World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(Review Article)

Check for updates

Safeguarding the future: A comprehensive analysis of security measures for smart grids

Sharmwey A. Wasumwa *

Jaramogi Oginga Odinga University of Science & Technology, Kenya.

World Journal of Advanced Research and Reviews, 2023, 19(01), 847–871

Publication history: Received on 02 June 2023; revised on 17 July 2023; accepted on 19 July 2023

Article DOI: https://doi.org/10.30574/wjarr.2023.19.1.1387

Abstract

With the rapid advancement of technology and the growing reliance on renewable energy sources, smart grids have emerged as a transformative solution for enhancing the efficiency and reliability of power distribution systems. As the smart grid ecosystem evolves, security concerns become paramount due to the interconnectedness of various components, including advanced metering infrastructure, communication networks, and distributed energy resources. This paper presents a comprehensive analysis of smart grid security, focusing on the challenges, vulnerabilities, and potential threats that must be addressed to ensure the resilience of these intelligent infrastructures. It explores the diverse attack vectors that malicious actors may exploit to compromise smart grid operations and highlights the potential consequences of such security breaches, including power disruptions, data breaches, and financial losses. To counteract these risks, this paper delves into various state-of-the-art security measures and strategies that can be implemented to safeguard smart grids effectively. Moreover, the importance of collaboration between various stakeholders is described, including utility companies, government agencies, researchers, and technology vendors, to foster a holistic approach to smart grid security. By emphasizing the significance of information sharing and collaboration, this paper advocates for a robust and adaptive security framework to respond promptly to emerging threats and vulnerabilities. Furthermore, the paper explores emerging technologies such as artificial intelligence, blockchain, and intrusion detection systems, showcasing their potential contributions in fortifying smart grid defenses. It was noted that the integration of these innovative technologies can enhance anomaly detection, facilitate secure data exchange, and reinforce the resilience of the smart grid against sophisticated cyber-attacks. Towards the end of this paper, insights into future research directions and policy implications to foster a more secure and sustainable smart grid environment is provided. By acknowledging the evolving threat landscape and the dynamic nature of the smart grid domain, this work encourages continuous research and development to stay ahead of adversaries and establish a secure foundation for the future of energy distribution.

Keywords: Attacks; Privacy; Smart Grids; Protection; Efficiency

1. Introduction

The smart grid has emerged as a transformative solution for modernizing power distribution systems, enhancing energy efficiency, and integrating renewable energy sources into the existing infrastructure [1]-[4]. By leveraging advanced sensing, communication, and control technologies, smart grids enable real-time monitoring, intelligent decision-making, and two-way communication between energy providers and consumers [5], [6]. Fig.1 depicts the main smart grid design objectives.

*Corresponding author: Sharmwey A. Wasumwa

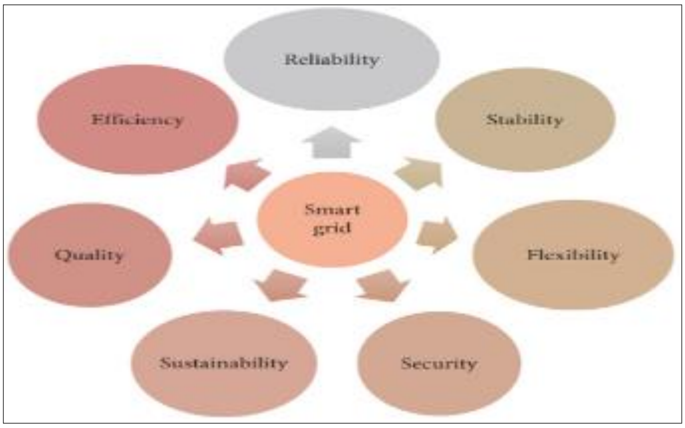

Figure 1 Smart grid design objectives

With the increasing complexity and interconnectedness of smart grid components, security has become a critical concern that must be addressed to ensure the reliable and secure operation of these intelligent infrastructures [7]-[11]. As shown in Fig.2, the integration of diverse technologies and communication networks in smart grids introduces new vulnerabilities and potential threats that can undermine the stability and resilience of the power grid [12]-[14].

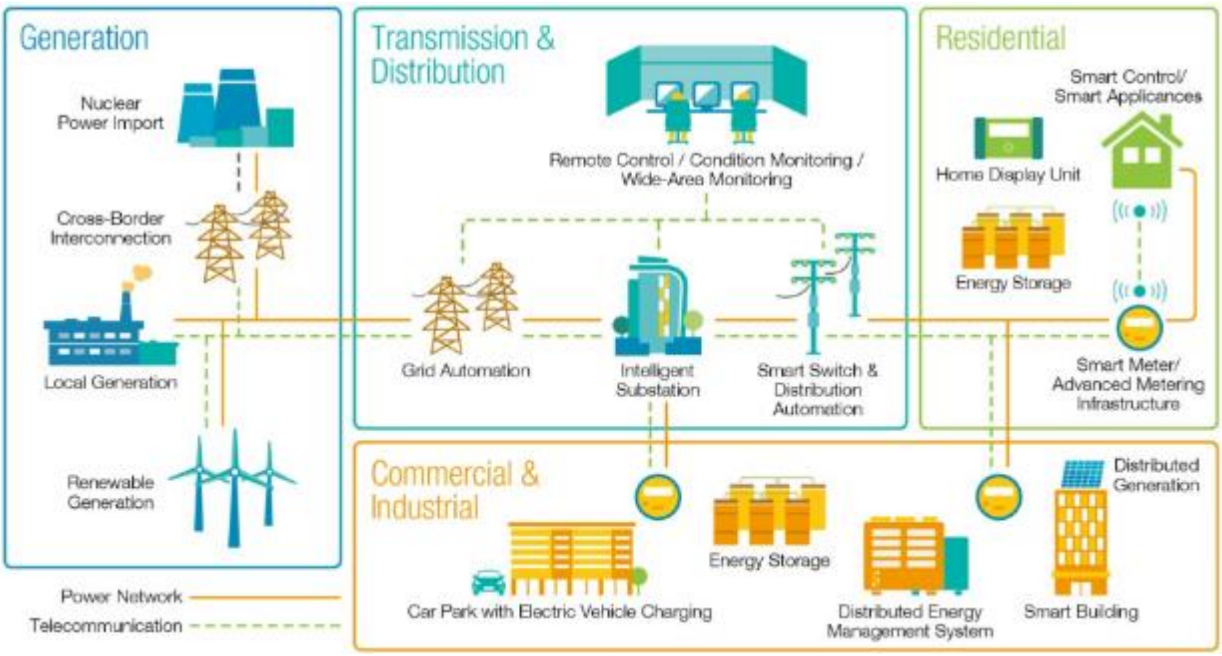

Figure 2 Smart grid ecosystem

Malicious actors, ranging from individual hackers to sophisticated state-sponsored organizations, are constantly seeking to exploit these vulnerabilities for various purposes, including disruption of power supply, unauthorized access to sensitive data, and financial gain [15], [16]. As smart grids become more pervasive, the potential impact of successful attacks on critical infrastructures becomes increasingly severe.

The consequences of security breaches in smart grids extend beyond financial losses and service disruptions. They can result in compromised customer privacy, data integrity issues, and even physical damage to equipment [17]-[21]. The interconnected nature of the smart grid ecosystem means that a single weak link in the system can have cascading effects on the entire network, leading to widespread consequences. Therefore, addressing smart grid security is not only crucial for ensuring the stability and reliability of power supply but also for safeguarding national security and protecting public safety [22]-[25]. The complexity of smart grid systems, which involve numerous interconnected components such as advanced metering infrastructure, distribution automation systems, energy management systems, and communication networks, presents unique challenges in terms of security management [26]-[30]. These challenges include securing diverse endpoints, ensuring the integrity of data exchange, mitigating the risk of unauthorized access, and detecting and responding to emerging threats in real-time [31], [32].Moreover, the ever-evolving nature of cyber threats necessitates proactive measures and continuous improvement of security mechanisms to stay ahead of adversaries.

To tackle these challenges and protect smart grids from potential security breaches, a multidimensional approach is required. This approach involves a combination of technical solutions, policy frameworks, collaboration among stakeholders, and continuous research and development efforts. Various security measures, such as encryption, authentication, intrusion detection systems, and secure communication protocols, play a crucial role in fortifying the smart grid infrastructure against cyber-attacks [33]-[36]. The contributions of this paper include the following.

A comprehensive analysis of smart grid security is provided, focusing on the challenges, vulnerabilities, and potential threats that need to be addressed.

The paper delves into various state-of-the-art security measures and strategies that can be employed to enhance the resilience of smart grids.

Emerging technologies and research directions are explored that can further strengthen the security of smart grid infrastructures.

By shedding light on the importance of smart grid security and presenting effective countermeasures, this paper contributes to the establishment of a secure and reliable foundation for the future of energy distribution. The ultimate goal is to ensure the seamless integration of advanced technologies into the power grid while mitigating the associated security risks, thereby enabling the realization of a sustainable and resilient energy infrastructure for the benefit of society as a whole.

The rest of this paper is organized as follows: Section 2 describes the smart grid environment, while Section 3 discusses the need for smart grid security. On the other hand, Section 4 presents security solutions for smart grids, while the issues with current smart grid security solutions are discussed in Section 5. Towards the end of this paper, Section 6 and Section 7 presents research gaps and future research directions. Finally, Section 8 concludes this paper.

1.1. Smart grid environment

Smart grids involve various entities that work together to ensure the efficient and reliable operation of the electrical power system [37], [38]. These entities play distinct roles in the generation, transmission, distribution, and consumption of electricity. The main entities in smart grids include power producers/generators; Transmission System Operators (TSOs); Distribution System Operators (DSOs); Smart Meters and Advanced Metering Infrastructure (AMI); Energy Management Systems (EMS); Energy Storage Systems (ESS); Demand Response (DR) Providers; and consumers. Fig.3 shows communication and electrical flows in a typical smart grid environment.

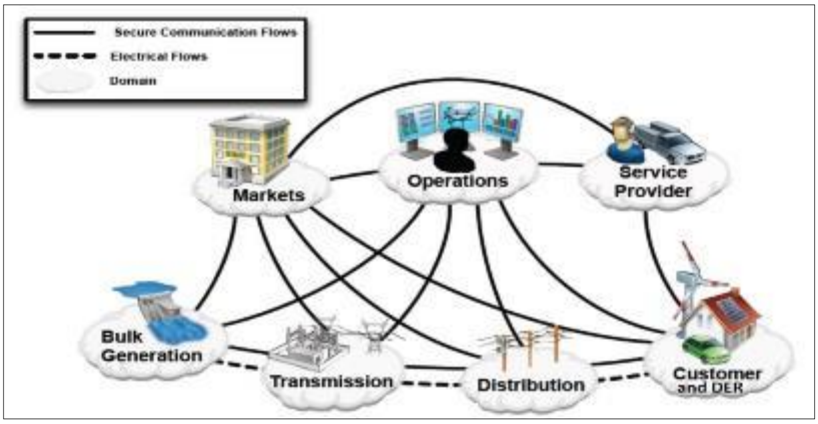

Figure 3 Communication and electrical flows

- *Power Producers/Generators:* Power producers are responsible for generating electricity from various sources, such as thermal power plants, renewable energy sources (solar, wind, hydro), and distributed energy resources (DERs) like rooftop solar panels. They play a crucial role in supplying electricity to the grid [39].
- *Transmission System Operators (TSOs):* TSOs are responsible for operating, maintaining, and managing the high-voltage transmission infrastructure that connects power generation facilities to distribution networks [40]. They ensure the reliable and secure transmission [41] of electricity over long distances, balancing supply and demand and managing grid stability.
- *Distribution System Operators (DSOs):* DSOs are responsible for the operation and maintenance of the distribution networks that deliver electricity to end consumers [42], [43]. They manage the low-voltage and medium-voltage networks, including substations, transformers, and distribution lines. DSOs coordinate with TSOs and manage the integration of DERs into the distribution grid.
- *Smart Meters and Advanced Metering Infrastructure (AMI):* Smart meters are electronic devices that measure and record electricity consumption at the consumer level [44], [45]. They provide two-way communication capabilities [46], enabling real-time data collection and remote monitoring. AMI refers to the infrastructure that supports smart meters, including data management systems, communication networks, and meter data analytics.
- *Energy Management Systems (EMS):* EMS is a software system used by grid operators to monitor, control, and optimize the operation of the power system [47], [48]. It integrates data from various sources, including SCADA (Supervisory Control and Data Acquisition) systems, smart meters, and generation units, to ensure grid stability, manage load balancing, and support efficient energy dispatch.
- *Energy Storage Systems (ESS):* Energy storage systems are used to store excess electricity generated during periods of low demand and supply it during high-demand periods [49], [51]. They help balance supply and demand, enhance grid stability, and facilitate the integration of intermittent renewable energy sources. Examples of energy storage systems include batteries, pumped hydro storage, and flywheels.
- *Demand Response (DR) Providers*: DR providers enable consumers to actively participate in managing electricity demand by adjusting their consumption patterns in response to price signals or grid conditions [52], [53]. They offer programs that incentivize consumers to reduce or shift their electricity usage during peak periods, thus supporting grid reliability and reducing stress on the system.
- *Consumers:* Consumers are the end users of electricity who utilize it for various purposes, such as residential, commercial, and industrial applications [54]. In smart grids, consumers play an active role by leveraging technologies like smart meters, home automation systems, and energy management tools to monitor and optimize their energy usage, reduce waste, and contribute to grid stability through demand response programs.

These entities work together within the smart grid ecosystem to ensure the efficient, reliable, and sustainable supply of electricity. Through advanced technologies, real-time communication, and data-driven decision-making, smart grids enable optimized energy management, integration of renewable energy sources, and improved overall system performance.

1.2. Need for smart grid security

The need for smart grid security arises from the increasing reliance on interconnected and intelligent energy distribution systems [55], [56]. Smart grids leverage advanced technologies, such as sensors, communication networks, and data analytics, to enable real-time monitoring, automation, and optimization of power generation, transmission, and consumption [57], [58]. While these advancements bring numerous benefits, they also introduce vulnerabilities and potential risks that must be addressed to ensure the integrity, reliability, and privacy of the smart grid infrastructure [59]-[62]. One of the primary drivers for smart grid security is the criticality of the power grid itself. Electricity is a vital resource that underpins various sectors of modern society, including healthcare, transportation, communication, and commerce. Disruptions to the power supply can have far-reaching consequences, causing financial losses, endangering public safety, and disrupting essential services. Therefore, protecting the smart grid infrastructure from malicious attacks and accidental failures is crucial to ensure the uninterrupted and reliable delivery of electricity [63]-[67].

Smart grids encompass a complex ecosystem consisting of diverse components, including power generation facilities, transmission and distribution networks, smart meters, data management systems, and communication infrastructure [68]. The interconnection and interoperability of these components create potential entry points for cyber-attacks. Malicious actors, ranging from individual hackers to organized crime groups and nation-state adversaries, may exploit these vulnerabilities to gain unauthorized access, manipulate data, disrupt operations, or cause physical damage [69]-

[72]. There is need to mitigate these risks and protect the integrity and availability of the grid. Furthermore, the integration of renewable energy sources and distributed energy resources (DERs) into the smart grid introduces new security challenges [73]-[75]. DERs, such as solar panels and wind turbines, often rely on communication networks to transmit data and receive instructions. If compromised, these resources can be manipulated to inject false information, disrupt grid stability, or even cause blackouts [76], [77]. Therefore, securing the communication channels and control mechanisms of DERs is crucial to maintain the stability and resilience of the smart grid.

Another factor driving the need for smart grid security is the increasing amount of data generated by smart meters, sensors, and other grid devices [78], [79]. This data includes detailed information about energy consumption patterns, customer behavior, and grid performance, which can be valuable to attackers. Safeguarding the privacy and confidentiality of this data is essential to protect consumer rights and maintain public trust in smart grid technologies [80]-[82]. Adequate security measures, such as encryption, access controls, and secure data storage and transmission, are required to ensure the privacy of sensitive information [83], [84].

Moreover, the evolving threat landscape calls for proactive security measures in smart grids. Cyber-attacks are becoming more sophisticated, with attackers employing advanced techniques and tools to exploit vulnerabilities [85]-[87]. The rapid proliferation of connected devices and the Internet of Things (IoT) further expands the attack surface, increasing the potential entry points for attackers. To stay ahead of adversaries, continuous research and development efforts are needed to identify emerging threats, develop robust defense mechanisms, and enhance the resilience of smart grid systems [88], [89].

In a nutshell, the need for smart grid security stems from the criticality of the power grid, the complexity and interconnectedness of smart grid components, the integration of renewable energy sources and distributed resources, the need to protect consumer privacy, and the evolving threat landscape. By implementing comprehensive security measures and fostering collaboration among stakeholders, it is possible to enhance the resilience, reliability, and privacy of smart grids, ensuring the sustainable and secure delivery of electricity in the digital age [90]-[92].

1.3. Vulnerabilities in the smart grids

The smart grid, while offering numerous benefits in terms of efficiency and reliability, is susceptible to various vulnerabilities that can be exploited by malicious actors. These vulnerabilities can compromise the integrity, availability, and confidentiality of the smart grid infrastructure. Table 1 details some of the key vulnerabilities in the smart grid.

Table 1 Smart grid vulnerabilities

Vulnerability	Explanation
Insecure communication networks	The communication networks used in smart grids are susceptible to interception, eavesdropping, and unauthorized access. Weak or outdated encryption protocols, inadequate authentication mechanisms, and unsecured communication channels can expose sensitive data and allow attackers to manipulate or disrupt the flow of information within the grid [93]-[97].
Weak authentication and access control	Inadequate authentication and access control mechanisms can lead to unauthorized access to smart grid devices, control systems, and critical infrastructure [98]-[100]. Weak passwords, default credentials, or lack of strong authentication methods can allow attackers to gain unauthorized control over grid components and disrupt operations or manipulate data [101], [102].
Lack of security monitoring and incident response	Inadequate security monitoring and incident response capabilities can delay the detection and response to security incidents. Without timely detection and mitigation, attackers can exploit vulnerabilities and maintain persistent access to the smart grid infrastructure, causing prolonged disruptions or data breaches [103], [104].
Vulnerable software and firmware	Smart grid devices and control systems often run on software and firmware that may have vulnerabilities, such as unpatched software, weak encryption algorithms, or insecure configurations [105]-[107]. Exploiting these vulnerabilities can provide entry points for attackers to gain unauthorized access, manipulate data, or disrupt grid operations.

Physical security risks	Physical infrastructure, including substations, control centers, and grid equipment, can be vulnerable to physical attacks [108]. Unauthorized access to critical infrastructure, tampering with devices or equipment, or disrupting power supply through physical means can have severe consequences for the smart grid's functionality and reliability [109]-[113].
Lack of secure firmware and software updates	The process of updating firmware and software in smart grid devices can introduce vulnerabilities if not done securely [114]. Insecure update mechanisms or the lack of timely updates can leave devices exposed to known vulnerabilities, making them susceptible to attacks that have already been patched in newer versions [115]-[118].
Distributed energy resources (DERs)	The integration of distributed energy resources, such as solar panels and wind turbines, into the smart grid introduces additional vulnerabilities [119]. Insecure communication interfaces, lack of standardized security protocols, and limited oversight on DER installations can allow attackers to manipulate power generation, inject false data, or disrupt grid stability [120], [121].
Insider threats	Insiders with authorized access to smart grid systems, such as employees or contractors, can pose a significant threat [122], [123]. Insiders may misuse their privileges, intentionally introduce vulnerabilities, or inadvertently compromise the security of the grid through negligence or social engineering attacks [124], [125].
Third-party integration and supply chain risks	The integration of third-party components, software, and services into the smart grid ecosystem introduces supply chain risks [126]. Insecure components or compromised software from third-party vendors can introduce vulnerabilities that can be exploited by attackers to gain unauthorized access or manipulate the grid infrastructure [127], [128].

Addressing these vulnerabilities requires a comprehensive and multi-layered approach to smart grid security. It involves implementing robust encryption and authentication mechanisms, ensuring secure software and firmware updates, establishing strong access controls, conducting regular security assessments, and fostering a security-conscious culture among stakeholders involved in the design, implementation, and operation of the smart grid.

1.4. Notable attacks in power systems

There have been several notable attacks on power systems that have highlighted the vulnerabilities and potential consequences of cyber-attacks on critical infrastructure. Some of these notable attacks are presented in Table 2 below.

Table 2 Notable attacks in smart grids

Attack	Description
Ukraine cyber-attack (2015)	In December 2015, Ukraine experienced a significant cyber-attack targeting its power grid. Attackers used malware to gain access to control systems and remotely manipulate equipment, resulting in widespread power outages [129]. It was one of the first known instances of a cyber-attack causing a large-scale disruption in a power system.
Dragonfly/energetic bear (2014-2017)	Dragonfly, also known as Energetic Bear, was a sophisticated cyber-espionage campaign targeting energy sector organizations, including power utilities, in Europe and North America [130]. The attackers gained access to control systems and conducted reconnaissance, potentially positioning themselves for future disruptive attacks.
Stuxnet worm (2010)	Stuxnet was a highly sophisticated worm discovered in 2010 that targeted industrial control systems, including those used in power plants [131]. It specifically targeted Iran's nuclear program but inadvertently spread worldwide. Stuxnet exploited multiple zero-day vulnerabilities and disrupted the functioning of centrifuges, causing physical damage to Iran's uranium enrichment facility.
BlackEnergy attacks (2015-2016)	The BlackEnergy malware was used in a series of cyber-attacks targeting Ukrainian energy companies [132]. These attacks resulted in power outages and disrupted critical infrastructure. The malware was delivered through spear-phishing emails

	[133] and was capable of stealing information, conducting surveillance, and controlling infected systems.
CrashOverride/Industroyer (2016)	CrashOverride, also known as Industroyer, is a sophisticated malware specifically designed to target electric grid control systems [134], [135]. It has the ability to map and control industrial communication protocols, potentially enabling attackers to disrupt power distribution. It was responsible for the 2016 power outage in Ukraine.
Triton (Trisis) (2017)	The Triton malware was discovered in a Saudi Arabian petrochemical facility in 2017. It was specifically designed to target safety instrumented systems (SIS), which are critical for preventing accidents in industrial processes [136], [137]. Triton sought to reprogram the SIS to disable safety mechanisms, posing a significant risk to plant personnel and the surrounding environment.

These attacks serve as a stark reminder of the potential impact of cyber-attacks on power systems. They highlight the vulnerabilities in control systems, the importance of secure communication networks, and the need for robust security measures to protect critical infrastructure [138]. They also emphasize the need for continuous monitoring, threat intelligence, and proactive defense mechanisms to detect and respond to emerging cyber threats in the power sector. These incidents have spurred increased awareness and investment in power system security, driving the development of more resilient and secure smart grid infrastructures. However, as the threat landscape evolves, it remains crucial to stay vigilant, invest in advanced security solutions, and promote collaboration among stakeholders to mitigate the risks posed by cyber-attacks on power systems.

1.5. Security solutions for smart grids

Security solutions for smart grids encompass a range of technical, operational, and policy measures aimed at safeguarding the infrastructure, data, and operations of the grid [139]- [141]. These solutions address the unique challenges and vulnerabilities associated with smart grids and aim to mitigate the risks posed by cyber threats and physical attacks [142], [143]. Some key security solutions for smart grids include access control and authentication; encryption and data security; Intrusion Detection and Prevention Systems (IDPS); secure communication networks; secure firmware and software updates; incident response and recovery; security awareness and training; collaboration and information sharing; and regulatory frameworks and standards.

According to [144], implementing strong access control mechanisms is crucial to prevent unauthorized access to smart grid devices and systems. Fig.4 shows a typical access control mechanism is smart grids. This includes user authentication, role-based access control, and secure login protocols [145]-[148]. Multi-factor authentication, such as using biometrics or smart cards, adds an extra layer of security.

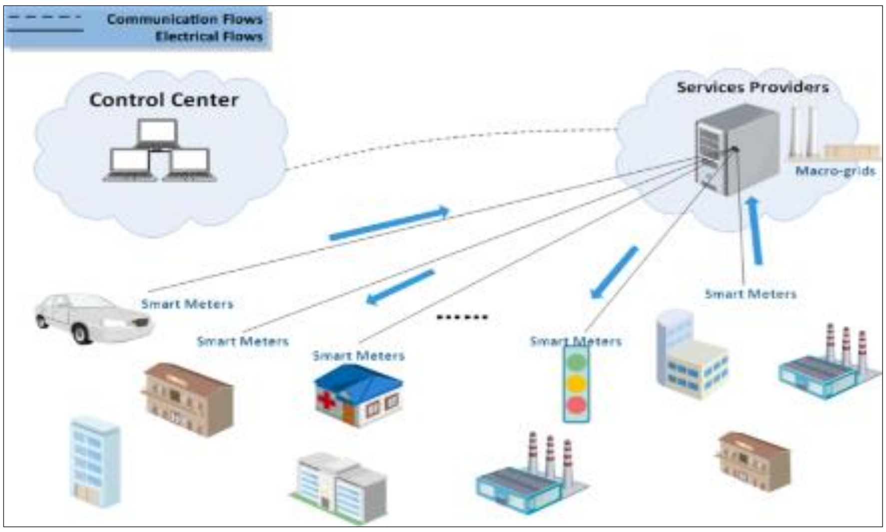

Figure 4 Access control in smart grids

As explained in [149], data encryption is essential to protect sensitive information transmitted over smart grid communication networks. Encryption techniques, such as Secure Socket Layer (SSL) or Transport Layer Security (TLS), ensure that data is securely transmitted and can only be accessed by authorized recipients [150]. As shown in Fig.5, IDPS continuously monitor smart grid networks and devices for suspicious activities or anomalies that could indicate a potential security breach [151]-[153]. These systems employ techniques such as signature-based detection, anomaly detection, and behavior analysis to identify and respond to security incidents in real-time.

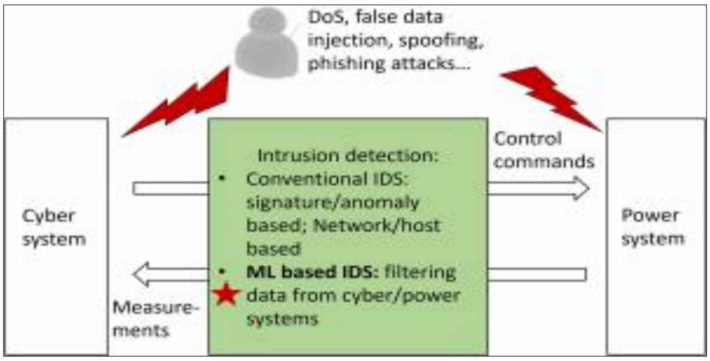

Figure 5 IDPS monitoring in smart grid networks

Regarding secure communication networks, authors in [154] explain that smart grid communication networks should be designed with security in mind. This involves implementing secure protocols, such as secure Message Queuing Telemetry Transport (MQTT) or Advanced Encryption Standard (AES), to protect the integrity and confidentiality of data transmitted between grid components [155]-[158]. Fig.6 shows a classic encryption in smart grids. Virtual private networks (VPNs) can be employed to establish secure connections between different parts of the smart grid infrastructure.

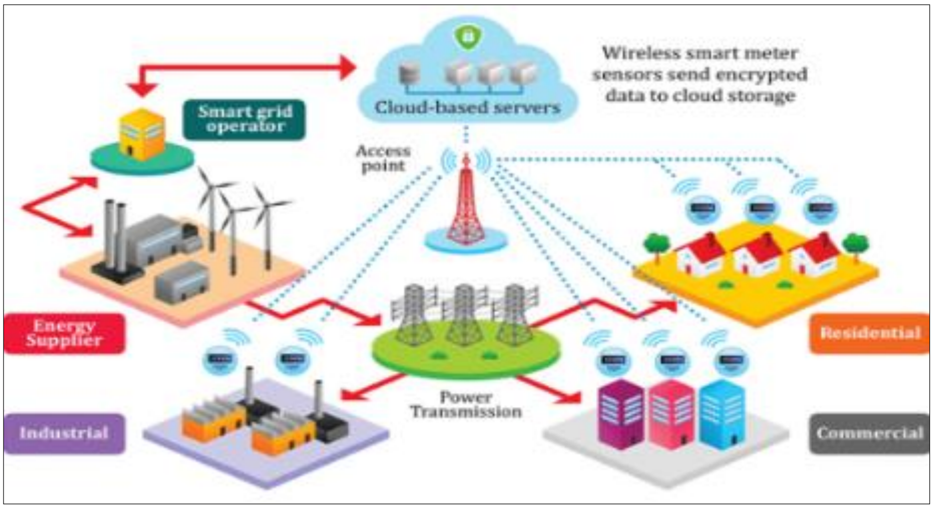

Figure 6 Classic encryption in smart grids

Pertaining secure firmware and software updates, authors in [159] discuss that regular firmware and software updates are essential for patching security vulnerabilities and addressing known weaknesses in smart grid devices and systems. Secure update mechanisms should be implemented to ensure the authenticity and integrity of updates, preventing malicious actors from injecting unauthorized code into the grid infrastructure [160]-[163]. On the other hand, having a well-defined incident response plan has been noted in [164] to be critical in minimizing the impact of security incidents and swiftly recover from disruptions. This includes establishing protocols for incident detection, reporting, containment, investigation, and system restoration [165], [166]. Regular security drills and exercises can help prepare grid operators and personnel for potential security incidents.

According to [167], security awareness and training involves educating personnel and users about smart grid security best practices is crucial. Training programs should cover topics such as recognizing phishing attempts [168], handling suspicious emails, and adhering to password hygiene. Promoting a culture of security awareness helps mitigate risks associated with human error or insider threats. Regarding collaboration and information sharing, researchers in [169] explain that collaboration among stakeholders, including utility companies, technology vendors, researchers, and government agencies, is vital for addressing smart grid security challenges collectively. Sharing information about emerging threats, vulnerabilities, and best practices enables a proactive approach to security and fosters a stronger defense against evolving cyber threats [170], [171]. Concerning regulatory frameworks and standards, authors in [172] note that governments and regulatory bodies play a significant role in establishing security requirements and standards for smart grid deployments. These frameworks provide guidelines for grid operators, technology vendors, and service providers to ensure compliance with security practices and promote a consistent security posture across the industry.

By implementing a combination of these security solutions, smart grid operators can enhance the resilience and protection of their infrastructure against potential cyber-attacks, physical threats, and operational disruptions [173], [174]. Continuous evaluation, monitoring, and improvement of security measures are essential to stay ahead of emerging threats and ensure the long-term security and reliability of smart grids.

1.6. Issues with current smart grid security solutions

While current smart grid security solutions aim to address the unique challenges associated with protecting the infrastructure, data, and operations of the grid, several persistent challenges remain. These challenges can hinder the effectiveness and robustness of smart grid security solutions. Table 3 presents some of the main challenges with current smart grid security solutions.

Table 3 Smart grid security solutions challenges

Challenge	Explanation
Complexity and interconnectedness	Smart grids are complex ecosystems that involve numerous interconnected components, including generation plants, transmission lines, distribution networks, smart meters, and control systems [175]. The interdependencies among these components create a vast attack surface, making it challenging to identify and protect against all potential vulnerabilities and entry points [175]-[178].
Rapid technological advancements	The rapid evolution of technology introduces new vulnerabilities and attack vectors [179]. Smart grid systems often incorporate emerging technologies such as cloud computing, Internet of Things (IoT), and artificial intelligence [180]-[183]. These technologies may have inherent security weaknesses or require specialized security solutions that are still under development or lack maturity.
Lack of standardization	The absence of standardized security protocols and frameworks across different smart grid components can create compatibility and interoperability issues [184], [185]. Inconsistent security implementations make it challenging to manage security policies, perform comprehensive risk assessments, and coordinate incident response efforts. Standardization efforts are necessary to ensure a consistent and harmonized approach to smart grid security [186].
Privacy concerns	Smart grids generate vast amounts of data related to energy consumption, user behavior, and grid performance. Protecting the privacy of this data is crucial [187], [188]. However, achieving a balance between data security and maintaining individual privacy rights can be challenging. Proper anonymization techniques, data access controls, and transparency in data handling practices are necessary to address privacy concerns [189]-[193].
Lack of security awareness	Despite the growing importance of smart grid security, a lack of security awareness among personnel and end-users remains a challenge [194]. Users may fall victim to social engineering attacks or unknowingly engage in risky behaviors that compromise the security of the grid. Increasing security awareness through training programs and educational initiatives is crucial to address this challenge [195]-[198].
Legacy infrastructure	Many existing power grid systems were not originally designed with security in mind [199], [200]. Retrofitting security solutions onto legacy infrastructure can be complex and expensive. Legacy systems may lack necessary security features or have outdated protocols

	and hardware that are more susceptible to cyber-attacks. Securing legacy systems without disrupting critical operations is a significant challenge.
Resource constraints	Smart grid operators often face resource constraints, including limited budgets and expertise. Implementing and maintaining robust security solutions require significant investments in technology, personnel, and ongoing security operations [201]. Many organizations struggle to allocate sufficient resources to continuously monitor and update security measures, leaving them vulnerable to emerging threats.
Insider threats	While external cyber threats often receive significant attention, insider threats pose a persistent challenge. Insiders with authorized access to smart grid systems may misuse their privileges or inadvertently introduce security risks [202], [203]. Ensuring proper access controls, conducting regular personnel training, and implementing strong monitoring mechanisms are essential to mitigate insider threats [204].

Tackling these issues requires a comprehensive and holistic approach to smart grid security. Collaboration among stakeholders, including grid operators, technology vendors, researchers, and policymakers, is crucial to developing standardized security practices, sharing threat intelligence, and coordinating efforts. Continuous research and development, along with ongoing investments in security infrastructure and personnel training, are necessary to stay ahead of evolving threats and ensure the resilience and integrity of smart grid systems.

1.7. Research gaps

While significant progress has been made in the field of smart grid security, several research gaps remain that need to be addressed. These research gaps are crucial for enhancing the security posture of smart grids and addressing emerging challenges. Some of the pertinent research gaps in smart grid security include the following.

Threat intelligence and analytics: Developing advanced threat intelligence capabilities specific to smart grids is essential [205]. As shown in Fig.7, this might involve the usage of artificial intelligence. This involves understanding and analyzing the evolving threat landscape, including new attack vectors, techniques, and motivations of adversaries targeting smart grid infrastructures [206], [207].

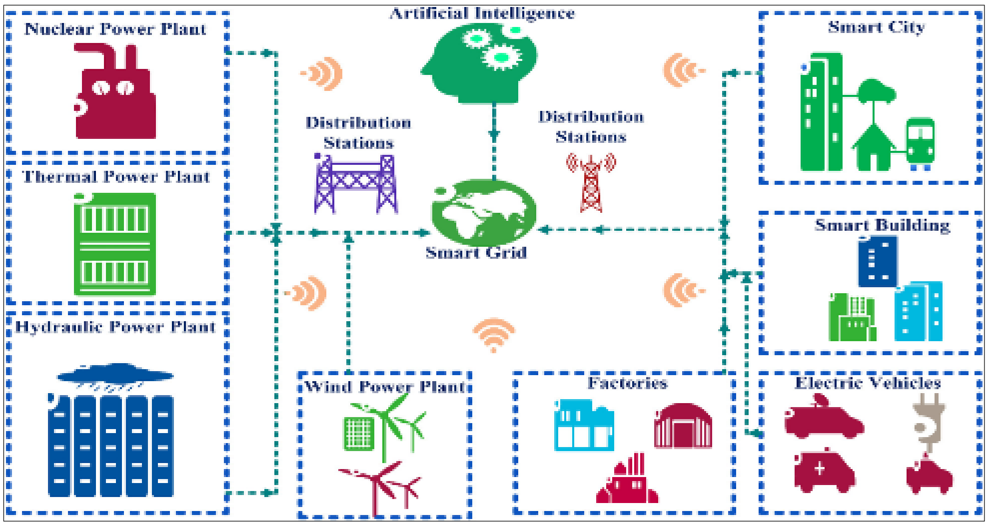

Figure 7 Artificial intelligence incorporation in smart grids

The development of sophisticated analytics techniques and tools to identify [208], predict, and respond to emerging threats in real-time is crucial for proactive security measures.

- *Resilience and recovery*: While smart grids have mechanisms to handle disruptions and failures, there is a need to explore and develop advanced techniques to enhance the resilience and recovery of the grid in the face of cyber-attacks and physical threats [209], [210]. This includes developing strategies for rapid detection, containment, and restoration of services, as well as understanding the cascading effects of attacks on different components of the grid.

- *Secure Integration of Distributed Energy Resources (DERs):* With the increasing integration of DERs, such as solar panels and wind turbines, into the grid, there is a need for research on secure integration mechanisms [211], [212]. This includes secure communication protocols, authentication mechanisms [213], and control strategies to ensure the integrity and stability of the grid while accommodating fluctuating power generation from distributed sources.
- *Privacy-preserving techniques*: As smart grids collect and process large amounts of data, preserving consumer privacy becomes crucial [214]. There is a need to develop privacy-enhancing techniques that allow for data analysis while protecting the privacy of individuals [215]-[218]. This includes techniques such as differential privacy, secure multiparty computation, and privacy-preserving data aggregation.
- *Secure firmware and software updates*: Ensuring the security of firmware and software updates for smart grid devices is critical [219]. Research is needed to develop secure update mechanisms that guarantee the authenticity, integrity, and non-repudiation of updates [220]. This includes exploring techniques such as secure bootstrapping, secure code delivery, and secure over-the-air update protocols.
- *Human factors and usability*: Considering the human factors and usability aspects of smart grid security is important [221]. Research is needed to develop user-friendly interfaces, security education programs, and effective security awareness campaigns to mitigate human error and improve overall security hygiene in the operation and management of smart grid systems [222].
- *Risk assessment and mitigation*: Developing comprehensive risk assessment frameworks specific to smart grid environments is crucial [223]. This involves understanding the unique risks, vulnerabilities [224], and impacts associated with smart grid systems and developing effective risk mitigation strategies. Integration of risk assessment techniques with security operations can enable proactive decision-making and resource allocation.
- *Standardization and interoperability*: The lack of standardized security protocols and frameworks across different smart grid components hinders interoperability and coordination of security measures [225]. Research is needed to develop harmonized security standards and protocols that ensure consistent and effective security implementations across different vendors, devices, and systems in smart grids.
- *Socio-technical considerations*: Smart grid security research should not be limited to technical aspects alone. Consideration of the socio-technical aspects, including policy, legal, regulatory, and ethical dimensions, is vital [226]. Understanding the implications of security measures on privacy, consumer acceptance, and societal impact can help shape effective security policies and regulations.

The effective tackling of these research gaps will contribute to a more robust and resilient smart grid security framework. Collaboration between academia, industry, and government entities is essential to drive research in these areas and develop innovative solutions that enhance the security and reliability of smart grid infrastructures.

1.8. Future research directions

Future research directions in smart grid security will play a crucial role in addressing emerging challenges and ensuring the resilience and integrity of smart grid infrastructures. Some of the potential future research directions in smart grid security are described in Table 4 below.

Table 4 Future research directions in smart grid security

Domain	Discussion
Quantum-safe cryptography	With the advent of quantum computing, future research should focus on developing quantum-safe cryptographic algorithms that can resist attacks from quantum computers [227], [228]. Quantum-resistant encryption and key distribution techniques are essential for ensuring the long-term security of smart grid systems.
Artificial intelligence and machine learning	Exploring the applications of artificial intelligence (AI) and machine learning (ML) techniques [229] in smart grid security is a promising area for future research [230]-[233]. AI/ML algorithms can help detect anomalies [234], identify patterns of cyber-attacks, and enable predictive security analytics. Developing AI-driven security solutions can enhance threat detection capabilities and enable proactive responses to emerging threats.
Privacy-preserving data sharing	Future research should focus on developing advanced privacy-preserving techniques for sharing sensitive data in smart grids [235]-[238]. This includes techniques such as secure multi-party

	computation, federated machine learning [239], and homomorphic encryption to enable secure data analysis and collaboration among multiple entities without compromising privacy.
Blockchain technology	Blockchain technology has the potential to revolutionize smart grid security by providing decentralized and tamper-proof transaction records [240]-[243]. Research can focus on integrating blockchain into smart grids to ensure secure and transparent data exchange [244], establish trust among stakeholders, and enable secure peer-to-peer energy trading.
Threat intelligence and information sharing	Enhancing the capabilities for threat intelligence and information sharing among smart grid stakeholders is important [245]. Future research should focus on developing collaborative frameworks, sharing platforms, and standards to facilitate timely sharing of threat intelligence, best practices, and lessons learned. This will enable a more coordinated and proactive response to emerging threats.
Resilience and cyber-physical security	As smart grids become more interconnected with physical systems, future research should investigate the security challenges arising from cyber-physical systems (CPS) integration [246]. This includes exploring techniques to enhance the resilience of CPS components, such as sensors, actuators, and control systems to cyber-attacks, physical threats, and potential cascading effects.
Human-centric security	Future research should address the human factors and usability aspects of smart grid security [247]. This includes developing user-friendly security interfaces, conducting user studies to understand security behaviors and decision-making, and designing effective security awareness and training programs to mitigate human error and improve overall security hygiene.
Legal and regulatory considerations	Future research should address the legal and regulatory challenges associated with smart grid security. This includes examining the legal frameworks for data protection, privacy, liability, and compliance [248]. Research can contribute to the development of policies and regulations that strike a balance between security requirements, consumer privacy rights, and regulatory compliance.
Testing and evaluation	Developing comprehensive testing and evaluation frameworks specific to smart grid security is vital. Future research should focus on creating realistic testbeds and simulation environments to assess the security and resilience of smart grid systems under various attack scenarios [249]. This will help identify vulnerabilities, evaluate the effectiveness of security solutions, and inform the design of robust security architectures.

By exploring these future research directions, academia, industry, and government entities can drive innovation and develop advanced solutions that address the evolving security challenges in smart grid infrastructures. Collaboration and interdisciplinary approaches will be key to advancing smart grid security research and ensuring the secure and sustainable operation of future energy distribution systems.

2. Conclusion

Smart grid security is a critical aspect that must be addressed to ensure the reliable, resilient, and secure operation of modern energy distribution systems. The complexity and interconnectedness of smart grids, coupled with the evolving threat landscape, present unique challenges that require continuous research, innovation, and collaboration among stakeholders. In this paper, the need for smart grid security has been explored. The challenges associated with smart grid security, including the complexity of the infrastructure, rapid technological advancements, legacy systems, insider threats, and privacy concerns have been explained, highlight the importance of developing robust and comprehensive security measures. It has been noted that threat intelligence, resilience and recovery, privacy-preserving techniques, secure integration of distributed energy resources, and human-centric security provide valuable insights into the areas that require further investigation. By addressing these research gaps, future researches can enhance the security posture of smart grids and stay ahead of emerging threats. There is also need to apply techniques such as artificial intelligence and machine learning, blockchain technology, quantum-safe cryptography, and human-centric security to provide opportunities for developing innovative solutions that can strengthen the security and resilience of smart grid infrastructures. Since smart grid security is an ongoing and dynamic process, as technology evolves, so do the threats and vulnerabilities. As such, a holistic and collaborative approach is essential, involving academia, industry, government entities, and regulatory bodies, to continuously monitor, adapt, and improve smart grid security practices.

Compliance with ethical standards

Acknowledgments

I would like to thank all the people who offered some assistance during the course of developing this paper.

References

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] Zidi S, Mihoub A, Qaisar SM, Krichen M, Al-Haija QA. Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment. Journal of King Saud University-Computer and Information Sciences. 2023 Jan 1;35(1):13-25.

[6] 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.

[7] Ravinder M, Kulkarni V. A Review on Cyber Security and Anomaly Detection Perspectives of Smart Grid. In2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT) 2023 Jan 23 (pp. 692-697). IEEE.

[8] 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.

[9] 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.

[10] Haghshenas SH, Hasnat MA, Naeini M. A temporal graph neural network for cyber attack detection and localization in smart grids. In2023 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT) 2023 Jan 16 (pp. 1-5). IEEE.

[11] 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.

[12] Ghelani D. Cyber Security in Smart Grids, Threats, and Possible Solutions. Authorea Preprints. 2022 Sep 22.

[13] Gunduz MZ, Das R. Cyber-security on smart grid: Threats and potential solutions. Computer networks. 2020 Mar 14;169:107094.

[14] 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.

[15] Vahidi S, Ghafouri M, Au M, Kassouf M, Mohammadi A, Debbabi M. Security of wide-area monitoring, protection, and control (WAMPAC) systems of the smart grid: A survey on challenges and opportunities. IEEE Communications Surveys & Tutorials. 2023 Mar 8.

[16] Nyangaresi VO. Privacy Preserving Three-factor Authentication Protocol for Secure Message Forwarding in Wireless Body Area Networks. Ad Hoc Networks. 2023 Apr 1;142:103117.

[17] Zhao H, Liu G, Sun H, Zhong G, Pang S, Qiao S, Lv Z. An enhanced intrusion detection method for AIM of smart grid. Journal of Ambient Intelligence and Humanized Computing. 2023 Feb 3:1-3.

[18] 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.

[19] Ortega-Fernandez I, Liberati F. A Review of Denial of Service Attack and Mitigation in the Smart Grid Using Reinforcement Learning. Energies. 2023 Jan 5;16(2):635.

[20] 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.

[21] 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 4;13(2):691.

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

[23] Habib AA, Hasan MK, Alkhayyat A, Islam S, Sharma R, Alkwai LM. False data injection attack in smart grid cyber physical system: Issues, challenges, and future direction. Computers and Electrical Engineering. 2023 Apr 1;107:108638.

[24] 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.

[25] Immaniar D, Aryani AA, Ula SZ, Firmansyah MR, Rahman Y. Challenges Smart Grid in Blockchain Applications. Blockchain Frontier Technology. 2023;2(2):1-9.

[26] 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.

[27] 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.

[28] Zhao M, Ding Y, Tang S, Liang H, Wang H. A blockchain-based framework for privacy-preserving and verifiable billing in smart grid. Peer-to-Peer Networking and Applications. 2023 Jan;16(1):142-55.

[29] 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.

[30] Bousbiat H, Bousselidj R, Himeur Y, Amira A, Bensaali F, Fadli F, Mansoor W, Elmenreich W. Crossing Roads of Federated Learning and Smart Grids: Overview, Challenges, and Perspectives. arXiv preprint arXiv:2304.08602. 2023 Apr 17.

[31] 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.

[32] Bandeiras F, Gomes Á, Gomes M, Coelho P. Exploring Energy Trading Markets in Smart Grid and Microgrid Systems and Their Implications for Sustainability in Smart Cities. Energies. 2023 Jan 10;16(2):801.

[33] Berghout T, Benbouzid M, Amirat Y. Towards Resilient and Secure Smart Grids against PMU Adversarial Attacks: A Deep Learning-Based Robust Data Engineering Approach. Electronics. 2023 Jun 6;12(12):2554.

[34] Mashal I, Khashan OA, Hijjawi M, Alshinwan M. The determinants of reliable smart grid from experts' perspective. Energy Informatics. 2023 Dec;6(1):1-23.

[35] Lu Y, Tang X, Liu L, Yu FR, Dustdar S. Speeding at the Edge: An Efficient and Secure Redactable Blockchain for IoT-based Smart Grid Systems. IEEE Internet of Things Journal. 2023 Mar 7.

[36] Al Sibahee MA, Nyangaresi VO, Ma J, Abduljabbar ZA. Stochastic Security Ephemeral Generation Protocol for 5G Enabled Internet of Things. InInternational Conference on Internet of Things as a Service 2021 Dec 13 (pp. 3-18). Cham: Springer International Publishing.

[37] Abdella J, Shuaib K. Peer to peer distributed energy trading in smart grids: A survey. Energies. 2018 Jun 14;11(6):1560.

[38] Dong Z, Luo F, Liang G. Blockchain: a secure, decentralized, trusted cyber infrastructure solution for future energy systems. Journal of Modern Power Systems and Clean Energy. 2018 Sep;6(5):958-67.

[39] Kapse MM, Patel NR, Narayankar SK, Malvekar SA, Liyakat KK. Smart Grid Technology. International Journal of Information Technology & Computer Engineering (IJITC) ISSN: 2455-5290. 2022 Oct 18;2(06):10-7.

[40] 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.

[41] 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.

[42] Laayati O, El Hadraoui H, Guennoui N, Bouzi M, Chebak A. Smart Energy Management System: Design of a Smart Grid Test Bench for Educational Purposes. Energies. 2022 Apr 6;15(7):2702.

[43] Tran QT, Besanger Y, Labonne A. Complementary business models for distribution system operator in a peer-to-peer electricity market. In2021 IEEE International Conference on Environment and Electrical Engineering and 2021 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe) 2021 Sep 7 (pp. 1-6). IEEE.

[44] Martins JF, Pronto AG, Delgado-Gomes V, Sanduleac M. Smart meters and advanced metering infrastructure. InPathways to a smarter power system 2019 Jan 1 (pp. 89-114). Academic Press.

[45] Hansen A, Staggs J, Shenoi S. Security analysis of an advanced metering infrastructure. International Journal of Critical Infrastructure Protection. 2017 Sep 1;18:3-19.

[46] Abduljabbar ZA, Omollo Nyangaresi V, Al Sibahee MA, Ghrabat MJ, Ma J, Qays Abduljaleel I, Aldarwish AJ. Session-Dependent Token-Based Payload Enciphering Scheme for Integrity Enhancements in Wireless Networks. Journal of Sensor and Actuator Networks. 2022 Sep 19;11(3):55.

[47] Hashmi SA, Ali CF, Zafar S. Internet of things and cloud computing-based energy management system for demand side management in smart grid. International Journal of Energy Research. 2021 Jan;45(1):1007-22.

[48] Arraño-Vargas F, Konstantinou G. Modular design and real-time simulators toward power system digital twins implementation. IEEE Transactions on Industrial Informatics. 2022 May 30;19(1):52-61.

[49] Guney MS, Tepe Y. Classification and assessment of energy storage systems. Renewable and Sustainable Energy Reviews. 2017 Aug 1;75:1187-97.

[50] Zhang Z, Ding T, Zhou Q, Sun Y, Qu M, Zeng Z, Ju Y, Li L, Wang K, Chi F. A review of technologies and applications on versatile energy storage systems. Renewable and Sustainable Energy Reviews. 2021 Sep 1;148:111263.

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

[52] Hussain M, Gao Y. A review of demand response in an efficient smart grid environment. The Electricity Journal. 2018 Jun 1;31(5):55-63.

[53] Alfaverh F, Denai M, Sun Y. Demand response strategy based on reinforcement learning and fuzzy reasoning for home energy management. IEEE access. 2020 Feb 17;8:39310-21.

[54] Shreenidhi HS, Ramaiah NS. A two-stage deep convolutional model for demand response energy management system in IoT-enabled smart grid. Sustainable Energy, Grids and Networks. 2022 Jun 1;30:100630.

[55] Kim Y, Hakak S, Ghorbani A. Smart grid security: Attacks and defence techniques. IET Smart Grid. 2023 Apr;6(2):103-23.

[56] Haq EU, Pei C, Zhang R, Jianjun H, Ahmad F. Electricity-theft detection for smart grid security using smart meter data: A deep-CNN based approach. Energy Reports. 2023 Mar 1;9:634-43.

[57] 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.

[58] Jafari M, Kavousi-Fard A, Chen T, Karimi M. A review on digital twin technology in smart grid, transportation system and smart city: Challenges and future. IEEE Access. 2023 Feb 1.

[59] Mirzaee PH, Shojafar M, Cruickshank H, Tafazolli R. Smart grid security and privacy: From conventional to machine learning issues (threats and countermeasures). IEEE access. 2022 May 11;10:52922-54.

[60] Inayat U, Zia MF, Mahmood S, Berghout T, Benbouzid M. Cybersecurity enhancement of smart grid: Attacks, methods, and prospects. Electronics. 2022 Nov 23;11(23):3854.

[61] Reda HT, Anwar A, Mahmood A. Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts. Renewable and Sustainable Energy Reviews. 2022 Jul 1;163:112423.

[62] Abduljabbar, Z. A., Nyangaresi, V. O., Ma, J., Al Sibahee, M. A., Khalefa, M. S., & Honi, D. G. (2022, September). MAC-Based Symmetric Key Protocol for Secure Traffic Forwarding in Drones. In Future Access Enablers for Ubiquitous and Intelligent Infrastructures: 6th EAI International Conference, FABULOUS 2022, Virtual Event, May 4, 2022, Proceedings (pp. 16-36). Cham: Springer International Publishing.

[63] Raja DJ, Sriranjani R, Parvathy A, Hemavathi N. A review on distributed denial of service attack in smart grid. In2022 7th International Conference on Communication and Electronics Systems (ICCES) 2022 Jun 22 (pp. 812-819). IEEE.

[64] Prabhakar P, Arora S, Khosla A, Beniwal RK, Arthur MN, Arias-Gonzáles JL, Areche FO. Cyber Security of Smart Metering Infrastructure Using Median Absolute Deviation Methodology. Security and Communication Networks. 2022 Oct 7;2022.

[65] Mohammed A, George G. Vulnerabilities and strategies of cybersecurity in smart grid-evaluation and review. In2022 3rd International Conference on Smart Grid and Renewable Energy (SGRE) 2022 Mar 20 (pp. 1-6). IEEE.

[66] 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.

[67] Nyangaresi VO, Ogundoyin SO. Certificate based authentication scheme for smart homes. In2021 3rd Global Power, Energy and Communication Conference (GPECOM) 2021 Oct 5 (pp. 202-207). IEEE.

[68] Panda DK, Das S. Smart grid architecture model for control, optimization and data analytics of future power networks with more renewable energy. Journal of Cleaner Production. 2021 Jun 10;301:126877.

[69] Borgaonkar R, Anne Tøndel I, Zenebe Degefa M, Gilje Jaatun M. Improving smart grid security through 5G enabled IoT and edge computing. Concurrency and Computation: Practice and Experience. 2021 Sep 25;33(18):e6466.

[70] Sakhnini J, Karimipour H, Dehghantanha A, Parizi RM, Srivastava G. Security aspects of Internet of Things aided smart grids: A bibliometric survey. Internet of things. 2021 Jun 1;14:100111.

[71] Kawoosa AI, Prashar D. A review of cyber securities in smart grid technology. In2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM) 2021 Jan 19 (pp. 151-156). IEEE.

[72] Nyakomitta PS, Nyangaresi VO, Ogara SO. Efficient authentication algorithm for secure remote access in wireless sensor networks. Journal of Computer Science Research. 2021 Oct 14;3(4):43-50.

[73] Zhang Y, Wang J, Li Z. Uncertainty modeling of distributed energy resources: techniques and challenges. Current Sustainable/Renewable Energy Reports. 2019 Jun 15;6:42-51.

[74] Xu S, Xue Y, Chang L. Review of power system support functions for inverter-based distributed energy resources-standards, control algorithms, and trends. IEEE open journal of Power electronics. 2021 Feb 2;2:88-105.

[75] Twaisan K, Barışçı N. Integrated Distributed Energy Resources (DER) and Microgrids: Modeling and Optimization of DERs. Electronics. 2022 Sep 6;11(18):2816.

[76] Mahmud K, Khan B, Ravishankar J, Ahmadi A, Siano P. An internet of energy framework with distributed energy resources, prosumers and small-scale virtual power plants: An overview. Renewable and Sustainable Energy Reviews. 2020 Jul 1;127:109840.

[77] 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.

[78] de Souza RW, Moreira LR, Rodrigues JJ, Moreira RR, de Albuquerque VH. Deploying wireless sensor networks–based smart grid for smart meters monitoring and control. International Journal of Communication Systems. 2018 Jul 10;31(10):e3557.

[79] Gaggero GB, Marchese M, Moheddine A, Patrone F. A possible smart metering system evolution for rural and remote areas employing unmanned aerial vehicles and internet of things in smart grids. Sensors. 2021 Feb 26;21(5):1627.

[80] Ghosal A, Conti M. Key management systems for smart grid advanced metering infrastructure: A survey. IEEE Communications Surveys & Tutorials. 2019 Mar 28;21(3):2831-48.

[81] Triantafyllou A, Jimenez JA, Torres AD, Lagkas T, Rantos K, Sarigiannidis P. The challenges of privacy and access control as key perspectives for the future electric smart grid. IEEE Open Journal of the Communications Society. 2020 Nov 11;1:1934-60.

[82] 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.

[83] El Mrabet Z, Kaabouch N, El Ghazi H, El Ghazi H. Cyber-security in smart grid: Survey and challenges. Computers & Electrical Engineering. 2018 Apr 1;67:469-82.

[84] Alattab AA, Irshad RR, Yahya AA, Al-Awady AA. Privacy Protected Preservation of Electric Vehicles' Data in Cloud Computing Using Secure Data Access Control. Energies. 2022 Oct 31;15(21):8085.

[85] Haque AB, Bhushan B, Dhiman G. Conceptualizing smart city applications: Requirements, architecture, security issues, and emerging trends. Expert Systems. 2022 Jun;39(5):e12753.

[86] Bera B, Saha S, Das AK, Vasilakos AV. Designing blockchain-based access control protocol in IoT-enabled smart-grid system. IEEE Internet of Things Journal. 2020 Oct 13;8(7):5744-61.

[87] 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.

[88] Wang X, Wang X, Zhang M, Wang S. Detection-based active defense of biased injection attack based on robust adaptive controller. Internet of Things and Cyber-Physical Systems. 2023 Jan 1;3:14-23.

[89] Rouzbahani HM, Karimipour H, Lei L. Multi-layer defense algorithm against deep reinforcement learning-based intruders in smart grids. International Journal of Electrical Power & Energy Systems. 2023 Mar 1;146:108798.

[90] Wang Y, Pal B. Destabilizing attack and robust defense for inverter-based microgrids by adversarial deep reinforcement learning. IEEE Transactions on Smart Grid. 2023 Mar 30.

[91] 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.

[92] Nyangaresi VO, Morsy MA. Towards privacy preservation in internet of drones. In2021 IEEE 6th International Forum on Research and Technology for Society and Industry (RTSI) 2021 Sep 6 (pp. 306-311). IEEE.

[93] Priyadarshini I, Kumar R, Sharma R, Singh PK, Satapathy SC. Identifying cyber insecurities in trustworthy space and energy sector for smart grids. Computers & Electrical Engineering. 2021 Jul 1;93:107204.

[94] 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.

[95] Win LL, Tonyalı S. Security and privacy challenges, solutions, and open issues in smart metering: A review. In2021 6th International Conference on Computer Science and Engineering (UBMK) 2021 Sep 15 (pp. 800-805). IEEE.

[96] Marksteiner S, Vallant H, Nahrgang K. Cyber security requirements engineering for low-voltage distribution smart grid architectures using threat modeling. Journal of Information Security and Applications. 2019 Dec 1;49:102389.

[97] Mohammad Z, Nyangaresi V, Abusukhon A. On the Security of the Standardized MQV Protocol and Its Based Evolution Protocols. In2021 International Conference on Information Technology (ICIT) 2021 Jul 14 (pp. 320-325). IEEE.

[98] 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.

[99] Khan R, McLaughlin K, Laverty D, Sezer S. STRIDE-based threat modeling for cyber-physical systems. In2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe) 2017 Sep 26 (pp. 1-6). IEEE.

[100] Akkad A, Wills G, Rezazadeh A. An information security model for an IoT-enabled Smart Grid in the Saudi energy sector. Computers and Electrical Engineering. 2023 Jan 1;105:108491.

[101] Das D, Banerjee S, Chatterjee P, Ghosh U, Biswas U, Mansoor W. Security, trust, and privacy management framework in cyber-physical systems using blockchain. In2023 IEEE 20th Consumer Communications & Networking Conference (CCNC) 2023 Jan 8 (pp. 1-6). IEEE.

[102] Nyangaresi VO, Petrovic N. Efficient PUF based authentication protocol for internet of drones. In2021 International Telecommunications Conference (ITC-Egypt) 2021 Jul 13 (pp. 1-4). IEEE.

[103] Kure HI, Islam S. Assets focus risk management framework for critical infrastructure cybersecurity risk management. IET Cyber-Physical Systems: Theory & Applications. 2019 Dec;4(4):332-40.

[104] Riggs H, Tufail S, Parvez I, Tariq M, Khan MA, Amir A, Vuda KV, Sarwat AI. Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. Sensors. 2023 Apr 17;23(8):4060.

[105] Upadhyay D, Sampalli S. SCADA (Supervisory Control and Data Acquisition) systems: Vulnerability assessment and security recommendations. Computers & Security. 2020 Feb 1;89:101666.

[106] Martín-Liras L, Prada MA, Fuertes JJ, Morán A, Alonso S, Domínguez M. Comparative analysis of the security of configuration protocols for industrial control devices. International Journal of Critical Infrastructure Protection. 2017 Dec 1;19:4-15.

[107] 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.

[108] Sun CC, Hahn A, Liu CC. Cyber security of a power grid: State-of-the-art. International Journal of Electrical Power & Energy Systems. 2018 Jul 1;99:45-56.

[109] Konstantinou C, Maniatakos M. Hardware-layer intelligence collection for smart grid embedded systems. Journal of Hardware and Systems Security. 2019 Jun 15;3:132-46.

[110] Rahimpour H, Tusek J, Abuadbba A, Seneviratne A, Phung T, Musleh A, Liu B. Cybersecurity Challenges of Power Transformers. arXiv preprint arXiv:2302.13161. 2023 Feb 25.

[111] Liu C, Alrowaili Y, Saxena N, Konstantinou C. Cyber risks to critical smart grid assets of industrial control systems. Energies. 2021 Sep 3;14(17):5501.

[112] Zografopoulos I, Ospina J, Liu X, Konstantinou C. Cyber-physical energy systems security: Threat modeling, risk assessment, resources, metrics, and case studies. IEEE Access. 2021 Feb 10;9:29775-818.

[113] 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.

[114] Anand P, Singh Y, Selwal A, Singh PK, Felseghi RA, Raboaca MS. Iovt: Internet of vulnerable things? threat architecture, attack surfaces, and vulnerabilities in internet of things and its applications towards smart grids. Energies. 2020 Sep 15;13(18):4813.

[115] Lombardi F, Aniello L, De Angelis S, Margheri A, Sassone V. A blockchain-based infrastructure for reliable and cost-effective IoT-aided smart grids.

[116] Gope P, Sikdar B. A Reconfigurable and Secure Firmware Updating Framework for Advanced Metering Infrastructure. In2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm) 2022 Oct 25 (pp. 453-459). IEEE.

[117] Bindra A. Securing the power grid: Protecting smart grids and connected power systems from cyberattacks. IEEE Power Electronics Magazine. 2017 Sep 8;4(3):20-7.

[118] Al Sibahee MA, Abdulsada AI, Abduljabbar ZA, Ma J, Nyangaresi VO, Umran SM. Lightweight, Secure, Similar-Document Retrieval over Encrypted Data. Applied Sciences. 2021 Dec 17;11(24):12040.

[119] Diahovchenko I, Kolcun M, Čonka Z, Savkiv V, Mykhailyshyn R. Progress and challenges in smart grids: Distributed generation, smart metering, energy storage and smart loads. Iranian Journal of Science and Technology, Transactions of Electrical Engineering. 2020 Dec;44:1319-33.

[120] Zografopoulos I, Konstantinou C, Hatziargyriou ND. Distributed energy resources cybersecurity outlook: Vulnerabilities, attacks, impacts, and mitigations. arXiv preprint arXiv:2205.11171. 2022 May 23.

[121] 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.

[122] Chen Q, Zhou M, Cai Z, Su S. Compliance Checking Based Detection of Insider Threat in Industrial Control System of Power Utilities. In2022 7th Asia Conference on Power and Electrical Engineering (ACPEE) 2022 Apr 15 (pp. 1142-1147). IEEE.

[123] Nyangaresi VO. A Formally Verified Authentication Scheme for mmWave Heterogeneous Networks. Inthe 6th International Conference on Combinatorics, Cryptography, Computer Science and Computation (605-612) 2021.

[124] Li B, Lu R, Xiao G, Bao H, Ghorbani AA. Towards insider threats detection in smart grid communication systems. IET Communications. 2019 Jul;13(12):1728-36.

[125] Makrakis GM, Kolias C, Kambourakis G, Rieger C, Benjamin J. Industrial and critical infrastructure security: Technical analysis of real-life security incidents. Ieee Access. 2021 Dec 6;9:165295-325.

[126] Rao VV, Marshal R, Gobinath K. The IoT Supply Chain Attack Trends-Vulnerabilities and Preventive Measures. In2021 4th International Conference on Security and Privacy (ISEA-ISAP) 2021 Oct 27 (pp. 1-4). IEEE.

[127] Tufail S, Parvez I, Batool S, Sarwat A. A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid. Energies. 2021 Sep 17;14(18):5894.

[128] 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.

[129] Presekal A, Ştefanov A, Rajkumar VS, Palensky P. Attack graph model for cyber-physical power systems using hybrid deep learning. IEEE Transactions on Smart Grid. 2023 Jan 16.

[130] Khan FB, Asad A, Durad H, Mohsin SM, Kazmi SN. Dragonfly Cyber Threats: A Case Study of Malware Attacks Targeting Power Grids. Journal of Computing & Biomedical Informatics. 2023 Mar 29;4(02):172-85.

[131] Sridhar B, Nivas BS, Raji K, Nandhini S. Survey on Wireless Sensor Network Attack Detection using Machine Learning Approach. In2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) 2023 May 17 (pp. 1347-1351). IEEE.

[132] Kumar R, Kela R, Singh S, Trujillo-Rasua R. APT attacks on industrial control systems: A tale of three incidents. International Journal of Critical Infrastructure Protection. 2022 Jul 1;37:100521.

[133] Nyangaresi VO. Terminal independent security token derivation scheme for ultra-dense IoT networks. Array. 2022 Sep 1;15:100210.

[134] Srivastava G, Parizi RM, Dehghantanha A. The future of blockchain technology in healthcare internet of things security. Blockchain cybersecurity, trust and privacy. 2020:161-84.

[135] Erdődi L, Kaliyar P, Houmb SH, Akbarzadeh A, Waltoft-Olsen AJ. Attacking power grid substations: an experiment demonstrating how to attack the SCADA protocol IEC 60870-5-104. InProceedings of the 17th International Conference on Availability, Reliability and Security 2022 Aug 23 (pp. 1-10).

[136] Di Pinto A, Dragoni Y, Carcano A. TRITON: The first ICS cyber attack on safety instrument systems. Proc. Black Hat USA. 2018 Aug;2018:1-26.

[137] Mekdad Y, Bernieri G, Conti M, Fergougui AE. A threat model method for ICS malware: the TRISIS case. InProceedings of the 18th ACM International Conference on Computing Frontiers 2021 May 11 (pp. 221-228).

[138] Mutlaq KA, Nyangaresi VO, Omar MA, Abduljabbar ZA. Symmetric Key Based Scheme for Verification Token Generation in Internet of Things Communication Environment. InEAI International Conference on Applied Cryptography in Computer and Communications 2022 May 14 (pp. 46-64). Cham: Springer Nature Switzerland.

[139] Mazhar T, Irfan HM, Haq I, Ullah I, Ashraf M, Shloul TA, Ghadi YY, Imran, Elkamchouchi DH. Analysis of Challenges and Solutions of IoT in Smart Grids Using AI and Machine Learning Techniques: A Review. Electronics. 2023 Jan 3;12(1):242.

[140] Tanveer M, Alasmary H. LACP-SG: Lightweight Authentication Protocol for Smart Grids. Sensors. 2023 Feb 19;23(4):2309.

[141] Alsuwian T, Shahid Butt A, Amin AA. Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review. Sustainability. 2022 Oct 31;14(21):14226.

[142] Agnew D, Aljohani N, Mathieu R, Boamah S, Nagaraj K, McNair J, Bretas A. Implementation aspects of smart grids cyber-security cross-layered framework for critical infrastructure operation. Applied Sciences. 2022 Jul 7;12(14):6868.

[143] Nyangaresi VO. A formally validated authentication algorithm for secure message forwarding in smart home networks. SN Computer Science. 2022 Jul 9;3(5):364.

[144] Fan X, Gong G. Security challenges in smart-grid metering and control systems. Technology Innovation Management Review. 2013;3(7).

[145] Islam SN, Baig Z, Zeadally S. Physical layer security for the smart grid: Vulnerabilities, threats, and countermeasures. IEEE Transactions on Industrial Informatics. 2019 Jul 26;15(12):6522-30.

[146] Namane S, Ben Dhaou I. Blockchain-based access control techniques for iot applications. Electronics. 2022 Jul 16;11(14):2225.

[147] Fragkos G, Johnson J, Tsiropoulou EE. Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach. IEEE Transactions on Human-Machine Systems. 2022 Apr 22;52(4):761-73.

[148] Nyakomitta SP, Omollo V. Biometric-Based Authentication Model for E-Card Payment Technology. IOSR Journal of Computer Engineering (IOSRJCE). 2014;16(5):137-44.

[149] Zhu L, Li M, Zhang Z, Du X, Guizani M. Big data mining of users' energy consumption patterns in the wireless smart grid. IEEE Wireless Communications. 2018 Feb 28;25(1):84-9.

[150] Tajammul M, Shaw RN, Ghosh A, Parveen R. Error Detection Algorithm for Cloud Outsourced Big Data. Advances in Applications of Data-Driven Computing. 2021:105-16.

[151] Banerjee M, Lee J, Choo KK. A blockchain future for internet of things security: a position paper. Digital Communications and Networks. 2018 Aug 1;4(3):149-60.

[152] Patel A, Alhussian H, Pedersen JM, Bounabat B, Júnior JC, Katsikas S. A nifty collaborative intrusion detection and prevention architecture for smart grid ecosystems. Computers & Security. 2017 Jan 1;64:92-109.

[153] Nyangaresi VO. Hardware assisted protocol for attacks prevention in ad hoc networks. InEmerging Technologies in Computing: 4th EAI/IAER International Conference, iCETiC 2021, Virtual Event, August 18–19, 2021, Proceedings 4 2021 (pp. 3-20). Springer International Publishing.

[154] Hittini H, Abdrabou A, Zhang L. FDIPP: false data injection prevention protocol for smart Grid distribution systems. Sensors. 2020 Jan 26;20(3):679.

[155] Khudhur DD, Croock MS. Developed security and privacy algorithms for cyber physical system. International Journal of Electrical and Computer Engineering. 2021 Dec 1;11(6):5379.

[156] Ramyasri G, Murthy GR, Itapu S, Krishna SM. Data transmission using secure hybrid techniques for smart energy metering devices. e-Prime-Advances in Electrical Engineering, Electronics and Energy. 2023 Jun 1;4:100134.

[157] Bhardwaj S, Harit S, Shilpa, Anand D. Message queuing telemetry transport-secure connection: a power-efficient secure communication. International Journal of Sensor Networks. 2023;42(1):29-40.

[158] Abood EW, Hussien ZA, Kawi HA, Abduljabbar ZA, Nyangaresi VO, Ma J, Al Sibahee MA, Kalafy A, Ahmad S. Provably secure and efficient audio compression based on compressive sensing. International Journal of Electrical & Computer Engineering (2088-8708). 2023 Feb 1;13(1).

[159] Alladi T, Chamola V, Sikdar B, Choo KK. Consumer IoT: Security vulnerability case studies and solutions. IEEE Consumer Electronics Magazine. 2020 Feb 3;9(2):17-25.

[160] Yaacoub JP, Salman O, Noura HN, Kaaniche N, Chehab A, Malli M. Cyber-physical systems security: Limitations, issues and future trends. Microprocessors and microsystems. 2020 Sep 1;77:103201.

[161] Pour MM, Anzalchi A, Sarwat A. A review on cyber security issues and mitigation methods in smart grid systems. SoutheastCon 2017. 2017 Mar 30:1-4.

[162] Lamba A. Protecting 'cybersecurity & resiliency'of nation's critical infrastructure–energy, oil & gas. International Journal of Current Research. 2018;10:76865-76.

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

[164] Martins RD, Knob LA, da Silva EG, Wickboldt JA, Schaeffer-Filho A, Granville LZ. Specialized CSIRT for incident response management in smart grids. Journal of Network and Systems Management. 2019 Jan 15;27:269-85.

[165] Langås M, Løfqvist S, Katt B, Haugan T, Jaatun MG. With a Little Help from Your Friends: Collaboration with Vendors During Smart Grid Incident Response Exercises. InEuropean Interdisciplinary Cybersecurity Conference 2021 Nov 10 (pp. 46-53).

[166] Atif Y, Ding J, Lindström B, Jeusfeld M, Andler SF, Yuning J, Brax C, Gustavsson PM. Cyber-threat intelligence architecture for smart-grid critical infrastructures protection. InThe International Conference on Critical Information Infrastructures Security, CRITIS 2017, Lucca, Italy, October 8-13, 2017 2017.

[167] Chowdhury N, Gkioulos V. Cyber security training for critical infrastructure protection: A literature review. Computer Science Review. 2021 May 1;40:100361.

[168] 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).

[169] IqtiyaniIlham N, Hasanuzzaman M, Hosenuzzaman M. European smart grid prospects, policies, and challenges. Renewable and Sustainable Energy Reviews. 2017 Jan 1;67:776-90.

[170] Brass I, Sowell JH. Adaptive governance for the Internet of Things: Coping with emerging security risks. Regulation & Governance. 2021 Oct;15(4):1092-110.

[171] Chatfield AT, Reddick CG. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in US federal government. Government Information Quarterly. 2019 Apr 1;36(2):346-57.

[172] Minoli D, Sohraby K, Occhiogrosso B. IoT considerations, requirements, and architectures for smart buildings—Energy optimization and next-generation building management systems. IEEE Internet of Things Journal. 2017 Jan 4;4(1):269-83.

[173] Nyangaresi VO. Lightweight key agreement and authentication protocol for smart homes. In2021 IEEE AFRICON 2021 Sep 13 (pp. 1-6). IEEE.

[174] Butt OM, Zulqarnain M, Butt TM. Recent advancement in smart grid technology: Future prospects in the electrical power network. Ain Shams Engineering Journal. 2021 Mar 1;12(1):687-95.

[175] Ma Z. Business ecosystem modeling-the hybrid of system modeling and ecological modeling: an application of the smart grid. Energy Informatics. 2019 Nov 21;2(1):35.

[176] Iganibo I, Albanese M, Mosko M, Bier E, Brito AE. An attack volume metric. Security and Privacy. 2023:e298.

[177] Braun T, Fung BC, Iqbal F, Shah B. Security and privacy challenges in smart cities. Sustainable cities and society. 2018 May 1;39:499-507.

[178] Omollo VN, Musyoki S. Blue bugging Java Enabled Phones via Bluetooth Protocol Stack Flaws. International Journal of Computer and Communication System Engineering. 2015 Jun 9, 2 (4):608-613.

[179] Derbyshire R, Green B, Prince D, Mauthe A, Hutchison D. An analysis of cyber security attack taxonomies. In2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2018 Apr 23 (pp. 153-161). IEEE.

[180] Chen S, Wen H, Wu J, Lei W, Hou W, Liu W, Xu A, Jiang Y. Internet of things based smart grids supported by intelligent edge computing. IEEE access. 2019 Jun 3;7:74089-102.

[181] Gill SS, Tuli S, Xu M, Singh I, Singh KV, Lindsay D, Tuli S, Smirnova D, Singh M, Jain U, Pervaiz H. Transformative effects of IoT, Blockchain and Artificial Intelligence on cloud computing: Evolution, vision, trends and open challenges. Internet of Things. 2019 Dec 1;8:100118.

[182] Esenogho E, Djouani K, Kurien AM. Integrating artificial intelligence Internet of Things and 5G for next-generation smartgrid: A survey of trends challenges and prospect. IEEE Access. 2022 Jan 6;10:4794-831.

[183] 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.

[184] Kuzlu M, Pipattanasompom M, Rahman S. A comprehensive review of smart grid related standards and protocols. In2017 5th International Istanbul Smart Grid and Cities Congress and Fair (ICSG) 2017 Apr 19 (pp. 12-16). IEEE.

[185] Bagherzadeh L, Shahinzadeh H, Shayeghi H, Dejamkhooy A, Bayindir R, Iranpour M. Integration of cloud computing and IoT (CloudIoT) in smart grids: Benefits, challenges, and solutions. In2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE) 2020 Jul 29 (pp. 1-8). IEEE.

[186] Faheem M, Shah SB, Butt RA, Raza B, Anwar M, Ashraf MW, Ngadi MA, Gungor VC. Smart grid communication and information technologies in the perspective of Industry 4.0: Opportunities and challenges. Computer Science Review. 2018 Nov 1;30:1-30.

[187] Bhattarai BP, Paudyal S, Luo Y, Mohanpurkar M, Cheung K, Tonkoski R, Hovsapian R, Myers KS, Zhang R, Zhao P, Manic M. Big data analytics in smart grids: state-of-the-art, challenges, opportunities, and future directions. IET Smart Grid. 2019 Jun;2(2):141-54.

[188] 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.

[189] Alcaraz C, Rubio JE, Lopez J. Blockchain-assisted access for federated smart grid domains: Coupling and features. Journal of Parallel and Distributed Computing. 2020 Oct 1;144:124-35.

[190] Tyagi AK, Aswathy SU, Aghila G, Sreenath N. AARIN: affordable, accurate, reliable and innovative mechanism to protect a medical cyber-physical system using blockchain technology. International Journal of Intelligent Networks. 2021 Jan 1;2:175-83.

[191] Ardagna CA, Bellandi V, Damiani E, Bezzi M, Hebert C. Big Data Analytics-as-a-Service: Bridging the gap between security experts and data scientists. Computers & Electrical Engineering. 2021 Jul 1;93:107215.

[192] Al Sadawi A, Hassan MS, Ndiaye M. A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. IEEE Access. 2021 Apr 2;9:54478-97.

[193] 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.

[194] 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.

[195] Maraj A, Rogova E, Jakupi G. Testing of network security systems through DoS, SQL injection, reverse TCP and social engineering attacks. International Journal of Grid and Utility Computing. 2020;11(1):115-33.

[196] Xiangyu L, Qiuyang L, Chandel S. Social engineering and insider threats. In2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 2017 Oct 12 (pp. 25-34). IEEE.

[197] Soykan EU, Bagriyanik M, Soykan G. Disrupting the power grid via EV charging: The impact of the SMS Phishing attacks. Sustainable Energy, Grids and Networks. 2021 Jun 1;26:100477.

[198] 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.

[199] Krause T, Ernst R, Klaer B, Hacker I, Henze M. Cybersecurity in power grids: Challenges and opportunities. Sensors. 2021 Sep 16;21(18):6225.

[200] Sullivan JE, Kamensky D. How cyber-attacks in Ukraine show the vulnerability of the US power grid. The Electricity Journal. 2017 Apr 1;30(3):30-5.

[201] Reagin MJ, Gentry MV. Enterprise cybersecurity: Building a successful defense program. Frontiers of health services management. 2018 Oct 1;35(1):13-22.

[202] Telo J. Smart City Security Threats and Countermeasures in the Context of Emerging Technologies. International Journal of Intelligent Automation and Computing. 2023 Feb 27;6(1):31-45.

[203] 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.

[204] Mughal AA. Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges. Applied Research in Artificial Intelligence and Cloud Computing. 2019 Jan 12;2(1):1-31.

[205] Sen Ö, van der Velde D, Wehrmeister KA, Hacker I, Henze M, Andres M. On using contextual correlation to detect multi-stage cyber attacks in smart grids. Sustainable Energy, Grids and Networks. 2022 Dec 1;32:100821.

[206] Zheng T, Liu M, Puthal D, Yi P, Wu Y, He X. Smart Grid: Cyber Attacks, Critical Defense Approaches, and Digital Twin. arXiv preprint arXiv:2205.11783. 2022 May 24.

[207] Kotsias J, Ahmad A, Scheepers R. Adopting and integrating cyber-threat intelligence in a commercial organisation. European Journal of Information Systems. 2023 Jan 2;32(1):35-51.

[208] 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.

[209] Wang Q, Zhang G, Wen F. A survey on policies, modelling and security of cyber-physical systems in smart grids. Energy Conversion and Economics. 2021 Dec;2(4):197-211.

[210] Das L, Munikoti S, Natarajan B, Srinivasan B. Measuring smart grid resilience: Methods, challenges and opportunities. Renewable and Sustainable Energy Reviews. 2020 Sep 1;130:109918.

[211] Daramola AS, Ahmadi SE, Marzband M, Ikpehai A. A cost-effective and ecological stochastic optimization for integration of distributed energy resources in energy networks considering vehicle-to-grid and combined heat and power technologies. journal of energy storage. 2023 Jan 1;57:106203.

[212] Moafi M, Ardeshiri RR, Mudiyanselage MW, Marzband M, Abusorrah A, Rawa M, Guerrero JM. Optimal coalition formation and maximum profit allocation for distributed energy resources in smart grids based on cooperative game theory. International Journal of Electrical Power & Energy Systems. 2023 Jan 1;144:108492.

[213] Nyangaresi VO, Abduljabbar ZA, Al Sibahee MA, Ibrahim A, Yahya AN, Abduljaleel IQ, Abood EW. Optimized Hysteresis Region Authenticated Handover for 5G HetNets. InArtificial Intelligence and Sustainable Computing: Proceedings of ICSISCET 2021 2022 Nov 16 (pp. 91-111). Singapore: Springer Nature Singapore.

[214] Şimşek MU, Yıldırım Okay F, Mert D, Özdemir S. TPS3: A privacy preserving data collection protocol for smart grids. Information Security Journal: A Global Perspective. 2018 Mar 4;27(2):102-18.

[215] Tran HY, Hu J, Yin X, Pota HR. An Efficient Privacy-enhancing Cross-silo Federated Learning and Applications for False Data Injection Attack Detection in Smart Grids. IEEE Transactions on Information Forensics and Security. 2023 Apr 17.

[216] Lin C, He D, Zhang H, Shao L, Huang X. Privacy-enhancing decentralized anonymous credential in smart grids. Computer Standards & Interfaces. 2021 Apr 1;75:103505.

[217] Knirsch F. Privacy enhancing technologies in the smart grid user domain. it-Information Technology. 2017 Feb 20;59(1):13-22.

[218] 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.

[219] Chan J, Ip R, Cheng KW, Chan KS. Advanced metering infrastructure deployment and challenges. In2019 IEEE PES GTD Grand International Conference and Exposition Asia (GTD Asia) 2019 Mar 19 (pp. 435-439). IEEE.

[220] Mtetwa NS, Tarwireyi P, Abu-Mahfouz AM, Adigun MO. Secure firmware updates in the internet of things: A survey. In2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC) 2019 Nov 21 (pp. 1-7). IEEE.

[221] Naqvi B, Clarke N, Porras J. Incorporating the human facet of security in developing systems and services. Information & Computer Security. 2021 May 10;29(1):49-72.

[222] Sarker A, Shen H, Rahman M, Chowdhury M, Dey K, Li F, Wang Y, Narman HS. A review of sensing and communication, human factors, and controller aspects for information-aware connected and automated vehicles. IEEE transactions on intelligent transportation systems. 2019 Mar 15;21(1):7-29.

[223] Lamba V, Šimková N, Rossi B. Recommendations for smart grid security risk management. Cyber-Physical Systems. 2019 Apr 3;5(2):92-118.

[224] Nyangaresi VO. Provably secure protocol for 5G HetNets. In2021 IEEE International Conference on Microwaves, Antennas, Communications and Electronic Systems (COMCAS) 2021 Nov 1 (pp. 17-22). IEEE.

[225] Rivas AE, Abrao T. Faults in smart grid systems: Monitoring, detection and classification. Electric Power Systems Research. 2020 Dec 1;189:106602.

[226] Gumz J, Fettermann DC. Better deployments come with acceptance: an investigation of factors driving consumers' acceptance of smart meters. Current Sustainable/Renewable Energy Reports. 2023 Feb 18:1-3.

[227] Xu G, Mao J, Sakk E, Wang SP. An Overview of Quantum-Safe Approaches: Quantum Key Distribution and Post-Quantum Cryptography. In2023 57th Annual Conference on Information Sciences and Systems (CISS) 2023 Mar 22 (pp. 1-6). IEEE.

[228] Wang J, Liu L, Lyu S, Wang Z, Zheng M, Lin F, Chen Z, Yin L, Wu X, Ling C. Quantum-safe cryptography: crossroads of coding theory and cryptography. Science China Information Sciences. 2022 Jan;65(1):111301.

[229] 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.

[230] Hossain E, Khan I, Un-Noor F, Sikander SS, Sunny MS. Application of big data and machine learning in smart grid, and associated security concerns: A review. Ieee Access. 2019 Jan 24;7:13960-88.

[231] Diaba SY, Elmusrati M. Proposed algorithm for smart grid DDoS detection based on deep learning. Neural Networks. 2023 Feb 1;159:175-84.

[232] Ravinder M, Kulkarni V. Intrusion detection in smart meters data using machine learning algorithms: A research report. Frontiers in Energy Research. 2023 Feb 16;11:1147431.

[233] Kandasamy M, Anto S, Baranitharan K, Rastogi R, Satwik G, Sampathkumar A. Smart Grid Security Based on Blockchain with Industrial Fault Detection Using Wireless Sensor Network and Deep Learning Techniques. Journal of Sensors. 2023 May 9;2023.

[234] Nyangaresi VO, El-Omari NK, Nyakina JN. Efficient Feature Selection and ML Algorithm for Accurate Diagnostics. Journal of Computer Science Research. 2022 Jan 25;4(1):10-9.

[235] 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.

[236] 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.

[237] Albaseer A, Abdallah M. Privacy-Preserving Honeypot-Based detector in smart grid networks: A new design for Quality-Assurance and fair incentives federated learning framework. In2023 IEEE 20th Consumer Communications & Networking Conference (CCNC) 2023 Jan 8 (pp. 722-727). IEEE.

[238] Wang H, Gong Y, Ding Y, Tang S, Wang Y. Privacy-preserving data aggregation with dynamic billing in fog-based smart grid. Applied Sciences. 2023 Jan 5;13(2):748.

[239] Ghrabat MJ, Hussien ZA, Khalefa MS, Abduljabba ZA, Nyangaresi VO, Al Sibahee MA, Abood EW. Fully automated model on breast cancer classification using deep learning classifiers. Indonesian Journal of Electrical Engineering and Computer Science. 2022 Oct;28(1):183-91.

[240] Kulkarni V, Kulkarni K. A blockchain-based smart grid model for rural electrification in India. In2020 8th International conference on smart grid (icSmartGrid) 2020 Jun 17 (pp. 133-139). IEEE.

[241] Mika B, Goudz A. Blockchain-technology in the energy industry: Blockchain as a driver of the energy revolution? With focus on the situation in Germany. Energy Systems. 2021 May;12:285-355.

[242] Kim SK, Huh JH. A study on the improvement of smart grid security performance and blockchain smart grid perspective. Energies. 2018 Jul 30;11(8):1973.

[243] Liu C, Zhang X, Chai KK, Loo J, Chen Y. A survey on blockchain-enabled smart grids: Advances, applications and challenges. IET Smart Cities. 2021 Jun;3(2):56-78.

[244] 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.

[245] Marín-López A, Chica-Manjarrez S, Arroyo D, Almenares-Mendoza F, Díaz-Sánchez D. Security information sharing in smart grids: Persisting security audits to the blockchain. Electronics. 2020 Nov 6;9(11):1865.

[246] Alguliyev R, Imamverdiyev Y, Sukhostat L. Cyber-physical systems and their security issues. Computers in Industry. 2018 Sep 1;100:212-23.

[247] Cobilean V, Mavikumbure HS, McBride BJ, Vaagensmith B, Singh VK, Li R, Rieger C, Manic M. A Review of Visualization Methods for Cyber-Physical Security: Smart Grid Case Study. IEEE Access. 2023 Jun 14.

[248] Giannopoulou A. Data protection compliance challenges for self-sovereign identity. InInternational Congress on Blockchain and Applications 2020 Jun 17 (pp. 91-100). Cham: Springer International Publishing.

[249] De Souza E, Ardakanian O, Nikolaidis I. A co-simulation platform for evaluating cyber security and control applications in the smart grid. InICC 2020-2020 IEEE International Conference on Communications (ICC) 2020 Jun 7 (pp. 1-7). IEEE.