Energy Reports 12 (2024) 2914–2932

Contents lists available at ScienceDirect

Energy Reports

journal homepage: www.elsevier.com/locate/egyr

Research paper

Cyber-physical attack and the future energy systems: A review

Sayawu Yakubu Diaba [a,*], Miadrezah Shafie-khah [b], Mohammed Elmusrati [a]

[a] Department of Computer Science Engineering, School of Technology and Innovations, University of Vaasa, Vaasa 65200, Finland
[b] Department of Electrical Engineering, School of Technology and Innovations, University of Vaasa, Vaasa 65200, Finland

ARTICLE INFO

Keywords:
Cyber-physical systems
Cyber security
Energy storage
Future energy systems
Smart grids
Renewable energy sources

ABSTRACT

As the world increasingly relies on interconnected energy systems, the threat of cyber-physical attacks on these vital infrastructures has escalated, posing significant challenges to the security and reliability of future energy systems. We meticulously examine the potential threats and vulnerabilities associated with smart grids, including the integration of renewable energy sources and energy storage technologies. The potential impacts of cyber-physical attacks on various components of energy systems, such as power plants, transmission and distribution networks, and energy storage facilities are analyzed. The review extends to an assessment of current cybersecurity measures, such as intrusion detection systems, encryption, and access controls, evaluating their effectiveness in safeguarding against these emerging threats. We delve into the challenges and opportunities in the development of advanced cybersecurity strategies aimed at countering the evolving nature of threats to smart grids. The potential benefits and advancements that smart grids offer for the energy sector's future are explored. This includes the enhancement of grid security, and synergy with cutting-edge technologies such as the Internet of Things, virtual reality, virtual power plants, nano-grids, and wireless power transmission. These developments not only present opportunities for innovation but also necessitate a proactive and sophisticated approach to cybersecurity.

1. Introduction

A smart grid is a new energy generation, transmission, distribution, and consumption paradigm (Aurangzeb et al., 2024). They aim to supply sustainable, economical, and secure electric energy while guaranteeing its use is cost-effective and environmentally sustainable (Hassan et al., 2023). This is accomplished by intelligently integrating all stakeholders in the energy supply chain's behavior and actions. The continuous integration and collaboration of cyber systems' information sensing, processing, intelligence, and control with energy network infrastructure as physical systems has exposed the system to multiple security vulnerabilities (Suleiman et al., 2015; Mrabet et al., 2018). Elsewhere, customers can communicate with the grid, integrating it more deeply into their daily life. With the smart grid, users will have access to new technology that has facilitated ease of life; as a result, consumers will probably start to see some big benefits from the smart grid. For instance, customers may use a remote interface on their mobile devices to turn on their air conditioners, pool pumps, and other appliances. Customers will be able to use technology to reduce their energy expenses, but more crucially, they will be able to access their home energy network remotely (Park et al., 2014; Kappagantu and Daniel, 2018; Paul et al., 2014).

The utility will also experience lower costs if the full potential of the smart grid is utilized. It will enable utility companies to adopt renewable energy, transition away from nonrenewable energy production, and save money simultaneously. The difficulty in getting to this position is directly related to the initial investments needed to develop smart grid technology and the security issues that would arise with its adoption (Malik and Bouzguenda, 2013; Giordano and Fulli, 2012).

The smart electricity market has evolved significantly from its early days of smart meters and AMI to the current landscape of AI (SaberiKamarposhti et al., 2024; Sankarananth et al., 2023), blockchain (Hanggoro et al., 2024; Sadeghi et al., 2024; Mohamed et al., 2024; Syamala et al., 2024), and decentralized energy systems (Guo et al., 2022). This evolution is driven by the need for greater efficiency, reliability, sustainability, and consumer empowerment in the face of growing energy demand and climate change challenges. The future holds even more promise as technology continues to advance and regulatory frameworks adapt to support innovation and resilience in the electricity market.

Cyber-physical systems (CPS) interact with computers,

* Corresponding author.
E-mail address: sdiaba@uwasa.fi (S.Y. Diaba).

https://doi.org/10.1016/j.egyr.2024.08.060
Received 28 November 2023; Received in revised form 31 July 2024; Accepted 21 August 2024
Available online 6 September 2024

Nomenclatures

ANN	Artificial Neural Networks
AC	Alternating Current
AMI	Advanced Metering Infrastructure
CAES	Compressed Air Energy Storage
CPS	Cyber-Physical Systems
CPS-IP	CPS Interconnection Protocol
DG	Distribution Generation
DA	Distribution Automation
DR	Demand Response
DER	Distribution Energy Resources
EV	Electric Vehicle
HAN	Home Area Network
HEM	Home Energy Management
IT	Information Technology
IoT	Internet of Things
IP	Internet Protocol
IDPS	Intrusion Detection and Prevention Systems
MFA	Multi Factor Authentication
OT	Operation Technology
PLC	Programmable Logic Control
PMU	Phasor Measurement Unit
RF	Radio Frequency
RES	Renewable Energy Sources
RTU	Remote Telemetry Unit
SSL	Secure Socket Layer
SCADA	Supervisory Control and Data Acquisition
SIEM	Security Information and Event Management
TLS	Transport Layer Security
VR	Virtual Reality
VVP	Virtual Power Plant

communication pathways, and physical objects to address real-world issues. As the Industry 4.0 (Tao et al., 2019) revolution is gaining traction, CPS has become one of the top targets for hackers, and any harm to them results in significant losses (Nguyen et al., 2020a). While there have been numerous security breaches in CPS, these issues have received significant attention in research, yet remain understudied (Mohammad et al., 2018).

The U.S. National Science Foundation first introduced the term CPSs in 2006. It describes a broad range of advanced, interdisciplinary systems that blend embedded computing technologies (the "cyber" aspect) with the physical world. These next-generation systems are characterized by their sophisticated integration of computational and physical components. The European form of CPSs emphasizes interaction with human issues and cyberspace/cloud. The American version emphasizes the connection between embedded systems and the physical world. In the Chinese version, a CPS is a large-scale, embedded, hybrid complex system that unifies sensing, processing, intelligence, and control (Yu and Xue, 2016).

In the smart grid context, CPS refers to integrating physical components, such as power generation plants, transformers, and transmission lines, with digital technologies, including communication networks, software systems, and data analytics tools (Jha et al., 2021). The goal is to create a reliable, more efficient, and resilient power system that adapts to changing demand and supply conditions. CPS in the smart grid relies on various sensors and data sources to monitor and control the flow of electricity in real-time. These systems use machine learning algorithms and advanced analytics to identify patterns and anomalies in the data, enabling operators to optimize the grid's performance and prevent disruptions (Pal and Prasanna, 2017; He and Yan, 2016).

An example of CPS in the smart grid is using phasor measurement units (PMUs). These devices are designed to measure the voltage, current, and phase angle of electricity flowing through transmission lines (Labrador Rivas et al., 2020). The measurements are transmitted to control centers in real-time. Enabling operators to monitor the status of the grid and respond swiftly to any issues that may arise (Khalaf et al., 2024; Ayar et al., 2017). Also, demand response (DR) programs (Gharavi et al., 2015) allow customers to adjust their energy usage in response to changes in grid conditions. Customers may make informed decisions about when and how to consume electricity by using real-time information about their energy usage from these programs, which rely on smart meters and other digital technology.

Developing a cyber-physical distribution power system has led to significant cyber-security challenges directly tied to how the system functions because of the exponentially improving information and communication technology (Dong and Zhang, 2021). In the CPS architecture, the cross-layer framework that connects the scattered devices

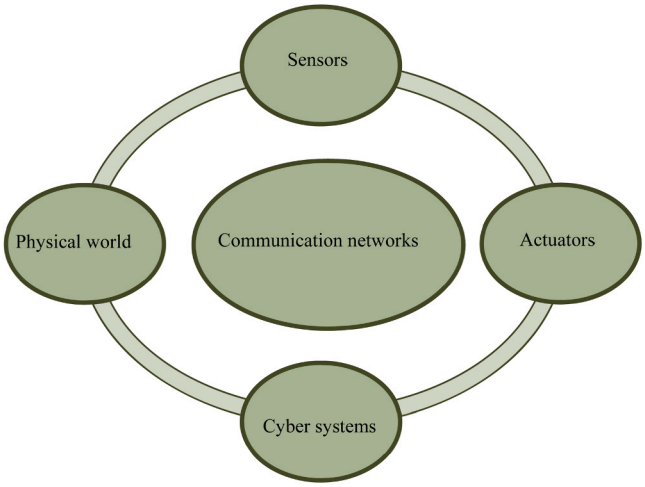

Fig. 1. The framework of CPS.

results in an ongoing increase in the communication load on the networks. The CPS Interconnection Protocol (CPS-IP) is extensively utilized to establish standard communication links across heterogeneous devices and systems. It is designed specifically for special-purpose CPS systems necessitating worldwide regulation and performance assurance for cyber-physical interactions. CPS-IP enables the seamless interconnection and interoperability of these systems (Dong and Zhang, 2021).

Cyber-physical attacks are a growing concern for the energy sector due to the increasing reliance on digital technology and communication systems. A cyber-physical attack compromises a physical system by utilizing its digital or cyber components (Langer et al., 2016). In the energy sector, cyber-physical attacks can have serious consequences, including power outages, infrastructure damage, and data loss. For example, recent events in the U.S., such as attacks on power systems and substations, have exposed vulnerabilities, causing widespread power outages in states including Maryland, North Carolina, Washington, and South Carolina. The Federal Energy Regulatory Commission highlighted the risks of combined cyber and physical attacks on power systems, particularly during extreme weather conditions. In May 2023, Denmark experienced its largest attack against critical infrastructure, with 22 energy organizations compromised within a few days. Hackers exploited vulnerabilities in Zyxel firewalls, gaining complete control over the systems. This attack highlighted the growing sophistication and coordination of cyber threats against critical infrastructure, specifically

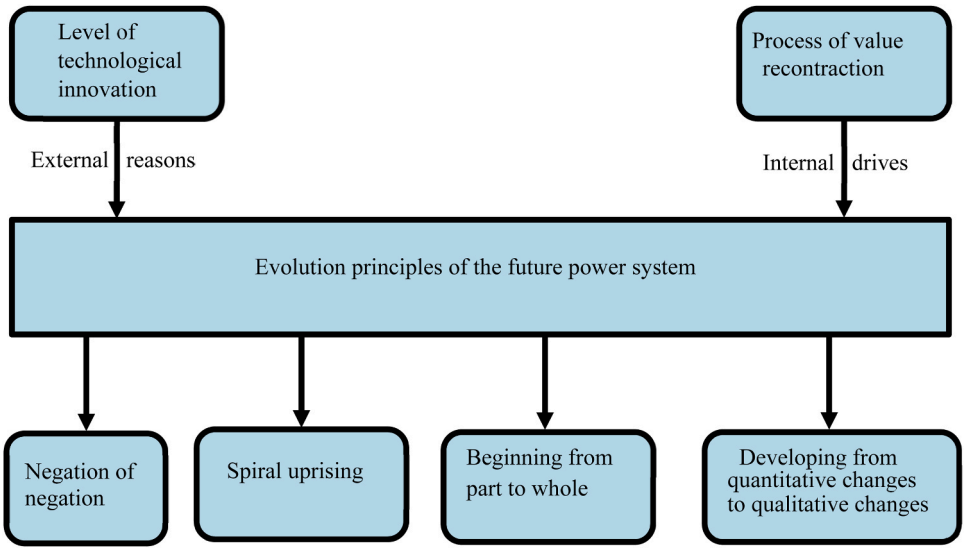

Fig. 2. Evolution principle of the future power system.

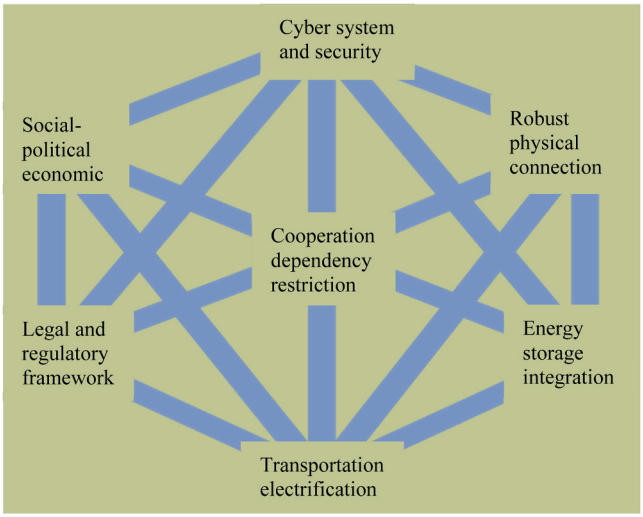

Fig. 3. The interdisciplinary digitalized future energy systems template and interaction scenarios.

targeting Denmark's energy sector. Energy One, an Australian energy trading software company, faced a cyberattack in 2023, affecting its systems in Australia and the UK. This incident raised concerns about the vulnerability of foreign-made solar panel technology, notably solar inverters, to cyberattacks. The Cyber Security Cooperative Research Centre in Australia warned of the increasing cyber risks associated with web-connected solar inverters, underlining the potential for catastrophic consequences on the power supply from such attacks.

The risk of cyber-physical attacks has increased as the energy system becomes more decentralized and reliant on renewable energy sources (RES). The increasing reliance on the IoT and other connected devices has created new vulnerabilities that attackers can exploit (Cardenas et al., 2020). The integration of dispersed energy resources, such as small renewable energy generators and energy storage systems, has resulted in a more intricate energy system that is challenging to safeguard. In addressing these challenges, the energy sector must prioritize cyber security and develop robust measures to protect against threats (Tvaronavičienė et al., 2020).

Some specific measures to improve cyber security in the energy sector are implementing strong authentication methods and access controls to prevent unauthorized access; encrypting sensitive data to protect it from being accessed or stolen; regularly updating and patching systems to address vulnerabilities; conducting security assessments to identify and address vulnerabilities; and training employees and other personnel in cyber security best practices. By addressing these issues, the energy sector can ensure the reliability and resilience of future energy systems (Gkioulos and Chowdhury, 2021).

Inspired by the aforementioned evidence, the main highlights of this study are summarized as follows:

1. Exploration of recent cyber-physical attack: we delve into some recent and significant cyber-physical attacks on energy systems, providing up-to-date case studies that reflect the evolving nature of cybersecurity threats. This exploration of recent cyber physical attack scenarios is a key novelty of our article, offering a fresh perspective on the current landscape of security challenges in energy systems.
2. Current strategies and technologies: the article analyzes cutting-edge research by incorporating the latest research findings from 2010 to 2024, offering a current perspective on the strategies and technologies being developed to counteract cyber-physical threats in energy systems.
3. Multidisciplinary framework: we propose a unique multidisciplinary framework that combines elements from cybersecurity, energy systems engineering, and policy analysis. This approach offers a multidimensional understanding of the challenges and solutions in protecting energy systems from cyber-physical threats, showcasing the innovative scope of our article.
4. Future research directions: we highlight future directions by not only reviewing current state-of-the-art practices but also identifying potential future research directions and technologies that are critical in advancing the field of cyber-physical security in energy systems.

The rest of the paper is structured as follows: Section 2 introduces the concept of the smart grid, covering computing models for the smart grid, smart grid security, malicious and non-malicious threats, transmission and bulk electric systems, distribution security, home area network (HAN), and home energy management (HEM). Section 3 discusses the future of the smart grid, including virtual reality, nano-grid, smart grid management at the microscopic level, and nanoscale communication networks. Section 4 covers wireless power transmission, including inductive and resonance coupling and far-field wireless power transmissions. The future of energy storage, energy storage and cyber

security, energy Internet, and smart grid 2.0 are presented in Section Finally, Section 6 presents the conclusions of the paper.

2. The concept of the smart grid

Smart grid technology has gained traction recently as a potential solution to the world's current energy consumption issues. This section will explore the advantages of smart grid technology, examine the challenges of implementing a smart grid system, and investigate the potential benefits of smart grid technology for future energy consumption. Analyzing current research will clarify why smart grid technology is viable for future energy consumption. The benefits of smart grid technology have been explored in several studies, including (Fang et al., 2012). According to the study, smart grids have numerous benefits, better energy efficiency and reliability, reduced power interruptions, and increased customer satisfaction. They also aid in cutting operational expenses, improving load management, and enabling new services. Hence, smart grids are critical in reducing the environmental effects of energy systems (Hossain et al., 2016; Tang et al., 2023). This can be seen through the increased use of energy storage systems, which allow energy to be stored when generation is high and used when generation is low (Alotaibi et al., 2020).

However, implementing a smart grid system presents numerous problems. The authors of (Saleh et al., 2022) discussed how the smart grid system is designed to optimize energy generation, distribution, and consumption. This presents a challenge as the energy production and distribution system must be constantly monitored and adjusted to ensure optimal energy efficiency. The system must also be able to handle any changes in consumers' energy usage patterns. It requires the system to accurately assess a user's energy usage and provide them with appropriate solutions. In addition, smart grid systems are sourced for a large amount of data, which must be collected, analyzed, and stored; this presents a challenge in terms of cost and complexity. The system must be secure to protect the data from unauthorized access. It must integrate with other systems and devices to facilitate data exchange and provide a comprehensive overview of the whole system.

In (Hui et al., 2020), the advantages of the smart grid for future energy consumption are explored. The authors highlighted how the smart grid effectively reduces the environmental impact of electricity consumption and ensures a reliable energy supply. They proposed that smart grids improve energy efficiency and eliminate energy waste, dramatically lowering the carbon footprint of electricity usage. It has the potential to facilitate the integration of renewable energy sources into the grid and permit energy storage, which can assist in reducing the carbon emissions connected with power usage. It can monitor and forecast energy demand, optimizing energy production and distribution, resulting in more efficient energy usage. All these benefits can assist in lessening the environmental impact of electricity consumption while still ensuring a reliable energy source. As a result, the smart grid is a useful network for future energy use.

Smart grids promise a connected, intelligent electrical delivery and usage infrastructure. It benefits users by reducing electricity costs and greenhouse gas emissions (Liu et al., 2022), improving the reliability and security of electrical power, and enabling two-way communication between electricity users and providers. They are essential for maintaining and enhancing electricity reliability, affordability, and sustainability in the 21st century. Ultimately, smart grids are a promising development in the history of modern energy management and are set to revolutionize how we interact with electricity (Brown, 2008; Gungor et al., 2011). The development of smart energy grids has resulted in a more intricate cyber-physical ecosystem of infrastructures, including new carbon-free power sources, sophisticated monitoring and control systems, and a wide range of rapidly developing contemporary physical hardware technologies. The dynamic smart grid networks' unparalleled complexity and heterogeneity make them more susceptible to new dangers like cyberattacks. Given the rapid advancement and deployment of sophisticated network monitoring and communication systems and power grids' growing interdependence with numerous critical lifeline infrastructures, comprehensive defense strategies are required to protect power grids from cyber adversaries (Nguyen et al., 2020b).

One of the key features of a smart grid is the use of Advanced Metering Infrastructure (AMI), which includes smart meters that can measure and communicate electricity usage in real time. Smart meters can provide detailed information about electricity consumption, such as how much energy is being used at a particular time, how much it costs (Khalaf et al., 2024), and how much carbon dioxide is emitted. This information can be used to optimize the flow of electricity and reduce energy waste (Brown, 2008). Smart grids also use advanced control systems that use algorithms and data analytics to maximize the flow of electricity. These systems can detect and respond to changes in demand and supply and help balance the grid by adjusting the output of power plants and other energy sources. It also uses distribution energy resources (Qi et al., 2016), such as small-scale renewable energy generators and energy storage systems that can be connected to the grid. These distribution energy resources can help reduce reliance on fossil fuels and provide a backup power source in the event of an outage (Brown, 2008).

Power distribution networks face various risks and are prone to numerous interruptions, such as equipment failure, weather events, human error, and cyber security breaches. Therefore, power authorities must implement strategies that minimize disruptions to ensure a reliable and safe power supply. To achieve this, Supervisory Control and Data Acquisition (SCADA) systems provide a cost-effective solution that enhances visibility and control of the distribution network, thereby reducing downtime. The primary function of SCADA systems in the power distribution network is to monitor and control the distribution sectors, optimize the network's overall efficiency, and enhance its reliability and sustainability (CHERIFI and HAMAMI, 2018). They collect data from the distribution system, mainly from substations monitored and controlled in real-time using Programmable Logic Controllers (PLCs), Remote Telemetry Units (RTUs), circuit breakers, and power monitors. The collected data is transmitted to a central SCADA node at the substation, connected to the main control center (Lee and Hong, 2020). The SCADA system can pinpoint the exact location of a power outage and alert the operators via an alarm. The operators can design an action plan to prevent more disruptions based on the severity of the notice. Because of its real-time responsiveness, the SCADA system can implement mitigation methods quickly, often before downstream customers know of possible power supply difficulties.

In substations, the SCADA system automatically regulates isolators, switches, and circuit breakers that violate parameter limits, ensuring continuous inspection of parameters without requiring line workers at each isolation point. It significantly enhances worker safety and system efficiency. Also, the SCADA system performs various functions, including controlling transformer voltage taps to optimize network efficiency, monitoring and controlling sectionalized and reclosers, continuously monitoring electrical parameters during normal and abnormal conditions, and alerting operators to power supply, quality, or safety issues through trending and alarming (Wei et al., 2010; Fu and Wang, 2024). The interrelated parts of a smart grid system are depicted in Fig. 4, which emphasizes how central management systems and cutting-edge communication networks are integrated with the residential, commercial, and industrial sectors.

2.1. Computing model for smart grid

Computing models for smart grids include a wide range of technologies that are used for data processing, analysis, and decision-making. These models enable the smart grid to respond to changing conditions in real-time, optimize energy consumption, and reduce energy waste. According to the authors of (Yigit et al., 2014), implementing computing models effectively manages the complexity of smart grids. The

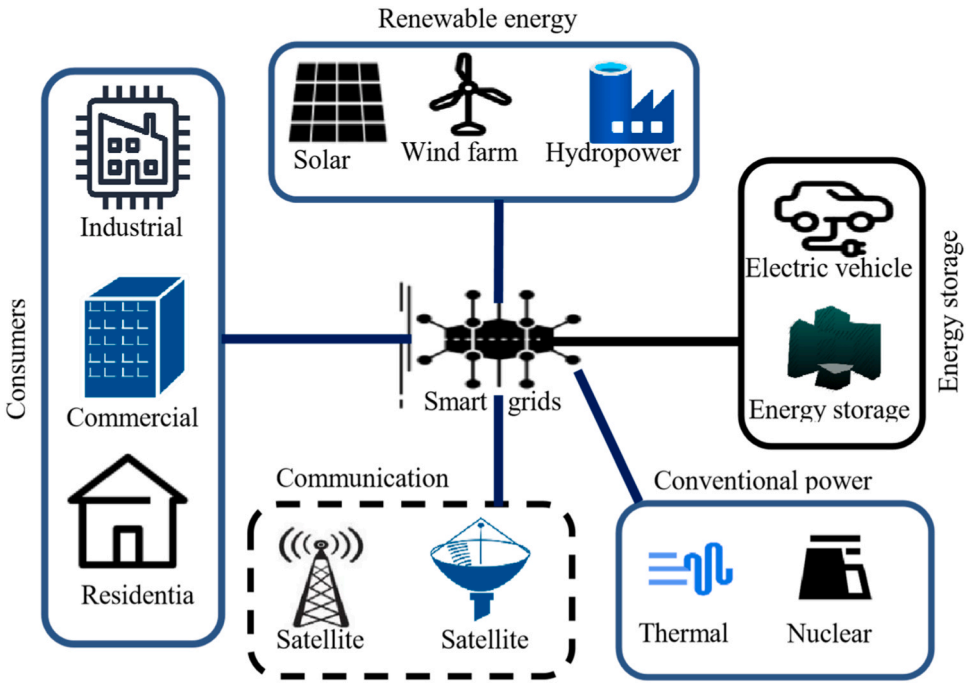

Fig. 4. The architecture of the smart grid.

components and circumstances of the smart grid may be efficiently controlled, observed, and analyzed using the models. This will make it possible for the smart grid to react promptly to changes and issues.

Furthermore, using computational models can increase the accuracy of data acquired by smart grids due to computing models' increased data processing capabilities, which can reduce errors and boost data accuracy. It can lower the cost of the smart grid by optimizing the system and reducing energy waste. The challenges of utilizing computing models for smart grids are multi-faceted, as was mentioned in (Diamantoulakis et al., 2015). Computing models for smart grids must be able to handle a large amount of data from various sources, and data must be integrated and analyzed in real-time. The models must be able to make predictions about future events and respond quickly and accurately. Since data must be shielded from bad parties and breaches, security is another key worry. They must be capable of considering every element of the system, from the grid's physical architecture to the software and algorithms that control it. It must be able to communicate with both the physical devices linked to the grid and the people using the system. The challenges of utilizing computing models for the smart grid are numerous and require a comprehensive, multi-faceted approach to ensure that the models are effective and secure (Diamantoulakis et al., 2015).

Computing models in the modern energy grid must be able to process large volumes of data and make decisions in real-time. The author of (Chaichi et al., 2015) proposes some strategies to overcome these challenges. First, they suggest that

"multiagent" systems, composed of many interacting nodes, can solve certain tasks more effectively than a centralized approach. Second, they propose using "autonomous intelligent agents to perform decision-making." These agents can process large amounts of data and make decisions quickly. Third, they recommend using artificial neural networks (ANN), which can identify patterns and make decisions. Finally, they suggest "federated learning," enabling distributed decision-making." Each of these strategies can help to overcome the challenges of computing models for the smart grid.

Fig. 5 illustrates the different types of computing paradigms that can be utilized within a smart grid or modern energy management system. The figure consists of four quadrants, each representing a distinct computing model: distributed computing, cloud computing, edge computing, and fog computing. These models play a critical role in processing, analyzing, and managing data within the grid to optimize performance and reliability.

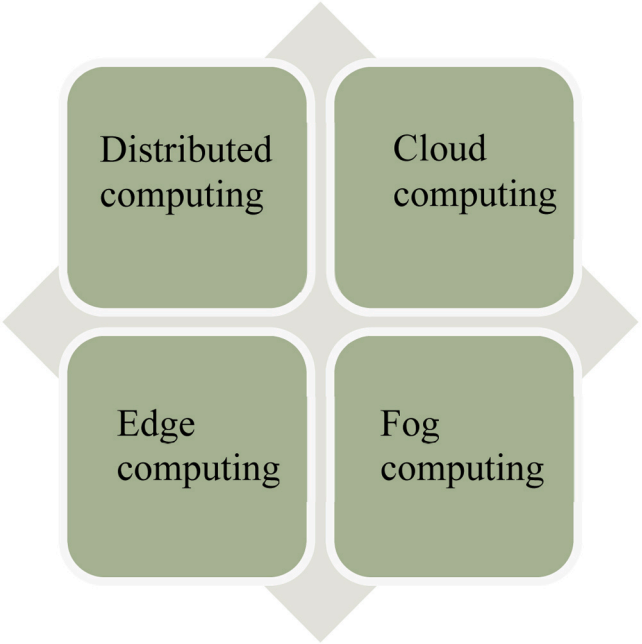

Fig. 5. Illustration of different computing models.

- Distributed computing: In this model, computing is distributed across many devices or nodes in the grid. Each device or node is responsible for performing a precise task or function, and the overall system is decentralized, with no single point of failure. This model is often used in smart grids to ensure reliability, scalability, and security (Yigit et al., 2014).

- Cloud computing: This model uses a remote network of servers, often called a “cloud,” to provide computing resources on demand (Yusop and Abawajy, 2014). Smart grid applications can use cloud computing to store and process large amounts of data, such as energy usage data or sensor readings, without requiring a local computing infrastructure.
- Edge computing: This model involves using computing resources at the “edge” of the network, close to the devices or sensors generating data. Thus, the amount of data that needs to be communicated over the network can be decreased, and data processing can be done more quickly and reliably.
- Fog computing: This model is similar to edge computing but involves intermediate nodes between the edge devices and the central cloud or data center. These intermediate nodes, often referred to as “fog nodes,” can help reduce the amount of data transmitted over the network and improve the speed and reliability of data processing.

Regardless of the specific computing model chosen, smart grid systems must be able to manage massive volumes of data, process data instantaneously, and scale up or down as needed to meet changing demand. Computing models for the smart grid are an increasingly useful innovation in modernizing the outdated electricity grid. They provide users with greater reliability and accuracy of power deliverance throughout power grids, as well as flexibility and practicality, greatly reducing the possibility of failure and unexpected power outages. Also, these models open up options for reducing emissions, using renewable energy sources, and providing better functionality for consumers. They are, without a doubt, a useful way to bring the electricity grid into the 21st century (Bera et al., 2015).

Table 1
Computing models pros and cons.

Computing paradigm	Pros	Cons
Distributed computing	Improves efficiency and redundancy by sharing computational tasks across multiple computers. Enhances fault tolerance and reliability. Scalability allows for incremental addition of resources.	Requires a robust network infrastructure to handle distributed tasks and communication. Can be complex to manage and coordinate the distributed resources. Potential security risks due to multiple access points.
Cloud computing	Provides scalability and accessibility by utilizing remote servers. Reduces the need for local hardware and maintenance. Offers flexible resource allocation and cost efficiency.	Dependent on internet connectivity, which can be a limitation in some areas. Latency issues due to the distance between data source and cloud servers. Data security and privacy concerns due to centralized data storage.
Edge computing	Reduces latency by bringing computation and storage closer to the data source. Decreases bandwidth use by processing data locally. Enhances real-time data processing and decision-making.	Limited computational power compared to centralized data centers. Can be costly to implement across many locations. Requires consistent updates and maintenance of edge devices.
Fog computing	Extends cloud capabilities to the edge, providing local data processing while benefiting from central cloud resources. Enhances data security by processing sensitive information locally. Reduce latency and bandwidth	Similar to edge computing, it has limited computational power compared to central cloud services. Can involve complex network architecture and management. Potential interoperability issues between edge devices and cloud infrastructure.

Table 2
Summary of the section two.

Section title	Key points
2. The concept of the smart grid	Smart grid technology is presented as a solution to current energy consumption issues. Smart grids offer benefits such as better energy efficiency, reliability, reduced power interruptions, and increased customer satisfaction. Implementation challenges include high initial costs, security issues, and the complexity of monitoring and adjusting the system. Smart grids can integrate renewable energy sources and enable energy storage to balance supply and demand. AMI is a key feature, allowing real-time data on electricity consumption and facilitating optimized energy use. SCADA systems play a vital role in monitoring and controlling the distribution network, enhancing visibility and control. Smart grids can improve load management, reduce operational expenses, and enable new services. The development of smart grids has resulted in a complex cyber-physical ecosystem requiring comprehensive defense strategies against cyberattacks. Importance of regular security updates, employee training, and incident response plans to ensure grid reliability and security

Table 3
Summary of the section three.

Section title	Key points
The future of the smart grid	The future of the smart grid involves greater integration with other technologies, particularly IoT. VR can enhance grid management by simulating scenarios for better training and planning. VPPs enable the aggregation of distributed energy resources to act as a single power source. VPPs can help integrate renewable energy sources and provide a reliable, flexible power supply. Nano-grids are small-scale, decentralized power systems ideal for remote areas and improving power system resilience. Smart grid management at the microscopic level involves using smart appliances and devices to optimize energy distribution. Nanoscale communication networks utilize small-scale devices for real-time data collection and analysis to enhance grid reliability. The use of advanced algorithms and machine learning for energy optimization and fault detection is emphasized. Future advancements will address the challenges of integrating renewable energy, improving grid resilience, and ensuring cybersecurity.

2.2. Smart grid security

Smart grid technology research and implementation have become increasingly important for modern civilization, yet with this improvement comes significant security threats and weaknesses. This section examines the need for improved smart grid security solutions and the difficulties in safeguarding smart grid infrastructure. It assesses risk and devises methods to address smart grid security flaws.

The need for enhanced security solutions for smart grids has progressively become important in recent years. Improved security has become a critical issue with the ever-growing complexity of the smart grid system. As outlined in (Metke and Ekl, 2010), the vulnerability of smart grids to malicious attacks has become a major concern. According to the authors, the current security solutions for smart grids lack the necessary features to protect against malicious actors adequately. They suggested developing more sophisticated information security tools and methods to protect against malicious attacks. They proposed the use of distributed security architectures and intrusion detection solutions to

Table 4
Summary of the section four.

Section title	Key points
Wireless power transmission	Wireless power transmission refers to the transfer of electrical energy without physical cables or wires. Nikola Tesla pioneered the concept using electromagnetic induction, a method still in use today. Various methods include inductive coupling, resonant coupling, RF, laser, and microwave transmission. Inductive coupling is common in applications like wireless charging pads but has limited range and efficiency. Resonant coupling allows energy transfer over longer distances but requires precise frequency matching. RF communication is crucial in smart grids for applications like AMI, DA, and DR, providing real-time data and enabling efficient grid management. Microwave transmission can transfer energy over long distances but requires a direct line of sight and can interfere with other devices. Far-field wireless power transmission could revolutionize power delivery for EVs, remote sensing, and more, but faces challenges like efficiency and cost. The development of new technologies such as solar power satellites and near-field transmission promises further advancements.

Table 5
Summary of the section five.

Section title	Key points
The future of the smart grid	Energy storage is crucial for balancing supply and demand in renewable energy systems. Advancements in battery technology, such as lithium-ion and solid-state batteries, are key to future energy storage. The rise of electric EVs is driving demand for more efficient and affordable battery technologies. New energy storage technologies, including hydrogen fuel cells and thermal energy storage, offer unique advantages for certain applications. Flow batteries and superconductors are emerging technologies with potential for large-scale energy storage solutions. Flow batteries use liquid electrolytes for scalable energy storage, ideal for long-term storage and renewable integration. Supercapacitors provide high power density and fast charging times, making them suitable for applications requiring rapid energy delivery. Cybersecurity is critical in energy storage systems to protect against unauthorized access and manipulation The development of an energy internet integrates renewable energy sources, storage systems, and traditional energy into a cohesive network. Future advancements will address the challenges of integrating renewable energy, improving grid resilience, and ensuring cybersecurity. Smart grid 2.0 will incorporate advanced analytics, machine learning, and cybersecurity to enhance grid reliability and efficiency.

increase the level of security. They concluded that these solutions would provide a better defense against malicious actors and reduce the need for manual security measures.

Dealing with various devices and protocols is one of the most difficult aspects of safeguarding smart grid infrastructure. Because it is difficult to keep track of all the different systems and ensure that each one is secure and up-to-date with the latest security protocols. It is suggested that most current security protocols are not designed with smart grids in mind (Amin et al., 2021) and are, therefore, inadequate for keeping the infrastructure secure. Likewise, the large scale and complexity of the smart grid infrastructure makes it difficult to develop and implement effective security measures (Wang and Lu, 2013a).

Risks are often due to inadequate security measures or a lack of proper maintenance. To mitigate such risks, (Wang and Lu, 2013b) suggested a comprehensive risk assessment as a first step. The evaluation should consider both physical and cyber threats and the potential impacts of a successful attack. The authors recommended developing a comprehensive strategy to protect the grid. The system should not only involve the implementation of security measures but also the development of plans to respond to potential attacks. With the right risk assessment and mitigation strategy, the potential risks associated with a smart grid can be greatly reduced (Hasan et al., 2024).

Security is a critical component of successfully implementing smart grids. It aims to guarantee the privacy, confidentiality, and integrity of the data transmitted through a system and defend it from malicious attacks and unauthorized access. In addition, authentication and authorization processes must be implemented to thwart malicious actors from accessing the network and/or manipulating/stealing data. Encryption and digital signature technologies should be deployed to ensure secure communication and data integrity. Thus, smart grid security is essential for these systems and networks to function effectively, and to protect data against malicious actors (ANON; Lu et al., 2010; Gunduz and Das, 2020a).

Hackers and cybercriminals may attempt to gain unauthorized access to the grid to disrupt its operation, steal sensitive data, or cause other damage. Strong cyber security measures must be implemented to address these threats. These measures can include network security protocols that protect against unauthorized access, encryption of sensitive data (Farraj et al., 2018). Regular security updates and patches, advanced security analytics tools that can detect and respond to potential threats in real-time, training and awareness programs for employees and other users of the grid (Wang and Lu, 2013a). It is also important for smart grid operators to have robust incident response plans in place in the event of a cyber security breach. These plans should include procedures for identifying and responding to threats and measures to minimize the impact of any disruptions or damage (Gunduz and Das, 2020b). Network security protocols can be enhanced by adopting the following measures, and protection against unauthorized access can be ensured.

- Implement strong authentication methods: Use multi-factor authentication (MFA) to confirm the identity of users before allowing them access to the network (Chen et al., 2023; Aleluya and Vicente, 2018). This can include techniques such as passwords, security tokens, or biometric authentication.
- Use secure protocols: Use secure protocols such as Secure Socket Layer/Transport Layer Security (SSL/TLS) to encrypt data transmission (Abolade et al., 2021) and protect against man-in-the-middle attacks.
- Use firewalls and intrusion detection systems: Use firewalls to block unauthorized access and intrusion detection systems to alert administrators of potential security breaches.
- Implementation of access controls: Use access controls such as permissions and access lists to limit the areas of the network that users can access.
- Regular update and patch systems: Regularly apply updates and patches to ensure that systems are secure and up to date.
- Conduct security assessments: Regularly conduct security assessments to identify vulnerabilities and implement measures to address them.
- Train employees: Train employees on security best practices and the importance of maintaining secure access controls.

Provision of regular security updates and patches is vital to smart grid security and integrity. These procedures serve as preventive measures against potential risks and add to the energy distribution system's dependability and endurance. It is paramount to establish a robust process to ensure the timely application of updates and patches, to reduce the likelihood of any vulnerabilities being exploited (Yadav and Paul, 2021).

The following are some of the benefits of applying security updates and patches to smart grids:

Improved cybersecurity: Security updates and patches are designed to fix vulnerabilities (Sawadogo et al., 2020) in smart grid components' software, hardware, and firmware. Applying these updates reduces the cyber-attack risk, making the grid more resilient.

Compliance with regulations: Governments and regulatory bodies impose standards and regulations on critical infrastructure security, including smart grids. Utilities can comply with these regulations and avoid penalties by applying security updates and patches (De Lacerda Filho et al., 2022).

Better performance: Besides addressing security vulnerabilities, security updates, and patches often include new features, bug fixes, and other improvements that enhance the overall performance (Sawadogo et al., 2020) of smart grid components. By keeping the software up-to-date, utilities can take advantage of these improvements to optimize the performance of the smart grid.

Cost savings: Cybersecurity incidents can be expensive, from equipment replacement to lawsuits and fines. By applying security updates and patches, utilities can avoid these costs, reducing the overall cost of operating the smart grid infrastructure.

Reputation management: A successful cyber-attack on a smart grid can damage the utility's reputation and reduce public trust in the reliability and security of the grid. Utilities can demonstrate their commitment to cybersecurity and protect their reputation by applying security updates and patches.

The application of security updates and patches to smart grids is critical for ensuring the resilience and security of the smart grid infrastructure. Utilities should create a robust patch management program and routinely update their smart grid components to reduce cybersecurity risks and improve performance. Utilities may protect their customers, maintain regulatory compliance, and secure their reputations by doing so.

Several advanced security analytics tools can be used to detect and respond to potential threats in real-time in the context of a smart grid. Some examples include:

- Intrusion detection and prevention systems (IDPS): IDPS are designed to identify and prevent unauthorized access or attacks on a network or system. They do this by continuously monitoring network traffic and comparing it against predefined rules or patterns (called "signatures") that indicate the presence of a known threat (Lima et al., 2022; Patel et al., 2013). IDPS can also use anomaly-based detection, which involves analyzing traffic patterns and identifying deviations from normal behavior that may indicate a potential threat. IDPS can use behavior-based detection, which consists of analyzing the behavior of individual users or devices to identify deviations from normal activity that may indicate a potential threat (Amin et al., 2021).
- Security information and event management (SIEM) systems: SIEM systems are designed to collect and analyze data from various bases, such as network logs, system logs, and security devices, to identify potential security threats and alert administrators. A predetermined set of regulations or models is employed to detect possible security breaches, which helps recognize dubious activities and trigger notifications upon identifying a probable threat (Patel et al., 2013).
- Traffic analysis tools: These tools monitor network traffic and use machine learning algorithms to identify anomalies and potential threats, such as malware infections, unauthorized access, and data exfiltration. This is done by analyzing traffic patterns and identifying deviations from normal behavior that may indicate a potential threat.
- Vulnerability management tools: These tools help identify and prioritize vulnerabilities in the smart grid infrastructure and provide guidance on how to fix them. To identify any system weaknesses, the network is subjected to a thorough analysis that involves scrutinizing for vulnerabilities.
- Endpoint security tools: Individual devices, such as smart meters, are protected from threats by these tools, which monitor their activities and prohibit harmful operations. The device's activity is constantly monitored and cross examined against a pre-established set of criteria or models to detect potential dangers. It is crucial to highlight that the usefulness of these tools depends on the quality of the data given to them and the skill of the analysts who analyze the results. Therefore, proper training and regular maintenance are critical to ensuring these instruments work optimally.
- The most pressing issue about the security of the smart grid is how events will be found and, more importantly, how they will be dealt with once they happen. This is due to the direct impact cyber security incidents will have on the dependability of the smart grid. Moreover, as time passes and the smart grid begins to advance, we will probably see frequent cybersecurity incidents that impact it. The usage of information technology (IT) resources in this area and the growing number of connections are the main causes of this. The likelihood of an incident will rise as the grid switches from traditional communications infrastructures to Internet Protocol (IP) communications infrastructures (Wang and Lu, 2013a).

The proliferation of IP-based infrastructures in the utility industry has introduced new cybersecurity risks previously considered insignificant. To strengthen the smart grid, there will likely be an increase in IT involvement in automating security procedures. Utilities must establish stronger connections with vendors and other utilities to manage their cyber security risks. As operations technology (OP) relies more on IP-based communications, the existing "air gap" between operations and corporate data networks may diminish. To mitigate these threats, utilities must implement security protocols and solutions to protect their IP-based operations networks. Operations are in the business of running the grid's assets, not the massive IT infrastructures that will be required to run those assets (Wei et al., 2010).

An attack that seeks to weaken an operational network will probably result in instability problems. This is so because a threat's value would create instability, whereas the operations network aims to support reliability. If a threat is present on an operations network, it must be quickly found, contained, and eliminated. In such an environment, there are primarily two categories of threats: *Malicious* and *Non-malicious*.

2.2.1. Malicious threat

Malicious threats refer to intentional actions or objects designed to cause harm or damage (Whitehead et al., 2017) to individuals, organizations, or systems. These threats can encompass a wide range of activities, from physical acts to digital attacks. A malicious threat may attempt to alter the information in a working environment (Mousavian et al., 2018) such that operators unintentionally make a mistake. Scenarios that can significantly impact operations involve threats that modify information, resulting in outcomes that differ from what operators expect (Whitehead et al., 2017). An operator may be coerced into opening a breaker without justifiable cause in certain scenarios. Such instances may arise, for example, when an IT system is manipulated by a hacktivist to falsely indicate a fault in a particular line's status. This intentional deception could trigger an automated system to trip a breaker, causing an unnecessary outage. This poses a challenge for operators as it would require them to take additional measures to restore the circuit. In other situations, someone will probably be killed if they work on a line intended to be de-energized but got energized.

To protect their infrastructure, utility companies keep their operational network separate from the internet and corporate data networks. They accomplish this through access control measures like firewalls, which only allow specified ports and services to pass through. The operational network oversees substation operations and connects with field equipment for maintenance. In contrast, the control system

network, such as SCADA, is likewise separated and protected from the operational network by firewalls. This organizational approach creates a boundary between the internal and external parts of the network, as illustrated in Fig. 6.

Although it may appear illogical for utility company employees to deliberately target customers, various situations might motivate them to do so (Fullerton and Punj, 2004). Disgruntled workers behaving disruptively in the workplace is not novel (Yadav et al., 2016). Employees frequently express dissatisfaction towards their superiors due to poor performance evaluations, inadequate remuneration, potential downsizing, and differences with management. Such behavior may have an unintended negative impact on customers.

Fig. 6 shows the linked networks that make up a smart grid system's framework. The central integration point for different network segments is represented by the cloud symbol in the center. This central hub is linked to the following four important network components: the corporate network, the generation network, the operation network, and SCADA. Each one of these networks is essential to the smart grid's overall effectiveness and usefulness (Sorebo and Echols, 2012).

2.2.2. Non-Malicious threat

Non-malicious assaults are unintended events or errors that can cause problems or disruptions in a system's operation. Non-malicious attacks on the smart grid can occur for a variety of causes, including human mistakes, equipment faults, and environmental conditions. These smart grid attacks can do significant damage, especially if they go unnoticed. A simple error, such as misconfigured equipment or incorrect parameter setting, might result in voltage fluctuations, system instability, or even a blackout. A natural calamity, such as a storm, earthquake, or flood, can also damage vital infrastructure and cause power outages, causing the entire grid to fail (Gunduz and Das, 2018).

One of the foremost difficulties associated with non-malicious attacks is their inherent unpredictability, which poses a formidable challenge in terms of planning for and mitigating their impact. Unlike their malicious counterparts, non-malicious attacks may transpire without warning, rendering them more arduous to forestall and detect. It can be problematic to differentiate between non-malicious and malicious attacks, thereby impeding the determination of their root causes and origins. Among the most prevalent forms of non-malicious attacks on the smart grid is equipment malfunction. Given the intricate web of interconnected devices and equipment that constitute the smart grid, a breakdown in a single component can trigger a domino effect, leading to a series of malfunctions throughout the system. This risk is particularly pronounced concerning critical components such as transformers, circuit breakers, and protection relays, which, if faulty, may cause significant disruptions to the smart grid (Fullerton and Punj, 2004).

Another type of non-malicious attack is human error, which can occur at any point in the system's operation. For example, an operator may make a mistake in setting a parameter or entering data, leading to incorrect control actions and disruptions in the grid's operation. Similarly, a maintenance technician may accidentally damage equipment during repairs or upgrades, causing system downtime and outages. Environmental factors such as extreme weather events can also cause non-malicious attacks on the smart grid. For example, a storm or lightning strike can damage power lines, transformers, or other critical components, leading to power outages and grid operation interruptions.

To mitigate the impact of non-malicious attacks, robust monitoring and control systems must be implemented to detect and respond to anomalies in real-time. Regular maintenance and testing of equipment can help prevent failures due to wear and tear or other non-malicious factors. Training and education of personnel can help reduce the risk of human errors, ensuring efficient operation and safety of the smart grid.

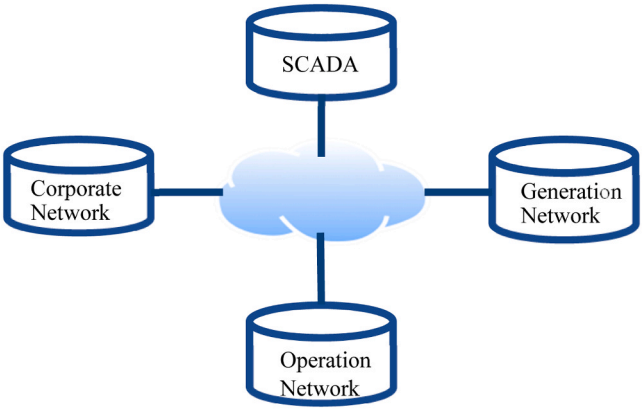

Fig. 6. Access point.

2.3. Distribution system security

Distribution system security refers to the measures put in place to ensure that the electricity distribution system is protected from cyber-attacks, physical attacks, and other threats that may compromise the system's availability, integrity, and confidentiality. The distribution system involves transporting power from the transmission system to residences, businesses, and other facilities. It consists of a complex network of lines, transformers, and other equipment that must be protected from various threats. Cyber-attacks are one of the most serious risks to distribution system security. These attacks can originate from multiple sources, including hackers, cybercriminals, and foreign governments. Cyber-attacks can take many forms, such as phishing, malware, and denial-of-service attacks. To protect against these threats, distribution system operators must implement robust cybersecurity measures, such as firewalls, intrusion detection systems, and encryption. Another threat to distribution system security is physical attacks. Physical attacks, such as vandalism or sabotage, can cause widespread power outages and disrupt people's daily lives. On the other hand, cyber-attacks can compromise the communication and control systems of the distribution system, leading to system failures and potential power outages. The consequences of such attacks can be catastrophic and lead to unprecedented destabilization of the entire electric grid (Lewis).

Saboteurs may attempt to disrupt the system by cutting power lines or damaging transformers. To protect against physical attacks, distribution system operators must implement physical security measures, such as fences, locks, and surveillance cameras. They may also install alarms and other detection systems to alert them to potential threats. They must ensure their personnel are properly trained in security procedures and protocols. This includes training on how to detect and respond to cyber-attacks, as well as how to respond to physical security threats. Regular training can help ensure that personnel are prepared to handle any security threat that may arise.

In conclusion, distribution system security is a critical component of ensuring the reliability of the electricity distribution system. To protect against cyber-attacks, physical attacks, and other threats, distribution system operators must implement robust cybersecurity and physical security measures and train their personnel in security procedures and protocols. These steps can help ensure the distribution system remains secure and reliable, even in the face of potential threats.

2.4. Home area network

A HAN of power systems refers to a network of electrical devices and appliances within a single residence (Liang et al., 2014) or dwelling connected to the larger electricity grid. This network typically includes computers, laptops, tablets, smartphones, art televisions, and other internet-connected devices such as thermostats, home security systems, and appliances. The core drive of a HAN is to form a more convenient

and efficient way of managing and accessing these devices. With a HAN, homeowners can easily control their home appliances, track their energy consumption, and adjust their home security systems from a single interface (Mendes et al., 2015). The HAN is usually connected through a router or modem, which serves as the network's central hub. This hub is responsible for distributing internet connectivity to each device within the network. The devices can be wired or wireless, with wireless being the more popular option due to its convenience and flexibility. One of the primary benefits of a HAN is the ability to automate various tasks within the home. A homeowner, for example, can program their smart thermostat to turn on the air conditioner before they return home from work. They can even design their smart lights to turn on and off at specific times of the day or configure their home security system to notify them when someone enters their home. Another advantage of using a HAN is the ability to share resources among devices. A printer linked to one computer on the network, for example, can be accessible by other devices on the network, allowing for more efficient resource use (Mendes et al., 2015; Alohali et al., 2014).

However, there are also some risks associated with HANs. Security is a major concern, as these networks can be vulnerable to cyber-attacks. Homeowners need to take proper security measures, such as using strong passwords, keeping software up to date, and monitoring network activity (Alohali et al., 2014).

The components and structure of a HAN inside a smart grid system are shown in Fig. 7. It illustrates how different home appliances and gadgets are networked and interact with the utility network via a router and smart meter, allowing for effective energy monitoring and control. The larger energy distribution network that the utility business oversees is represented by the utility network. The term "power plant" refers to the location of the energy source, which may be either non-renewable or renewable. A crucial element that tracks electric energy use and relays that data to the utility network is the smart meter. It serves as a link between the home area network and the utility network, enabling real-time energy management and monitoring (Alohali et al., 2014).

2.5. Home energy management

HEMS are devices that allow homeowners to monitor and control their electricity usage (Dinh et al., 2020) from a central location, such as a smartphone or tablet. HEM refers to the process of controlling, monitoring, and optimizing the use of energy in a residential setting. HEMS are devices or software programs that allow homeowners to monitor and control their energy usage from a central location, such as a smartphone or tablet (Mahapatra and Nayyar, 2022). To use a HEM system, homeowners typically need to install a device or software program to monitor and control their energy usage. This device or software program is generally connected to the home's electricity meter and other appliances and devices, such as lights and thermostats. In summary, HEM systems can help homeowners save energy, reduce their electricity bills, and maximize the comfort and security of their homes (Zhou et al., 2016; Merdanoğlu et al., 2020; Beaudin and Zareipour, 2015). However, like any connected system, HEMS can be vulnerable to cyber security attacks, such as unauthorized access, data tempering denial-of-service, and distributed denial-of-service.

3. Future of the smart grid

The future of the smart grid looks bright with its ability to incorporate renewable energy sources, optimize energy usage, and improve grid security, it has the potential to greatly improve the reliability and sustainability of the power grid (Paul et al., 2014). The smart grid will become even more integrated with other technologies, such as IoT, in the future. This will allow for much more control and efficiency in electricity delivery. It could also lead to new business models, such as allowing consumers to sell excess energy back to the grid (Monnier).

3.1. Virtual reality

In recent years, virtual reality (VR) has grown in popularity with its

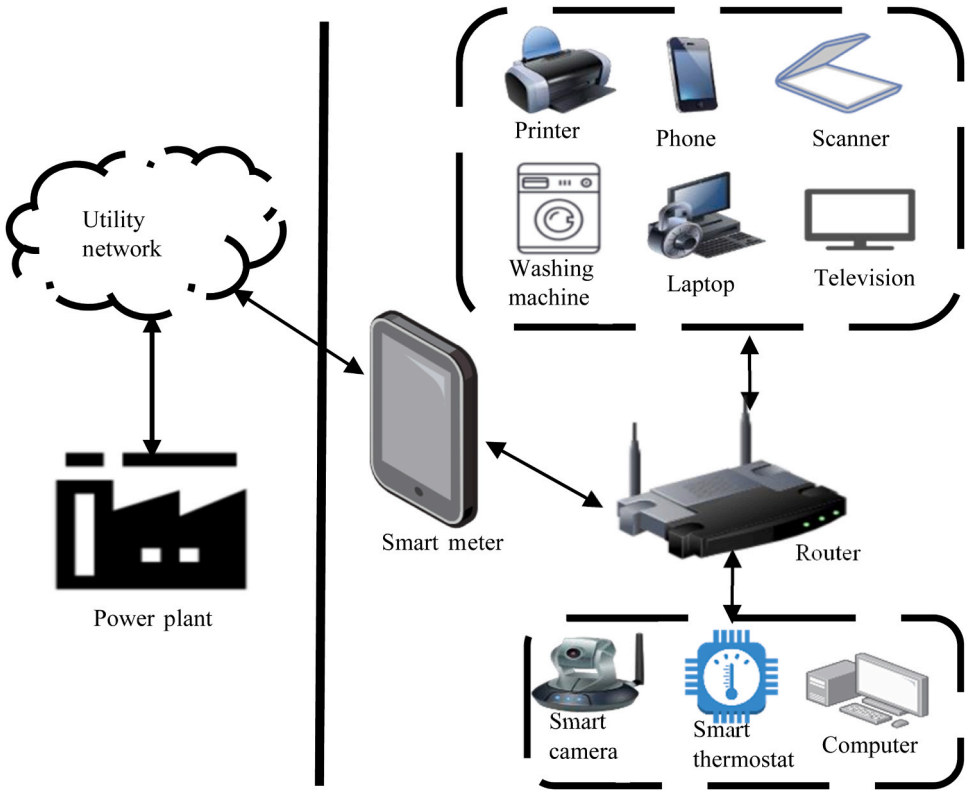

Fig. 7. HAN network.

ability to provide immersive experiences that can simulate real-life environments. One area where VR has the potential to make a significant impact is smart grids. VR in smart grids can provide many benefits, including improved efficiency, safety, and reliability. One of the key advantages of adopting VR in smart grids is the capacity to mimic various scenarios and environments. For example, VR can simulate power outages and other emergencies, allowing grid operators to test various reactions and determine the most effective solutions (Bottani and Vignali, 2019). This can help increase the grid's overall efficiency while lowering the likelihood of outages and other disturbances.

Another key benefit of using VR in smart grids is the increased safety it can provide. By simulating different scenarios, grid operators can identify potential hazards and develop mitigation strategies (Palmarini et al., 2018). For example, VR can be used to simulate the impact of catastrophic weather events on the grid, such as hurricanes and wildfires. This can assist operators in identifying vulnerable regions and developing methods to protect them. Finally, VR can increase the grid's overall reliability. Operators can identify possible bottlenecks and other issues affecting grid performance by modeling various scenarios. It can aid in identifying places where repairs and other enhancements are required and improve the grid's overall efficiency (Masoni et al., 2017). As the energy industry evolves and new technologies emerge, VR will most certainly play an increasingly essential role in the construction and operation of smart grids. Yet, there are still challenges, such as the cost of incorporating VR technology.

3.2. Virtual power plant

A virtual power plant (VPP) is a concept that refers to a distributed network of small-scale power generation systems that are collectively managed and operated as a single power plant (Tajeddini et al., 2014). These power generation systems can include renewable energy sources such as solar, wind, hydropower and conventional sources such as natural gas and diesel generators (Nosratabadi et al., 2017). The VPP concept emerged as a response to the challenges posed by the increasing adoption of renewable energy sources, which are intermittent in nature and can be difficult to integrate into the grid. By connecting these smaller power generation systems through a central platform, VPPs can provide a more reliable and flexible source of power that can respond to changes in demand and supply (Tian et al., 2020). It also helps to reduce the overall cost of electricity by reducing the need for expensive peak-load power plants and transmission infrastructure. Likewise, VPPs can provide a range of ancillary services, such as frequency control and voltage regulation, which can help stabilize the grid, improve its resilience, and reduce reliance on conventional power plants that emit harmful emissions (Naval and Yusta, 2021). While VPPs are still relatively new, they are rapidly gaining popularity worldwide as a key component of transitioning to a more sustainable and decentralized energy system.

VPPs also offer several advantages to consumers and energy retailers. For instance, consumers with DERs can participate in DR programs and earn incentives for reducing their energy usage during peak demand periods. On the other hand, energy retailers can use VPPs to participate in energy trading activities in wholesale markets, taking advantage of market fluctuations and earning additional revenue (Naval and Yusta, 2021). Robust cybersecurity measures are essential in the wholesale market to safeguard against cyber-attacks. Such attacks could manipulate prices, disrupt supply chains, cause significant financial losses, and potentially create safety hazards (Zhang et al., 2023). There are different VPPs, including cloud- based VPPs, which use remote servers to manage energy resources, and hybrid VPPs, which combine cloud-based and on-premises control systems. Ongoing research is focused on optimizing VPP performance, improving communication and control systems, and addressing cybersecurity concerns.

The elements of a VPP and how they work together to provide a decentralized, adaptable, and effective power system are shown in Fig. 7. The VPP, which unifies several distributed energy resources (DERs) and runs them as a single, cohesive power plant, is at the heart of the system. This single entity balances supply and demand in real time, improving grid efficiency and dependability. The VPP incorporates several essential elements (Rouzbahani et al., 2021) to increase resilience and dependability, microgrids are small, localized groupings of electrical sources and loads that may run separately from the main grid. Batteries and other energy storage devices assist integrating intermittent renewable energy sources and balance supply and demand by storing surplus energy produced by renewable sources for later use. To minimize transmission losses and improve energy security, distributed generation uses small-scale power generating sources, such as solar panels and wind turbines, that are positioned near to the energy's point of consumption.

VPPs are vulnerable to cyber threats (Yao et al., 2024) due to their interconnected energy resources, including storage, electric cars, and microgrids. To protect their reliability and integrity, strong cybersecurity defenses are necessary, including encryption, secure communication routes, regular security upgrades, and incident response plans. Monitoring network abnormalities and taking appropriate action can help reduce cyberattacks. In conclusion, VPPs are a game-changing technology that has the potential to revolutionize the energy sector by enabling the integration of renewable energy sources, optimizing energy production and consumption, and enhancing grid resilience. The ongoing advancements in VPP technology are a promising sign of a sustainable and secure energy future. Yet, since VPPs rely on digital communication and control systems to coordinate the operation of these distributed resources (Bai et al., 2024), they can be susceptible to various types of cyber threats.

3.3. Nano grid

The growing demand for electricity, particularly in developing countries, has led to the need for innovative and cost-effective solutions to provide reliable and sustainable power to remote and off-grid areas. One such solution is the concept of nano-grids, which are small-scale, decentralized power systems that can operate independently or in conjunction with the main grid (Rocky et al., 2014). Nano-grids have emerged as a promising technology for providing affordable and reliable electricity to communities in developing countries and improving the resilience of power systems in developed countries. It is a power system that typically serves a single building (Ding et al., 2019) or a small group

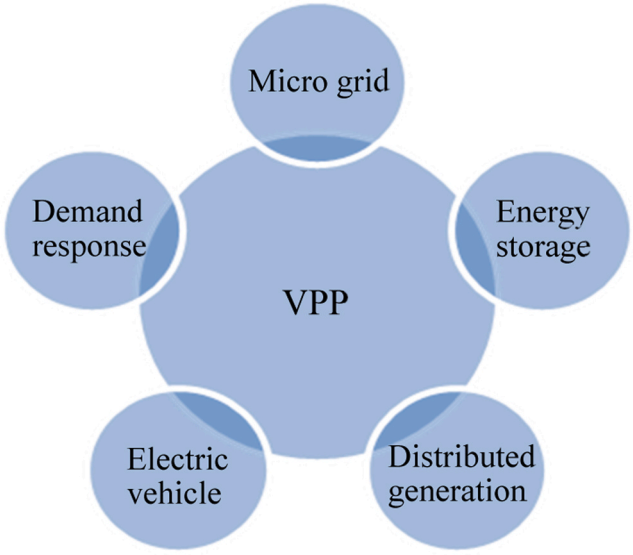

Fig. 8. DER amassed in VVP.

of buildings. Its modularity, flexibility, and scalability allow it to be tailored to the specific energy needs of the end users (Bari et al., 2014). The components of a nano-grid typically include a power source, energy storage system, power electronics, and a control system. The power source may be a renewable energy system, such as solar or wind (Rodriguez-Diaz et al., 2016), or a conventional generator, such as a diesel or gasoline generator. The energy storage system may consist of batteries or other devices that can store excess energy generated by the power source for later use (Willis et al., 2018). The power electronics are used to convert the energy from the power source and energy storage system into a form that the end-users can use, and the control system is used to manage the energy flow within the nano-grid.

Nano-grids are innovative energy systems that offer several benefits over traditional centralized power systems. One of the main advantages of nano-grids is their flexibility and scalability (Judy) making them highly customizable to meet end-users' specific energy needs. Unlike centralized power systems, nano-grids can be designed to provide power to a single building or a small community. This ability to tailor energy solutions to the needs of rural and remote areas is a significant advantage of nano-grids. Another important advantage of nano-grids is their ability to expand or reconfigure to accommodate changing energy needs or the addition of new energy sources. As a result, they can easily adjust to the distinctive energy needs of many communities and geographic areas (Bhattacharyya, 2018).

Nano-grids have a wide range of potential applications, including providing electricity to remote and off-grid areas, improving the resilience of power systems (Kezunovic et al., 2019) in developed countries, and enabling the integration of renewable energy sources into the grid. Nano-grids can improve the power system's resilience by providing backup power in the event of a disruption to the main grid. They are promising technology for providing affordable and reliable electricity to communities in developing countries (Hamatwi et al., 2016) and improving power systems' resilience in developed countries.

3.4. Smart-grid management at the microscopic level

Smart grid management at the microscopic scale refers to the use of advanced control and monitoring systems to optimize the flow of electricity at a very small scale, such as at the level of individual appliances or devices. Smart grid management can be implemented at the microscopic scale by using smart appliances and devices. Smart appliances and devices are equipped with sensors and communication systems to control and monitor them remotely (Depuru et al., 2011). This allows utilities and homeowners to optimize these appliances and devices, reducing energy consumption and costs.

Smart grid management at the microscopic level also involves using advanced algorithms and machine learning techniques to optimize energy distribution and reduce energy waste. These techniques enable the system to predict energy usage patterns and adjust energy distribution accordingly. For example, if the system detects that a particular area is experiencing high energy demand, it can automatically reroute energy from other areas to meet the demand. By doing this, the likelihood of brownouts and blackouts is decreased, in addition to ensuring that energy is delivered more efficiently (Depuru et al., 2011).

In conclusion, smart grid management at the microscopic level is a promising approach to managing energy distribution more efficiently and sustainably. By incorporating advanced technologies, algorithms, and renewable energy sources, this approach reduces energy waste, optimizes energy distribution, and reduces the overall cost of energy management. As society continues to move towards a more sustainable future, smart grid management at the microscopic level will play a critical role in ensuring that we can meet our energy needs while protecting the environment.

3.5. Nanoscale communication networks

A nanoscale communication network in a smart grid refers to using small-scale devices such as nano sensors, nanorobots, and nano cameras to collect, transmit, and analyze data in real-time (Bush and Goel, 2013). The data collected by these devices can be used to monitor energy consumption, detect faults in the power grid, and provide real-time feedback to the grid operators. One of the key advantages of a nanoscale communication network is its ability to detect faults and quickly respond to them. With the help of nano sensors, it is possible to detect and locate faults in the power grid, such as power outages, voltage fluctuations, and system failures. This information can be transmitted in real-time (Abedi et al., 2024) to the grid operators, who can take corrective actions to restore the power supply and prevent further damage to the grid. Also, nano cameras can be used to monitor the power lines and detect any signs of wear and tear, which can help in predicting and preventing potential faults before they occur. Another benefit of a nanoscale communication network in a smart grid is its ability to optimize energy consumption and distribution. With the help of nanorobots, it is possible to control the flow of electricity and manage the energy demand more effectively. For instance, nanorobots can be used to switch off the power supply to certain appliances during peak hours or adjust the voltage levels to match the energy demand. This can help reduce overall energy consumption, reduce the carbon footprint, and save costs for both consumers and energy companies.

4. Wireless power transmission

Wireless power transmission (Fan et al., 2023), also known as wireless energy transmission or wireless energy transfer, refers to the transfer of electrical energy from a power source to a device or load without the use of physical cables or wires (Costanzo et al., 2014; Khan et al., 2020). A range of industries, including consumer electronics and transportation, might be significantly impacted by this technology, which has the potential to transform the way we power electrical gadgets. This section will examine the various wireless power transmission systems and techniques, prospective uses, and technical difficulties.

One of the earliest forms of wireless power transmission was developed by Nikola Tesla in the late 1800s (Yedavalli et al., 2017). Tesla demonstrated the concept by lighting up a lamp wirelessly (Garnica et al., 2013a) using high frequency alternating current (AC) waves. This method, known as electromagnetic induction, is based on the principle that a changing magnetic field can induce a current in a conductor. In Tesla's experiment, the lamp was connected to a resonant circuit tuned to the frequency of the transmitted AC waves. The resonant circuit acted as a transformer, converting the high-frequency AC waves into a lower-frequency current (Xie et al., 2013) that could be used to power the lamp.

Another wireless power transmission method is based on the principle of resonant energy transfer, in which energy is transferred between two objects that are resonating at the same frequency. This method requires using two resonant circuits, one at the transmitter and one at the receiver, which are both tuned to the same frequency. The transmitter circuit generates an oscillating electromagnetic field, which is picked up by the receiver circuit and converted into a usable form of energy (Xie et al., 2013). Wireless power transmission has the potential to revolutionize the way we power electronic devices and could have a wide range of applications in various industries. For example, in the transportation industry, wireless charging pads could be installed on roads and highways to charge electric vehicles (EVs) as they drive over them. It would eliminate the need for plug-in charging stations and make it easier for EVs to travel longer distances. In the healthcare industry, wireless power transmission could power medical devices such as pacemakers, eliminating the need for batteries or external power sources.

Several challenges must be overcome before wireless power

transmission becomes widespread technology. One of the biggest challenges is the limited range (Alam et al., 2024a) of most wireless power transmission systems. Most systems can only transfer energy over a few feet, and the transfer efficiency decreases as the distance between the transmitter and receiver increases. Another challenge is the potential for interference with other electronic devices, as wireless power transmission uses electromagnetic waves that can interfere with different radio frequencies.

Yet, wireless power transmission is a promising technology with the potential to revolutionize how we power electronic devices and could have a wide range of applications in various industries. While challenges need to be overcome, the potential benefits of this technology make it worth exploring and developing further. Several technologies and methods are used for wireless power transmission, including inductive coupling, resonant coupling, radio frequency (RF), laser, and microwave wireless power transmission (Alam et al., 2024a). Each of these technologies and methods has advantages and disadvantages, and the most appropriate method will depend on the application's specific requirements

Inductive coupling and resonant coupling: Inductive coupling and resonant coupling are both techniques that can be used to transmit power wirelessly. Inductive coupling involves using electromagnetic fields to transfer energy from a transmitter to a receiver. This is typically done using two coils of wire: one at the transmitter and one at the receiver (Borges Carvalho et al., 2014). The transmitter coil generates an alternating magnetic field when an electrical current is passed through it, and the receiver coil picks up the alternating magnetic field and converts it into a usable form of electrical energy (Xie et al., 2013). It is used in various wireless power transmission applications, including wireless charging pads for electronic devices and EV charging stations. It is relatively simple and inexpensive to implement but has limited range and efficiency.

Resonant coupling: Resonant coupling, or resonant energy transfer, involves energy transfer between two objects resonating at the same frequency. This is typically done using two resonant circuits, one at the transmitter and one at the receiver. The transmitter circuit generates an oscillating electromagnetic field, which is picked up by the receiver circuit and converted into a usable form of energy. Resonant coupling is typically used for longer range wireless power transmission applications and is less affected by obstacles such as walls and furniture. However, it requires precise frequency matching between the transmitter and receiver and can be more expensive than other methods (Li and Mi, 2015).

Radio frequency: RF communication plays a crucial role in the implementation of a smart grid. RF communication is a key technology that enables the smart grid to achieve these goals. RF communication is used in several smart grid applications such as AMI, distribution automation (DA), and DR. AMI allows utilities to collect real-time data on energy consumption from smart meters installed in homes and businesses. This data is transmitted using RF communication to the utility company, which can then analyze it and provide better customer service. DA involves using sensors, control devices, and communication networks to monitor and control electricity distribution. RF communication transmits data between these devices, enabling utilities to detect and respond to faults quickly. DR programs allow utilities to reduce energy demand during peak periods by incentivizing customers to reduce their energy consumption (Hui et al., 2020). RF communication sends signals to smart devices such as smart thermostats or smart appliances, which can adjust their energy consumption accordingly.

One of the main advantages of RF communication in the smart grid is its ability to provide real-time data on energy consumption. This data can be used to monitor and manage the grid more efficiently, reducing the risk of blackouts and improving the system's overall reliability. RF communication also allows utilities to detect and respond to defects more quickly, resulting in shorter outages and more customer satisfaction. They can assist utilities in making the best use of renewable energy sources. Furthermore, by gathering real-time energy production and consumption data, utilities may match supply and demand more effectively, minimizing the need for fossil-fuel-based power generation. However, there are also some challenges associated with the use of RF communication in the smart grid. One of the main challenges is ensuring the security and privacy of the data transmitted over the communication network.

Microwave wireless power transmission: This method involves using microwaves to transfer energy from a transmitter to a receiver (Wang and Lu, 2023). Microwave wireless power transmission (Dong et al., 2024) can transfer energy over long distances and is not affected by obstacles, but it requires a direct line of sight between the transmitter and receiver and can interfere with other electronic devices that use the same frequency.

Several emerging technologies are being developed for wireless power transmission, including solar power satellites, which use microwaves to transmit energy from a satellite in orbit to a receiver on the ground, and near-field wireless power transmission (Alam et al., 2024b; Wang and Lu, 2023), which uses magnetic fields to transfer energy over short distances without the need for a direct line of sight.

4.1. Far-field

Far-field wireless power transmission, or long-range wireless power transmission, refers to transferring electrical energy over long distances, typically greater than a few meters. This contrasts near-field wireless power transmission, which refers to transferring electrical energy over short distances, typically a few centimeters to a few meters. In general, the range of a far-field wireless power transmission system is determined by the power density of the transmitted electromagnetic field, which is a measure of the intensity of the field at a given distance from the transmitter (Garnica et al., 2013b). Far-field wireless power transmission has the potential to revolutionize the way we power electronic devices and could have a wide range of applications in various industries (Bevacqua et al., 2021). For example, it could charge EVs in motion, power remote sensing and communication devices, and transmit electricity to remote locations. However, several challenges need to be overcome before far-field wireless power transmission can become a widespread technology, including limited range and efficiency, the potential for interference with other electronic devices, and the high cost of implementation.

There are several other factors to consider when discussing far-field wireless power transmission. One of the main challenges of far-field wireless power transmission is most systems' limited range and efficiency. Most systems can only transfer energy over a few meters, and the transfer efficiency decreases as the distance between the transmitter and receiver increases. This means that far-field wireless power transmission is currently only suitable for applications where the transmitter and receiver are relatively close to each other. Another challenge is the potential for interference with other electronic devices, as wireless power transmission uses electromagnetic waves that can interfere with other radio frequencies. This can be especially problematic in crowded urban environments, where many other electronic devices operate in the same frequency range. The high cost of implementation is also a challenge for far-field wireless power transmission (Bevacqua et al., 2021).

Many of the technologies and methods used for far-field wireless power transmission are still in the early stages of development and are not yet commercially viable. It means the cost of implementing far-field wireless power transmission systems is much higher than traditional wired power systems. Despite these obstacles, far-field wireless power transfer has the potential to transform the way we power electronic devices and has a wide range of applications in various industries. It might, for example, be used to charge EVs in motion, power remote sensing and communication devices, and send electricity to faraway locations. As research and development in this sector continue, the range and efficiency of far-field wireless power transmission systems

will likely improve, as will the cost of implementation, making it a more viable option.

5. The future of energy storage

The future of energy storage is very promising (Starke et al., 2021). With the increasing demand for clean and sustainable energy, there is a growing need for efficient and reliable energy storage systems to support renewable energy sources. It will likely be characterized by the continued development and adoption of new and innovative technologies that can store excess energy efficiently and cost-effectively. These technologies will ensure a reliable and stable power supply in an increasingly renewable energy-dependent world. Various trends and advancements are impacting the direction of energy storage in the future (de Sisternes et al., 2016).

Advancements in battery technology: Battery technology is constantly evolving, and advancements are being made to improve its efficiency, capacity, and durability. For example, lithium-ion batteries are becoming increasingly popular due to their high energy density and long cycle life. Researchers are also exploring new materials and chemistries for batteries, such as solid-state batteries, which promise to deliver even higher energy densities and longer lifetimes.

Increased use of renewable energy: As renewable energy sources such as solar and wind power increase, the need for reliable energy storage systems becomes more critical. Energy storage systems can help smooth out these sources' intermittent output, ensuring a more stable and consistent energy supply (Song, 2021).

Growth of EVs: The increasing adoption of EVs drives demand for more efficient and affordable battery technology. As EVs become more widespread, battery costs are expected to continue to fall, making energy storage systems more accessible and affordable.

Development of new energy storage technologies: In addition to batteries, other energy storage technologies are being developed, such as hydrogen fuel cells and thermal energy storage. These technologies have the potential to offer unique advantages in certain applications, such as providing backup power for critical infrastructure. The future of energy storage is very promising (Starke et al., 2021). With the increasing demand for clean and sustainable energy, there is a growing need for efficient and reliable energy storage systems to support renewable energy sources. It will likely be characterized by the continued development and adoption of new and innovative technologies that can store excess energy efficiently and cost-effectively. These technologies will ensure a reliable and stable power supply in an increasingly renewable energy-dependent world. Various trends and advancements are impacting the direction of energy storage in the future (de Sisternes et al., 2016).

Advancements in battery technology: Battery technology is constantly evolving, and advancements are being made to improve its efficiency, capacity, and durability. For example, lithium-ion batteries are becoming increasingly popular due to their high energy density and long cycle life. Researchers are also exploring new materials and chemistries for batteries, such as solid-state batteries, which promise to deliver even higher energy densities and longer lifetimes.

Increased use of renewable energy: As renewable energy sources such as solar and wind power increase, the need for reliable energy storage systems becomes more critical. Energy storage systems can help smooth out these sources' intermittent output, ensuring a more stable and consistent energy supply (Song, 2021).

5.1. Energy storage and cyber security

Energy storage is a crucial aspect of the modern electricity grid, allowing excess energy to be stored and used when needed. Several different technologies can be used for energy storage, including batteries, flywheels, pumped hydro (Djelailia et al., 2019), and compressed air energy storage (CAES) (Jayachandran et al., 2021). Like any other critical infrastructure, energy storage systems are vulnerable to cyber-attacks, and there are several ways by which they can be targeted. For example, attackers may try to gain unauthorized access to the system and manipulate the stored energy, or they may try to disrupt the system's operations (Ghosh et al., 2018) by introducing malware or other malicious software. To protect against these threats, energy storage systems must be designed with robust cybersecurity measures that include encryption, access control, and intrusion detection.

Encryption is the process of encoding data so only authorized users can access it. It can protect sensitive data, such as user credentials, from cybercriminals intercepting it. Access control is another important cybersecurity measure that limits access to the system to authorized users only. This can be achieved through passwords, biometric authentication, or other security measures (Elmenyawi et al., 2024). Intrusion detection systems can also identify and respond to potential cyber threats. These systems monitor the energy storage system for unusual activity or behavior and alert system administrators if any suspicious activity is detected.

In addition to these technical cybersecurity measures, it is also important to have policies and procedures in place to ensure energy storage systems' safe and secure operation. This includes training for system operators, regular security assessments, and incident response plans.

5.2. Flow battery

Flow batteries are rechargeable batteries that use two electrolyte solutions to store and release energy. Unlike traditional batteries, which store energy in solid electrodes, flow batteries use liquid electrolytes that flow through a membrane to produce electricity. This design allows for a high degree of flexibility in capacity, energy density, and charging times. In a flow battery system, the two electrolytes are stored in separate tanks (Morozov et al., 2024) and are pumped through a series of electrodes when electricity is needed. When the electrolytes meet at the membrane, they undergo a chemical reaction that produces an electrical charge. The charged electrolytes are then pumped back into their respective tanks until they are needed again.

One of the key advantages of flow batteries is their scalability. By simply increasing the size of the tanks and the membrane, flow batteries can be easily expanded to meet the energy storage needs of various applications, from small-scale residential use to large-scale utility applications. Also, their ability to discharge energy over long periods. They are also environmentally friendly, as they do not contain the heavy metals or toxic chemicals in some traditional batteries. Intermittent renewable energy sources like wind and solar produce energy at varying levels during the day, which makes them a great match for storing energy (Quirós et al., 2023; Guan and Huang, 2021).

However, flow batteries have some limitations, including their relatively low energy density compared to traditional batteries and the cost of the large tanks and membranes required for scalability. Despite these challenges, flow batteries are becoming an increasingly popular choice for energy storage, particularly in applications with critical long-term energy storage and flexibility, such as off-grid or remote locations.

5.3. Supercapacitors

Supercapacitors, also known as ultracapacitors, are energy storage devices (Zhao et al., 2017) that have gained popularity recently due to their high-power density, fast charging times, and long cycle life. Unlike traditional batteries, which store energy in chemical reactions, supercapacitors store energy electrostatically in an electrostatic field between two conductive plates. These plates are typically made of activated carbon or other high-surface-area materials separated by an electrolyte. When a voltage is applied, ions in the electrolyte accumulate on the surface of the plates, creating an electrostatic charge that can be used to power electronic devices or store energy for later use (Chen et al., 2018).

One of the key advantages of supercapacitors is their ability to charge and discharge quickly, making them ideal for applications that require rapid energy delivery, such as EVs or power tools. Supercapacitors also have a longer cycle life than traditional batteries, which can be charged and discharged many times without degrading performance.

Supercapacitors also have a high-power density, meaning they can deliver a large amount of energy in a short amount of time. This makes them particularly well-suited for applications that require bursts of power, such as starting a car engine or powering a camera flash. However, there are some limitations to supercapacitors. One of the main drawbacks is their relatively low energy density (Burke, 2000) compared to traditional batteries, which limits their ability to store large amounts of energy for long periods. Supercapacitors can be more expensive than conventional batteries, particularly for high-capacity applications. Despite these limitations, supercapacitors are a promising energy storage and power delivery technology. They are well-suited for applications requiring fast charging times, high power density, and long cycle life. They are increasingly used in various industries, including automotive, aerospace, and renewable energy. With ongoing research and development, supercapacitors will likely continue to play an important role in the future of energy storage and power delivery (Burke, 2000).

5.4. Energy internet

There has been a growing interest in developing an energy internet in smart grid systems in recent years. The concept of an energy internet involves the integration of renewable energy sources, energy storage systems, and traditional energy sources into a cohesive and interconnected network (Kawoosa and Prashar, 2021). Energy internet would allow for more efficient and cost-effective energy distribution and management, reducing carbon emissions and reliance on nonrenewable energy sources. Energy storage systems such as batteries and pumped hydro storage are also critical components of the energy internet. These systems allow excess energy from renewable sources to be stored and used during periods of high demand or when renewable sources are not producing energy. This helps to ensure a consistent and reliable supply of energy to consumers. The energy internet also incorporates traditional energy sources such as coal, natural gas, and nuclear power. Integrating these sources into the energy internet can be used more efficiently and effectively, reducing waste and minimizing carbon emissions.

5.5. The proliferation of EVs and charging points

The rise of EVs is a significant shift in global transportation, driven by technological advancements and environmental concerns. The transition is seen as a strategy to reduce greenhouse gas emissions, mitigate climate change, and decrease dependence on fossil fuels. The evolution of EV technology has improved vehicle performance, range, and affordability, with advancements in lithium-ion battery technology, solid-state batteries, lithium-sulfur batteries, electric motors, power electronics, thermal management systems, regenerative braking systems, autonomous driving capabilities, and vehicle-to-everything communication systems (Bharathidasan et al., 2022).

The widespread adoption of EVs is linked to the availability of robust charging infrastructure. Public charging stations have seen exponential growth, with innovations in residential charging solutions and ultra-fast chargers being crucial for long-distance travel. Government policies play a pivotal role in fostering the adoption of EVs and developing charging infrastructure, with financial incentives, emission regulations, and collaboration between governments and private enterprises.

Despite significant progress, challenges impede the widespread adoption of EVs, including concerns about vehicle range and charging points, expanding and optimizing the charging network, ensuring the economic viability of EVs and charging infrastructure (Cao et al., 2023a), and addressing the environmental impact of battery production, recycling, and disposal. Cyber threats pose a growing concern for the EV ecosystem (Khalaf et al., 2024), necessitating robust cybersecurity measures to protect data, maintain charging network integrity, and ensure the safety and reliability of EV operations.

5.6. Smart grid 2.0

Smart grid 2.0 is an advanced version of the smart grid that enhances the existing infrastructure by integrating new technologies and capabilities. This upgraded system is designed to improve the efficiency and sustainability of the smart grid (Xinhua and Lianshun, 2014). It aims to enhance the grid's flexibility, resilience, and reliability (Curiale, 2014) to accommodate renewable energy sources better and support the transition to a low-carbon economy. Smart grid 2.0 incorporates several new technologies and capabilities that were not available when the first generation of the smart grid was developed (Cespedes, 2013). Some of the key features of smart grid 2.0 include:

- Advanced analytics and machine learning: Advanced analytics and machine learning are used in smart grid 2.0 to increase the precision of demand forecasting, energy usage monitoring, and grid optimization. With these technologies, utilities may better control energy demand and supply, reduce energy waste, and use RES best.
- Distributed energy resources integration: With DERs integrated into the grid, such as solar panels, wind turbines, and energy storage systems, the grid may be supplied with energy during high demand and can absorb extra energy during off-peak hours. This is known as smart grid 2.0. With this skill, utilities may control grid stability more effectively, increase reliability, and use RESs more frequently.
- Cybersecurity: To safeguard the grid from cyberattacks and guarantee the dependability and security of the electric power system, smart grid 2.0 combines cutting-edge cybersecurity measures. These precautions include capability for incident response, threat identification, and real-time monitoring.
- Blockchain technology: Blockchain technology is used in smart grid 2.0 to increase the security and transparency of energy transactions (Cao et al., 2023b), allowing utilities to manage the energy markets better and promote the integration of new energy services and business models. In conclusion, the energy internet in smart grid systems has numerous advantages, including enhanced efficiency, reliability, and sustainability. They will become increasingly significant in controlling and distributing energy cost effectively and environmentally sustainably as the globe transitions toward RESs (Mohammed et al., 2024).

It is worth noting that, from the standpoint of smart grid 2.0, which entails linked, massive power networks across nations or regions, cyberattacks have the potential to cause catastrophic damage (Lewis).

6. Conclusion

This comprehensive review has delved into the multifaceted impact of cyber-physical attacks on future energy systems, with an emphasis on the smart grid. As a modernized electricity grid, the smart grid leverages advanced technologies to enhance energy efficiency, integrate renewable energy sources, and facilitate the monitoring and forecasting of energy demand. However, the inherent complexity and heterogeneity of the smart grids expose it to diverse cyber threats, both malicious and non-malicious, posing significant risks to the energy system's security and reliability. A key innovation of our work is the proposal of a multidisciplinary framework that synergizes elements from cybersecurity, energy systems engineering, and policy analysis. This framework presents a comprehensive understanding of the smart grid's vulnerabilities and the necessary protective measures. We have also identified and highlighted future research directions and emerging technologies

that are vital for advancing the field. These include the integration of the smart grid with IoT and virtual reality, as well as the exploration of new concepts like nanogrids, wireless power transmission, and VPP. In light of our findings, it is imperative for the energy industry to prioritize cybersecurity to safeguard the smart grid's operation. This encompasses adopting robust security solutions like network security protocols, encryption, and advanced security analytics tools, as well as fostering a culture of cybersecurity through employee training and awareness programs. The paper underscores the significance of implementing comprehensive monitoring and control systems, regular maintenance, and personnel training to mitigate the impact of non-malicious attacks. In conclusion, our review elucidates the criticality of cybersecurity in the secure and dependable functioning of future energy systems. To realize the full potential of the smart grid and ensure a sustainable, secure energy future, continuous research, innovation, and a proactive approach to cybersecurity are indispensable.

6.1. Policy implementation

Implementing effective policies is crucial for the successful deployment and operation of smart grids. Based on the findings of this study, the following policy recommendations are proposed:

- Incentivize technology adoption: Governments should provide financial incentives, such as tax credits and grants, to encourage utilities and consumers to adopt smart grid technologies. This can accelerate the transition to a more efficient and resilient energy infrastructure.
- Enhance cybersecurity regulations: Regulatory bodies should establish stringent cybersecurity standards for smart grid systems. This includes mandating regular security assessments, implementing robust encryption protocols, and requiring utilities to have comprehensive incident response plans in place.
- Promote renewable integration: Policies should support the integration of renewable energy sources by facilitating the deployment of DER and energy storage systems. This can be achieved through streamlined permitting processes, subsidies for renewable energy installations, and mandates for renewable energy targets.
- Data privacy and security: Regulations should ensure the protection of consumer data by enforcing strict data privacy laws and requiring utilities to implement secure data handling practices. This includes the use of advanced encryption techniques and secure communication protocols.
- Support research and development: Governments should invest in research and development initiatives aimed at advancing smart grid technologies and addressing emerging cybersecurity threats. This can include funding for academic research, public-private partnerships, and innovation hubs focused on smart grid solutions.

6.2. Findings

- Increasing sophistication of cyber-physical attacks: Recent case studies reveal that cyber-physical attacks on energy systems are becoming more sophisticated and coordinated, posing significant risks to the security and reliability of smart grids.
- Efficacy of current cybersecurity measures: While current cybersecurity measures such as intrusion detection systems, encryption, and access controls are effective to some extent, they need continuous improvement to keep pace with evolving threats.
- Importance of advanced technologies: The integration of advanced technologies like machine learning, blockchain, and advanced analytics is essential for enhancing the detection, prevention, and response to cyber-physical threats in energy systems.
- Need for a holistic approach: The proposed multidisciplinary framework highlights the necessity of combining technical, engineering, and policy perspectives to develop robust solutions for cyber-physical security.
- Role of DERs: The study emphasizes the importance of optimizing the control and coordination of DERs, such as solar panels and energy storage systems, to increase grid resilience and reduce reliance on centralized power plants.
- Emergence of VPPs: VPPs are identified as a promising approach to managing DER by aggregating them into a single virtual entity. However, challenges related to communication, control systems, and cybersecurity need to be addressed.

By addressing these findings, the study contributes valuable insights into the current landscape of cybersecurity threats and the evolving strategies and technologies to counteract them, offering a roadmap for future research and policy development in the field of cyber-physical security for energy systems.

6.3. Limitations and future directions

The article explores the increasing sophistication of cyber-physical attacks on energy systems, providing detailed case studies and analyzing advanced cybersecurity technologies such as machine learning, blockchain, and advanced analytics. It highlights the importance of a multidisciplinary approach that combines cybersecurity, energy systems engineering, and policy analysis to protect smart grids from evolving threats. However, the study points out a number of issues that need to be fixed. For example, there should be more case studies from different parts of the world and with different kinds of energy systems. There should also be more research into how advanced technologies can be used in real life, and there should be a full cost-benefit analysis to see what the financial effects and economic benefits of better cyber-physical security measures are.

Future work should address these limitations by expanding case studies to provide a global perspective, delving into the technical details of integrating advanced technologies into existing infrastructures, and conducting detailed cost-benefit analyses. Additionally, future research should collect empirical data from real-world implementations, emphasize organizational and human aspects of cybersecurity, and develop specific policy guidelines tailored to different regulatory environments. To move the field of cyber-physical security in energy systems forward and make sure there are complete and useful solutions for protecting critical infrastructure, it will also be important to look into new threats, trends, and ways to combine strategies from different fields.

Authors statement

The authors equally contributed to all aspects of this manuscript, including study conception and design, data collection, data analysis, interpretation of results, and manuscript preparation.

CRediT authorship contribution statement

Sayawu Diaba: Writing – original draft, Conceptualization. **Mohammed Elmusrati:** Writing – review & editing, Supervision. **Miadreza Shafie-khah:** Writing – review & editing, Supervision.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data Availability

No data was used for the research described in the article.

References

Abedi, A.F.A., Goh, P., Alkhayyat, A., 2024. Nano-sensors communications and networking for healthcare systems: Review and outlooks (Sep.). J. Comput. Sci. vol. 81. https://doi.org/10.1016/j.jocs.2024.102367.

Abolade, O., et al., 2021. Overhead effects of data encryption on TCP throughput across IPSEC secured network (Sep.). Sci. Afr. vol. 13. https://doi.org/10.1016/j.sciaf.2021.e00855.

K.S. Alam *et al.*, "Towards net zero: A technological review on the potential of space-based solar power and wireless power transmission," May 15, 2024a, Elsevier Ltd. doi: 10.1016/j.heliyon.2024.e29996.

K.S. Alam *et al.*, "Towards net zero: A technological review on the potential of space-based solar power and wireless power transmission," May 15, 2024b, Elsevier Ltd. doi: 10.1016/j.heliyon.2024.e29996.

Aleluya, E.R.M., Vicente, C.T., 2018. Faceture ID: Face and hand gesture multi-factor authentication using deep learning. in *Procedia Computer Science*. Elsevier B.V., pp. 147–154. https://doi.org/10.1016/j.procs.2018.08.160

B. Alohali, M. Merabti, and K. Kifayat, *A New Key Management Scheme for Home Area Network (HAN) In Smart Grid*. 2014. [Online]. Available: ⟨https://www.researchgate.net/publication/303524586⟩.

I. Alotaibi, M.A. Abido, M. Khalid, and A.V. Savkin, "A comprehensive review of recent advances in smart grids: A sustainable future with renewable energy resources," Dec. 01, 2020, MDPI AG. doi: 10.3390/en13236269.

Amin, M., El-Sousy, F.F.M., Aziz, G.A.A., Gaber, K., Mohammed, O.A., 2021. CPS attacks mitigation approaches on power electronic systems with security challenges for smart grid applications: a review. IEEE Access vol. 9, 38571–38601. https://doi.org/10.1109/ACCESS.2021.3063229.

ANON "Analysis of System and Interoperability Impact from Securing Communications for Distributed Energy Resources".

Aurangzeb, M., et al., 2024. Enhancing cybersecurity in smart grids: Deep black box adversarial attacks and quantum voting ensemble models for blockchain privacy-preserving storage (Jun.). Energy Rep. vol. 11, 2493–2515. https://doi.org/10.1016/j.egyr.2024.02.010.

Ayar, M., Obuz, S., Trevizan, R.D., Bretas, A.S., Latchman, H.A., 2017. A Distributed Control Approach for Enhancing Smart Grid Transient Stability and Resilience (Nov.). IEEE Trans. Smart Grid vol. 8 (6), 3035–3044. https://doi.org/10.1109/TSG.2017.2714982.".

Bai, X., Fan, Y., Hao, R., Yu, J., 2024. Data-driven virtual power plant aggregation method. Electr. Eng. https://doi.org/10.1007/s00202-024-02544-z.

A. Bari, J. Jiang, W. Saad, and A. Jaekel, "Challenges in the smart grid applications: An overview," 2014. doi: 10.1155/2014/974682.

M. Beaudin and H. Zareipour, "Home energy management systems: A review of modelling and complexity," 2015, Elsevier Ltd. doi: 10.1016/j.rser.2015.01.046.

Bera, S., Misra, S., Rodrigues, J.J.P.C., 2015. Cloud Computing Applications for Smart Grid: A Survey, 1 May IEEE Trans. Parallel Distrib. Syst. vol. 26 (5), 1477–1494. https://doi.org/10.1109/TPDS.2014.2321378.".

Bevacqua, M.T., Bellizzi, G.G., Merenda, M., 2021. An efficient far-field wireless power transfer via field intensity shaping techniques (Jul.). Electron. (Switz.) vol. 10 (14). https://doi.org/10.3390/electronics10141609.

M. Bharathidasan, V. Indragandhi, V. Suresh, M. Jasiński, and Z. Leonowicz, "A review on electric vehicle: Technologies, energy trading, and cyber security," Nov. 01, 2022, Elsevier Ltd. doi: 10.1016/j.egyr.2022.07.145.

Bhattacharyya, S.C., 2018. Mini-grids for the base of the pyramid market: A critical review (Apr.). Energ. (Basel) vol. 11 (4). https://doi.org/10.3390/en11040813.

Borges Carvalho, N., et al., 2014. Wireless Power Transmission: R&D Activities Within Europe,' in (April). IEEE Trans. Microw. Theory Tech. vol. 62 (4), 1031–1045. https://doi.org/10.1109/TMTT.2014.2303420.

Bottani, E., Vignali, G., 2019. Augmented reality technology in the manufacturing industry: A review of the last decade (Mar.). IISE Trans. vol. 51 (3), 284–310. https://doi.org/10.1080/24725854.2018.1493244.

Brown, R.E., 2008. Impact of Smart Grid on distribution system design. 2008 IEEE Power Energy Soc. Gen. Meet. - Convers. Deliv. Electr. Energy 21st Century, Pittsburgh, PA, USA 1–4. https://doi.org/10.1109/PES.2008.4596843.

A. Burke, "Ultracapacitors: why, how, and where is the technology," 2000. [Online]. Available: ⟨www.elsevier.comrlocaterjpowsour⟩.

Bush, S.F., Goel, S., 2013. Persistence Length as a Metric for Modeling and Simulation of Nanoscale Communication Networks (December). IEEE J. Sel. Areas Commun. vol. 31 (12), 815–824. https://doi.org/10.1109/JSAC.2013.SUP2.12130014.

Y. Cao *et al.*, "Towards cyber security for low-carbon transportation: Overview, challenges and future directions," Sep. 01, 2023a, Elsevier Ltd. doi: 10.1016/j.rser.2023.113401.

Y.N. Cao, Y. Wang, Y. Ding, Z. Guo, Q. Wu, and H. Liang, "Blockchain-empowered security and privacy protection technologies for smart grid," Apr. 01, 2023b, Elsevier B.V. doi: 10.1016/j.csi.2022.103708.

Cardenas, D.J.S., Hahn, A., Liu, C.-C., 2020. Assessing Cyber-Physical Risks of IoT-Based Energy Devices in Grid Operations. IEEE Access vol. 8, 61161–61173. https://doi.org/10.1109/ACCESS.2020.2983313.

Cespedes, R., 2013. Planning the electrical energy system 2.0 with Smart Grids. 2013 IEEE Power Energy Soc. Gen. Meet., Vanc., BC, Can. 1–4. https://doi.org/10.1109/PESMG.2013.6673065.

Chaichi, N., Lavoie, J., Zarrin, S., Khalifa, R., Sie, F., 2015. A comprehensive assessment of cloud computing for smart grid applications: a multi-perspectives framework. 2015 Portland Int. Conf. Manag. Eng. Technol. (PICMET), Portland, OR, USA 2541–2547. https://doi.org/10.1109/PICMET.2015.7273227.".

H. Chen *et al.*, "Exploring Chemical, Mechanical, and Electrical Functionalities of Binders for Advanced Energy-Storage Devices," Sep. 26, 2018, American Chemical Society. doi: 10.1021/acs.chemrev.8b00241.

Chen, C., Guo, H., Wu, Y., Gao, Y., Liu, J., 2023. A novel two-factor multi-gateway authentication protocol for WSNs (Mar.). Ad Hoc Netw. vol. 141. https://doi.org/10.1016/j.adhoc.2023.103089.

CHERIFI, T., HAMAMI, L., 2018. A practical implementation of unconditional security for the IEC 60780-5-101 SCADA protocol (Mar.). Int. J. Crit. Infrastruct. Prot. vol. 20, 68–84. https://doi.org/10.1016/j.ijcip.2017.12.001.

Costanzo, A., et al., 2014. Electromagnetic energy harvesting and wireless power transmission: a unified approach (Nov.). Proc. IEEE vol. 102 (11), 1692–1711. https://doi.org/10.1109/JPROC.2014.2355261.".

Curiale, M., 2014. From smart grids to smart city. 2014 Saudi Arab. Smart Grid Conf. (SASG), Jeddah, Saudi Arab. 1–9. https://doi.org/10.1109/SASG.2014.7274280.

De Lacerda Filho, E.M., Filho, G.P.P.R., De Sousa, R.T., Goncalves, V.P., 2022. Improving Data Security, Privacy, and Interoperability for the IEEE Biometric Open Protocol Standard. IEEE Access vol. 10, 26985–27001. https://doi.org/10.1109/ACCESS.2020.3046630.

de Sisternes, F.J., Jenkins, J.D., Botterud, A., 2016. The value of energy storage in decarbonizing the electricity sector (Aug.). Appl. Energy vol. 175, 368–379. https://doi.org/10.1016/j.apenergy.2016.05.014.

Depuru, S.S.S.R., Wang, L., Devabhaktuni, V., Gudi, N., 2011. Smart meters for power grid — Challenges, issues, advantages and status. 2011 IEEE/PES Power Syst. Conf. Expo., Phoenix, AZ, USA 1–7. https://doi.org/10.1109/PSCE.2011.5772451.

Diamantoulakis, P.D., Kapinas, V.M., Karagiannidis, G.K., 2015. Big Data Analytics for Dynamic Energy Management in Smart Grids (Sep.). Big Data Res. vol. 2 (3), 94–101. https://doi.org/10.1016/j.bdr.2015.03.003.

Ding, Y., Wang, Z., Liu, S., Wang, X., 2019. Energy management strategy of pv grid-connected household nano-grid system. 2019 IEEE Power Energy Soc. Gen. Meet. (PESGM), Atlanta, GA, USA 1–5. https://doi.org/10.1109/PESGM40551.2019.8973404.".

Dinh, H.T., Yun, J., Kim, D.M., Lee, K.-H., Kim, D., 2020. A Home Energy Management System With Renewable Energy and Energy Storage Utilizing Main Grid and Electricity Selling. IEEE Access vol. 8, 49436–49450. https://doi.org/10.1109/ACCESS.2020.2979189.".

Djelailia, O., Necaibia, S., Kelaiaia, M.S., Merad, F., Labar, H., Chouial, H., 2019. Optimal Fuel Consumption Planning and Energy Management Strategy for a Hybrid Energy System with Pumped Storage. 2019 1st Int. Conf. Sustain. Renew. Energy Syst. Appl. (ICSRESA), Tebessa, Algeria 1–6. https://doi.org/10.1109/ICSRESA49121.2019.9182506.

Dong, H.J., Cho, J., Lee, H.L., 2024. Low complexity on-board vector calibration network for optimal microwave wireless power transmission and enhanced RF-to-DC conversion efficiency (Jun.). Appl. Energy vol. 363. https://doi.org/10.1016/j.apenergy.2024.123030.

Dong, Z.Y., Zhang, Y., 2021. Interdisciplinary vision of the digitalized future energy systems. IEEE Open Access J. Power Energy vol. 8, 557–569. https://doi.org/10.1109/OAJPE.2021.3108937.

Elmenyawi, M.A., Abdel Aziem, N.M., Bahaa-Eldin, A.M., 2024. Efficient and secure color image encryption system with enhanced speed and robustness based on binary tree (Sep.). Egypt. Inform. J. vol. 27. https://doi.org/10.1016/j.eij.2024.100487.

Y. Fan, L. Zhang, D. Li, and Z. Wang, "Progress in self-powered, multi-parameter, micro sensor technologies for power metaverse and smart grids," Dec. 15, 2023, Elsevier Ltd. doi: 10.1016/j.nanoen.2023.108959.

Fang, X., Misra, S., Xue, G., Yang, D., 2012. 'Smart Grid — The New and Improved Power Grid: A Survey (Fourth Quarter). IEEE Commun. Surv. Tutor. vol. 14 (4), 944–980. https://doi.org/10.1109/SURV.2011.101911.00087.".

Farraj, A., Hammad, E., Kundur, D., 2018. A Cyber-Physical Control Framework for Transient Stability in Smart Grids (March). IEEE Trans. Smart Grid vol. 9 (2), 1205–1215. https://doi.org/10.1109/TSG.2016.2581588.".

Fu, R., Wang, L., 2024. Research on control and management of smart grid optical network based on optical transmission control Protocol (OTN) technology (Aug.). Therm. Sci. Eng. Prog. vol. 53, 102763. https://doi.org/10.1016/j.tsep.2024.102763.

Fullerton, R.A., Punj, G., 2004. Repercussions of promoting an ideology of consumption: Consumer misbehavior (Nov.). J. Bus. Res vol. 57 (11), 1239–1249. https://doi.org/10.1016/S0148-2963(02)00455-1.

Garnica, J., Chinga, R.A., Lin, J., 2013a. Wireless power transmission: from far field to near field (June). Proc. IEEE vol. 101 (6), 1321–1331. https://doi.org/10.1109/JPROC.2013.2251411.

Garnica, J., Chinga, R.A., Lin, J., 2013b. Wireless Power Transmission: From Far Field to Near Field (June). Proc. IEEE vol. 101 (6), 1321–1331. https://doi.org/10.1109/JPROC.2013.2251411.

Gharavi, H., Chen, H.-H., Wietfeld, C., 2015. Guest Editorial Special Section on Cyber-Physical Systems and Security for Smart Grid (Sept.). IEEE Trans. Smart Grid vol. 6 (5), 2405–2408. https://doi.org/10.1109/TSG.2015.2464911.".

Ghosh, S., Ali, M.H., Dasgupta, D., 2018. Effects of Cyber-Attacks on the Energy Storage in a Hybrid Power System. 2018 IEEE Power Energy Soc. Gen. Meet. (PESGM), Portland, OR, USA 1–5. https://doi.org/10.1109/PESGM.2018.8586636.

Giordano, V., Fulli, G., 2012. A business case for smart grid technologies: a systemic perspective. Energy Policy vol. 40 (1), 252–259. https://doi.org/10.1016/j.enpol.2011.09.066.

V. Gkioulos and N. Chowdhury, "Cyber security training for critical infrastructure protection: A literature review," May 01, 2021, Elsevier Ireland Ltd. doi: 10.1016/j.cosrev.2021.100361.

Guan, W., Huang, X., 2021. A Modular Active Balancing Circuit for Redox Flow Battery Applied in Energy Storage System. IEEE Access vol. 9, 127548–127558. https://doi.org/10.1109/ACCESS.2021.3112902.
Gunduz, M.Z., Das, R., 2018. Analysis of cyber-attacks on smart grid applications. 2018 Int. Conf. Artif. Intell. Data Process. (IDAP), Mal., Turk. 1–5. https://doi.org/10.1109/IDAP.2018.8620728.
Gunduz, M.Z., Das, R., 2020a. Cyber-security on smart grid: threats and potential solutions (Mar.). Comput. Netw. vol. 169. https://doi.org/10.1016/j.comnet.2019.107094.
Gunduz, M.Z., Das, R., 2020b. Cyber-security on smart grid: Threats and potential solutions (Mar.). Comput. Netw. vol. 169. https://doi.org/10.1016/j.comnet.2019.107094.
Gungor, V.C., et al., 2011. Smart Grid Technologies: Communication Technologies and Standards (Nov.). IEEE Trans. Ind. Inform. vol. 7 (4), 529–539. https://doi.org/10.1109/TII.2011.2166794.".
Guo, Y., Wan, Z., Cheng, X., 2022. When blockchain meets smart grids: A comprehensive survey (Jun.). High. -Confid. Comput. vol. 2 (2). https://doi.org/10.1016/j.hcc.2022.100059.
Hamatwi, E., Davidson, I.E., Agee, J., Venayagamoorthy, G., 2016. Model of a hybrid distributed generation system for a DC nano-grid. 2016 Clemson Univ. Power Syst. Conf. (PSC), Clemson, SC, USA 1–8. https://doi.org/10.1109/PSC.2016.7462851.
Hanggoro, D., Windiatmaja, J.H., Muis, A., Sari, R.F., Pournaras, E., 2024. Energy-aware Proof-of-Authority: Blockchain Consensus for Clustered Wireless Sensor Network (Jun.). Block.: Res. Appl., 100211. https://doi.org/10.1016/j.bcra.2024.100211.
M.K. Hasan, R.A. Abdulkadir, S. Islam, T.R. Gadekallu, and N. Safie, "A review on machine learning techniques for secured cyber-physical systems in smart grid networks," Jun. 01, 2024, Elsevier Ltd. doi: 10.1016/j.egyr.2023.12.040.
Hassan, M.K., Habib, A.K.M.Ahasan, Shukur, Zarina, Ibrahim, Fazil, Islam, Shayla, Razzaque, Md. Abdur, Hasan, Mohammad Kamrul, 2023. Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations (a). J. Netw. Comput. Appl.
He, H., Yan, J., 2016. Cyber-physical attacks and defences in the smart grid: a survey (Dec.). IET Cyber-Phys. Syst.: Theory Appl. vol. 1 (1), 13–27. https://doi.org/10.1049/iet-cps.2016.0019.
M.S. Hossain, N.A. Madlool, N.A. Rahim, J. Selvaraj, A.K. Pandey, and A.F. Khan, "Role of smart grid in renewable energy: An overview," Jul. 01, 2016, Elsevier Ltd. doi: 10.1016/j.rser.2015.09.098.
H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, and J. Yan, "5G network-based Internet of Things for demand response in smart grid: A survey on application potential," Jan. 01, 2020, Elsevier Ltd. doi: 10.1016/j.apenergy.2019.113972.
Jayachandran, M., Reddy, C.R., Padmanaban, S., Milyani, A.H., 2021. Operational planning steps in smart electric power delivery system (Dec.). Sci. Rep. vol. 11 (1). https://doi.org/10.1038/s41598-021-96769-8.
Jha, A.V., et al., 2021. Smart grid cyber-physical systems: communication technologies, standards and challenges (May). Wirel. Netw. vol. 27 (4), 2595–2613. https://doi.org/10.1007/s11276-021-02579-1.
Judy, "Title Future Roles of Milli-, Micro-, and Nano-Grids." [Online]. Available: ⟨https://escholarship.org/uc/item/8214x1t7⟩.
Kappagantu, R., Daniel, S.A., 2018. Challenges and issues of smart grid implementation: A case of Indian scenario (Dec.). J. Electr. Syst. Inf. Technol. vol. 5 (3), 453–467. https://doi.org/10.1016/j.jesit.2018.01.002.
Kawoosa, A.I., Prashar, D., 2021. A review of cyber securities in smart grid technology. 2021 2nd Int. Conf. Comput., Autom. Knowl. Manag. (ICCAKM), Dubai, U. Arab Emir. 151–156. https://doi.org/10.1109/ICCAKM50778.2021.9357698.
Kezunovic, M., Soleimani, M., Abu-Rub, H., Bayhan, S., Trabelsi, M., 2019. Hardware in the Loop Simulation of a Nano-Grid Transactive Energy Exchange. 2019 2nd Int. Conf. Smart Grid Renew. Energy (SGRE), Doha, Qatar 1–6. https://doi.org/10.1109/SGRE46976.2019.9020686.
Khalaf, M., Ayad, A., Tushar, M.H.K., Kassouf, M., Kundur, D., 2024. A Survey on Cyber-Physical Security of Active Distribution Networks in Smart Grids. IEEE Access vol. 12, 29414–29444. https://doi.org/10.1109/ACCESS.2024.3364362.
S.R. Khan, S.K. Pavuluri, G. Cummins, and M.P.Y. Desmulliez, "Wireless power transfer techniques for implantable medical devices: A review," Jun. 01, 2020, MDPI AG. doi: 10.3390/s20123487.
Labrador Rivas, A.E., da Silva, N., Abrão, T., 2020. Adaptive current harmonic estimation under fault conditions for smart grid systems (Jun.). Electr. Power Syst. Res. vol. 183. https://doi.org/10.1016/j.epsr.2020.106276.
Langer, L., Smith, P., Hutle, M., Schaeffer-Filho, A., 2016. Analysing cyber-physical attacks to a smart grid: a voltage control use case. 2016 Power Syst. Comput. Conf. (PSCC), Genoa, Italy 1–7. https://doi.org/10.1109/PSCC.2016.7540819.
Lee, J.-M., Hong, S., 2020. Keeping Host Sanity for Security of the SCADA Systems. IEEE Access vol. 8, 62954–62968. https://doi.org/10.1109/ACCESS.2020.2983179.
J.A. Lewis, "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats." [Online]. Available: ⟨https://www.researchgate.net/publication/245508226⟩.
Li, S., Mi, C.C., 2015. Wireless Power Transfer for Electric Vehicle Applications (March). IEEE J. Emerg. Sel. Top. Power Electron. vol. 3 (1), 4–17. https://doi.org/10.1109/JESTPE.2014.2319453.
Liang, H., Tamang, A.K., Zhuang, W., Shen, X.S., 2014. Stochastic information management in smart grid (Third Quarter). IEEE Commun. Surv. Tutor. vol. 16 (3), 1746–1770. https://doi.org/10.1109/SURV.2014.020614.00115.
Lima, M., Lima, R., Lins, F., Bonfim, M., 2022. Beholder – A CEP-based intrusion detection and prevention systems for IoT environments (Sep.). Comput. Secur vol. 120. https://doi.org/10.1016/j.cose.2022.102824.
Liu, N., Tan, L., Sun, H., Zhou, Z., Guo, B., 2022. Bilevel heat–electricity Energy sharing for integrated energy systems with energy hubs and prosumers,' (June). IEEE Trans. Ind. Inform. vol. 18 (6), 3754–3765. https://doi.org/10.1109/TII.2021.3112095.".
Lu, Z., Lu, X., Wang, W., Wang, C., 2010. Review and evaluation of security threats on the communication networks in the smart grid. 2010 - MILCOM 2010 MILITARY Commun. Conf., San. Jose, CA, USA 1830–1835. https://doi.org/10.1109/MILCOM.2010.5679551.
Mahapatra, B., Nayyar, A., 2022. Home energy management system (HEMS): concept, architecture, infrastructure, challenges and energy management schemes (Aug.). Energy Syst. vol. 13 (3), 643–669. https://doi.org/10.1007/s12667-019-00364-w.
Malik, A.S., Bouzguenda, M., 2013. Effects of smart grid technologies on capacity and energy savings - a case study of Oman (Jun.). Energy vol. 54, 365–371. https://doi.org/10.1016/j.energy.2013.03.025.
Masoni, R., et al., 2017. Supporting Remote Maintenance in Industry 4.0 through Augmented Reality. in *Procedia Manufacturing*. Elsevier B.V., pp. 1296–1302. https://doi.org/10.1016/j.promfg.2017.07.257
Mendes, T.D.P., Godina, R., Rodrigues, E.M.G., Matias, J.C.O., Catalão, J.P.S., 2015. Smart home communication technologies and applications: Wireless protocol assessment for home area network resources. Energ. (Basel) vol. 8 (7), 7279–7311. https://doi.org/10.3390/en8077279.
Merdanoğlu, H., Yakıcı, E., Doğan, O.T., Duran, S., Karatas, M., 2020. Finding optimal schedules in a home energy management system (May). Electr. Power Syst. Res. vol. 182. https://doi.org/10.1016/j.epsr.2020.106229.
Metke, A.R., Ekl, R.L., 2010. Security Technology for Smart Grid Networks (June). IEEE Trans. Smart Grid vol. 1 (1), 99–107. https://doi.org/10.1109/TSG.2010.2046347.
Mohamed, M. vall O., Abdelaziz, A.Y., Abo-Elyousr, F.K., 2024. Blockchain-based approach for load frequency control of smart grids under denial-of-service attacks (May). Comput. Electr. Eng. vol. 116. https://doi.org/10.1016/j.compeleceng.2024.109150.
Mohammad, A.N., et al., 2018. A NEW TAXONOMY OF INSIDER THREATS; AN INITIAL STEP IN UNDERSTANDING AUTHORIZED ATTACK. Int. J. Inf. Syst. Manag. vol. 1 (1), 1. https://doi.org/10.1504/ijisam.2018.10014439.
Mohammed, S.H., et al., 2024. A Review on the Evaluation of Feature Selection Using Machine Learning for Cyber-Attack Detection in Smart Grid. IEEE Access vol. 12, 44023–44042. https://doi.org/10.1109/ACCESS.2024.3370911.
O. Monnier, "A smarter grid with the Internet of Things."
Morozov, A., et al., 2024. Optimal Flow Factor Determination in Vanadium Redox Flow Battery Control. IEEE Access vol. 12, 19277–19284. https://doi.org/10.1109/ACCESS.2024.3361830.
Mousavian, S., Erol-Kantarci, M., Wu, L., Ortmeyer, T., 2018. A Risk-Based Optimization Model for Electric Vehicle Infrastructure Response to Cyber Attacks (Nov.). IEEE Trans. Smart Grid vol. 9 (6), 6160–6169. https://doi.org/10.1109/TSG.2017.2705188.
Mrabet, Z.El, Kaabouch, N., Ghazi, H.El, Ghazi, H.El, 2018. Cyber-security in smart grid: Survey and challenges (Apr.). Comput. Electr. Eng. vol. 67, 469–482. https://doi.org/10.1016/j.compeleceng.2018.01.015.
N. Naval and J.M. Yusta, "Virtual power plant models and electricity markets - A review," Oct. 01, 2021, Elsevier Ltd. doi: 10.1016/j.rser.2021.111393.
Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., Dehghanian, P., 2020a. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. IEEE Access vol. 8, 87592–87608. https://doi.org/10.1109/ACCESS.2020.2993233.".
Nguyen, T., Wang, S., Alhazmi, M., Nazemi, M., Estebsari, A., Dehghanian, P., 2020b. Electric Power Grid Resilience to Cyber Adversaries: State of the Art. IEEE Access vol. 8, 87592–87608. https://doi.org/10.1109/ACCESS.2020.2993233.".
S.M. Nosratabadi, R.A. Hooshmand, and E. Gholipour, "A comprehensive review on microgrid and virtual power plant concepts employed for distributed energy resources scheduling in power systems," Jan. 01, 2017, Elsevier Ltd. doi: 10.1016/j.rser.2016.09.025.
Pal, R., Prasanna, V., 2017. The STREAM Mechanism for CPS Security The Case of the Smart Grid,' in (April). IEEE Trans. Comput. -Aided Des. Integr. Circuits Syst. vol. 36 (4), 537–550. https://doi.org/10.1109/TCAD.2016.2565201.
R. Palmarini, J.A. Erkoyuncu, R. Roy, and H. Torabmostaedi, "A systematic review of augmented reality applications in maintenance," Feb. 01, 2018, Elsevier Ltd. doi: 10.1016/j.rcim.2017.06.002.
Park, C.K., Kim, H.J., Kim, Y.S., 2014. A study of factors enhancing smart grid consumer engagement. Energy Policy vol. 72, 211–218. https://doi.org/10.1016/j.enpol.2014.03.017.
A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," Jan. 2013. doi: 10.1016/j.jnca.2012.08.007.
Paul, S., Rabbani, M.S., Kundu, R.K., Zaman, S.M.R., 2014. A review of smart technology (Smart Grid) and its features. 2014 1st Int. Conf. Non Conv. Energy (ICONCE 2014), Kalyani, India 200–203. https://doi.org/10.1109/ICONCE.2014.6808719.".
Paul S., Rabbani M. S., Kundu R. K., and Zaman S. M. R., "A review of smart technology (smart grid) and its features," Proc. 2014 1st Int. Conf. Non Conv. Energy Search Clean Safe Energy, ICONCE 2014, no. Iconce, pp. 200–203, 2014, doi: 10.1109/ICONCE.2014.6808719.
Qi, J., Hahn, A., Lu, X., Wang, J., Liu, C., 2016. Cybersecurity for distributed energy resources and smart inverters. IET Cyber-Phys. Syst.: Theory Appl. 1 (1), 28–39. https://doi.org/10.1049/iet-cps.2016.0018".
Quirós, A.B. De, Quintero, A.E., Francés, A., Maurice, A.A., Uceda, J., 2023. Electrical Model of a Membraneless Micro Redox Flow Battery - Fluid Dynamics Influence. IEEE Access vol. 11, 46132–46143. https://doi.org/10.1109/ACCESS.2023.3273927.

Rocky, T.H., Islam, R., Saha, U.K., 2014. Nano solar grid (NSG): A solution for rural market power crisis. 2nd Int. Conf. Green. Energy Technol., Dhaka, Bangladesh 14–17. https://doi.org/10.1109/ICGET.2014.6966653.".

Rodriguez-Diaz, E., Vasquez, J.C., Guerrero, J.M., 2016. Intelligent DC Homes in Future Sustainable Energy Systems: When efficiency and intelligence work together (Jan.). IEEE Consum. Electron. Mag. vol. 5 (1), 74–80. https://doi.org/10.1109/MCE.2015.2484699.

H.M. Rouzbahani, H. Karimipour, and L. Lei, "A review on virtual power plant for energy management," Oct. 01, 2021, Elsevier Ltd. doi: 10.1016/j.seta.2021.101370.

SaberiKamarposhti, M., et al., 2024. A comprehensive review of AI-enhanced smart grid integration for hydrogen energy: Advances, challenges, and future prospects (May). Int J. Hydrog. Energy vol. 67, 1009–1025. https://doi.org/10.1016/j.ijhydene.2024.01.129.

Sadeghi, R., Sadeghi, S., Memari, A., Rezaeinejad, S., Hajian, A., 2024. A peer-to-peer trading model to enhance resilience: A blockchain-based smart grids with machine learning analysis towards sustainable development goals (Apr.). J. Clean. Prod. vol. 450. https://doi.org/10.1016/j.jclepro.2024.141880.

Saleh, A.D., Hilal, N.A., Haggag, M., 2022. Developing a Smart Grid System in the UAE: Challenges and Opportunities (Nov.). Buildings vol. 12 (11). https://doi.org/10.3390/buildings12111863.

Sankarananth, S., Karthiga, M., Suganya, E., Sountharrajan, S., Bavirisetti, D.P., 2023. AI-enabled metaheuristic optimization for predictive management of renewable energy production in smart grids (Nov.). Energy Rep. vol. 10, 1299–1312. https://doi.org/10.1016/j.egyr.2023.08.005.

A.D. Sawadogo *et al.*, "Learning to Catch Security Patches," Jan. 2020, [Online]. Available: ⟨http://arxiv.org/abs/2001.09148⟩.

Song, C.H., 2021. Exploring and predicting the knowledge development in the field of energy storage: Evidence from the emerging startup landscape (Sep.). Energ. (Basel) vol. 14 (18). https://doi.org/10.3390/en14185822.

Sorebo, G.N. and Echols, M.C., 2012. Smart grid security: an end-to-end view of security in the new electrical grid. CRC Press.".

Starke, M., et al., 2021. Secondary Use-Plug-and-Play Energy Storage System Composed of Multiple Energy Storage Technologies. 2021 IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT), Wash., DC, USA 1–5. https://doi.org/10.1109/ISGT49243.2021.9372177.".

Suleiman, H., Alqassem, I., Diabat, A., Arnautovic, E., Svetinovic, D., 2015. Integrated smart grid systems security threat model (Jun.). Inf. Syst. vol. 53, 147–160. https://doi.org/10.1016/j.is.2014.12.002.

Syamala, M., Gowri, U., Babu, D.V., Sahaya Anselin Nisha, A., Ahmed, M.A., Muniyandy, E., 2024. Transactive energy management system for smart grids using Multi-Agent Modeling and Blockchain (Sep.). Sustain. Comput.: Inform. Syst. vol. 43. https://doi.org/10.1016/j.suscom.2024.101001.

Tajeddini, M.A., Rahimi-Kian, A., Soroudi, A., 2014. Risk averse optimal operation of a virtual power plant using two stage stochastic programming (Aug.). Energy vol. 73, 958–967. https://doi.org/10.1016/j.energy.2014.06.110.

Tang, D., Fang, Y.P., Zio, E., 2023. Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods (Jul.). Reliab Eng. Syst. Saf. vol. 235. https://doi.org/10.1016/j.ress.2023.109212.

Tao, F., Zhang, H., Liu, A., Nee, A.Y.C., 2019. Digital Twin in Industry: State-of-the-Art (April). IEEE Trans. Ind. Inform. vol. 15 (4), 2405–2415. https://doi.org/10.1109/TII.2018.2873186.

Tian, L., Cheng, L., Wan, Y., Yuan, K., Liu, R., Wu, K., 2020. From Distributed Energy Resources to Virtual Power Plants: A Cyber-Physical System Solution for Integrating Demand-side in Smart Grid. 2020 IEEE 4th Conf. Energy Internet Energy Syst. Integr. (EI2), Wuhan., China 3463–3467. https://doi.org/10.1109/EI250167.2020.9346925.".

Tvaronavičienė, Manuela, Plėta, Tomas, Casa, Silvia Della, Latvys, Juozas, 2020. Cyber security management of critical energy infrastructure in national cybersecurity strategies: cases of USA, UK, France, Estonia and Lithuania. Insights into Reg. Dev. 2 (4), 802–813. https://doi.org/10.9770/ird.2020.2.4(6). ⟨hal-03298796⟩.

W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Apr. 07, 2013a, Elsevier B.V. doi: 10.1016/j.comnet.2012.12.017.

W. Wang and Z. Lu, "Cyber security in the Smart Grid: Survey and challenges," Apr. 07, 2013b, Elsevier B.V. doi: 10.1016/j.comnet.2012.12.017.

Wang, X., Lu, M., 2023. Wireless power transmission based on retro-reflective beamforming technique (Jun.). Space Sol. Power Wirel. Transm.. https://doi.org/10.1016/j.sspwt.2023.08.001.

Wei, Dong, Lu, Yan, Jafari, M., Skare, P., Rohde, K., 2010. An integrated security system of protecting Smart Grid against cyber attacks,'. 2010 Innov. Smart Grid Technol. (ISGT), Gaithersburg, MD, USA 1–7. https://doi.org/10.1109/ISGT.2010.5434767.

Whitehead, D.E., Owens, K., Gammel, D., Smith, J., 2017. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. 2017 70th Annu. Conf. Prot. Relay Eng. (CPRE), Coll. Station, TX, USA 1–8. https://doi.org/10.1109/CPRE.2017.8090056.".

D.J. Willis *et al.*, "Wind energy research: State-of-the-art and future research directions," Sep. 01, 2018, Elsevier Ltd. doi: 10.1016/j.renene.2018.02.049.

Xie, L., Shi, Y., Hou, Y.T., Lou, A., 2013. Wireless power transfer and applications to sensor networks (August). IEEE Wirel. Commun. vol. 20 (4), 140–145. https://doi.org/10.1109/MWC.2013.6590061.

Xinhua, Xu, Lianshun, Mu, 2014. The vision of smart grid 2.0,'. 2014 China Int. Conf. Electr. Distrib. (CICED), Shenzhen 1639–1644. https://doi.org/10.1109/CICED.2014.6991984.

Yadav, S.A., Kumar, S.R., Sharma, S., Singh, A., 2016. 'A review of possibilities and solutions of cyber attacks in smart grids,'. 2016 Int. Conf. Innov. Chall. Cyber Secur. (ICICCS-INBUSH), Gt. Noida, India 60–63. https://doi.org/10.1109/ICICCS.2016.7542359.

G. Yadav and K. Paul, "Architecture and security of SCADA systems: A review," Sep. 01, 2021, Elsevier B.V. doi: 10.1016/j.ijcip.2021.100433.

Yao, S., et al., 2024. An efficient authentication protocol with privacy-preserving for virtual power plant. in *Journal of Physics: Conference Series*. Institute of Physics. https://doi.org/10.1088/1742-6596/2741/1/012014.

Yedavalli, P.S., Riihonen, T., Wang, X., Rabaey, J.M., 2017. Far-Field RF Wireless Power Transfer with Blind Adaptive Beamforming for Internet of Things Devices. IEEE Access vol. 5, 1743–1752. https://doi.org/10.1109/ACCESS.2017.2666299.".

M. Yigit, V.C. Gungor, and S. Baktir, "Cloud Computing for Smart Grid applications," Sep. 09, 2014, Elsevier B.V. doi: 10.1016/j.comnet.2014.06.007.

Yu, X., Xue, Y., 2016. Smart Grids: A Cyber–Physical Systems Perspective,' (May). Proc. IEEE vol. 104 (5), 1058–1070. https://doi.org/10.1109/JPROC.2015.2503119.".

Yusop, Z.M., Abawajy, J., 2014. Analysis of Insiders Attack Mitigation Strategies (May). Procedia Soc. Behav. Sci. vol. 129, 581–591. https://doi.org/10.1016/j.sbspro.2014.03.716.

Zhang, Z., Yang, Z., Yau, D.K.Y., Tian, Y., Ma, J., 2023. Data security of machine learning applied in low-carbon smart grid: A formal model for the physics-constrained robustness (Oct.). Appl. Energy vol. 347. https://doi.org/10.1016/j.apenergy.2023.121405.

Zhao, J., Gao, Y., Burke, A.F., 2017. Performance testing of supercapacitors: Important issues and uncertainties. J. Power Sources vol. 363, 327–340. https://doi.org/10.1016/j.jpowsour.2017.07.066.

B. Zhou *et al.*, "Smart home energy management systems: Concept, configurations, and scheduling strategies," Aug. 01, 2016, Elsevier Ltd. doi: 10.1016/j.rser.2016.03.047.