Research Article OPEN ACCESS

Strengthening Smart Grids Through Security Measures: A Focus on Real-Time Monitoring, Redundancy, and Cross-Sector Collaboration

Yusri Bin Yusof
Computer Science Department at Universiti Malaysia Kelantan (UMK)

Tan Hooi Ping
Electrical and Electronic Engineering Department at Universiti Malaysia Perlis (UniMAP)

Farah Binti Mohd. Isa
Computer Science Department at Universiti Teknikal Malaysia Melaka (UTeM)

Abstract

In the era of interconnected power systems, the resilience of smart grids against cyber-physical attacks has emerged as a paramount concern. The integration of renewable energy sources, digital communication, and advanced control systems has transformed modern power grids, but it has also exposed them to a new array of vulnerabilities. This research focuses on a comprehensive approach to enhance the resilience of smart grids against these threats. The study encompasses the implementation of multi-layer security measures, including physical security through surveillance, access controls, and intrusion detection; cyber security measures such as firewalls, intrusion detection systems (IDS), encryption, and secure communication protocols; and operational security involving policies, procedures, and regular training. Real-time monitoring and anomaly detection are addressed through the utilization of machine learning and data analytics to detect unusual patterns indicative of an attack, and the development of real-time monitoring tools for situational awareness. Redundancy and fail-safe mechanisms are considered by designing the grid with redundant paths and components, and implementing automatic failover systems to maintain stability. Interoperability and standardization are achieved by adhering to industry standards such as NERC CIP, and designing interoperable systems. Collaboration and information sharing are emphasized through collaboration with other industries, government agencies, and international bodies, and the creation of platforms for sharing real-time information about threats and vulnerabilities. The research emphasizes the need for a holistic approach that integrates these various aspects, contributing to the ongoing efforts to build robust, resilient, and secure smart grids that can withstand the evolving landscape of cyber-physical threats.

Keywords: Smart Grids, Cyber-Physical Security, Resilience, Real-Time Monitoring, Interoperability

Declarations

Competing interests:

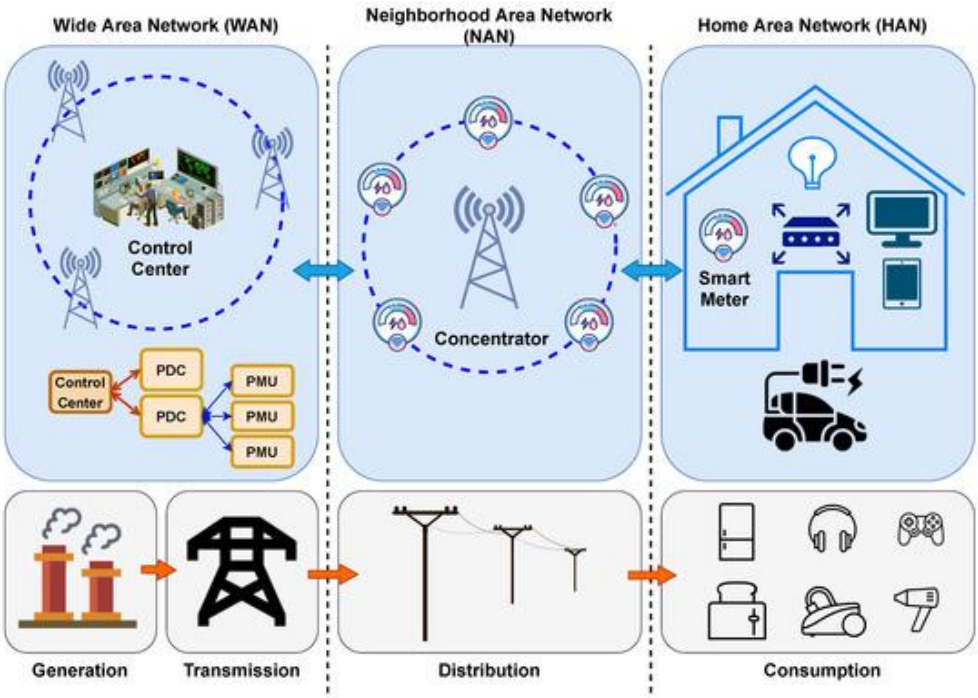
The author declares no competing interests.

Introduction

Smart Grids represent a significant evolution in the way energy is managed, distributed, and consumed [1], [2]. At its core, a Smart Grid is an electricity network that uses digital technology to monitor and manage the production, distribution, and consumption of electricity in a more efficient, sustainable, and reliable manner. The main components that constitute a Smart Grid include Advanced Metering Infrastructure (AMI), Demand Response Systems, Distributed Energy Resources (DERs), Energy Management Systems (EMS), and Grid Automation and Control [3]–[5].

Advanced Metering Infrastructure (AMI) is a crucial component of Smart Grids, enabling two-way communication between utilities and consumers [6]. AMI consists of smart meters, communication networks, and data management systems that allow real-time monitoring and control of energy usage [7]. This technology enables utilities to gather detailed consumption data, which can be used to optimize energy distribution, reduce costs, and provide consumers with more detailed information about their energy usage [8]–[10].

Figure 1. Smart Grid Architecture [11]



Demand Response Systems are another vital part of Smart Grids, allowing for a more flexible and responsive energy network. These systems enable consumers to respond to price signals or other incentives from utilities by reducing or shifting their electricity consumption during peak demand periods. By doing so, Demand Response Systems help to balance supply and demand,

reduce the need for additional generation capacity, and minimize the risk of blackouts or other grid instabilities [12]–[14].

Distributed Energy Resources (DERs) refer to a variety of small-scale energy resources that can be located close to where the energy is consumed. This includes renewable energy sources like solar panels and wind turbines, as well as energy storage systems like batteries [15]. DERs can be controlled and integrated into the Smart Grid to provide a more resilient and flexible energy system. By decentralizing energy production, DERs can reduce transmission losses, increase energy efficiency, and enable a more sustainable energy future [16]–[18].

Energy Management Systems (EMS) and Grid Automation and Control are essential components that enable the intelligent operation of Smart Grids [19]. EMS provides utilities with the tools to monitor, control, and optimize the generation, transmission, and distribution of energy. It helps in maintaining grid stability, reducing energy losses, and improving efficiency. Grid Automation and Control, on the other hand, involves the use of sensors, controllers, and other technologies to automate various grid functions. This automation enhances the reliability, efficiency, and flexibility of the grid, allowing for more sophisticated control and management of energy flows [20]–[22]. Contrasting traditional grids with Smart Grids reveals significant differences in their operation and capabilities. Traditional grids are characterized by a centralized, one-way flow of electricity from large power plants to consumers, with limited ability to monitor or control energy usage [23].

Smart Grids, however, enable a two-way flow of information and electricity, integrating various technologies and resources to create a more responsive and efficient energy system. The incorporation of AMI, Demand Response Systems, DERs, EMS, and Grid Automation and Control in Smart Grids allows for real-time monitoring and control, decentralized energy production, enhanced reliability, and a more sustainable approach to energy management. This transformation represents a fundamental shift in the way energy is produced, distributed, and consumed, paving the way for a more resilient and sustainable energy future [24]–[26]. The evolution of Smart Grids is driven by several key technologies that enable more efficient, reliable, and sustainable energy management. These technologies include Advanced Sensors and Monitoring, Communication Infrastructure, Big Data and Analytics, and Energy Storage Solutions [27].

Advanced Sensors and Monitoring play a critical role in the modernization of Smart Grids. Real-time data collection through various sensors allows utilities to monitor the grid's performance continuously, detecting any anomalies or inefficiencies. This real-time monitoring enables predictive maintenance [28], where potential issues can be identified and addressed before they escalate into significant problems. By utilizing advanced sensors, utilities can ensure that the grid operates at optimal efficiency, reducing downtime and maintenance costs [29]–[32]. Communication Infrastructure is another vital aspect of Smart Grid evolution, providing the necessary connectivity between different components of the grid [33]. The role of the Internet of Things (IoT) is particularly significant in this context, as it enables seamless communication between various devices and systems within the grid [34]. IoT allows for the integration of diverse technologies [35], from smart meters to renewable energy sources, creating a cohesive and intelligent energy network [36] [37] [38]. Secure data transmission is also a crucial

consideration, ensuring that sensitive information related to energy consumption, pricing, and grid performance is protected from unauthorized access or tampering [39]–[41]. Big Data and Analytics are at the heart of Smart Grids, providing the tools to process and derive insights from the massive data streams generated by the grid's various components [42]. The ability to analyze this data in real-time allows utilities to make informed decisions, optimizing energy distribution and consumption. By leveraging Big Data and Analytics, utilities can identify trends, predict future energy needs [43] , and implement strategies to enhance efficiency and sustainability. This data-driven approach enables a more proactive and responsive energy management system, aligning energy production and consumption with actual demand [44].

Energy Storage Solutions are essential in addressing some of the challenges associated with renewable energy sources, such as their intermittency. Solar and wind energy, for example, are not always available, depending on weather conditions and time of day. Energy Storage Solutions, such as batteries, can store excess energy produced during favorable conditions and release it when needed, ensuring a consistent energy supply. Additionally, energy storage plays a vital role in peak demand management, allowing utilities to store energy during off-peak times and release it during periods of high demand. This capability helps in balancing the grid, reducing the need for additional generation capacity, and contributing to a more stable and resilient energy system [45].

Deep learning in Smart Grids resilience against Cyber-Physical Attacks (CPA) leverages neural networks to enhance the security and robustness of the grid. The smart grid is an interconnected network that integrates information technology with electrical infrastructure, making it susceptible to various cyber-physical threats. Deep learning algorithms, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), are employed to analyze the vast amount of data generated by the grid. By processing this data, the algorithms can identify patterns and anomalies that may signify an impending or ongoing attack. This real-time analysis enables the system to respond promptly, minimizing potential damage [46]–[48]. The application of deep learning in Smart Grids resilience is not confined to threat detection alone. It also extends to the development of adaptive defense mechanisms [49]. When a potential threat is detected, the system must respond in a manner that neutralizes the threat without disrupting the normal operation of the grid. Deep Reinforcement Learning (DRL) is often used to create adaptive control strategies that can dynamically adjust to the changing threat landscape. By continuously learning from the environment and adjusting its actions accordingly, DRL can help the grid maintain stability and efficiency even in the face of sophisticated attacks.

Another critical aspect of deep learning in Smart Grids resilience is the integration of physical and cyber security measures. Since the grid is a cyber-physical system, attacks can manifest in both the digital and physical domains [50].Deep learning models can be trained to recognize the complex interactions between these domains, allowing for a more holistic security approach. For example, a cyber-attack that aims to overload a physical component of the grid can be detected through the analysis of both network traffic and electrical load data. By understanding the interdependencies between the cyber and physical aspects of the grid, deep learning enhances the system's ability to anticipate and mitigate multifaceted attacks [51].

The implementation of deep learning in Smart Grids resilience also necessitates a robust and secure data management framework. The effectiveness of the deep learning models relies heavily on the quality and integrity of the data they process [52]. Ensuring that the data is accurate, timely, and free from tampering is vital to the success of the deep learning approach [53]. Techniques such as data encryption, secure multi-party computation, and blockchain can be integrated with deep learning to create a secure data ecosystem. This not only protects the data but also ensures that the deep learning models are trained on reliable information, enhancing their accuracy and effectiveness [54]–[56]. The deployment of deep learning in Smart Grids resilience against Cyber-Physical Attacks requires careful consideration of the ethical and regulatory landscape. The use of deep learning algorithms can raise concerns about privacy, accountability, and transparency. Ensuring that the implementation complies with relevant laws and regulations, and adheres to ethical principles, is essential to maintaining public trust and support. This includes conducting regular audits, implementing transparent decision-making processes, and engaging with stakeholders to address concerns and expectations [57].

By taking a responsible and comprehensive approach to the integration of deep learning, Smart Grids can enhance their resilience against Cyber-Physical Attacks while maintaining alignment with societal values and norms [58].

Security Measure

Multi-Layer Security Measures

The security of Smart Grids is a multifaceted challenge that requires a comprehensive approach, encompassing Physical Security, Cyber Security, and Operational Security. These three aspects work in tandem to create a robust defense against potential threats, ensuring the integrity, availability, and confidentiality of the energy grid [59]–[61]. Physical Security is a critical component in protecting the tangible assets of the Smart Grid, such as substations, transformers, and control centers [62].

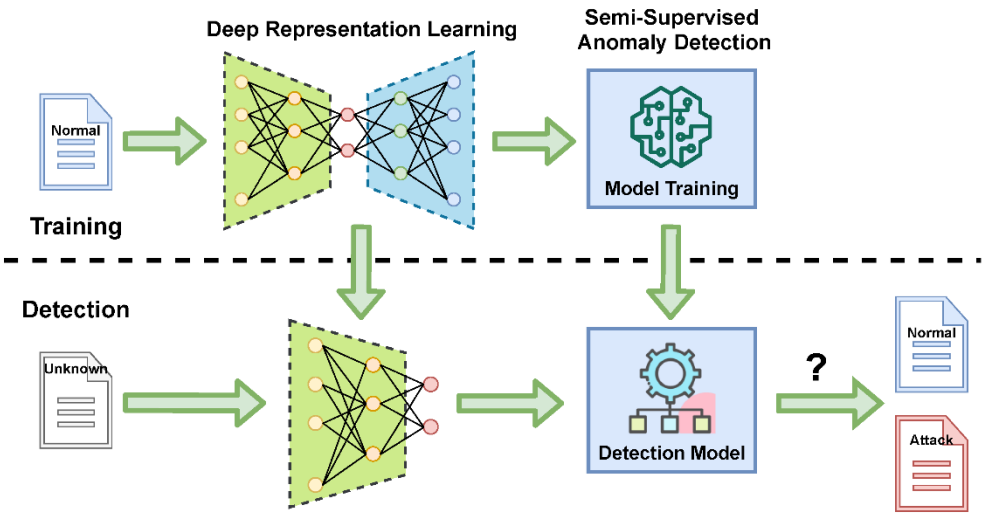
Implementing robust physical security measures involves the use of surveillance cameras, access controls, and intrusion detection systems. Surveillance cameras monitor critical areas, providing real-time visibility and aiding in the detection of unauthorized activities [63]. Access controls regulate who can enter specific locations, ensuring that only authorized personnel have access to sensitive areas. Intrusion detection systems alert security teams to any unauthorized entry, allowing for immediate response. Together, these measures create a formidable barrier against physical threats, protecting the hardware that is vital to the grid's operation [64]–[66]. Cyber Security focuses on safeguarding the digital aspects of the Smart Grid, which are increasingly targeted by cybercriminals.

Utilizing firewalls, intrusion detection systems (IDS), encryption, and secure communication protocols, Cyber Security measures protect against unauthorized access, data breaches, and other cyber threats. Firewalls act as a barrier between the internal network and external threats, filtering out malicious traffic. Intrusion detection systems monitor network activity, identifying suspicious patterns that may indicate an attack [67]. Encryption ensures that data transmitted across the network is unreadable to unauthorized parties, while secure communication protocols provide a safe channel for data exchange. These measures collectively create a secure

digital environment, protecting the information and systems that are essential to the Smart Grid's functionality [68]–[70].

Operational Security recognizes the human element's role in the overall security of the Smart Grid and emphasizes the importance of implementing security policies, procedures, and regular training. Even the most advanced physical and cyber security measures can be undermined by human error or negligence [71]. Operational Security addresses this vulnerability by ensuring that employees are aware of security best practices and are trained to respond to potential threats. Regular training sessions keep staff up to date on the latest threats and countermeasures, while clear policies and procedures provide guidelines for maintaining security in daily operations [72]–[74] . By focusing on the human aspect, Operational Security complements physical and cyber security, creating a holistic approach to Smart Grid protection [75].

Figure 2. Detecting cyber attacks in smart grids with deep learning [11]



In conclusion, the security of Smart Grids requires a comprehensive and integrated approach that combines Physical Security, Cyber Security, and Operational Security [76]–[78] . By addressing the potential threats to both the physical hardware and digital systems, and recognizing the human element's role, Smart Grids can be safeguarded against a wide range of risks. The implementation of surveillance, access controls, intrusion detection, firewalls, encryption, secure communication protocols, policies, procedures, and training creates a multi-layered defense that ensures the reliability and integrity of the energy grid. This robust security framework is essential in an increasingly interconnected and digitalized world, where the energy grid's resilience is vital to societal well-being and economic stability [79] [80].

Real-Time Monitoring and Anomaly Detection

The modernization and digitization of energy grids have led to the integration of advanced technologies like Data Analytics and Situational Awareness, which play a crucial role in enhancing the security and efficiency of Smart Grids [81]. These technologies provide intelligent tools to monitor, analyze, and respond to potential threats and anomalies within the grid,

ensuring its stability and resilience [82]–[84]. Data Analytics, particularly when combined with machine learning, offers a powerful tool for detecting unusual patterns in the grid that may indicate an attack or other security threats [85]. By continuously analyzing vast amounts of data generated by the grid's various components, machine learning algorithms can identify deviations from normal behavior, such as unexpected spikes in energy consumption or irregular communication patterns [86] . These anomalies may signal an attempted intrusion or other malicious activities. Utilizing machine learning and data analytics enables a proactive approach to security, where potential threats can be detected and addressed before they escalate into significant issues. This data-driven insight enhances the grid's overall security by providing an additional layer of intelligence and responsiveness [87].

Situational Awareness takes the concept of real-time monitoring to a new level, developing tools that provide operators with a comprehensive view of the grid's status at any given moment [88] [89] [90]. By integrating data from various sensors, control systems, and other sources, Situational Awareness creates a unified and detailed picture of the grid's performance, condition, and potential vulnerabilities [91]. This real-time visibility enables operators to quickly respond to any anomalies, whether they are security-related or indicative of a technical malfunction. For example, if a sudden drop in voltage is detected in a specific part of the grid, operators can immediately investigate the cause and take appropriate action to prevent further issues. Situational Awareness not only enhances security but also contributes to the overall efficiency and reliability of the grid by enabling a more informed and agile response to changing conditions [92]–[94].

Data Analytics and Situational Awareness represent vital advancements in the ongoing evolution of Smart Grids, providing intelligent tools to enhance security and operational efficiency. By leveraging machine learning and real-time monitoring, these technologies enable a more nuanced understanding of the grid's behavior and condition, allowing for a proactive and informed response to potential threats and anomalies [95] . The integration of Data Analytics and Situational Awareness into the Smart Grid's architecture creates a more resilient and intelligent energy system, capable of adapting to the complex and dynamic challenges of modern energy management. These technologies not only contribute to the grid's security but also pave the way for a more sustainable and responsive energy future, reflecting the growing importance of data-driven insights and real-time visibility in an increasingly interconnected world [96]–[98].

Redundancy and Fail-Safe Mechanisms

The resilience and reliability of Smart Grids are paramount in ensuring uninterrupted energy supply and maintaining stability in the face of unexpected challenges or threats. Two essential strategies that contribute to these goals are System Redundancy and the implementation of Fail-Safe Mechanisms. Both of these approaches are designed to minimize the impact of failures, whether they result from technical malfunctions, natural disasters, or malicious attacks [99]–[101].

System Redundancy involves designing the grid with redundant paths and components, providing alternative routes for energy flow if part of the system is compromised. This redundancy can be achieved at various levels, including the duplication of critical hardware, the

creation of parallel transmission lines, and the utilization of diverse energy sources. By having these backup options in place, the grid can continue to function even if a key component fails or is damaged [102]. For example, if a major transmission line is taken offline due to a storm, the redundant paths can be activated to reroute the power, ensuring that the affected areas continue to receive electricity. System Redundancy enhances the grid's resilience, providing a buffer against unexpected disruptions and contributing to a more stable and reliable energy system [103]–[105].

Fail-Safe Mechanisms take the concept of resilience a step further by implementing automatic failover systems that can detect issues and take immediate action to maintain stability [106] . These mechanisms are designed to isolate affected areas and reroute power as needed, minimizing the impact of a failure on the broader grid. For instance, if a cyberattack targets a specific substation, the fail-safe mechanisms can quickly identify the anomaly and isolate the compromised area, preventing the attack from spreading to other parts of the grid [107]. By rerouting power through unaffected paths, the grid can continue to operate normally, even as the issue is being addressed [108] [109] [110]. Fail-Safe Mechanisms provide an additional layer of protection, enabling a rapid and automated response to potential threats or failures [111]–[113].

Deep learning plays a crucial role in real-time monitoring and anomaly detection [114], particularly in complex systems like electrical grids. By employing deep learning algorithms, systems can be trained to recognize normal patterns and behaviors within the grid [115]. When these patterns are disrupted, the algorithms can identify the anomalies and alert operators to potential issues. This is particularly vital in detecting unusual patterns that may indicate an attack. Deep learning models, such as autoencoders, can be trained on vast amounts of historical data to understand the typical behavior of the grid. When a deviation from this pattern occurs, the model can flag it as an anomaly, allowing for immediate investigation and response [116]–[118].

Utilizing machine learning and data analytics in the context of anomaly detection involves sophisticated techniques that can process large volumes of data in real-time [119]. Deep learning models can sift through the noise and detect subtle changes that might be indicative of an impending problem or attack. These models can be trained to recognize complex relationships between different variables in the grid, such as voltage levels, current flow, and frequency. By understanding these relationships, the models can detect inconsistencies that may not be apparent through traditional monitoring methods. This enables a more proactive approach to grid management, where potential issues can be addressed before they escalate into significant problems [120]–[122].

Situational awareness in the context of grid monitoring refers to the ability to have a comprehensive view of the grid's status at any given moment. Deep learning contributes to this by developing real-time monitoring tools that provide operators with detailed insights into the grid's functioning [123] . These tools can include visualizations, predictive analytics [124], and other advanced features that allow operators to see not just what is happening, but also what might happen in the near future. By leveraging deep learning, these tools can process and

interpret vast amounts of data quickly, enabling operators to respond to anomalies with speed and precision [125].

The integration of deep learning models with existing monitoring systems is a complex but essential aspect of real-time monitoring and anomaly detection. By working in conjunction with traditional monitoring tools, deep learning can provide a more nuanced understanding of the grid's behavior. This integration often involves the use of APIs [126] [127] [128] [129], specialized hardware, and tailored algorithms that can work with the specific characteristics of the grid [130]. The result is a more robust monitoring system that can adapt to new challenges [131] [132] [133], learn from new data, and provide a more resilient defense against potential attacks or failures [134]–[136].

Despite the significant advancements in deep learning for real-time monitoring and anomaly detection, there are still challenges to be addressed. The complexity of deep learning models can make them difficult to interpret, leading to potential issues in understanding why a particular anomaly has been detected [137]. There is also the challenge of ensuring that the models are trained on representative data, as biases in the training data can lead to incorrect anomaly detection. Looking forward, the field is likely to see continued innovation, with new algorithms, better integration with existing systems, and improved methods for interpreting the results of deep learning models [138]–[140]. The ongoing collaboration between researchers, engineers, and grid operators will be essential in realizing the full potential of deep learning in this critical area [141].

System Redundancy and Fail-Safe Mechanisms are vital strategies in enhancing the resilience and reliability of Smart Grids. By designing the grid with redundant paths and components and implementing automatic failover systems, these approaches ensure that the grid can continue to operate even in the face of unexpected challenges. Whether dealing with technical malfunctions, natural disasters, or malicious attacks, the integration of System Redundancy and Fail-Safe Mechanisms provides a robust defense, minimizing disruptions and maintaining stability. These strategies reflect a proactive and comprehensive approach to grid design and operation, recognizing the complex and dynamic nature of modern energy systems. By prioritizing resilience and reliability, Smart Grids are better equipped to meet the demands of an increasingly interconnected and dependent world, contributing to a more secure and sustainable energy future [142]–[144].

Interoperability and Standardization

The complexity and interconnected nature of modern Smart Grids necessitate a comprehensive approach to security and functionality. Two critical aspects that contribute to this are Standards Compliance, particularly adherence to industry standards like NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), and the design of Interoperable Systems. Both of these elements play a vital role in ensuring a consistent, secure, and coordinated energy grid [145].

Standards Compliance involves adhering to established industry standards and regulations that define the minimum requirements for the security and reliability of the energy grid. NERC CIP, for instance, sets forth specific guidelines and best practices for protecting critical infrastructure within the North American electric grid. Compliance with these standards ensures that utilities

and other stakeholders maintain a consistent level of security across the grid, addressing potential vulnerabilities and implementing necessary safeguards. By following these standardized protocols, organizations can demonstrate their commitment to security, facilitate regulatory compliance, and foster a culture of continuous improvement [146]. Standards Compliance not only enhances the grid's overall security but also promotes trust and collaboration among various entities involved in energy production, distribution, and consumption [147].

Interoperable Systems focus on designing systems within the grid that can work together seamlessly, regardless of the manufacturer or specific technology used. Interoperability allows for more effective coordination and response in the event of an attack or other emergency, as different systems can communicate and collaborate without compatibility issues. For example, if a cyberattack targets a particular part of the grid, interoperable systems can quickly share information and coordinate a unified response, isolating the affected area and rerouting power as needed [148]. Interoperability also facilitates the integration of diverse technologies, such as renewable energy sources, energy storage solutions, and advanced monitoring tools, creating a more flexible and resilient grid. By ensuring that various components of the grid can interact seamlessly, Interoperable Systems enhance the grid's overall efficiency, reliability, and adaptability [149]–[151].

Standards Compliance and Interoperable Systems represent essential strategies in the ongoing development and security of Smart Grids [152] [153] [154] [155]. By adhering to industry standards like NERC CIP and designing systems that can work together seamlessly, these approaches contribute to a consistent, secure, and coordinated energy grid. Standards Compliance ensures that all stakeholders adhere to a common set of guidelines, promoting a unified approach to security and reliability. Interoperable Systems, on the other hand, enable more effective coordination and flexibility, allowing the grid to adapt to changing conditions and respond to potential threats more efficiently [156]. Together, these strategies reflect a comprehensive and forward-thinking approach to grid design and operation, recognizing the importance of collaboration, standardization, and adaptability in an increasingly complex and interconnected energy landscape. The integration of Standards Compliance and Interoperable Systems into the Smart Grid's architecture contributes to a more resilient and intelligent energy system, paving the way for a more secure and sustainable energy future [157].

Collaboration and Information Sharing

Cross-sector collaboration plays a pivotal role in enhancing the security and efficiency of operations. Collaborating with other industries, government agencies, and international bodies to share threat intelligence and best practices is not just a strategic move but a necessity in today's interconnected world. By working together, different sectors can pool their resources and expertise to identify, analyze, and mitigate threats more effectively. This collaboration fosters a unified approach to security, where the strengths of one sector can compensate for the weaknesses of another. It also promotes a culture of continuous learning and improvement, where industries can learn from each other's experiences and adopt best practices that have been proven to work in different contexts [158].

ServiceOps, or Service Operations focuses on delivering high-quality services to customers by integrating various operational processes and methodologies [159] . It emphasizes the alignment of service delivery with business goals, ensuring that the services provided are efficient, effective, and in line with the organization's objectives. ServiceOps is often associated with IT services, but it can be applied to any service-oriented industry. It encompasses a wide range of practices, including service design, service transition, service delivery, and continuous service improvement. The goal is to create a seamless experience for the customers while optimizing the resources and processes within the organization [160]–[164].

ServiceOps, with its focus on delivering high-quality services, must also prioritize security to ensure the integrity, confidentiality, and availability of the services provided. Security in the context of ServiceOps is not just about protecting data and systems; it's about building trust with customers and stakeholders by demonstrating that the organization takes its responsibilities seriously [165]. This involves implementing robust security measures across all aspects of service delivery, from design and transition to ongoing management and improvement [166]–[168].

In the design phase of ServiceOps, security must be considered from the outset. This means identifying potential risks and vulnerabilities and incorporating security controls to mitigate them [169]. It involves selecting appropriate technologies, defining security policies, and establishing procedures that align with industry standards and regulations. By integrating security into the design, organizations can ensure that it is an integral part of the service, rather than an afterthought. During the transition phase, security measures must be rigorously tested and validated to ensure that they function as intended. This includes conducting security assessments, penetration testing, and compliance audits to identify and address any weaknesses before the service is deployed.

The creation of information sharing platforms is a critical component of ServiceOps, enabling real-time communication about threats and vulnerabilities with relevant stakeholders. These platforms act as a centralized hub where information from various sources is collected, analyzed, and disseminated. By providing a common ground for different entities to share their insights, these platforms enable a coordinated response to emerging threats. They facilitate the rapid exchange of information, ensuring that all parties are aware of the latest developments and can take appropriate action in a timely manner [170].

The security and resilience of Smart Grids in an interconnected world require a collaborative approach that extends beyond individual utilities or sectors. Cross-Sector Collaboration and Information Sharing Platforms are two vital strategies that facilitate this broader cooperation, enhancing the collective ability to respond to threats and vulnerabilities [171]–[173].

Cross-Sector Collaboration involves collaborating with other industries, government agencies, and international bodies to share threat intelligence and best practices. The interconnected nature of modern infrastructure means that a threat to one sector can have ripple effects across others [174] [175] [176]. By fostering collaboration across different industries and governmental levels, stakeholders can gain a more comprehensive understanding of potential risks and develop coordinated strategies to address them [177]. For example, a utility company might collaborate with a telecommunications provider to understand and mitigate potential

cyber threats that could affect both sectors. Similarly, working with government agencies can facilitate alignment with national security priorities and regulatory compliance. International collaboration further extends this network, allowing for the sharing of insights and strategies across borders. Cross-Sector Collaboration enhances the collective ability to identify, understand, and respond to threats, creating a more resilient and secure energy landscape.

Information Sharing Platforms play a crucial role in enabling this collaboration by creating platforms for sharing real-time information about threats and vulnerabilities with relevant stakeholders. These platforms can take various forms, including secure online portals, regular briefings, or joint task forces, and serve as a centralized hub for disseminating critical intelligence [178]. By providing timely and accurate information about emerging threats, vulnerabilities, and best practices, Information Sharing Platforms enable a coordinated and agile response. Utilities, regulators, law enforcement, and other stakeholders can quickly assess the situation, share insights, and develop a unified strategy to address the issue. These platforms also foster a sense of community and trust among different entities, encouraging ongoing collaboration and information sharing. Information Sharing Platforms not only enhance the immediate response to threats but also contribute to the continuous improvement of security measures and protocols.

Cross-Sector Collaboration and Information Sharing Platforms represent essential strategies in the ongoing effort to secure and enhance Smart Grids. By fostering collaboration across industries, government agencies, and international bodies, and creating platforms for real-time information sharing, these approaches enable a more coordinated and effective response to potential threats and vulnerabilities. Cross-Sector Collaboration broadens the perspective and resources available to address complex challenges, while Information Sharing Platforms facilitate timely and informed decision-making. Together, these strategies reflect a recognition of the interconnected and interdependent nature of modern infrastructure, emphasizing the importance of collaboration, communication, and community in creating a more resilient and secure energy system. The integration of Cross-Sector Collaboration and Information Sharing Platforms into the Smart Grid's architecture contributes to a more robust and coordinated energy landscape, reflecting the evolving challenges and opportunities of an increasingly globalized and digitalized world [179]–[181].

Conclusion

Multi-Layer Security Measures are essential in today's interconnected world, where the risk of unauthorized access and malicious attacks is ever-present. These measures are often categorized into different layers to provide a comprehensive approach to security [182] [183] [184]. Physical Security is the first layer, focusing on the protection of tangible assets such as hardware, buildings, and other physical infrastructure. Implementing robust physical security measures involves the use of surveillance cameras, access controls, and intrusion detection systems. Surveillance ensures constant monitoring of critical areas, while access controls limit entry to authorized personnel only. Intrusion detection systems are designed to identify unauthorized access or breaches, allowing for immediate response. Together, these measures create a secure physical environment that protects critical hardware and infrastructure from theft, vandalism, or sabotage [185] [186].

Cyber Security, the second layer, emphasizes the protection of digital assets and information. This involves utilizing firewalls, intrusion detection systems (IDS), encryption, and secure communication protocols. Firewalls act as barriers between trusted and untrusted networks, filtering out potentially harmful data. Intrusion detection systems monitor network traffic for suspicious activities, while encryption ensures that sensitive information is unreadable to unauthorized users. Secure communication protocols like HTTPS provide a secure channel for transmitting data over the internet. These measures collectively form a robust defense against cyber threats, protecting data integrity and confidentiality [187] [188]

Operational Security is the third layer, focusing on the human element of security. This involves implementing security policies, procedures, and regular training to ensure that employees and other stakeholders are aware of their roles and responsibilities in maintaining security. Policies and procedures provide a framework for acceptable behavior and actions, while regular training ensures that everyone is equipped with the necessary knowledge and skills to identify and respond to potential threats. By addressing the human factor, operational security helps in minimizing the risks associated with human error or malicious intent.

Real-Time Monitoring and Anomaly Detection is the fourth layer, which is crucial for timely detection and response to potential threats. This involves utilizing machine learning and data analytics to detect unusual patterns in the grid that may indicate an attack [189]. Machine learning algorithms can analyze vast amounts of data to identify patterns and anomalies that might signify a security breach. Data analytics tools can further investigate these anomalies, providing insights into the nature and source of the threat. This real-time analysis enables quick and effective response, minimizing potential damage.

Situational Awareness is the fifth layer, focusing on developing real-time monitoring tools that provide operators with a comprehensive view of the grid's status. This enables quick response to any anomalies, ensuring that operators have the information they need to make informed decisions. Tools like SCADA (Supervisory Control and Data Acquisition) systems provide real-time data on various aspects of the grid, allowing for continuous monitoring and control. By maintaining situational awareness, operators can detect and respond to changes in the grid's status, whether due to technical malfunctions or malicious attacks. This comprehensive view of the grid's status enhances the ability to maintain stability and security, ensuring uninterrupted service and protection against potential threats [190]–[192].

Redundancy and Fail-Safe Mechanisms are vital components in the design and operation of critical systems like the power grid, where uninterrupted service is essential [193]. System Redundancy involves designing the grid with redundant paths and components to ensure continued operation even if part of the system is compromised. This means having backup systems or parallel pathways that can take over if a primary component fails. For example, in a power grid, having multiple transmission lines connecting the same locations ensures that if one line fails, the others can carry the load. This redundancy enhances the resilience of the system, allowing it to withstand failures without a significant impact on overall functionality.

Fail-Safe Mechanisms are another critical aspect, involving the implementation of automatic failover systems that can isolate affected areas and reroute power to maintain stability. These mechanisms are designed to detect failures and respond automatically, minimizing the potential

for cascading failures that could lead to widespread outages. For example, if a substation fails, the fail-safe mechanisms can isolate the affected area and reroute power through other substations, ensuring that the rest of the grid remains stable. This automatic response enhances the system's resilience, allowing it to recover quickly from unexpected failures. Interoperability and Standardization are essential for a consistent and coordinated approach to security across different systems and sectors [194].

Standards Compliance, such as adhering to industry standards like NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection), ensures a consistent level of security across the grid [195]–[197]. These standards define the minimum requirements for protecting critical infrastructure, providing a common framework that all operators must follow. By adhering to these standards, operators ensure that they are implementing recognized best practices, creating a uniform level of protection that enhances the overall security of the grid [198], [199].

Interoperable Systems involve designing systems that can work together seamlessly, allowing for more effective coordination and response in the event of an attack. This means that different systems, whether within the same organization or across different organizations, can communicate and cooperate without compatibility issues. Interoperability enables a more coordinated response to threats, allowing different systems to work together to detect, analyze, and respond to potential attacks. This seamless integration enhances the efficiency and effectiveness of the response, minimizing potential damage. Collaboration and Information Sharing are crucial for a comprehensive and coordinated approach to security, involving multiple stakeholders across different sectors and regions.

Cross-Sector Collaboration involves collaborating with other industries, government agencies, and international bodies to share threat intelligence and best practices. This collaboration enables a more comprehensive understanding of the threat landscape, allowing for a more informed and coordinated response. By working together, different sectors can leverage their unique expertise and resources, enhancing the overall ability to detect and respond to threats.

Information Sharing Platforms involve creating platforms for sharing real-time information about threats and vulnerabilities with relevant stakeholders. These platforms enable a coordinated response by providing timely and accurate information to all those involved in maintaining security. Whether through formal channels like Information Sharing and Analysis Centers (ISACs) or more informal networks, information sharing ensures that all stakeholders have the information they need to respond effectively. This collaborative approach enhances the overall ability to detect, analyze, and respond to threats, ensuring a more resilient and secure environment.

References

[1] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber Security and Privacy Issues in Smart Grids,” *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, Fourth 2012.

[2] F. Dalipi and S. Y. Yayilgan, “Security and Privacy Considerations for IoT Application on Smart Grids: Survey and Research Challenges,” in *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*, 2016, pp. 63–68.

[3] J. S. Choi, "A Hierarchical Distributed Energy Management Agent Framework for Smart Homes, Grids, and Cities," *IEEE Commun. Mag.*, vol. 57, no. 7, pp. 113–119, Jul. 2019.
[4] J. Aghaei and M.-I. Alizadeh, "Demand response in smart electricity grids equipped with renewable energy sources: A review," *Renewable Sustainable Energy Rev.*, vol. 18, pp. 64–72, Feb. 2013.
[5] K. M. R. Pothireddy, S. Vuddanti, and S. R. Salkuti, "Impact of Demand Response on Optimal Sizing of Distributed Generation and Customer Tariff," *Energies*, vol. 15, no. 1, p. 190, Dec. 2021.
[6] A. Aljarbouh, M. S. Ahmed, M. Vaquera, and B. D. Dirting, "Intellectualization of information processing systems for monitoring complex objects and systems," *Современные инновации, системы и технологии*, vol. 2, no. 1, pp. 9–17, 2022.
[7] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, "Overview of the Security and Privacy Issues in Smart Grids," in *Smart Grids: Security and Privacy Issues*, K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, Eds. Cham: Springer International Publishing, 2017, pp. 1–16.
[8] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Computer Networks*, vol. 169, p. 107094, Mar. 2020.
[9] S.-K. Kim and J.-H. Huh, "A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective," *Energies*, vol. 11, no. 8, p. 1973, Jul. 2018.
[10] C. Peng, H. Sun, and M. Yang, "A survey on security communication and control for smart grids under malicious cyber attacks," *IEEE Transactions on*, 2019.
[11] R. Qi, C. Rasband, J. Zheng, and R. Longoria, "Detecting cyber attacks in smart grids using semi-supervised anomaly detection and deep representation learning," *Information (Basel)*, vol. 12, no. 8, p. 328, Aug. 2021.
[12] V. Delgado-Gomes, J. F. Martins, C. Lima, and P. N. Borza, "Smart grid security issues," in *2015 9th International Conference on Compatibility and Power Electronics (CPE)*, 2015, pp. 534–538.
[13] P. Jokar, N. Arianpoo, and V. C. M. Leung, "A survey on security issues in smart grids," *Secur. Commun. Netw.*, vol. 9, no. 3, pp. 262–273, Feb. 2016.
[14] L. T. Berger and K. Iniewski, *Smart Grid Applications, Communications, and Security*. Nashville, TN: John Wiley & Sons, 2012.
[15] H. M. Khalid, Q. Ahmed, and J. C.-H. Peng, "Health monitoring of li-ion battery systems: A median expectation diagnosis approach (MEDA)," *IEEE Transactions on Transportation Electrification*, vol. 1, no. 1, pp. 94–105, 2015.
[16] F. Aloul, A. R. Al-Ali, R. Al-Dalky, M. Al-Mardini, and W. El-Hajj, "Smart grid security: Threats, vulnerabilities and solutions," *Int. J. Smart Grid Clean Energy*, pp. 1–6, 2012.
[17] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Cyber Security for Smart Grid Communications," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 998–1010, Fourth 2012.
[18] T. Flick and J. Morehouse, *Securing the smart grid: Next generation power grid security*. Syngress Publishing, 2014.
[19] A. Aljarbouh and B. Caillaud, "On the regularization of chattering executions in real time simulation of hybrid systems," 2015, p. 49.
[20] M. B. Line, I. A. Tøndel, and M. G. Jaatun, "Cyber security challenges in Smart Grids," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, pp. 1–8.
[21] K. G. Boroojeni, M. Hadi Amini, and S. S. Iyengar, *Smart Grids: Security and Privacy Issues*. Springer International Publishing, 2017.

[22] A. R. Metke and R. L. Ekl, “Smart Grid security technology,” in *2010 Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1–7.
[23] H. M. Khalid, Q. Ahmed, J. C.-H. Peng, and G. Rizzoni, “Pack-level current-split estimation for health monitoring in Li-ion batteries,” 2016, pp. 1506–1511.
[24] T. Baumeister, “Literature review on smart grid cyber security,” *Development Laboratory at the University of …*, 2010.
[25] W. Wang and Z. Lu, “Cyber security in the Smart Grid: Survey and challenges,” *Computer Networks*, vol. 57, no. 5, pp. 1344–1371, Apr. 2013.
[26] P. McDaniel and S. McLaughlin, “Security and Privacy Challenges in the Smart Grid,” *IEEE Secur. Priv.*, vol. 7, no. 3, pp. 75–77, May 2009.
[27] S. Jahandari, “Graph-theoretic Identification of Dynamic Networks.” University of Minnesota, 2022.
[28] X. Wu, Z. Bai, J. Jia, and Y. Liang, “A Multi-Variate Triple-Regression Forecasting Algorithm for Long-Term Customized Allergy Season Prediction,” *arXiv preprint arXiv:2005.04557*, 2020.
[29] A. R. Metke and R. L. Ekl, “Security Technology for Smart Grid Networks,” *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, Jun. 2010.
[30] N. Komninos, E. Philippou, and A. Pitsillides, “Survey in Smart Grid and Smart Home Security: Issues, Challenges and Countermeasures,” *IEEE Communications Surveys & Tutorials*, vol. 16, no. 4, pp. 1933–1954, Fourthquarter 2014.
[31] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, “Smart-grid security issues,” *IEEE Secur. Priv.*, vol. 8, no. 1, pp. 81–85, Jan. 2010.
[32] A. O. Otuoze, M. W. Mustafa, and R. M. Larik, “Smart grids security challenges: Classification by sources of threats,” *Journal of Electrical Systems and*, 2018.
[33] A. Aljarbouh, “Selection of the optimal set of versions of N-version software using the ant colony optimization,” 2021, vol. 2094, p. 032026.
[34] S. Umamaheswar, L. G. Kathawate, W. B. Shirsath, S. Gadde, and P. Saradha, “Recent turmeric plants agronomy analysis and methodology using Artificial intelligence,” *International Journal of Botany Studies*, vol. 7, no. 2, pp. 233–236, 2022.
[35] A. Aljarbouh and B. Caillaud, “Robust simulation for hybrid systems: chattering path avoidance,” *arXiv preprint arXiv:1512.07818*, 2015.
[36] W. Hammad, T. O. Sweidan, M. I. Abuashour, H. M. Khalid, and S. M. Muyeen, “Thermal management of grid-tied PV system: A novel active and passive cooling design-based approach,” *IET Renew. Power Gener.*, vol. 15, no. 12, pp. 2715–2725, 2021.
[37] E. Aljdaeh *et al.*, “Performance enhancement of self-cleaning hydrophobic nanocoated photovoltaic panels in a dusty environment,” *Energies*, vol. 14, no. 20, p. 6800, 2021.
[38] N. Osman, H. M. Khalid, O. S. Tha’er, M. I. Abuashour, and S. M. Muyeen, “A PV powered DC shunt motor: Study of dynamic analysis using maximum power Point-Based fuzzy logic controller,” *Energy Conversion and Management: X*, vol. 15, p. 100253, 2022.
[39] G. N. Ericsson, “Cyber security and power system communication—essential parts of a smart grid infrastructure,” *IEEE Trans. Power Delivery*, 2010.
[40] S. Clements and H. Kirkham, “Cyber-security considerations for the smart grid,” *IEEE PES general meeting*, 2010.
[41] J. Liu, Y. Xiao, S. Li, W. Liang, and C. L. P. Chen, “Cyber security and privacy issues in smart grids,” *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 981–997, 2012.
[42] H. M. Khalid, Q. Ahmed, J. C.-H. Peng, and G. Rizzoni, “Current-split estimation in Li-ion battery pack: An enhanced weighted recursive filter method,” *IEEE Transactions on Transportation Electrification*, vol. 1, no. 4, pp. 402–412, 2015.

[43] Z. Bai, R. Yang, and Y. Liang, "Mental task classification using electroencephalogram signal," *arXiv preprint arXiv:1910.03023*, 2019.
[44] S. Jahandari and D. Materassi, "Optimal observations for identification of a single transfer function in acyclic networks," 2021, pp. 852–857.
[45] S. Jahandari and D. Materassi, "Identification of dynamical strictly causal networks," 2018, pp. 4739–4744.
[46] S. Ruj and A. Nayak, "A Decentralized Security Framework for Data Aggregation and Access Control in Smart Grids," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 196–205, Mar. 2013.
[47] T. M. Chen, "Survey of cyber security issues in smart grids," *visual analytics for homeland defense and security …*, 2010.
[48] Z. Lu, X. Lu, W. Wang, and C. Wang, "Review and evaluation of security threats on the communication networks in the smart grid," *2010-Milcom 2010 Military*, 2010.
[49] A. S. Musleh, H. M. Khalid, S. M. Muyeen, and A. Al-Durra, "A prediction algorithm to enhance grid resilience toward cyber attacks in WAMCS applications," *IEEE Syst. J.*, vol. 13, no. 1, pp. 710–719, 2017.
[50] A. Aljarbouh *et al.*, "Application of the K-medians Clustering Algorithm for Test Analysis in E-learning," in *Proceedings of the Computational Methods in Systems and Software*, Springer, 2022, pp. 249–256.
[51] A. Padma, S. Gadde, B. S. P. Rao, and G. Ramachandran, "Effective Cleaning System management using JSP and Servlet Technology," 2021, pp. 1472–1478.
[52] S. Jahandari, A. Kalhor, and B. N. Araabi, "A self tuning regulator design for nonlinear time varying systems based on evolving linear models," *Evolving Systems*, vol. 7, pp. 159–172, 2016.
[53] A. Aljarbouh, A. Duracz, Y. Zeng, B. Caillaud, and W. Taha, "Chattering-free simulation for hybrid dynamical systems," *HAL*, vol. 2016, 2016.
[54] K. Kimani, V. Oduol, and K. Langat, "Cyber security challenges for IoT-based smart grid networks," *Int. J. Crit. Infrastruct.*, 2019.
[55] A. Anwar and A. N. Mahmood, "Cyber security of smart grid infrastructure," *arXiv preprint arXiv:1401.3936*, 2014.
[56] Z. Ni and S. Paul, "A Multistage Game in Smart Grid Security: A Reinforcement Learning Solution," *IEEE Trans Neural Netw Learn Syst*, vol. 30, no. 9, pp. 2684–2695, Sep. 2019.
[57] H. M. Khalid, S. M. Muyeen, and J. C.-H. Peng, "Cyber-attacks in a looped energy-water nexus: An inoculated sub-observer-based approach," *IEEE Syst. J.*, vol. 14, no. 2, pp. 2054–2065, 2019.
[58] K. Thiagarajan, C. K. Dixit, M. Panneerselvam, C. A. Madhuvappan, S. Gadde, and J. N. Shrote, "Analysis on the Growth of Artificial Intelligence for Application Security in Internet of Things," 2022, pp. 6–12.
[59] S. Shapsough, F. Qatan, R. Aburukba, F. Aloul, and A. R. Al Ali, "Smart grid cyber security: Challenges and solutions," in *2015 International Conference on Smart Grid and Clean Energy Technologies (ICSGCE)*, 2015, pp. 170–175.
[60] I. L. G. Pearson, "Smart grid cyber security for Europe," *Energy Policy*, 2011.
[61] S. Tan, D. De, W.-Z. Song, J. Yang, and S. K. Das, "Survey of Security Advances in Smart Grid: A Data Driven Approach," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397–422, Firstquarter 2017.
[62] H. M. Khalid and J. C.-H. Peng, "Bidirectional charging in V2G systems: An in-cell variation analysis of vehicle batteries," *IEEE Syst. J.*, vol. 14, no. 3, pp. 3665–3675, 2020.
[63] A. Aljarbouh and B. Caillaud, "Chattering-free simulation of hybrid dynamical systems with the functional mock-up interface 2.0," 2016, vol. 124, pp. 95–105.

[64] C. Bekara, "Security issues and challenges for the IoT-based smart grid," *Procedia Comput. Sci.*, 2014.
[65] Y. Wang, D. Ruan, D. Gu, J. Gao, and D. Liu, "Analysis of smart grid security standards," *2011 IEEE*, 2011.
[66] E. Bou-Harb, C. Fachkha, and M. Pourzandi, "Communication security for smart grid distribution networks," *IEEE*, 2013.
[67] S. Jahandari, A. Kalhor, and B. N. Araabi, "Order determination and transfer function estimation of linear mimo systems: application to environmental modeling," *Environmental Modeling and Software*, 2016.
[68] E. Santacana, G. Rackliffe, and L. Tang, "Getting smart," *IEEE Power Energ. Mag.*, 2010.
[69] F. Skopik and P. D. Smith, "Smart grid security: Innovative solutions for a modernized grid," 2015.
[70] D. B. Rawat and C. Bajracharya, "Cyber security for smart grid systems: Status, challenges and perspectives," in *SoutheastCon 2015*, 2015, pp. 1–6.
[71] S. Jahandari, F. F. Beyglou, A. Kalhor, and M. T. Masouleh, "A robust adaptive linear control for a ball handling mechanism," 2014, pp. 376–381.
[72] A. Bari, J. Jiang, and W. Saad, "Challenges in the smart grid applications: An overview," *International Journal of*, 2014.
[73] D. Faquir, N. Chouliaras, V. Sofia, and K. Olga, "Cybersecurity in smart grids, challenges and solutions," *AIMS Electronics and*, 2021.
[74] S. M. Muyeen and S. Rahman, *Communication, control and security challenges for the smart grid*. Stevenage, England: Institution of Engineering and Technology, 2017.
[75] S. Jahandari, A. Kalhor, and B. N. Araabi, "Online forecasting of synchronous time series based on evolving linear models," *IEEE Trans. Syst. Man Cybern.*, vol. 50, no. 5, pp. 1865–1876, 2018.
[76] C. Barreto and A. A. Cárdenas, "Impact of the Market Infrastructure on the Security of Smart Grids," *IEEE Trans. Ind. Inf.*, vol. 15, no. 7, pp. 4342–4351, Jul. 2019.
[77] J. Wu, K. Ota, M. Dong, and J. Li, "Big data analysis-based security situational awareness for smart grid," *IEEE Transactions on Big*, 2016.
[78] I. Butun, A. Lekidis, and D. R. dos Santos, "Security and Privacy in Smart Grids: Challenges, Current Solutions and Future Opportunities," *ICISSP*, 2020.
[79] S. Jahandari and D. Materassi, "Topology identification of dynamical networks via compressive sensing," *IFAC-PapersOnLine*, vol. 51, no. 15, pp. 575–580, 2018.
[80] S. Jahandari and D. Materassi, "Sufficient and necessary graphical conditions for miso identification in networks with observational data," *IEEE Trans. Automat. Contr.*, vol. 67, no. 11, pp. 5932–5947, 2021.
[81] Z. Wang, D. Jiang, F. Wang, Z. Lv, and R. Nowak, "A polymorphic heterogeneous security architecture for edge-enabled smart grids," *Sustainable Cities and Society*, vol. 67, p. 102661, Apr. 2021.
[82] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. F. Wang, "Impact of cyber-security issues on Smart Grid," in *2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies*, 2011, pp. 1–7.
[83] F. Dalipi and S. Y. Yayilgan, "Security and privacy considerations for IoT application on smart grids: Survey and research challenges," *Conference on Future Internet of Things …*, 2016.
[84] A. Sanjab, W. Saad, I. Guvenc, and A. Sarwat, "Smart grid security: Threats, challenges, and solutions," *arXiv preprint arXiv*, 2016.
[85] A. Aljarbouh, Y. Zeng, A. Duracz, B. Caillaud, and W. Taha, "Chattering-free simulation for hybrid dynamical systems semantics and prototype implementation," 2016, pp. 412–422.

[86] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 697–707, 2015.
[87] K. Thiagarajan, M. Porkodi, S. Gadde, and R. Priyadharshini, "Application and Advancement of Sensor Technology in Bioelectronics Nano Engineering," 2022, pp. 841–845.
[88] D. Nelson-Gruel, Y. Chamaillard, and A. Aljarbouh, "Modeling and estimation of the pollutants emissions in the Compression Ignition diesel engine," 2016, pp. 317–322.
[89] A. Duracz *et al.*, "Advanced hazard analysis and risk assessment in the ISO 26262 functional safety standard using rigorous simulation," 2020, pp. 108–126.
[90] A. A. A. Ahmed, A. Aljabouh, P. K. Donepudi, and M. S. Choi, "Detecting fake news using machine learning: A systematic literature review," *arXiv preprint arXiv:2102.04458*, 2021.
[91] H. M. Khalid *et al.*, "Dust accumulation and aggregation on PV panels: An integrated survey on impacts, mathematical models, cleaning mechanisms, and possible sustainable solution," *Solar Energy*, vol. 251, pp. 261–285, 2023.
[92] L. Kotut and L. A. Wahsheh, "Survey of Cyber Security Challenges and Solutions in Smart Grids," in *2016 Cybersecurity Symposium (CYBERSEC)*, 2016, pp. 32–37.
[93] G. N. Sorebo and M. C. Echols, *Smart grid security: An end-to-end view of security in the new electrical grid*. Boca Raton, FL: CRC Press, 2011.
[94] S. Goel, Y. Hong, V. Papakonstantinou, and D. Kloza, "Smart grid security," 2015.
[95] H. M. Khalid and J. C.-H. Peng, "A Bayesian algorithm to enhance the resilience of WAMS applications against cyber attacks," *IEEE Trans. Smart Grid*, vol. 7, no. 4, pp. 2026–2037, 2016.
[96] J. Sakhnini, H. Karimipour, A. Dehghantanha, and R. M. Parizi, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," *Internet of things*, 2021.
[97] Z. El Mrabet, N. Kaabouch, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," *Comput. Electr. Eng.*, 2018.
[98] K. G. Boroojeni, M. H. Amini, and S. S. Iyengar, "Overview of the security and privacy issues in smart grids," *Smart grids: security and*, 2017.
[99] D. Ghelani, "Cyber Security in Smart Grids, Threats, and Possible Solutions," *Authorea Preprints*, 2022.
[100] Y. Mo *et al.*, "Cyber–Physical Security of a Smart Grid Infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–209, Jan. 2012.
[101] C. Clastres, "Smart grids: Another step towards competition, energy security and climate change objectives," *Energy Policy*, vol. 39, no. 9, pp. 5399–5408, Sep. 2011.
[102] S. Jahandari and A. Srivastava, "Adjusting for Unmeasured Confounding Variables in Dynamic Networks," *IEEE Control Systems Letters*, vol. 7, pp. 1237–1242, 2023.
[103] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research*, vol. 215, p. 108975, Feb. 2023.
[104] A. S. Bretas, N. G. Bretas, B. Carvalho, E. Baeyens, and P. P. Khargonekar, "Smart grids cyber-physical security as a malicious data attack: An innovation approach," *Electric Power Systems Research*, vol. 149, pp. 210–219, Aug. 2017.
[105] E.-K. Lee, M. Gerla, and S. Y. Oh, "Physical layer security in wireless smart grid," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 46–52, Aug. 2012.
[106] H. M. Khalid *et al.*, "WAMS operations in power grids: A track fusion-based mixture density estimation-driven grid resilient approach toward cyberattacks," *IEEE Syst. J.*, 2023.

[107] A. Aljarbouh, "Accelerated Simulation of Hybrid Systems: Method combining static analysis and run-time execution analysis.(Simulation Accélérée des Systèmes Hybrides: méthode combinant analyse statique et analyse à l'exécution)." University of Rennes 1, France, 2017.

[108] A. J. Albarakati *et al.*, "Real-time energy management for DC microgrids using artificial intelligence," *Energies*, vol. 14, no. 17, p. 5307, 2021.

[109] I. Trifonov, A. Aljarbouh, and A. Beketaeva, "Evaluating the effectiveness of turbulence models in the simulation of two-phases combustion," *International Review on Modelling and Simulations*, vol. 14, no. 4, pp. 291–300, 2021.

[110] R. Jabeur, Y. Boujoudar, M. Azeroual, A. Aljarbouh, and N. Ouaaline, "Microgrid energy management system for smart home using multi-agent system," *Int. J. Elect. Computer Syst. Eng.*, vol. 12, no. 2, pp. 1153–1160, 2022.

[111] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid — the new and improved power grid: A survey," *IEEE Commun. Surv. Tutor.*, vol. 14, no. 4, pp. 944–980, Fourth 2012.

[112] X. Li, X. Liang, R. Lu, X. Shen, and X. Lin, "Securing smart grid: cyber attacks, countermeasures, and challenges," *IEEE Communications*, 2012.

[113] S. N. Islam, Z. Baig, and S. Zeadally, "Physical Layer Security for the Smart Grid: Vulnerabilities, Threats, and Countermeasures," *IEEE Trans. Ind. Inf.*, vol. 15, no. 12, pp. 6522–6530, Dec. 2019.

[114] Y. Liang and W. Liang, "ResWCAE: Biometric Pattern Image Denoising Using Residual Wavelet-Conditioned Autoencoder," *arXiv preprint arXiv:2307.12255*, 2023.

[115] H. M. Khalid, F. Flitti, S. M. Muyeen, M. S. Elmoursi, O. S. Tha'er, and X. Yu, "Parameter estimation of vehicle batteries in V2G systems: An exogenous function-based approach," *IEEE Trans. Ind. Electron.*, vol. 69, no. 9, pp. 9535–9546, 2021.

[116] J. Y. Kim and Y. Kim, "Benefits of cloud computing adoption for smart grid security from security perspective," *J. Supercomput.*, 2016.

[117] M. K. Hasan, A. Habib, Z. Shukur, and F. Ibrahim, "Review on cyber-physical and cyber-security system in smart grid: Standards, protocols, constraints, and recommendations," *Journal of Network and*, 2023.

[118] C. P. Vineetha and C. A. Babu, "Smart grid challenges, issues and solutions," *Green Building and Smart Grid …*, 2014.

[119] Y. Liang, W. Liang, and J. Jia, "Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN," *arXiv e-prints*, p. arXiv-2303, 2023.

[120] M. Atalay and P. Angin, "A Digital Twins Approach to Smart Grid Security Testing and Standardization," in *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, 2020, pp. 435–440.

[121] S. Bera, S. Misra, and J. J. P. C. Rodrigues, "Cloud Computing Applications for Smart Grid: A Survey," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 5, pp. 1477–1494, May 2015.

[122] Q. Wang, G. Zhang, and F. Wen, "A survey on policies, modelling and security of cyber-physical systems in smart grids," *Energy Convers. Econ.*, vol. 2, no. 4, pp. 197–211, Dec. 2021.

[123] Y. Liang, "Structural Vibration Signal Denoising Using Stacking Ensemble of Hybrid CNN-RNN. Advances in Artificial Intelligence and Machine Learning. 2022; 3 (2): 65." 2006.

[124] Y. Zhu *et al.*, "Application of Physics-Informed Neural Network (PINN) in the Experimental Study of Vortex-Induced Vibration with Tunable Stiffness," in *The 33rd International Ocean and Polar Engineering Conference*, 2023.

[125] S. S. Devi, S. Gadde, K. Harish, C. Manoharan, R. Mehta, and S. Renukadevi, "IoT and image processing Techniques-Based Smart Sericulture Nature System," *Indian J. Applied & Pure Bio*, vol. 37, no. 3, pp. 678–683, 2022.

[126] D. Al Momani *et al.*, "Energy saving potential analysis applying factory scale energy audit–A case study of food production," *Heliyon*, vol. 9, no. 3, 2023.

[127] Z. Said *et al.*, "Intelligent approaches for sustainable management and valorisation of food waste," *Bioresour. Technol.*, p. 128952, 2023.

[128] A. S. Musleh, M. Debouza, H. M. Khalid, and A. Al-Durra, "Detection of false data injection attacks in smart grids: A real-time principle component analysis," 2019, vol. 1, pp. 2958–2963.

[129] A. Alamin, H. M. Khalid, and J. C.-H. Peng, "Power system state estimation based on Iterative Extended Kalman Filtering and bad data detection using normalized residual test," 2015, pp. 1–5.

[130] A. Chavez, D. Koutentakis, Y. Liang, S. Tripathy, and J. Yun, "Identify statistical similarities and differences between the deadliest cancer types through gene expression," *arXiv preprint arXiv:1903.07847*, 2019.

[131] I. Pozharkova, A. Aljarbouh, S. H. Azizam, A. P. Mohamed, F. Rabbi, and R. Tsarev, "A simulation modeling method for cooling building structures by fire robots," 2022, pp. 504–511.

[132] M. Azeroual, Y. Boujoudar, A. Aljarbouh, H. El Moussaoui, and H. El Markhi, "A multi-agent-based for fault location in distribution networks with wind power generator," *Wind Engineering*, vol. 46, no. 3, pp. 700–711, 2022.

[133] I. Haq *et al.*, "Machine Vision Approach for Diagnosing Tuberculosis (TB) Based on Computerized Tomography (CT) Scan Images," *Symmetry* , vol. 14, no. 10, p. 1997, 2022.

[134] A. K. Das and S. Zeadally, "Chapter 13 - Data Security in the Smart Grid Environment," in *Pathways to a Smarter Power System*, A. Taşcıkaraoğlu and O. Erdinç, Eds. Academic Press, 2019, pp. 371–395.

[135] F. A. Khan, M. Asif, A. Ahmad, and M. Alharbi, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustainable Cities and*, 2020.

[136] S. S. Ali and B. J. Choi, "State-of-the-art artificial intelligence techniques for distributed smart grids: A review," *Electronics*, 2020.

[137] H. M. Khalid, F. Flitti, M. S. Mahmoud, M. M. Hamdan, S. M. Muyeen, and Z. Y. Dong, "Wide area monitoring system operations in modern power grids: A median regression function-based state estimation approach towards cyber attacks," *Sustainable Energy, Grids and Networks*, vol. 34, p. 101009, 2023.

[138] S. M. Amin and A. M. Giacomoni, "Smart Grid, Safe Grid," *IEEE Power Energ. Mag.*, vol. 10, no. 1, pp. 33–40, Jan. 2012.

[139] S. De Dutta and R. Prasad, "Security for Smart Grid in 5G and Beyond Networks," *Wireless Personal Communications*, vol. 106, no. 1, pp. 261–273, May 2019.

[140] A. J. McBride and A. R. McGee, "Assessing smart Grid security," *Bell Labs Tech. J.*, vol. 17, no. 3, pp. 87–103, Dec. 2012.

[141] S. Jahandari and D. Materassi, "How Can We Be Robust Against Graph Uncertainties?," 2023, pp. 1946–1951.

[142] M. Shrestha, C. Johansen, J. Noll, and D. Roverso, "A Methodology for Security Classification applied to Smart Grid Infrastructures," *Int. J. Crit. Infrastruct. Prot.*, vol. 28, p. 100342, Mar. 2020.

[143] A. M. Kosek, "Contextual anomaly detection for cyber-physical security in Smart Grids based on an artificial neural network model," in *2016 Joint Workshop on Cyber- Physical Security and Resilience in Smart Grids (CPSR-SG)*, 2016, pp. 1–6.

[144] Y. F. Wang, W. M. Lin, T. Zhang, and Y. Y. Ma, "Research on application and security protection of Internet of Things in smart grid," p. 1.54-1.54, Jan. 2012.

[145] S. Jahandari, A. Kalhor, and B. N. Araabi, "Order determination and robust adaptive control of unknown deterministic input-affine systems: An operational controller," 2016, pp. 3831–3836.

[146] S. Gadde, E. Karthika, R. Mehta, S. Selvaraju, W. B. Shirsath, and J. Thilagavathi, "Onion growth monitoring system using internet of things and cloud," *Agricultural and Biological Research*, vol. 38, no. 3, pp. 291–293, 2022.

[147] S. Jahandari and D. Materassi, "Analysis and compensation of asynchronous stock time series," 2017, pp. 1085–1090.

[148] A. Aljarbouh, "Accelerated simulation of hybrid systems: method combining static analysis and run-time execution analysis." Rennes 1, 2017.

[149] P. Srikantha and D. Kundur, "A DER attack-mitigation differential game for smart grid security analysis," *IEEE Trans. Smart Grid*, 2015.

[150] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A Survey on Smart Grid Communication Infrastructures: Motivations, Requirements and Challenges," *IEEE Communications Surveys & Tutorials*, vol. 15, no. 1, pp. 5–20, First 2013.

[151] H. Maziku, S. Shetty, and D. M. Nicol, "Security risk assessment for SDN-enabled smart grids," *Comput. Commun.*, 2019.

[152] Z. Rafique, H. M. Khalid, and S. M. Muyeen, "Communication systems in distributed generation: A bibliographical review and frameworks," *IEEE Access*, vol. 8, pp. 207226–207239, 2020.

[153] S. Ashraf, M. H. Shawon, H. M. Khalid, and S. M. Muyeen, "Denial-of-service attack on IEC 61850-based substation automation system: A crucial cyber threat towards smart substation pathways," *Sensors* , vol. 21, no. 19, p. 6415, 2021.

[154] M. S. Mahmoud, H. M. Khalid, and M. M. Hamdan, *Cyberphysical infrastructures in power systems: architectures and vulnerabilities*. Academic Press, 2021.

[155] Z. Rafique, H. M. Khalid, S. M. Muyeen, and I. Kamwa, "Bibliographic review on power system oscillations damping: An era of conventional grids and renewable energy integration," *Int. J. Electr. Power Energy Syst.*, vol. 136, p. 107556, 2022.

[156] M. Sathanapriya *et al.*, "Analysis of Hydroponic System Crop Yield Prediction and Crop IoT-based monitoring system for precision agriculture," 2022, pp. 575–578.

[157] A. Aljarbouh, "Non-standard zeno-free simulation semantics for hybrid dynamical systems," 2019, pp. 16–31.

[158] S. Jahandari and A. Srivastava, "Detection of Delays and Feedthroughs in Dynamic Networked Systems," *IEEE Control Systems Letters*, vol. 7, pp. 1201–1206, 2022.

[159] H. Vijayakumar, A. Seetharaman, and K. Maddulety, "Impact of AIServiceOps on Organizational Resilience," 2023, pp. 314–319.

[160] R. K. Pandey and M. Misra, "Cyber security threats—Smart grid infrastructure," *2016 National power systems conference*, 2016.

[161] K. C. Sou, H. Sandberg, and K. H. Johansson, "On the Exact Solution to a Smart Grid Cyber-Security Analysis Problem," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 856–865, Jun. 2013.

[162] A. Hahn, A. Ashok, S. Sridhar, and M. Govindarasu, "Cyber-Physical Security Testbeds: Architecture, Application, and Evaluation for Smart Grid," *IEEE Trans. Smart Grid*, vol. 4, no. 2, pp. 847–855, Jun. 2013.

[163] D. Wei, Y. Lu, M. Jafari, and P. Skare, "An integrated security system of protecting smart grid against cyber attacks," *Innovative Smart Grid …*, 2010.

[164] T. N. Nguyen, B.-H. Liu, N. P. Nguyen, and J.-T. Chou, "Cyber Security of Smart Grid: Attacks and Defenses," in *ICC 2020 - 2020 IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[165] H. Vijayakumar, "Revolutionizing Customer Experience with AI: A Path to Increase Revenue Growth Rate," 2023, pp. 1–6.

[166] S. M. Amin, "Smart grid security, privacy, and resilient architectures: Opportunities and challenges," in *2012 IEEE Power and Energy Society General Meeting*, 2012, pp. 1–2.

[167] T. Alsuwian, A. Shahid Butt, and A. A. Amin, "Smart Grid Cyber Security Enhancement: Challenges and Solutions—A Review," *Sustain. Sci. Pract. Policy*, 2022.

[168] A. P. A. Ling and M. Masao, "Selection of Model in Developing Information Security Criteria on Smart Grid Security System," in *2011 IEEE Ninth International Symposium on Parallel and Distributed Processing with Applications Workshops*, 2011, pp. 91–98.

[169] H. Vijayakumar, "Business Value Impact of AI-Powered Service Operations (AIServiceOps)," *Available at SSRN 4396170*, 2023.

[170] S. Jahandari and D. Materassi, "Optimal selection of observations for identification of multiple modules in dynamic networks," *IEEE Trans. Automat. Contr.*, vol. 67, no. 9, pp. 4703–4716, 2022.

[171] R. Leszczyna, "Standards on cyber security assessment of smart grid," *Int. J. Crit. Infrastruct. Prot.*, vol. 22, pp. 70–89, Sep. 2018.

[172] E. D. Knapp and R. Samani, "Applied cyber security and the smart grid: implementing security controls into the modern power infrastructure," 2013.

[173] A. Goudarzi, F. Ghayoor, M. Waseem, S. Fahad, and I. Traore, "A Survey on IoT-Enabled Smart Grids: Emerging, Applications, Challenges, and Outlook," *Energies*, vol. 15, no. 19, p. 6984, Sep. 2022.

[174] J. A. Albarakati *et al.*, "Multi-Agent-Based Fault Location and Cyber-Attack Detection in Distribution System," *Energies*, vol. 16, no. 1, p. 224, 2022.

[175] Y. Boujoudar *et al.*, "Fuzzy logic-based controller of the bidirectional direct current to direct current converter in microgrid," *Int. J. Elect. Computer Syst. Eng.*, vol. 13, no. 5, pp. 4789–4797, 2023.

[176] A. J. Albarakati *et al.*, "Microgrid energy management and monitoring systems: A comprehensive review," *Frontiers in Energy Research*, vol. 10, p. 1097858, 2022.

[177] G. Samata, P. Sudhakar, and G. Jyothsna, "In silico Analysis of Spike Protein Glycoprotein A of Omicron variant and identification of variant specific peptide based Vaccine," *Research Journal of Biotechnology Vol*, vol. 18, p. 7, 2023.

[178] H. M. Khalid and J. C.-H. Peng, "Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 680–688, 2014.

[179] K. Moslehi and R. Kumar, "Smart Grid - a reliability perspective," in *2010 Innovative Smart Grid Technologies (ISGT)*, 2010, pp. 1–8.

[180] T. Vijayapriya and D. P. Kothari, "Smart Grid: An Overview," *Smart Grid Renew. Energy*, vol. 02, no. 04, pp. 305–311, 2011.

[181] P. Palensky and F. Kupzog, "Smart grids," *Annu. Rev. Environ. Resour.*, 2013.

[182] S. Alahmari *et al.*, "Hybrid Multi-Strategy Aquila Optimization with Deep Learning Driven Crop Type Classification on Hyperspectral Images," *Comput. Syst. Sci. Eng.*, vol. 47, no. 1, pp. 375–391, 2023.

[183] S. Yonbawi *et al.*, "Modified Metaheuristics with Transfer Learning Based Insect Pest Classification for Agricultural Crops," *Computer Systems Science & Engineering*, vol. 46, no. 3, 2023.

[184] E. Lee, F. Rabbi, H. Almashaqbeh, A. Aljarbouh, J. Ascencio, and N. V. Bystrova, "The issue of software reliability in program code cloning," 2023, vol. 2700.

[185] U. Inayat, M. F. Zia, S. Mahmood, H. M. Khalid, and M. Benbouzid, "Learning-based methods for cyber attacks detection in IoT systems: A survey on methods, analysis, and future prospects," *Electronics*, vol. 11, no. 9, p. 1502, 2022.

[186] H. M. Khalid, S. M. Muyeen, and I. Kamwa, "An improved decentralized finite-time approach for excitation control of multi-area power systems," *Sustainable Energy, Grids and Networks*, vol. 31, p. 100692, 2022.

[187] V. Rutskiy *et al.*, "Prospects for the Use of Artificial Intelligence to Combat Fraud in Bank Payments," in *Proceedings of the Computational Methods in Systems and Software*, Springer, 2022, pp. 959–971.

[188] N. Sharmili *et al.*, "Earthworm Optimization with Improved SqueezeNet Enabled Facial Expression Recognition Model," *Computer Systems Science & Engineering*, vol. 46, no. 2, 2023.

[189] W. Liang, Y. Liang, and J. Jia, "MiAMix: Enhancing Image Classification through a Multi-stage Augmented Mixied Sample Data Augmentation Method," *arXiv preprint arXiv:2308.02804*, 2023.

[190] M. Uslar *et al.*, *Standardization in Smart Grids*. Springer Berlin Heidelberg, 2013.

[191] H. Lei, B. Chen, and K. L. Butler-Purry, "Security and reliability perspectives in cyber-physical smart grids," *Innovative Smart Grid …*, 2018.

[192] Y. Simmhan, A. G. Kumbhare, B. Cao, and V. Prasanna, "An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds," in *2011 IEEE 4th International Conference on Cloud Computing*, 2011, pp. 582–589.

[193] A. Aljarbouh, M. Fayaz, and M. S. Qureshi, "Non-Standard Analysis for Regularization of Geometric-Zeno Behaviour in Hybrid Systems," *Systems*, vol. 8, no. 2, p. 15, 2020.

[194] H. M. Khalid and J. C.-H. Peng, "Tracking electromechanical oscillations: An enhanced maximum-likelihood based approach," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 1799–1808, 2015.

[195] L. Leffler, "The NERC program for the electricity sector critical infrastructure protection," *2001 IEEE Power Engineering Society Winter*, 2001.

[196] R. Lepofsky and R. Lepofsky, "North american energy council security standard for critical infrastructure protection (nerc cip)," *Security: A Concise Guide to the Weaker Side of …*, 2014.

[197] R. Slayton and A. Clark-Ginsberg, "Beyond regulatory capture: Coproducing expertise for critical infrastructure protection," *Regulation & Governance*, 2018.

[198] J. Marron, A. Gopstein, and D. Bogle, "Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards," *J. Res. Natl. Inst. Stand. Technol.*, 2021.

[199] T. Kuruganti, W. Dykas, W. Manges, and T. Flowers, "Wireless System Considerations When Implementing NERC Critical Infrastructure Protection Standards," *Energy Reliability, US …*, 2009.