World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Privacy and security issues in smart grids: A survey

Ogweno Jeremiah Okeyo *

Jaramogi Oginga Odinga University of Science and Technology, Bondo-Kenya.

World Journal of Advanced Engineering Technology and Sciences, 2023, 10(02), 182–202

Publication history: Received on 06 November 2023; revised on 19 December 2023; accepted on 22 December 2023

Article DOI: https://doi.org/10.30574/wjaets.2023.10.2.0306

Abstract

Smart grids have emerged as a transformative technology in the energy sector, enabling efficient electricity management, improved reliability, and integration of renewable energy sources. The necessity to promote smart grid (SG) has been recognized with a strong consensus. The SG integrates electrical grids and communication infrastructures and forms an intelligent electricity network working with all connected components to deliver sustainable electricity supplies. Many advanced communication technologies have been identified for SG applications with a potential to significantly enhance the overall efficiency of power grids. However, the widespread deployment of smart grids raises concerns about the privacy and security of the data collected and transmitted by these systems. To address these concerns, this paper proposes a comprehensive framework for ensuring privacy and security in smart grid systems. This framework includes encryption techniques, access control mechanisms, and robust authentication protocols. Additionally, this paper discusses the importance of user awareness and education in mitigating privacy and security risks. The research contributes to the existing literature on smart grid privacy and security by providing insights specific to the information technology security domain. The findings of this manuscript will be valuable for policymakers, energy providers, and researchers working towards the development of secure and privacy-preserving smart grid systems.

Keywords: Smart grids; Privacy; Security; Data protection

1. Introduction

In an era of rapidly advancing technology, the concept of a "Smart Grid" has emerged as a promising solution to modernize and enhance our electrical infrastructure. By integrating advanced communication and information technologies into the traditional power grid, Smart Grids offer numerous benefits such as improved efficiency, reliability, and sustainability [1]-[6]. However, as this transformative technology becomes more prevalent, concerns regarding privacy and security have also come to the forefront. This manuscript aims to delve into the privacy and security issues surrounding Smart Grids, examining the potential risks and vulnerabilities that arise from the collection and transmission of vast amounts of data. It will explore the implications of these concerns on individual privacy, national security, and societal trust in this evolving energy landscape. Table 1 presents the comparisons of the traditional power grid and smart grid systems. Through a comprehensive analysis of existing literature, case studies, and expert opinions, this manuscript seeks to shed light on the multifaceted challenges posed by Smart Grids and propose strategies to address these issues effectively. By understanding the complexities of privacy and security in the context of smart grids, we can pave the way for a safer, more sustainable future powered by intelligent energy systems.

* Corresponding author: Ogweno Jeremiah Okeyo

Table 1 Conventional power grids Vs. Smart grids

Traditional Power Grids	**Smart grids**
Centralized Control - Traditional grids typically have a centralized control system where power generation, distribution, and consumption are managed by a few large power plants.	Decentralized Control - Smart grids use decentralized control systems that allow for more distributed energy resources (DERs) such as solar panels and wind turbines. This enables better management of power flow.
One-way Communication - Communication in traditional grids is primarily one-way, from the power plant to the consumers. There is limited information exchange between different components of the grid.	Two-way Communication - Smart grids facilitate two-way communication between various components, including consumers. This enables real-time monitoring, control, and data exchange, providing more information for decision-making.
Limited Automation - Automation in traditional grids is relatively limited. Manual monitoring and control are common, and responses to faults or changes in demand may take time.	Advanced Automation - Smart grids leverage advanced automation and digital technologies, such as sensors and smart meters, to detect and respond to changes in demand or faults in real time.
Predictable Demand - Traditional grids are designed to handle predictable and steady power demand. They may struggle with managing intermittent renewable energy sources and accommodating fluctuations in demand.	Integration of Renewable Energy - Smart grids are designed to integrate renewable energy sources seamlessly. They can manage the variability of sources like solar and wind through advanced forecasting and energy storage solutions.
Infrastructure - The infrastructure in traditional grids is often less flexible and adaptable. Upgrading or making changes to the system can be time-consuming and costly.	Enhanced Resilience and Reliability - Smart grids are more resilient to disruptions. They can quickly identify and isolate faults, reducing downtime and improving overall reliability.
	Flexibility and Adaptability - Smart grids are more flexible and adaptable to changes in energy demand, technology, and infrastructure. They can incorporate new technologies and scale more easily.
	Demand Response - Smart grids enable demand response programs, allowing consumers to actively participate in managing their energy consumption based on price signals or grid conditions.

In the rapidly evolving landscape of modern energy infrastructure, Smart Grids have emerged as a transformative technology, promising increased efficiency, reliability, and sustainability in the management of electricity distribution [7]-[12]. Smart Grids leverage advanced digital communication and information technologies to enhance the two-way flow of data between utilities and consumers, enabling real-time monitoring, control, and optimization of the electrical grid. While these advancements bring about numerous benefits, such as improved grid management and the integration of renewable energy sources, they also raise significant concerns regarding privacy and security.

The integration of interconnected sensors, smart meters, and communication networks in Smart Grids creates a vast and intricate web of data exchange. This wealth of information, ranging from individual energy consumption patterns to grid performance data, poses a potential threat to privacy if not adequately protected [13]-[18]. Moreover, the increased reliance on digital systems makes Smart Grids susceptible to cyber threats, which could have far-reaching consequences, including disruptions to the energy supply, financial losses, and even compromise of personal safety.

This paper explores the intricate interplay between privacy and security within the realm of Smart Grids, shedding light on the challenges and considerations that arise as we navigate the path toward a more connected and intelligent energy infrastructure. As we delve into this discourse, it becomes apparent that striking a delicate balance between the benefits of innovation and safeguarding the privacy and security of individuals and the grid itself is imperative for the successful deployment and sustained advancement of Smart Grid technologies.

2. Emergence of the smart grids

The grid," refers to the electric grid, a network of transmission lines, substations, transformers and more that deliver electricity from the power plant to your home or business. Figure 1 shows the conventional power grid system. It's what you plug into when you flip on your light switch or power up your computer [19]-[24]. Our current electric grid was built in the 1890s and improved upon as technology advanced through each decade. Today, it consists of more than 9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines.

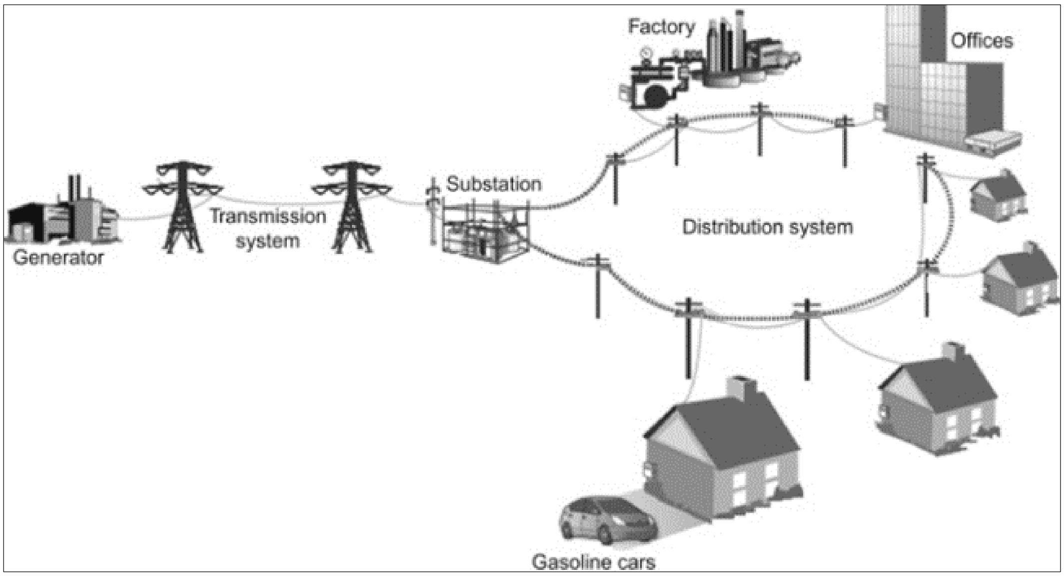

Figure 1 Conventional power grid system

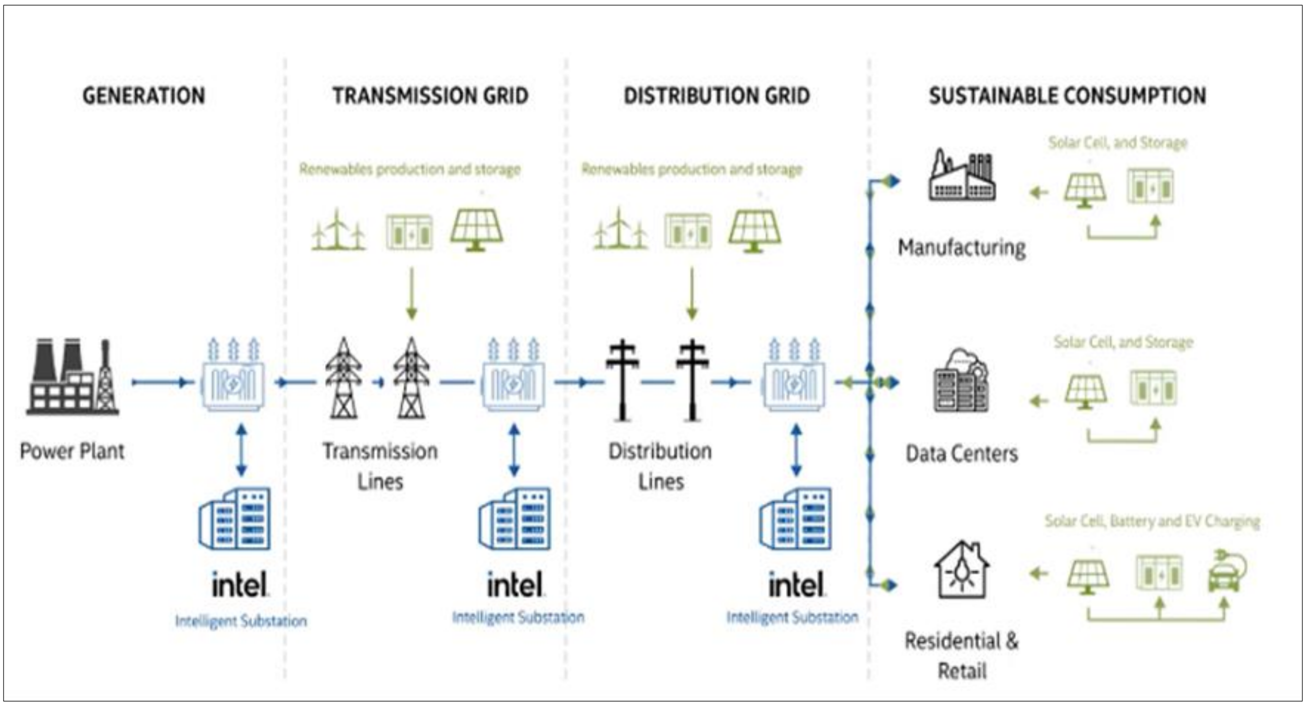

Figure 2 Smart grid communication

The digital technology that allows for two-way communication between the utility and its customers, and the sensing along the transmission lines is what makes the grid smart. Figure 2 illustrates the various components of the smart grid network. Like the Internet, the Smart Grid will consist of controls, computers, automation, and new technologies and equipment working together [25]. The Smart Grid represents an unprecedented opportunity to move the energy industry into a new era of reliability, availability, and efficiency that will contribute to our economic and environmental health [26]. The smart grid is not just about utilities and technologies. It is about giving one the information and tools he/she need to make choices about his energy use. A smarter grid enable unprecedented level of consumer participation. For example, you will no longer have to wait for your monthly statement to know how much electricity you use. With a smarter grid, you can have a clear and timely picture of it. "Smart meters," and other mechanisms, will allow you to see how much electricity you use, when you use it, and its cost [27]-[30].

The integration and management of renewable energy sources in the smart grid are facilitated by advanced technology in several ways: real-time monitoring and control: smart grids utilize advanced sensors and communication technologies to monitor the generation and consumption of renewable energy sources in real-time [31]-[36]. This allows operators to optimize the utilization of these sources based on their availability and demand patterns. Demand response programs: Smart Grids enable demand response programs, where consumers can adjust their energy usage based on the availability of renewable energy. Through advanced metering and communication systems, consumers can receive signals or incentives to shift their energy consumption to times when renewable energy sources are abundant. Energy storage integration: Advanced technologies such as battery storage systems are integrated into the Smart Grid to store excess renewable energy during periods of high generation and release it during times of low generation [37]-[42]. This helps to balance the intermittent nature of renewable energy sources and ensure a stable supply of electricity. Advanced forecasting and prediction: Smart Grids leverage data analytics and predictive algorithms to forecast the generation capacity of renewable energy sources. This enables better planning and management of the grid, ensuring that renewable energy sources are effectively utilized without compromising grid stability. Distributed energy resources management: The Smart Grid allows for the effective integration and management of distributed energy resources (DERs) such as rooftop solar panels and small wind turbines. Advanced technologies enable the seamless integration of these DERs into the grid, allowing them to contribute to the overall generation capacity and reducing reliance on centralized power plants [43]-[48]. Overall, the integration of advanced technology in the Smart Grid enables the effective management and utilization of renewable energy sources. By leveraging real-time monitoring, demand response programs, energy storage, forecasting, and distributed energy resource management, the Smart Grid maximizes the benefits of renewable energy while ensuring grid reliability and stability.

3. Data collection process in smart grids

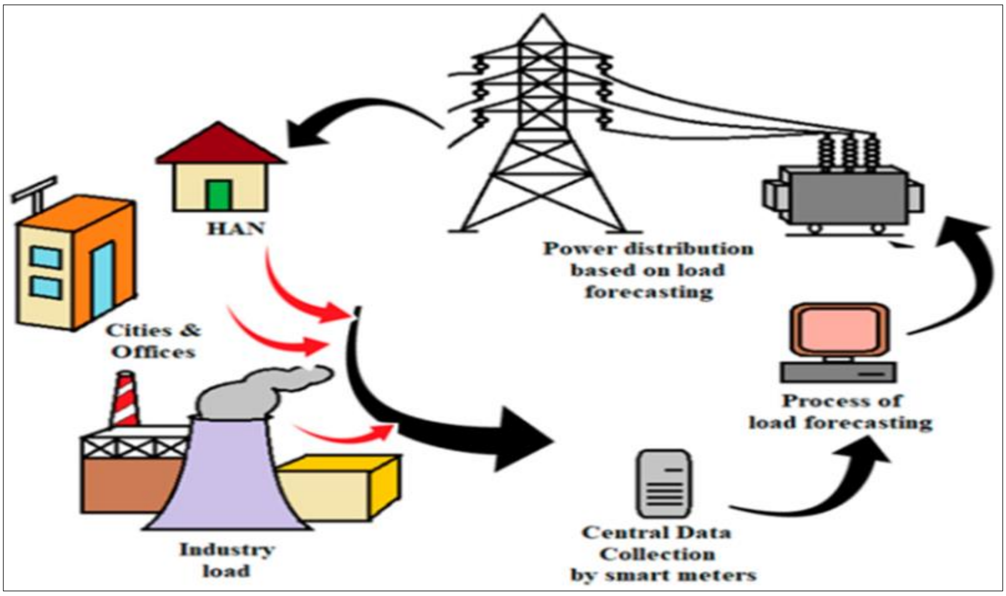

Figure 3 Data collection process in smart grids

For the mart grids to be able to perform its functionalities it will have to collect and store different types of data from the clients or the consumers [49], [50]. As shown in Figure 3, the data are collected and transmitted with help of smart meters which provide energy related information to both the utility company (or DSO) and customers. For the energy consumption of residential customers, the number of smart meter readings for a large utility company is expected to rise from 24 million a year to 220 million per day.

As an emerging component in electricity market and smart grid, electric vehicles (EVs) and plug-in hybrid EVs (PHEVs) have seen a growing popularity with the movement of electrification in transportation sector and progress of artificial intelligence. To control the normal operation status of the distribution system, DSO traditionally relies on the measurements in the primary sub- station, at the beginning of each MV feeder, where the protection systems are normally installed. The current magnitude information is also needed for the automatic on-load tap changer in HV/MV transformers for voltage regulation. The measurements of a typical smart meter include the node voltage, feeder current, power factor, active and reactive power, energy over a period, total harmonic distortion as well as load demand, etc. The intelligent devices for data collection in smart grid are listed as Table 2.

Table 2 Intelligent data collection devices in smart grid

Intelligent device	Technology	Application
Advanced metering infrastructure (AMI)	Integration of smart meters, data management systems and communication networks to provide bidirectional communication between customers and utilities	Remote meter configuration, dynamic tariffs, power quality monitoring and local control
Phasor measurement unit (PMU)	Real-time measurements (30 to 60 samples/ second) of multiple remote points with a common time source for synchronization	Electrical waves measurement of power grid
Wide area monitoring system (WAMS)	An application server to deal with the incoming information from PMUs	Dynamic stability of the grid
Remote terminal unit (RTU)	A microprocessor-controlled device that transmitting telemetry data	Information collection of system operation status
Supervisory control and data acquisition (SCADA)	Both manual and automatic	System monitoring, event processing and alarm

Smart grid is considered as a future of power grid which is able to manage the production, transmission and distribution of electricity by modern technology to resolve many issues of current power grid systems. Some of these obstacles such as voltage sags, blackouts, overloads and old grids are part of economic issue and other factors especially carbon emissions which contribute to the environmental problem [51]-[54]. Thus, considering both economic and environmental interests, application of smart grid will be essential for near future. Modernization of power grid by new facilities has been a reason for rapidly emerging of smart grid in many regions around the world especially in developed countries. Moreover, smart grid is necessary for developing countries in future due to integration with renewable energies and energy management features [55], [56]. However, there are many challenging aspects for this technology to expand due to its broad nature and multi-disciplinary aspects, that can make it becomes complicated and difficult to be implemented by governments in such countries.

4. Architecture of the Smart Grids

Just like traditional grids, smart grids have a number of moving components as shown in Figure 4. However, smart grids have parts that are more efficient in terms of design and functionality. For instance, there are intelligent appliances that are capable of deciding when to consume power based on the pre-set user preferences. There are also smart substations that control critical and non-critical operational data, such as power factor performance, breaker, and battery and transformer status [57]-[59]. Another critical component of a smart grid is the smart power meter that is capable of two-way communication [60] between the consumer and power provider. This makes detection of power outages, billing, data collection and dispatching of repair crews easier and faster. There is also smart distribution characterized by automated monitoring and analysis tools, superconducting cables for long-distance transmission, self-healing, self-optimization and self-balancing. Smart generation is another key component of a smart grid [61]. The system is capable of "learning" the unique behavior of power generation resources to optimize energy production and to automatically maintain voltage, frequency and power factor standards based on feedback from multiple points in the grid. There is also universal access to affordable, low-carbon electrical power generation and storage solutions. Smart grids are not only aligned perfectly with the needs and demands of our time, they are also predicted to have significant long-lasting effects. For instance, the technology will overhaul aging equipment and bring things up to speed. This will help to reduce the likelihood of blackouts, burnouts and power surges [62]-[65]. The technology will also reduce both the cost of energy consumption [66] and production.

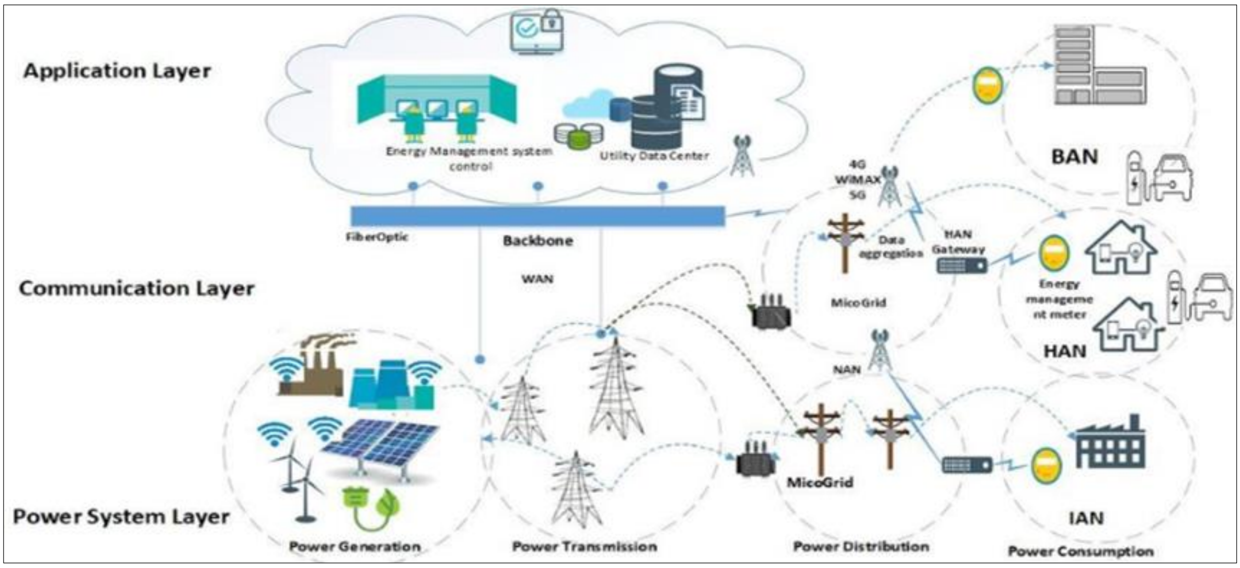

Figure 4 Architecture of the Smart Grids

With its full implementation, smart grids will make renewable power feasible and equip the grid to meet increasing energy demands. More importantly, however, the technology will give consumers near real-time control of their energy bills and facilitate large-scale electric vehicle charging. Switching to a smart grid is all about providing consumers with a financial edge not just improving power management and adopting greener technology [67].

5. Communication Pathways of smart grid

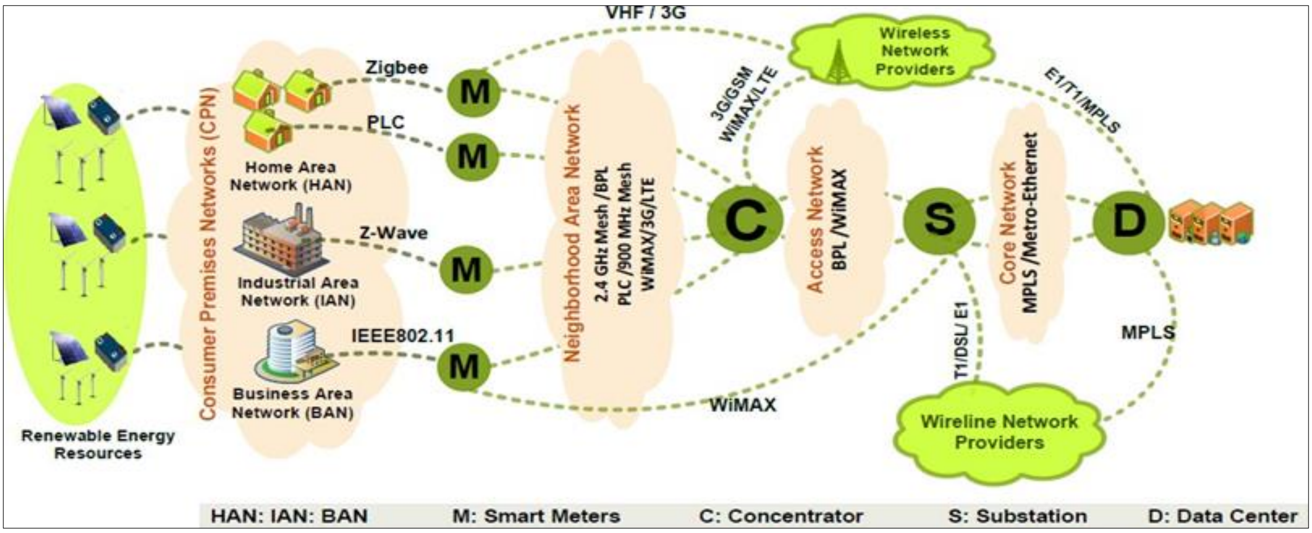

Figure 5 Basic Network Architecture

The updated smart grid conceptual model provides a high-level set of descriptions adequate to include the broad set of evolving trends in the smart grid. Yet interoperability requirements derive from specific system and device interfaces that are not sufficiently characterized by such high-level depictions. In this section, another set of communication infrastructures are provided as shown in Figure 5. Three different network types—the Local Area Network (LAN), Metropolitan Area Network (MAN), and Wide Area Network (WAN)—can serve as the foundation for the smart grid's communication infrastructure [68]-[72].

5.1. Local Area Network (LAN)

The Premise Area Network divides into three sections depending on the environment, HAN (Home Area Network), Building Area Network (BAN), and IAN (Industrial Area Network). These are wired or wireless networks within the end-user's premise. The purpose of the HAN is to provide communication between for example the smart meter and home automation, appliances, Home Energy Management Systems (HEMS), solar panels, or electric vehicles [73]-[77]. BAN and IAN are commercial and industrial focused and communicate typically with building automation systems such as heating and ventilation or energy management systems. These applications do not require large coverage, high speed, or high data rate [78], and can be managed with low power, low-cost technologies such as Power Line Communication (PLC), Wi-Fi, or ZigBee. The required bandwidth in HANs vary from 10 to 100 kbps for each device, depending on function. The premise networks should be expandable to allow for the number of connected devices to increase. Other applications for the smart metering devices within the premise area are delivering information such as power and real-time price information to the end-user through HEMS [79]-[82]. The end-user can then make decisions whether to use appliances during high price periods or wait for lower price. This can in turn help with peak demand reduction and load shifting.

5.2. Neighborhood Area Network (NAN) / Field Area Network (FAN)

The Neighborhood Area Network (NAN) and Field Area Network (FAN) are networks within the distribution domain, both enable the flow of information [83] between WAN and a Premise Area Network (HAN, BAN, IAN). The NAN connects premises networks within a neighborhood via smart meters at the end-user. The NAN enable services such as monitoring and controlling electricity delivery to each end-user, demand response and distribution automation [84]-[87]. The area NAN/FAN covers can in some cases be large, one of the features of NAN/FAN is communication between intelligent [88] electronic devices (IEDs). The data in a NAN/FAN is transmitted from a large number of sources to a data concentrator or substation. This requires a high data rate and large coverage distance. For the existing grid infrastructure in the NAN/FAN covered areas, it in most cases not possible to make extensive alterations to the infrastructure. Because of the varying nature of the physical environment of which the NAN/FAN operate, coverage requirements, etc., different technologies for communication are used. When the coverage requirements are lower, standards from NAN can be applied, if longer coverage is required, other technologies will be more suitable. The communication technologies used therefore have to be adapted to each specific situation. Both wired and wireless technologies are used in NAN/FAN, and the different communication technologies should be complementary [89]-[93]. As distributed energy generation are deployed, these are connected to the NAN/FAN. Communication technologies such as ZigBee, Wi-Fi, Ethernet, or PLC are widely used in these networks.

5.3. Wide Area Network (WAN)

Table 3 Communication infrastructure in smart grid

Type of network	Function	Characteristic
HAN	Enabling the communication among smart home or office devices and smart meters for local energy management	Deployed at house or small office with a relatively low transmission data rate (less than 1 Kbps
NAN	Consisting of several HANs for energy consumption data aggregation and storage at load data center (LDC)	Deployed within area of hundreds of meters with up to 2Kbps
WAN	Enabling the communication of all smart grid's components	Deployed within tens of kilometers with high data transmission capability up to few Gbps

A WAN forms the backbone of the communication network in the power grid. It connects smaller distributed networks [94] such as transmission substations, control systems and protection equipment, e.g., Supervisory Control and Data Acquisition (SCADA), Remote Terminal Unit (RTU), and Phasor Measurement Unit (PMU) to the utility companies' control centers. Other terms used for the WAN is the backbone network or Metropolitan Area Network. WAN applications require a higher number of data points at high data rates (10 Mbps–1 Gbps), and long-distance coverage

(10–100 km). Real-time measurements are taken throughout the power grid by measurement and control devices and sent to control centers [95]-[98]. In reverse, instructions and commands are sent from control centers to the devices. This communication requires both a high degree of distance coverage and speed to maintain stability. Suitable communication technologies for this application are PLC, fiber optic communication [99], cellular, or WiMAX. Satellite communication can be used as backup communication or in remote locations. Table 3 presents a summary of the communication infrastructure in smart grids.

6. Challenges of Smart Grid Communication

The deployment of smart grids introduces several challenges related to communication infrastructure. One significant hurdle is the need for robust and secure two-way communication systems to enable real-time data exchange between various components of the smart grid, including sensors, smart meters, and control systems. Ensuring the reliability and resilience of communication networks becomes crucial, as any disruptions or cyber-attacks could compromise the grid's functionality and pose serious threats to the stability of the entire energy infrastructure. Figure 6 presents some of the sources of threats to smart grid security.

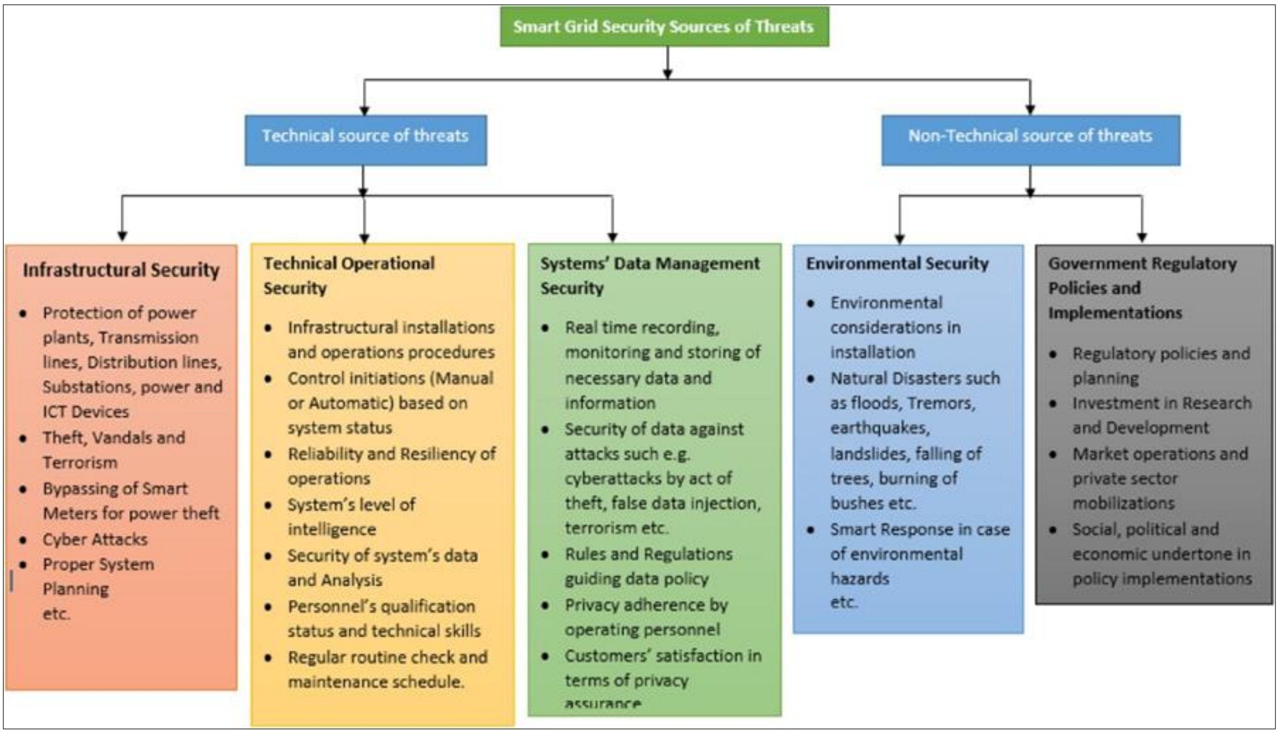

Figure 6 Sources of threats to smart grid security

Interoperability issues may arise due to the integration of diverse technologies and communication protocols, requiring standardized approaches to facilitate seamless connectivity. Additionally, concerns related to data privacy and security must be addressed to build public trust and ensure the protection of sensitive information generated by smart grid devices, further complicating the implementation of effective communication solutions for the evolving energy landscape. In this section we will discuss some challenges in smart grid communications and applications.

6.1. Privacy issues in smart grids

Communication in SGs is often linked to information related to individual customers and their lives. This is why securing authentication, authorization, and confidentiality is so important in a SG environment. It is of greatest importance not to disclose private data to anyone other than consented entities [100]-[105]. Private data include consumer identification, address, and energy usage information. Smart meters are expected to provide high accuracy reading of power consumption at defined time intervals to the utilities companies. This data is used for billing purposes and grid management. However, measurement data from smart meter may be used for other purposes. Usage pattern analysis can be useful for power saving, but involves a significant risk. The data holds a great amount of information about individual consumers. Non-intrusive Appliance Load Monitoring (NALM) technologies uses extracts detailed information on appliance use based on energy measurements. By analyzing data and usage patterns, it may be possible to predict when people are at home or away from home, or what appliances are in use [106]-[109]. This information is could be of interest for the police, tax authorities, insurance companies, etc. NIST have acknowledged that the major benefit of SGs is the ability to receive richer data from smart meters and devices, is also the biggest weakness from a privacy standpoint.

6.2. Reliable Transmission

Reliable transmission of information with high QoS [110] is one of the most prioritized requirements for SG communications. It will greatly improve the system robustness and reliability by harnessing the modern and secure communication protocols, the communication technologies, faster and more robust control devices and Intelligent Electronic Devices (IEDs) for the entire grid from substation and feeder to customer resources. As the use of communication systems in other scenarios, there are many challenges to achieve robust transmission because of limited bandwidth, limited power, or adverse transmission environment (interference, high path loss, etc.) [111]-[115]. As discussed in the previous sections, both wireless and wired communication technique consists important parts of the SG communication with its own advantages and disadvantages. In many cases, a hybrid communication technology mixed with wired and wireless solutions can be used in order to provide higher level of system reliability, robustness and availability.

6.3. Security

Cyber security is considered to be one of the biggest challenges to SG deployment as the power grid becomes more and more interconnected. With the number of connected devices increasing, the possibility for cyber-attacks against the power grid will increase. Cyber security is essential as every aspect of the SG must be secure [116]-[120]. Security measures must cover issues involving communication and automation that affects operation of the power system and the utilities managing them. It must address deliberate attacks as well as inadvertent accidents such as user error and equipment failure. SGs are vulnerable to cyber-attacks due to the integration of communication paths throughout the grid infrastructure. SGs are still evolving, and considering security in a new SG environment is important, but challenging. Undetected cyber-attacks can lead to critical damage affecting thousands or millions of customers and life threatening infrastructure. Securing the data is vital for both end-user and power companies to ensure trust. As more functions and capabilities are implemented to the SG importance of secure and safe communication increase. From distributed energy generation, energy storage, electric vehicles to power station and power grid control systems. Additionally, something possibly as trivial as securing that the reading from the end-user's smart meters are sending correct billing information, or that the utilities companies receive the correct information is essential. As for any other communication systems, security enhancement for SG communication can be achieved at different layer of the protocol by utilizing the techniques from the conventional upper layer cryptography to the physical layer security [121]-[125]. Different communication technologies, wired and wireless, interconnect and are required to operate the grid securely. Different authorities are responsible securing different data and security aspects in Smart Grid/smart metering.

6.4. Vulnerabilities and threats

Vulnerabilities and threats may also be categorized as consumer threat, naturally occurring threat, individual and organizational threat, impacts on consumer, and impacts on availability, financial impacts, and likelihood of attack. Attacks on Smart Grids can occur on all levels, from generation and distribution to home networks, it can be protocol-based attacks, routing attacks, intrusion, malware and denial-of-service attacks (DoS) [126]-[131]. Successful attacks can lead to grid instability, or in the worst case failure and blackouts. A reliable SG depends on avoiding attacks, or detecting and establishing mitigation measures [31]. Protection should be used within SG for message authentication, integrity, and encryption. Security must also address loss of communication, unauthorized access to network and devices (eavesdropping), network attacks, DoS, Distributed Denial of Service (DDoS), Man-in-the-middle (MITM), and jamming of radio signals. There have been several attacks on power companies in the last years, where some have led to system failure and blackout. In 2006 a nuclear power plant in Alabama, USA failed due to overload on the control system network. Investigations later identified the source to be manipulated smart meter power readings. In 2013–2014 an attack affected more than 1000 energy companies in 84 countries including Germany, France, Italy, Spain, Poland, and the US. In December 2015, Ukraine experienced a cyber-attack on three regional power distribution companies, leaving people in the dark for over six hours. Over two months after the attack, control centers were not fully operational. The attack was distributed via spear-phishing email, targeting IT staff and systems administrators in companies responsible for power distribution. By opening an attachment in an email, malicious firmware were uploaded SCADA-network. The intruders gained access to substation control centers via Virtual Private Networks (VPNs) and were able to send commands to disable Uninterruptible Power Supply (UPS) systems, and open breakers in substations. The blackout affected around 225,000 customers, and manual operations were required to turn the power back on. In 2016 Ukrainian power distribution was once again attacked, parts of the city of Kyiv lost power for an hour.

The malware enabled control of circuit breakers to the attackers. In 2020, the European Network of Transmission System Operations for Electricity experienced an attack on its office network. The attack did however not infect any of the systems responsible for controlling the power grid.

6.5. Types of attacks in smart grids

Table 4 Types of attacks in smart grids

Attacks	Details
Malware spreading	An attacker can develop malware and spread it to infect smart meters or company servers [138]. Malware can be used to replace or add any function to a device or a system such as sending sensitive information.
Access through database links	Control systems record their activities in a database on the control system network then mirror the logs into the business network. If the underneath database management systems are not properly configured, a skilled attacker can gain access to the business network database, and then use his skills to exploit the control system network [139]-[141].
Compromising communication equipment	An attacker may compromise some of the communication equipment such as multiplexers causing a direct damage or using it as a backdoor to launch future attacks [142], [143].
Injecting false information (Replay Attack)	An attacker can send packets to inject false information in the network, such as wrong meter data, false prices, fake emergency event, etc [144]-[148]. Fake information can have huge financial impact on the electricity markets.
Network Availability	Since smart grid uses IP protocol and TCP/IP stack, it becomes subject to DoS attacks and to the vulnerabilities inherent in the TCP/IP stack [149]-[153]. DoS attacks might attempt to delay, block, or corrupt information transmission in order to make smart grid resources unavailable.
Eavesdropping and traffic analysis	An adversary can obtain sensitive information by monitoring network traffic [154]-[160]. Examples of monitored information include future price information, control structure of the grid, and power usage.
Modbus security issue	The term SCADA refers to computer systems and protocols that monitor and control industrial, infrastructure, or facility-based processes such as smart grid processes [161]-[164]. Modbus protocol is one piece of the SCADA system that is responsible for exchanging SCADA information needed to control industrial processes. Given that the Modbus protocol was not designed for highly security-critical environments [165], several attacks are possible including: (a) sending fake broadcast messages to slave devices (Broadcast message spoofing), (b) replaying genuine recorded messages back to the master (Baseline response replay), (c) locking out a master and controlling one or more field devices (Direct slave control), (d) sending benign messages to all possible addresses to collect devices' information (Modbus network scanning), (e) reading Modbus messages (Passive reconnaissance), (f) delaying response messages intended for the masters (Response delay), and (g) attacking a computer with the appropriate adapters (Rouge interloper) [166]-[169].

The just mentioned vulnerabilities can be exploited by attackers with different motives and expertise and could cause different levels of damage to the network. Attackers could be script kiddies, elite hackers, terrorists, employees, competitors, or customers. Those attackers are normally driven by intellectual challenge and curiosity, Consumers driven by vengeance and vindictiveness towards other consumers making them figure out ways to shut down their home's power. Terrorists who view the smart grid as an attractive target as it affects millions of people making the terrorists' cause more visible. Employees disgruntled on the utility/customers or ill-trained employees causing unintentional errors. Competitors attacking each other for the sake of financial gain those attackers can cause a wide variety of attacks, classified into three main categories: Component-wise, protocol-wise, and topology-wise. Component-wise attacks target the field components that include Remote Terminal Unit (RTU). RTUs are traditionally used by engineers to remotely configure and troubleshoot the smart grid devices. This remote access feature can be subject to an attack that enables malicious users to take control over the devices and issue faulty states such as shutting down the devices [132], [133]. Protocol-wise attacks target the communication protocol itself using methods such as reverse engineering and false data injections. Topology-wise attacks target the topology of the smart grid by launching a Denial-of-Service (DoS) attack that prevents operators from having a full view of the power system causing inappropriate decision making [134]-[137]. More attacks are discussed in Table 4 below.

7. Future research directions

Privacy and security issues in Smart Grids are critical considerations as these systems become more integrated and interconnected. Future research in this field is essential to address emerging challenges and stay ahead of potential threats. Here are some potential research directions in privacy and security for Smart Grids:

Secure Communication Protocols- Develop and evaluate robust communication protocols that ensure secure and reliable data exchange among Smart Grid components [170]. This includes addressing issues such as data integrity, authentication, and encryption to prevent unauthorized access and tampering [171].

Blockchain Technology- Investigate the application of blockchain technology in Smart Grids to enhance security and privacy [172]-[175]. Blockchain can provide a decentralized and tamper-resistant ledger, ensuring the integrity and authenticity of transactions within the grid.

Privacy-Preserving Data Analytics- Develop advanced data analytics techniques that can extract meaningful insights from Smart Grid data without compromising individual user privacy [176], [177]. This involves exploring techniques like homomorphic encryption and differential privacy to protect sensitive information.

Intrusion Detection and Prevention Systems- Enhance the capabilities of intrusion detection and prevention systems specifically designed for Smart Grids. This includes the development of anomaly detection algorithms capable of identifying and mitigating cyber threats in real-time [178], [179].

Security of IoT Devices- Investigate security measures for the Internet of Things (IoT) devices within the Smart Grid [180], [181]. This involves securing sensors, smart meters, and other IoT devices to prevent unauthorized access, data manipulation [182], and potential exploitation by malicious actors.

Resilience and Disaster Recovery- Research strategies to enhance the resilience of Smart Grids against cyber-attacks and natural disasters [183]. This includes developing robust disaster recovery plans and mechanisms to quickly restore functionality in case of system disruptions.

Human Factors and User Awareness- Explore the human factors involved in Smart Grid security, including user awareness, training, and behavior [184]. Develop strategies to educate end-users and grid operators about security best practices to prevent social engineering attacks and improve overall system security.

Regulatory Frameworks- Evaluate and propose regulatory frameworks that ensure the privacy and security of Smart Grids [185], [186]. This involves collaboration between researchers, industry stakeholders, and policymakers to establish standards and guidelines for secure Smart Grid deployment.

Machine Learning for Threat Prediction- Utilize machine learning algorithms to predict and identify potential security threats in real-time [187], [188]. This involves developing models that can analyze large volumes of data to detect patterns indicative of cyber threats and take proactive measures to prevent attacks.

Secure firmware and software updates- Research methods to securely update firmware and software in Smart Grid components to patch vulnerabilities and improve overall system security [189]-[192]. This includes exploring secure over-the-air update mechanisms and ensuring the integrity of updates.

Quantum-safe cryptography- Anticipate the future threat of quantum computers on current cryptographic systems and develop quantum-safe cryptographic algorithms for securing Smart Grid communications against potential quantum attacks [193], [194].

Continuous collaboration between researchers, industry experts, and policymakers is crucial to addressing these challenges and ensuring the long-term security and privacy of Smart Grids.

8. Conclusion

This manuscript has shed light on the critical privacy and security issues surrounding smart grids. Through a comprehensive analysis of the various aspects of smart grid technology, it has become evident that while these systems offer numerous benefits such as improved energy efficiency and reliability, they also pose significant risks to the privacy and security of consumers and the overall grid infrastructure. The manuscript has highlighted the potential threats faced by smart grids, including unauthorized access, data breaches, and cyber-attacks. It has emphasized the importance of implementing robust security measures to safeguard sensitive consumer information and protect against potential disruptions to the grid's operation. Additionally, the manuscript has explored the challenges associated with ensuring privacy in a smart grid environment, particularly regarding the collection, storage, and sharing of consumer data. Furthermore, the manuscript has discussed various privacy-enhancing technologies and security frameworks that can be employed to mitigate these risks. It has emphasized the need for collaboration between stakeholders, including utilities, regulators, policymakers, and consumers, to establish comprehensive privacy and security policies and standards. Additionally, it has highlighted the significance of educating consumers about their rights and providing them with mechanisms to control their data within the smart grid ecosystem. Overall, this manuscript serves as a valuable resource for researchers, policymakers, and industry professionals by providing an in-depth understanding of the privacy and security challenges associated with smart grids. It underscores the urgency of addressing these issues to ensure the successful deployment and widespread adoption of this transformative technology. By incorporating the recommendations and insights presented in this manuscript, stakeholders can work towards building a secure and privacy-preserving smart grid infrastructure that maximizes its benefits while minimizing potential risks.

Compliance with ethical standard

Acknowledgement

I would like to thank all my friends who supported me when I was developing this paper.

Disclosure of conflict of interest

The author declares that he holds no conflict of interest.

References

[1] Ghiasi M, Wang Z, Mehrandezh M, Jalilian S, Ghadimi N. Evolution of smart grids towards the Internet of energy: Concept and essential components for deep decarbonisation. IET Smart Grid. 2023 Feb, 6(1):86-102.

[2] Bakare MS, Abdulkarim A, Zeeshan M, Shuaibu AN. A comprehensive overview on demand side energy management towards smart grids: challenges, solutions, and future direction. Energy Informatics. 2023 Dec, 6(1):1-59.

[3] Senyapar HN, Bayindir R. The Research Agenda on Smart Grids: Foresights for Social Acceptance. Energies. 2023 Sep 6, 16(18):6439.

[4] Habbak H, Mahmoud M, Metwally K, Fouda MM, Ibrahem MI. Load forecasting techniques and their applications in smart grids. Energies. 2023 Feb 2, 16(3):1480.

[5] Rind YM, Raza MH, Zubair M, Mehmood MQ, Massoud Y. Smart energy meters for smart grids, an internet of things perspective. Energies. 2023 Feb 16, 16(4):1974.

[6] Nyangaresi VO, Abd-Elnaby M, Eid MM, Nabih Zaki Rashed A. Trusted authority based session key agreement and authentication algorithm for smart grid networks. Transactions on Emerging Telecommunications Technologies. 2022 Sep, 33(9):e4528.

[7] Muqeet HA, Liaqat R, Jamil M, Khan AA. A State-of-the-Art Review of Smart Energy Systems and Their Management in a Smart Grid Environment. Energies. 2023 Jan 1, 16(1):472.

[8] Kang C, Kirschen D, Green TC. The Evolution of Smart Grids. Proceedings of the IEEE. 2023 Jul 11, 111(7):691-3.

[9] Ghiasi M, Niknam T, Wang Z, Mehrandezh M, Dehghani M, Ghadimi N. A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. Electric Power Systems Research. 2023 Feb 1, 215:108975.

[10] Hasan MK, Habib AA, Shukur Z, Ibrahim F, Islam S, Razzaque MA. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations. Journal of Network and Computer Applications. 2023 Jan 1, 209:103540.

[11] Choi KH, Kwon GH. Strategies for sensing innovation opportunities in smart grids: In the perspective of interactive relationships between science, technology, and business. Technological Forecasting and Social Change. 2023 Feb 1, 187:122210.

[12] Nyangaresi VO, Alsamhi SH. Towards secure traffic signaling in smart grids. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 196-201). IEEE.

[13] Llaria A, Dos Santos J, Terrasson G, Boussaada Z, Merlo C, Curea O. Intelligent buildings in smart grids: A survey on security and privacy issues related to energy management. Energies. 2021 May 10, 14(9):2733.

[14] Zografopoulos I, Hatziargyriou ND, Konstantinou C. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. IEEE Systems Journal. 2023 Sep 1.

[15] Ruan J, Liang G, Zhao J, Zhao H, Qiu J, Wen F, Dong ZY. Deep learning for cybersecurity in smart grids: Review and perspectives. Energy Conversion and Economics. 2023 Aug, 4(4):233-51.

[16] Otuoze AO, Mustafa MW, Larik RM. Smart grids security challenges: Classification by sources of threats. Journal of Electrical Systems and Information Technology. 2018 Dec 1, 5(3):468-83.

[17] Jha RK. Cybersecurity and Confidentiality in Smart Grid for Enhancing Sustainability and Reliability. Recent Research Reviews Journal. 2023 Dec, 2(2):215-41.

[18] Abduljabbar ZA, Nyangaresi VO, Jasim HM, Ma J, Hussain MA, Hussien ZA, Aldarwish AJ. Elliptic Curve Cryptography-Based Scheme for Secure Signaling and Data Exchanges in Precision Agriculture. Sustainability. 2023 Jun 28, 15(13):10264.

[19] Tuballa ML, Abundo ML. A review of the development of Smart Grid technologies. Renewable and Sustainable Energy Reviews. 2016 Jun 1, 59:710-25.

[20] Saxena SN. Smart Distribution Grid–and How to Reach the Goal. International Journal of Smart Grid. 2019 Dec 14, 3(4):188-200.

[21] Hossain E, Hossain J, Un-Noor F. Utility grid: Present challenges and their potential solutions. IEEE Access. 2018 Oct 4, 6:60294-317.

[22] Hasan MK, Habib AA, Islam S, Balfaqih M, Alfawaz KM, Singh D. Smart grid communication networks for electric vehicles empowering distributed energy generation: Constraints, challenges, and recommendations. Energies. 2023 Jan 20, 16(3):1140.

[23] Chothani N, Raichura M, Patel D. Transformer Infrastructure for Power Grid. InAdvancement in Power Transformer Infrastructure and Digital Protection 2023 Jul 30 (pp. 1-26). Singapore: Springer Nature Singapore.

[24] Hussien ZA, Abdulmalik HA, Hussain MA, Nyangaresi VO, Ma J, Abduljabbar ZA, Abduljaleel IQ. Lightweight Integrity Preserving Scheme for Secure Data Exchange in Cloud-Based IoT Systems. Applied Sciences. 2023 Jan, 13(2):691.

[25] Sayed K, Gabbar HA. SCADA and smart energy grid control automation. InSmart energy grid engineering 2017 Jan 1 (pp. 481-514). Academic Press.

[26] Al-Badi AH, Ahshan R, Hosseinzadeh N, Ghorbani R, Hossain E. Survey of smart grid concepts and technological demonstrations worldwide emphasizing on the Oman perspective. Applied system innovation. 2020 Jan 12, 3(1):5.

[27] Saleem MU, Shakir M, Usman MR, Bajwa MH, Shabbir N, Shams Ghahfarokhi P, Daniel K. Integrating smart energy management system with internet of things and cloud computing for efficient demand side management in smart grids. Energies. 2023 Jun 20, 16(12):4835.

[28] Waseem M, Adnan Khan M, Goudarzi A, Fahad S, Sajjad IA, Siano P. Incorporation of blockchain technology for different smart grid applications: Architecture, prospects, and challenges. Energies. 2023 Jan 11, 16(2):820.

[29] Ali SS, Choi BJ. State-of-the-art artificial intelligence techniques for distributed smart grids: A review. Electronics. 2020 Jun 22, 9(6):1030.

[30] Nyangaresi VO, Moundounga AR. Secure data exchange scheme for smart grids. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 312-316). IEEE.

[31] Kataray T, Nitesh B, Yarram B, Sinha S, Cuce E, Shaik S, Vigneshwaran P, Roy A. Integration of smart grid with renewable energy sources: Opportunities and challenges–A comprehensive review. Sustainable Energy Technologies and Assessments. 2023 Aug 1, 58:103363.

[32] Barman P, Dutta L, Bordoloi S, Kalita A, Buragohain P, Bharali S, Azzopardi B. Renewable energy integration with electric vehicle technology: A review of the existing smart charging approaches. Renewable and Sustainable Energy Reviews. 2023 Sep 1, 183:113518.

[33] Panda A, Dauda AK, Chua H, Tan RR, Aviso KB. Recent advances in the integration of renewable energy sources and storage facilities with hybrid power systems. Cleaner Engineering and Technology. 2023 Jan 24:100598.

[34] Liu J, Hu H, Yu SS, Trinh H. Virtual Power Plant with Renewable Energy Sources and Energy Storage Systems for Sustainable Power Grid-Formation, Control Techniques and Demand Response. Energies. 2023 Apr 26, 16(9):3705.

[35] Meraj ST, Yu SS, Rahman MS, Hasan K, Lipu MH, Trinh H. Energy management schemes, challenges and impacts of emerging inverter technology for renewable energy integration towards grid decarbonization. Journal of Cleaner Production. 2023 Mar 29:137002.

[36] Nyangaresi VO, Mohammad Z. Privacy preservation protocol for smart grid networks. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[37] Tan KM, Babu TS, Ramachandaramurthy VK, Kasinathan P, Solanki SG, Raveendran SK. Empowering smart grid: A comprehensive review of energy storage technology and application with renewable energy integration. Journal of Energy Storage. 2021 Jul 1, 39:102591.

[38] Sufyan M, Rahim NA, Aman MM, Tan CK, Raihan SR. Sizing and applications of battery energy storage technologies in smart grid system: A review. Journal of Renewable and Sustainable Energy. 2019 Jan 1, 11(1).

[39] Argyrou MC, Christodoulides P, Kalogirou SA. Energy storage for electricity generation and related processes: Technologies appraisal and grid scale applications. Renewable and Sustainable Energy Reviews. 2018 Oct 1, 94:804-21.

[40] Molina MG. Energy storage and power electronics technologies: A strong combination to empower the transformation to the smart grid. Proceedings of the IEEE. 2017 Sep 15, 105(11):2191-219.

[41] Krishan O, Suhag S. An updated review of energy storage systems: Classification and applications in distributed generation power systems incorporating renewable energy resources. International Journal of Energy Research. 2019 Oct 10, 43(12):6171-210.

[42] Nyangaresi VO, Abduljabbar ZA, Refish SH, Al Sibahee MA, Abood EW, Lu S. Anonymous Key Agreement and Mutual Authentication Protocol for Smart Grids. InCognitive Radio Oriented Wireless Networks and Wireless Internet: 16th EAI International Conference, CROWNCOM 2021, Virtual Event, December 11, 2021, and 14th EAI International Conference, WiCON 2021, Virtual Event, November 9, 2021, Proceedings 2022 Mar 31 (pp. 325-340). Cham: Springer International Publishing.

[43] Daneshvar M, Mohammadi-ivatloo B, Zare K. Integration of distributed energy resources under the transactive energy structure in the future smart distribution networks. InOperation of distributed energy resources in smart distribution networks 2018 Jan 1 (pp. 349-379). Academic Press.

[44] Sarmiento-Vintimilla JC, Torres E, Larruskain DM, Pérez-Molina MJ. Applications, operational architectures and development of virtual power plants as a strategy to facilitate the integration of distributed energy resources. Energies. 2022 Jan 21, 15(3):775.

[45] Strezoski L. Distributed energy resource management systems—DERMS: State of the art and how to move forward. Wiley Interdisciplinary Reviews: Energy and Environment. 2023 Jan, 12(1):e460.

[46] Patil SS, Patil SH, Pawar AM, Bewoor M, Patil NS. Soft Computing Techniques for the Integration of Distributed Energy Resources (DERs). Technology. 2022, 8(2):1-6p.

[47] Gulotta F, Daccò E, Bosisio A, Falabretti D. Opening of Ancillary Service Markets to Distributed Energy Resources: A Review. Energies. 2023 Mar 17, 16(6):2814.

[48] Nyangaresi VO. Masked Symmetric Key Encrypted Verification Codes for Secure Authentication in Smart Grid Networks. In2022 4th Global Power, Energy and Communication Conference (GPECOM) 2022 Jun 14 (pp. 427-432). IEEE.

[49] Daki H, El Hannani A, Aqqal A, Haidine A, Dahbi A. Big Data management in smart grid: concepts, requirements and implementation. Journal of Big Data. 2017 Dec, 4(1):1-9.

[50] Avancini DB, Rodrigues JJ, Martins SG, Rabêlo RA, Al-Muhtadi J, Solic P. Energy meters evolution in smart grids: A review. Journal of cleaner production. 2019 Apr 20, 217:702-15.

[51] Bhattarai TN, Ghimire S, Mainali B, Gorjian S, Treichel H, Paudel SR. Applications of smart grid technology in Nepal: status, challenges, and opportunities. Environmental Science and Pollution Research. 2023 Feb, 30(10):25452-76.

[52] Meliani M, Barkany AE, Abbassi IE, Darcherif AM, Mahmoudi M. Energy management in the smart grid: State-of-the-art and future trends. International Journal of Engineering Business Management. 2021 Jul 15, 13:18479790211032920.

[53] Refaat SS, Ellabban O, Bayhan S, Abu-Rub H, Blaabjerg F, Begovic MM. Smart Grid and Enabling Technologies. John Wiley & Sons, 2021 Aug 16.

[54] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Abood EW, Abduljaleel IQ. Dynamic Ephemeral and Session Key Generation Protocol for Next Generation Smart Grids. InAd Hoc Networks and Tools for IT: 13th EAI International Conference, ADHOCNETS 2021, Virtual Event, December 6–7, 2021, and 16th EAI International Conference, TRIDENTCOM 2021, Virtual Event, November 24, 2021, Proceedings 2022 Mar 27 (pp. 188-204). Cham: Springer International Publishing.

[55] Tajjour S, Chandel SS. A comprehensive review on sustainable energy management systems for optimal operation of future-generation of solar microgrids. Sustainable Energy Technologies and Assessments. 2023 Aug 1, 58:103377.

[56] Ponce-Jara MA, Ruiz E, Gil R, Sancristóbal E, Pérez-Molina C, Castro M. Smart Grid: Assessment of the past and present in developed and developing countries. Energy strategy reviews. 2017 Dec 1, 18:38-52.

[57] Khan B, Getachew H, Alhelou HH. Components of the smart-grid system. InSolving Urban Infrastructure Problems Using Smart City Technologies 2021 Jan 1 (pp. 385-397). Elsevier.

[58] Akram W, Niazi MA. A formal specification framework for smart grid components. Complex Adaptive Systems Modeling. 2018 Dec, 6:1-6.

[59] Singh AK, Kumar J. A privacy-preserving multidimensional data aggregation scheme with secure query processing for smart grid. The Journal of Supercomputing. 2023 Mar, 79(4):3750-70.

[60] Omollo VN, Musyoki S. Global Positioning System Based Routing Algorithm for Adaptive Delay Tolerant Mobile Adhoc Networks. International Journal of Computer and Communication System Engineering. 2015 May 11, 2(3): 399-406.

[61] Helmi AM, Ramadan HS, Idriss AI. Modular smart grid intelligence: Replicable concept for diverse scenarios. Sustainable Cities and Society. 2023 Sep 1, 96:104611.

[62] Viral R, Asija D, Salkuti S, editors. Big Data Analytics Framework for Smart Grids. CRC Press, 2023 Dec 22.

[63] Ningthoujam AD, Asija D, Viral RK. Necessities of Big Data in Smart Grid. InBig Data Analytics Framework for Smart Grids 2024 (pp. 1-25). CRC Press.

[64] Sharma K, Malik A, Batra I, Sanwar Hosen AS, Latif Sarker MA, Han DS. Technologies Behind the Smart Grid and Internet of Things: A System Survey. Computers, Materials & Continua. 2023 Jun 1, 75(3).

[65] Andresen AX, Kurtz LC, Hondula DM, Meerow S, Gall M. Understanding the social impacts of power outages in North America: a systematic review. Environmental Research Letters. 2023 May 1, 18(5):053004.

[66] Qiu Z, Ma J, Zhang H, Al Sibahee MA, Abduljabbar ZA, Nyangaresi VO. Concurrent pipeline rendering scheme based on GPU multi-queue and partitioning images. InInternational Conference on Optics and Machine Vision (ICOMV 2023) 2023 Apr 14 (Vol. 12634, pp. 143-149). SPIE.

[67] Dileep GJ. A survey on smart grid technologies and applications. Renewable energy. 2020 Feb 1, 146:2589-625.

[68] Judge MA, Khan A, Manzoor A, Khattak HA. Overview of smart grid implementation: Frameworks, impact, performance and challenges. Journal of Energy Storage. 2022 May 1, 49:104056.

[69] Suhaimy N, Radzi NA, Ahmad WS, Azmi KH, Hannan MA. Current and future communication solutions for smart grids: A review. IEEE Access. 2022 Apr 18, 10:43639-68.

[70] Goudarzi A, Ghayoor F, Waseem M, Fahad S, Traore I. A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook. Energies. 2022 Sep 23, 15(19):6984.

[71] Ding J, Qammar A, Zhang Z, Karim A, Ning H. Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. Energies. 2022 Sep 17, 15(18):6799.

[72] Nyangaresi VO, Mohammad Z. Session Key Agreement Protocol for Secure D2D Communication. InThe Fifth International Conference on Safety and Security with IoT: SaSeIoT 2021 2022 Jun 12 (pp. 81-99). Cham: Springer International Publishing.

[73] Ali W, Din IU, Almogren A, Kim BS. A novel privacy preserving scheme for smart grid-based home area networks. sensors. 2022 Mar 15, 22(6):2269.

[74] Ramalingam SP, Shanmugam PK. A Comprehensive Review on Wired and Wireless Communication Technologies and Challenges in Smart Residential Buildings. Recent Advances in Computer Science and Communications (Formerly: Recent Patents on Computer Science). 2022 Nov 1, 15(9):1140-67.

[75] Constantinou S, Konstantinidis A, Chrysanthis PK, Zeinalipour-Yazti D. Green planning of IoT home automation workflows in smart buildings. ACM Transactions on Internet of Things. 2022 Sep 6, 3(4):1-30.

[76] Hassan A, Afrouzi HN, Siang CH, Ahmed J, Mehranzamir K, Wooi CL. A survey and bibliometric analysis of different communication technologies available for smart meters. Cleaner Engineering and Technology. 2022 Apr 1, 7:100424.

[77] Qays MO, Ahmad I, Abu-Siada A, Hossain ML, Yasmin F. Key communication technologies, applications, protocols and future guides for IoT-assisted smart grid systems: A review. Energy Reports. 2023 Dec 1, 9:2440-52.

[78] Eid MM, Arunachalam R, Sorathiya V, Lavadiya S, Patel SK, Parmar J, Delwar TS, Ryu JY, Nyangaresi VO, Zaki Rashed AN. QAM receiver based on light amplifiers measured with effective role of optical coherent duobinary transmitter. Journal of Optical Communications. 2022 Jan 17(0).

[79] Rajendhar P, Jeyaraj BE. Application of DR and co-simulation approach for renewable integrated HEMS: a review. IET generation, transmission & distribution. 2019 Aug, 13(16):3501-12.

[80] Eissa MM. Developing incentive demand response with commercial energy management system (CEMS) based on diffusion model, smart meters and new communication protocol. Applied Energy. 2019 Feb 15, 236:273-92.

[81] Biswal SR, Choudhury TR, Panda B, Nayak B, Mahato GC. Smart Meter: Impact and Usefulness on smart Grids. In2021 IEEE 2nd International Conference on Applied Electromagnetics, Signal Processing, & Communication (AESPC) 2021 Nov 26 (pp. 1-6). IEEE.

[82] Abrahamsen FE, Ai Y, Cheffena M. Communication technologies for smart grid: A comprehensive survey. Sensors. 2021 Dec 3, 21(23):8087.

[83] Nyangaresi VO, Ma J. A Formally Verified Message Validation Protocol for Intelligent IoT E-Health Systems. In2022 IEEE World Conference on Applied Intelligence and Computing (AIC) 2022 Jun 17 (pp. 416-422). IEEE.

[84] Tiwari A, Pindoriya NM. Automated demand response in smart distribution grid: a review on metering Infrastructure, communication technology and optimization models. Electric Power Systems Research. 2022 May 1, 206:107835.

[85] Stanelyte D, Radziukyniene N, Radziukynas V. Overview of demand-response services: A review. Energies. 2022 Feb 23, 15(5):1659.

[86] Qi J, Kim Y, Chen C, Lu X, Wang J. Demand response and smart buildings: A survey of control, communication, and cyber-physical security. ACM Transactions on Cyber-Physical Systems. 2017 Oct 25, 1(4):1-25.

[87] Zafar U, Bayhan S, Sanfilippo A. Home energy management system concepts, configurations, and technologies for the smart grid. IEEE access. 2020 Jun 26, 8:119271-86.

[88] Honi DG, Ali AH, Abduljabbar ZA, Ma J, Nyangaresi VO, Mutlaq KA, Umran SM. Towards Fast Edge Detection Approach for Industrial Products. In2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS) 2022 Dec 19 (pp. 239-244). IEEE.

[89] León JP, Santos CL, Mezher AM, Barrera JC, Meng J, Guerra EC. Exploring the potential, limitations, and future directions of wireless technologies in smart grid networks: A comparative analysis. Computer Networks. 2023 Nov 1, 235:109956.

[90] Meydani A, Meidani A, Shahablavasani S. Implementation of the Internet of Things Technology in the Smart Power Grid. In2023 10th Iranian Conference on Renewable Energy & Distributed Generation (ICREDG) 2023 Mar 15 (pp. 1-8). IEEE.

[91] Cali U, Kuzlu M, Pipattanasomporn M, Kempf J, Bai L, Cali U, Kuzlu M, Pipattanasomporn M, Kempf J, Bai L. Smart grid applications and communication technologies. Digitalization of Power Markets and Systems Using Energy Informatics. 2021:17-38.

[92] Kabalci E, Kabalci Y. Introduction to smart grid architecture. Smart grids and their communication systems. 2019:3-45.

[93] Wan L, Huang Y, Li W, Zhang Y, Zhang Z. Low-Power Wide Area Networks: Changes for Smart Grid. InCommunications, Signal Processing, and Systems: Proceedings of the 2018 CSPS Volume III: Systems 7th 2020 (pp. 967-974). Springer Singapore.

[94] Nyangaresi VO. Provably Secure Pseudonyms based Authentication Protocol for Wearable Ubiquitous Computing Environment. In2022 International Conference on Inventive Computation Technologies (ICICT) 2022 Jul 20 (pp. 1-6). IEEE.

[95] Khalid HM, Qasaymeh MM, Muyeen SM, El Moursi MS, Foley AM, Tha'er OS, Sanjeevikumar P. WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks. IEEE Systems Journal. 2023 Jun 29.

[96] Sifat MM, Choudhury SM, Das SK, Ahamed MH, Muyeen SM, Hasan MM, Ali MF, Tasneem Z, Islam MM, Islam MR, Badal MF. Towards electric digital twin grid: Technology and framework review. Energy and AI. 2023 Jan 1, 11:100213.

[97] Shanmugapriya J, Baskaran K. Rapid Fault Analysis by Deep Learning-Based PMU for Smart Grid System. Intelligent Automation & Soft Computing. 2023 Feb 1, 35(2).

[98] Renugadevi N, Saravanan S, Sudha CN. IoT based smart energy grid for sustainable cites. Materials Today: Proceedings. 2023 Jan 1, 81:98-104.

[99] Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Spatial single mode laser source interaction with measured pulse based parabolic index multimode fiber. Journal of Optical Communications. 2022 Jun 21.

[100] Badr MM, Mahmoud M, Fang Y, Abdulaal M, Aljohani AJ, Alasmary W, Ibrahem MI. Privacy-preserving and communication-efficient energy prediction scheme based on federated learning for smart grids. IEEE Internet of Things Journal. 2023 Jan 3.

[101] Singh AK, Kumar J. A secure and privacy-preserving data aggregation and classification model for smart grid. Multimedia Tools and Applications. 2023 Feb 21:1-9.

[102] Wang Y, Ma J, Gao N, Wen Q, Sun L, Guo H. Federated fuzzy k-means for privacy-preserving behavior analysis in smart grids. Applied Energy. 2023 Feb 1, 331:120396.

[103] Abdulaal MJ, Mahmoud M, Bello SA, Khalid J, Aljohani AJ, Milyani AH, Abusorrah AM, Ibrahem MI. Privacy-preserving detection of power theft in smart grid change and transmit (cat) advanced metering infrastructure. IEEE Access. 2023 Jun 30.

[104] Chang Y, Li J, Li W. 2D2PS: A demand-driven privacy-preserving scheme for anonymous data sharing in smart grids. Journal of Information Security and Applications. 2023 May 1, 74:103466.

[105] Nyangaresi VO. ECC based authentication scheme for smart homes. In2021 International Symposium ELMAR 2021 Sep 13 (pp. 5-10). IEEE.

[106] Ma P, Cui S, Chen M, Zhou S, Wang K. Review of family-level short-term load forecasting and its application in household energy management system. Energies. 2023 Aug 4, 16(15):5809.

[107] Li J, Herdem MS, Nathwani J, Wen JZ. Methods and applications for Artificial Intelligence, Big Data, Internet of Things, and Blockchain in smart energy management. Energy and AI. 2023 Jan 1, 11:100208.

[108] Fakhar MZ, Yalcin E, Bilge A. A survey of smart home energy conservation techniques. Expert Systems with Applications. 2023 Mar 1, 213:118974.

[109] Pandiyan P, Saravanan S, Usha K, Kannadasan R, Alsharif MH, Kim MK. Technological advancements toward smart energy management in smart cities. Energy Reports. 2023 Nov 1, 10:648-77.

[110] Zaki Rashed AN, Ahammad SH, Daher MG, Sorathiya V, Siddique A, Asaduzzaman S, Rehana H, Dutta N, Patel SK, Nyangaresi VO, Jibon RH. Signal propagation parameters estimation through designed multi layer fibre with higher dominant modes using OptiFibre simulation. Journal of Optical Communications. 2022 Jun 23(0).

[111] Popli S, Jha RK, Jain S. A survey on energy efficient narrowband internet of things (NBIoT): architecture, application and challenges. IEEE Access. 2018 Nov 15, 7:16739-76.

[112] Ma Z, Xiao M, Xiao Y, Pang Z, Poor HV, Vucetic B. High-reliability and low-latency wireless communication for internet of things: Challenges, fundamentals, and enabling technologies. IEEE Internet of Things Journal. 2019 Mar 25, 6(5):7946-70.

[113] Hossain MA, Noor RM, Yau KL, Ahmedy I, Anjum SS. A survey on simultaneous wireless information and power transfer with cooperative relay and future challenges. IEEE access. 2019 Jan 29, 7:19166-98.

[114] Mohsan SA, Amjad H. A comprehensive survey on hybrid wireless networks: practical considerations, challenges, applications and research directions. Optical and Quantum Electronics. 2021 Sep, 53(9):523.

[115] Nyangaresi VO. Provably secure authentication protocol for traffic exchanges in unmanned aerial vehicles. High-Confidence Computing. 2023 Sep 15:100154.

[116] Tuyen ND, Quan NS, Linh VB, Van Tuyen V, Fujita G. A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. IEEE Access. 2022 Mar 30, 10:35846-75.

[117] More S, Hajari S, Majeed MA, Singh NK, Mahajan V. Cyber Security for Smart Grid: Vulnerabilities, Attacks, and Solution. InSustainable Technology and Advanced Computing in Electrical Engineering: Proceedings of ICSTACE 2021 2022 Nov 3 (pp. 835-857). Singapore: Springer Nature Singapore.

[118] Yohanandhan RV, Elavarasan RM, Pugazhendhi R, Premkumar M, Mihet-Popa L, Zhao J, Terzija V. A specialized review on outlook of future Cyber-Physical Power System (CPPS) testbeds for securing electric power grid. International Journal of Electrical Power & Energy Systems. 2022 Mar 1, 136:107720.

[119] Srivastava I, Bhat S, Singh AR. Smart Grid Communication: Recent Trends and Challenges. Next Generation Smart Grids: Modeling, Control and Optimization. 2022 Feb 1:49-75.

[120] Umran SM, Lu S, Abduljabbar ZA, Nyangaresi VO. Multi-chain blockchain based secure data-sharing framework for industrial IoTs smart devices in petroleum industry. Internet of Things. 2023 Dec 1, 24:100969.

[121] Sikiru IA, Olawoyin LA, Faruk N, Oloyede AA, Abdulkarim A, Olayinka IF, Sowande OA, Garba S, Imoize AL. Physical layer security using boundary technique for emerging wireless communication systems. Security and Privacy. 2023 May 1:e288.

[122] Abdel Hakeem SA, Hussein HH, Kim H. Security requirements and challenges of 6G technologies and applications. Sensors. 2022 Mar 2, 22(5):1969.

[123] Tefera MK, Jin Z, Zhang S. A Review of Fundamental Optimization Approaches and the Role of AI Enabling Technologies in Physical Layer Security. Sensors. 2022 May 9, 22(9):3589.

[124] Du H, Wang J, Niyato D, Kang J, Xiong Z, Guizani M, Kim DI. Rethinking wireless communication security in semantic Internet of Things. IEEE Wireless Communications. 2023 Jun, 30(3):36-43.

[125] Al-Chaab W, Abduljabbar ZA, Abood EW, Nyangaresi VO, Mohammed HM, Ma J. Secure and Low-Complexity Medical Image Exchange Based on Compressive Sensing and LSB Audio Steganography. Informatica. 2023 May 31, 47(6).

[126] Huseinović A, Mrdović S, Bicakci K, Uludag S. A survey of denial-of-service attacks and solutions in the smart grid. IEEE Access. 2020 Sep 25, 8:177447-70.

[127] Sahani N, Zhu R, Cho JH, Liu CC. Machine Learning-based Intrusion Detection for Smart Grid Computing: A Survey. ACM Transactions on Cyber-Physical Systems. 2023 Apr 19, 7(2):1-31.

[128] Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors. 2021 May 24, 21(11):3654.

[129] Adedeji KB, Abu-Mahfouz AM, Kurien AM. DDoS Attack and Detection Methods in Internet-Enabled Networks: Concept, Research Perspectives, and Challenges. Journal of Sensor and Actuator Networks. 2023 Jul 6, 12(4):51.

[130] Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Computers & Security. 2023 Jan 13:103096.

[131] Nyangaresi VO. Target Tracking Area Selection and Handover Security in Cellular Networks: A Machine Learning Approach. InProceedings of Third International Conference on Sustainable Expert Systems: ICSES 2022 2023 Feb 23 (pp. 797-816). Singapore: Springer Nature Singapore.

[132] Lehto M. Cyber-attacks against critical infrastructure. InCyber Security: Critical Infrastructure Protection 2022 Apr 3 (pp. 3-42). Cham: Springer International Publishing.

[133] Aqeel M, Ali F, Iqbal MW, Rana TA, Arif M, Auwul MR. A review of security and privacy concerns in the internet of things (IoT). Journal of Sensors. 2022 Sep 29, 2022.

[134] Mazhar T, Irfan HM, Khan S, Haq I, Ullah I, Iqbal M, Hamam H. Analysis of Cyber Security Attacks and Its Solutions for the Smart Grid Using Machine Learning and Blockchain Methods. Future Internet. 2023 Feb 19, 15(2):83.

[135] Bitirgen K, Filik ÜB. A hybrid deep learning model for discrimination of physical disturbance and cyber-attack detection in smart grid. International Journal of Critical Infrastructure Protection. 2023 Mar 1, 40:100582.

[136] Mohammadpourfard M, Khalili A, Genc I, Konstantinou C. Cyber-resilient smart cities: Detection of malicious attacks in smart grids. Sustainable Cities and Society. 2021 Dec 1, 75:103116.

[137] Abduljabbar ZA, Abduljaleel IQ, Ma J, Al Sibahee MA, Nyangaresi VO, Honi DG, Abdulsada AI, Jiao X. Provably secure and fast color image encryption algorithm based on s-boxes and hyperchaotic map. IEEE Access. 2022 Feb 11, 10:26257-70.

[138] Vähäkainu P, Lehto M, Kariluoto A. Cyberattacks Against Critical Infrastructure Facilities and Corresponding Countermeasures. InCyber Security: Critical Infrastructure Protection 2022 Apr 3 (pp. 255-292). Cham: Springer International Publishing.

[139] Garg A, Sharma B, Gupta A, Khan R. Security of Modern Networks and Its Challenges. Cyber Security Using Modern Technologies: Artificial Intelligence, Blockchain and Quantum Cryptography. 2023 Aug 2:57.

[140] Udaykumar HV. A Study on Network Threats, Attacks & Security Measures. Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596. 2023 Oct 30, 9(si1).

[141] Rizvi S, Zwerling T, Thompson B, Faiola S, Campbell S, Fisanick S, Hutnick C. A Modular Framework for Auditing IoT Devices and Networks. Computers & Security. 2023 Jun 13:103327.

[142] Abood EW, Abdullah AM, Al Sibahe MA, Abduljabbar ZA, Nyangaresi VO, Kalafy SA, Ghrabta MJ. Audio steganography with enhanced LSB method for securing encrypted text with bit cycling. Bulletin of Electrical Engineering and Informatics. 2022 Feb 1, 11(1):185-94.

[143] Grenar D, Frolka J, Slavicek K, Dostal O, Kyselak M. Network Physical Layer Attack in the Very High Capacity Networks. Advances in Electrical and Electronic Engineering. 2023 Dec 5, 21(1):37-47.

[144] Aoufi S, Derhab A, Guerroumi M. Survey of false data injection in smart power grid: Attacks, countermeasures and challenges. Journal of Information Security and Applications. 2020 Oct 1, 54:102518.

[145] Husnoo MA, Anwar A, Hosseinzadeh N, Islam SN, Mahmood AN, Doss R. False data injection threats in active distribution systems: A comprehensive survey. Future Generation Computer Systems. 2023 Mar 1, 140:344-64.

[146] Kumar P, Lin Y, Bai G, Paverd A, Dong JS, Martin A. Smart grid metering networks: A survey on security, privacy and open research issues. IEEE Communications Surveys & Tutorials. 2019 Feb 14, 21(3):2886-927.

[147] Unsal DB, Ustun TS, Hussain SS, Onen A. Enhancing cybersecurity in smart grids: false data injection and its mitigation. Energies. 2021 May 6, 14(9):2657.

[148] Nyangaresi VO. Extended Chebyshev Chaotic Map Based Message Verification Protocol for Wireless Surveillance Systems. InComputer Vision and Robotics: Proceedings of CVR 2022 2023 Apr 28 (pp. 503-516). Singapore: Springer Nature Singapore.

[149] Potorac AD. Vulnerabilities and new critical security challenges of the Internet of Things (IoT). InBiomedical Engineering Applications for People with Disabilities and the Elderly in the COVID-19 Pandemic and Beyond 2022 Jan 1 (pp. 325-333). Academic Press.

[150] Krishnan P, Jain K, Aldweesh A, Prabu P, Buyya R. OpenStackDP: a scalable network security framework for SDN-based OpenStack cloud infrastructure. Journal of Cloud Computing. 2023 Feb 28, 12(1):26.

[151] Macena B, Albuquerque C, Machado R. Cybersecurity and Privacy Protection in Vehicular Networks (VANETs). Advances in Internet of Things. 2023 Oct 30, 13(4):109-18.

[152] Anderson J. Universal Session Protocol: A Novel Approach to Session Management. arXiv preprint arXiv:2306.14339. 2023 Jun 25.

[153] Qassim QS, Ali MA, Tahir NM. Security Analysis of DNP3 Protocol in SCADA System. In2023 IEEE 13th International Conference on Control System, Computing and Engineering (ICCSCE) 2023 Aug 25 (pp. 314-319). IEEE.

[154] Abduljaleel IQ, Abduljabbar ZA, Al Sibahee MA, Ghrabat MJ, Ma J, Nyangaresi VO. A Lightweight Hybrid Scheme for Hiding Text Messages in Colour Images Using LSB, Lah Transform and Chaotic Techniques. Journal of Sensor and Actuator Networks. 2022 Dec, 11(4):66.

[155] Gaurav A, Gupta BB, Panigrahi PK. A comprehensive survey on machine learning approaches for malware detection in IoT-based enterprise information system. Enterprise Information Systems. 2023 Mar 4, 17(3):2023764.

[156] Sharma J, Mehra PS. Secure communication in IOT-based UAV networks: A systematic survey. Internet of Things. 2023 Jul 22:100883.

[157] Alanazi M, Mahmood A, Chowdhury MJ. SCADA vulnerabilities and attacks: A review of the state-of-the-art and open issues. Computers & Security. 2023 Feb 1, 125:103028.

[158] Liu P, Ji S, Fu L, Lu K, Zhang X, Qin J, Wang W, Chen W. How iot re-using threatens your sensitive data: exploring the user-data disposal in used iot devices. In2023 IEEE Symposium on Security and Privacy (SP) 2023 May 21 (pp. 3365-3381). IEEE.

[159] Mekdad Y, Aris A, Babun L, El Fergougui A, Conti M, Lazzeretti R, Uluagac AS. A survey on security and privacy issues of UAVs. Computer Networks. 2023 Apr 1, 224:109626.

[160] Nyangaresi VO. Lightweight anonymous authentication protocol for resource-constrained smart home devices based on elliptic curve cryptography. Journal of Systems Architecture. 2022 Dec 1, 133:102763.

[161] Manoj KS. Power System Automation: Build Secure Power System SCADA & Smart Grids. Notion Press, 2021 Feb 28.

[162] Abdulsalam KA, Adebisi J, Emezirinwune M, Babatunde O. An overview and multicriteria analysis of communication technologies for smart grid applications. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2023 Mar 1, 3:100121.

[163] Korki M, Jin J, Tian YC. Real-Time Cyber-physical Systems: State-of-the-Art and Future Trends. InHandbook of Real-Time Computing 2022 Aug 9 (pp. 509-540). Singapore: Springer Nature Singapore.

[164] Davydenko L, Davydenko N, Bosak A, Bosak A, Deja A, Dzhuguryan T. Smart Sustainable Freight Transport for a City Multi-Floor Manufacturing Cluster: A Framework of the Energy Efficiency Monitoring of Electric Vehicle Fleet Charging. Energies. 2022 May 20, 15(10):3780.

[165] Hussain MA, Hussien ZA, Abduljabbar ZA, Ma J, Al Sibahee MA, Hussain SA, Nyangaresi VO, Jiao X. Provably throttling SQLI using an enciphering query and secure matching. Egyptian Informatics Journal. 2022 Dec 1, 23(4):145-62.

[166] Martins T, Oliveira SV. Enhanced Modbus/TCP security protocol: Authentication and authorization functions supported. Sensors. 2022 Oct 20, 22(20):8024.

[167] Katulić F, Sumina D, Groš S, Erceg I. Protecting Modbus/TCP-Based Industrial Automation and Control Systems Using Message Authentication Codes. IEEE Access. 2023 May 11.

[168] Alzahrani A, Wangikar SM, Indragandhi V, Singh RR, Subramaniyaswamy V. Design and Implementation of SAE J1939 and Modbus Communication Protocols for Electric Vehicle. Machines. 2023 Feb 1, 11(2):201.

[169] Elamanov S, Son H, Flynn B, Yoo SK, Dilshad N, Song J. Interworking between Modbus and internet of things platform for industrial services. Digital Communications and Networks. 2022 Oct 6.

[170] Ding Z, He D, Qiao Q, Li X, Gao Y, Chan S, Choo KK. A Lightweight and Secure Communication Protocol for the IoT Environment. IEEE Transactions on Dependable and Secure Computing. 2023 Apr 17.

[171] Nyangaresi VO, Ahmad M, Alkhayyat A, Feng W. Artificial neural network and symmetric key cryptography based verification protocol for 5G enabled Internet of Things. Expert Systems. 2022 Dec, 39(10):e13126.

[172] Mololoth VK, Saguna S, Åhlund C. Blockchain and machine° learning for future smart grids: A review. Energies. 2023 Jan 3, 16(1):528.

[173] Khan AA, Laghari AA, Rashid M, Li H, Javed AR, Gadekallu TR. Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review. Sustainable Energy Technologies and Assessments. 2023 Jun 1, 57:103282.

[174] Park K, Lee J, Das AK, Park Y. BPPS: Blockchain-enabled privacy-preserving scheme for demand-response management in smart grid environments. IEEE Transactions on Dependable and Secure Computing. 2022 Mar 29, 20(2):1719-29.

[175] Kumari A, Chintukumar Sukharamwala U, Tanwar S, Raboaca MS, Alqahtani F, Tolba A, Sharma R, Aschilean I, Mihaltan TC. Blockchain-Based Peer-to-Peer Transactive Energy Management Scheme for Smart Grid System. Sensors. 2022 Jun 26, 22(13):4826.

[176] Alsamhi SH, Shvetsov AV, Kumar S, Shvetsova SV, Alhartomi MA, Hawbani A, Rajput NS, Srivastava S, Saif A, Nyangaresi VO. UAV computing-assisted search and rescue mission framework for disaster and harsh environment mitigation. Drones. 2022 Jun 22, 6(7):154.

[177] Chehri A, Fofana I, Yang X. Security risk modeling in smart grid critical infrastructures in the era of big data and artificial intelligence. Sustainability. 2021 Mar 15, 13(6):3196.

[178] Radoglou-Grammatikis PI, Sarigiannidis PG. Securing the smart grid: A comprehensive compilation of intrusion detection and prevention systems. Ieee Access. 2019 Apr 9, 7:46595-620.

[179] AlHaddad U, Basuhail A, Khemakhem M, Eassa FE, Jambi K. Ensemble Model Based on Hybrid Deep Learning for Intrusion Detection in Smart Grid Networks. Sensors. 2023 Aug 28, 23(17):7464.

[180] Ghasempour A. Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges. Inventions. 2019 Mar 26, 4(1):22.

[181] Alhasnawi BN, Jasim BH. Internet of Things (IoT) for smart grids: A comprehensive review. J. Xi'an Univ. Archit. 2020, 63:1006-7930.

[182] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Jan, 11(24):12040.

[183] Hossain E, Roy S, Mohammad N, Nawar N, Dipta DR. Metrics and enhancement strategies for grid resilience and reliability during natural disasters. Applied energy. 2021 May 15, 290:116709.

[184] Nafees MN, Saxena N, Cardenas A, Grijalva S, Burnap P. Smart grid cyber-physical situational awareness of complex operational technology attacks: A review. ACM Computing Surveys. 2023 Feb 2, 55(10):1-36.

[185] Sani AS, Yuan D, Jin J, Gao L, Yu S, Dong ZY. Cyber security framework for Internet of Things-based Energy Internet. Future Generation Computer Systems. 2019 Apr 1, 93:849-59.

[186] Ferrag MA, Maglaras L. DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids. IEEE Transactions on Engineering Management. 2019 Jul 9, 67(4):1285-97.

[187] Ayvaz S, Alpay K. Predictive maintenance system for production lines in manufacturing: A machine learning approach using IoT data in real-time. Expert Systems with Applications. 2021 Jul 1, 173:114598.

[188] Yenurkar GK, Mal S, Nyangaresi VO, Hedau A, Hatwar P, Rajurkar S, Khobragade J. Multifactor data analysis to forecast an individual's severity over novel COVID-19 pandemic using extreme gradient boosting and random forest classifier algorithms. Engineering Reports. 2023:e12678.

[189] Liu X, Qian C, Hatcher WG, Xu H, Liao W, Yu W. Secure Internet of Things (IoT)-based smart-world critical infrastructures: Survey, case study and research opportunities. IEEE Access. 2019 Jun 4, 7:79523-44.

[190] Shrestha M, Johansen C, Noll J, Roverso D. A methodology for security classification applied to smart grid infrastructures. International Journal of Critical Infrastructure Protection. 2020 Mar 1, 28:100342.

[191] Tonyali S, Akkaya K, Saputro N, Cheng X. An attribute & network coding-based secure multicast protocol for firmware updates in smart grid AMI networks. In2017 26th International Conference on Computer Communication and Networks (ICCCN) 2017 Jul 31 (pp. 1-9). IEEE.

[192] Kwon Y, Kim HK, Koumadi KM, Lim YH, Lim JI. Automated vulnerability analysis technique for smart grid infrastructure. In2017 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2017 Apr 23 (pp. 1-5). IEEE.

[193] Joshi KM, Dalal T, Chaudhary P. Quantum Computing and Grid Security. InISUW 2020: Proceedings of the 6th International Conference and Exhibition on Smart Grids and Smart Cities 2022 May 10 (pp. 179-188). Singapore: Springer Nature Singapore.

[194] Satrya GB, Agus YM, Mnaouer AB. A Comparative Study of Post-Quantum Cryptographic Algorithm Implementations for Secure and Efficient Energy Systems Monitoring. Electronics. 2023 Sep 10, 12(18):3824.