23] Zhang, F.; Mahler, M.; Li, Q. Flooding attacks against secure time-critical communications in the power grid. In Proceedings of the 2017 IEEE International Conference on Smart Grid Communications (SmartGridComm), Dresden, Germany, 23–27 October 2017; pp. 449–454.

[24] Lu, Z.; Lu, X.; Wang, W.; Wang, C. Review and evaluation of security threats on the communication networks in the smart grid. In Proceedings of the 2010—MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE, San Jose, CA, USA, 31 October–3 November 2010; pp. 1830–1835.

[25] Huseinovic, A.; Mrdovic, S.; Bicakci, K.; Uludag, S. A Taxonomy of the Emerging Denial-of-Service Attacks in the Smart Grid and Countermeasures. In Proceedings of the 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 20–21 November 2018; pp. 1–4.

[26] Liu, S.; Liu, X.P.; El Saddik, A. Denial-of-Service (dos) attacks on load frequency control in smart grids. In Proceedings of the 2013 IEEE PES Innovative Smart Grid Technologies Conference (ISGT), Washington, DC, USA, 24–27 February 2013; pp. 1–6.

[27] Huseinović, A.; Mrdović, S.; Bicakci, K.; Uludag, S. A Survey of Denial-of-Service Attacks and Solutions in the Smart Grid. IEEE Access 2020, 8, 177447–177470.

[28] Cameron, C.; Patsios, C.; Taylor, P.C.; Pourmirza, Z. Using Self-Organizing Architectures to Mitigate the Impacts of Denial-of-Service Attacks on Voltage Control Schemes. IEEE Trans. Smart Grid 2019, 10, 3010–3019.

[29] Kurt, M.N.; Yilmaz, Y.; Wang, X. Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid. IEEE Trans. Inf. Forensics Secur. 2019, 14, 498–513.

[30] Chatfield, B.; Haddad, R.J.; Chen, L. Low-Computational Complexity Intrusion Detection System for Jamming Attacks in Smart Grids. In Proceedings of the 2018 International Conference on Computing, Networking and Communications (ICNC), Maui, HI, USA, 5–8 March 2018; pp. 367–371.

[31] Reeves, A.; Delfabbro, P.; Calic, D. Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue. SAGE Open 2021, 11.

[32] Mugarza, I.; Flores, J.L.; Montero, J.L. Security issues and software updates management in the industrial internet of things (iiot) era. Sensors 2020, 20, 7160.

[33] Califano, A.; Dincelli, E.; Goel, S. Using features of cloud computing to defend smart grid against DDoS attacks. In Proceedings of the 10th Annual Symposium on Information Assurance (Asia 15), Albany, NY, USA, 2–3 June 2015; pp. 44–50.