# ***Summary***

## Article 153

The paper titled "Challenges of the Existing Security Measures Deployed in the Smart Grid Framework" presents an analysis of the security challenges faced by the smart grid infrastructure. The study aims to identify and address the unresolved problems related to privacy and security in the smart grid.

The paper starts with an introduction that highlights the importance of smart grid security and the increasing integration of smart devices in the smart grid infrastructure. The authors then provide an overview of the smart grid, its benefits, and the current scenario in India. In the next section, the paper delves into the security challenges in key operational technologies such as ICS, SCADA, and AMI. The vulnerabilities, attack surfaces, and types of attackers in these systems are discussed in detail. The paper also highlights the communication systems used in smart metering and the various techniques used for data tampering and manipulation.

The authors conclude the paper by highlighting the need for further research and development in the field of smart grid security. The paper provides a comprehensive analysis of the security challenges faced by the smart grid infrastructure and highlights the need for a robust and secure communication channel for data exchange between different entities in the smart grid ecosystem. Overall, the paper presents a valuable contribution to the field of smart grid security and highlights the need for continuous improvement and innovation in the area .

However, the paper does not present any new research or findings on these topics, it mostly reviews the existing literature and studies, and summarize the challenges in smart grid security. It also lacks any detail on the research methodology used in the paper. It also does not provide any solutions or recommendations to mitigate the challenges discussed in the paper.

## Article 154

The paper titled "Improving Cyber-Security of Smart Grid Systems via Anomaly Detection and Linguistic Domain Knowledge" proposes a novel anomaly detection architecture for enhancing the cyber-security of smart grid systems. The proposed system applies a previously developed network security cyber-sensor method to individual selected communication streams, allowing for learning accurate normal network behavior models. In addition, an Interval Type-2 Fuzzy Logic System (IT2 FLS) is used to model human background knowledge about the network system and to dynamically adjust the sensitivity threshold of the anomaly detection algorithms.

The authors argue that the complexity of common network architectures and the presence of multiple diverse communication streams make it difficult to build a single comprehensive normal behavior model

for a specific network communication system. They also point out that the performance of anomaly detection algorithms can be tuned by adjusting a sensitivity threshold, which inevitably leads to a trade-off between false positives and false negatives rates. The proposed system aims to alleviate these issues by applying a cyber-sensor method to individual selected communication streams and by using an IT2 FLS to model human background knowledge about the network system and to dynamically adjust the sensitivity threshold of the anomaly detection algorithms.

The authors provide a detailed description of the proposed system, including the use of Interval Type-2 Fuzzy Logic Systems (IT2 FLSs) for modeling linguistic uncertainty in describing the relationship between various network communication attributes and the possibility of a cyber-attack. They also present the results of the proposed method on an experimental smart grid system and demonstrate the enhanced cyber-security of the system. Overall, the paper provides a clear and well-structured presentation of the proposed system, and it is an interesting contribution in the field of cyber-security of smart grid systems. However, it would be valuable to have further evaluation of the proposed system in terms of its scalability, robustness, and its performance against different types of cyber-attacks.

## Article 155

The paper titled "Role of Cloud Computing for Smart Grid of India and its Cyber Security" discusses the potential benefits of using cloud computing to support the development of India's smart grid. The authors argue that the application of the cloud computing model meets the requirements of data and computing intensive smart grid applications, and that using internal network improves the calculation, storage capacity, and data security of the overall system, reducing the system expansion investment. They also focus on distributed verification protocol to guarantee the data storage security in cloud computing and propose an internet connectivity device model instead of having C.P.U. and discs, for cloud computing.

However, the paper also discusses the challenges and potential solutions related to ensuring data security and privacy in this context. The authors mention that Smart Grids have a greater exposure to cyber-attacks that can potentially disrupt power supply in a city, therefore, ensuring privacy of personally identifiable data within the utility‘s information integration platform is of growing concern. They highlight that Smart Grid applications will have to be designed with security and privacy in mind and favor the use of cloud as a security for smart grid.

In summary, the paper presents the potential benefits of using cloud computing for smart grid and its cyber security, but also acknowledges the challenges related to data security and privacy. The authors suggest solutions to improve data security by implementing distributed verification protocol and propose an internet connectivity device model, however, it does not provide any specific research results or conclusions about the effectiveness of these approaches, or the impact of these issues on the reliability of the system.

## Article 156

The paper entitled "Data Communication Security of Advanced Metering Infrastructure in Smart Grid" presents a method for enhancing the security of communication in the Advanced Metering Infrastructure (AMI) of a smart grid. The authors argue that the AMI is a critical component of a smart grid, as it involves the communication of vital data from smart meters to a central control center, and the security of this communication is essential for the overall security and reliability of the grid. To address the security challenges of the AMI, the authors propose a two-phase method that uses a dedicated authentication server to prevent unauthorized and malicious nodes from gaining access to the AMI communication network.

The authors evaluate the proposed method through simulations, and the results show that it is effective at improving the security and performance of the AMI communication network. Specifically, the results show that the proposed method can improve data integrity, confidentiality, and non-repudiation, as well as increase network throughput and packet delivery ratio. The authors also reported that the proposed method can address the key challenges related to the cyber security of smart grid systems, and it is a reliable communication solution for the AMI in a smart grid.

In conclusion, the paper provides a valuable contribution to the field of smart grid security by proposing a method for enhancing the security of communication in the AMI. The results of the simulation studies show that the proposed method is effective at improving the security and performance of the AMI communication network. This research can be a starting point for future research to implement and evaluate the proposed method in real-world smart grid systems, to validate.

## Article 157

The Advanced Metering Infrastructure (AMI) is a core component of smart grids that exhibit highly complex network configurations comprising of heterogeneous cyber-physical components. These components are interconnected through different communication media, protocols, and secure tunnels, and they are operated using different data delivery modes and security policies. The inherent complexity and heterogeneity in AMI significantly increase the potential of security threats due to misconfiguration or absence of defense, which may cause devastating damage to AMI.

To address this problem, in this research paper, the authors proposed Smart Analyzer, a formal security analysis tool, which offers manifold contributions: (i) formal modeling of AMI configuration including device configurations, topology, communication properties, interactions between the devices, data

flows, and security properties; (ii) formal modeling of AMI invariant and user-driven constraints based on the interdependencies between AMI device configurations, security properties, and security control guidelines; (iii) verifying the AMI configuration's compliances with security constraints using Satisfiability Modulo Theory (SMT) solver; (iv) generating a comprehensive security threat report with possible remediation plan based on the verification results.

The performance of Smart Analyzer was evaluated in terms of accuracy, usability, and scalability, using a combination of real and synthetic data. The results of the study suggest that Smart Analyzer is an effective tool for identifying and mitigating potential security threats in AMI systems in a smart grid, with strong performance in terms of accuracy, usability, and scalability. Smart Analyzer is a valuable contribution to the field of smart grid security and can be used to ensure the security and reliability of AMI systems in smart grids.

### Article 158

The research paper titled "Security Evaluation of Two Intrusion Detection Systems in Smart Grid SCADA Environment" presents the application of two anomaly-based intrusion detection systems (AbIDS) in detecting stealthy cyber-attacks on a SCADA control system. The authors have applied the IDS tools Snort and Bro in designing the IDS and later, compared their performances in terms of detection rate and latency in the alert packets with a motive of selecting a better IDS for the SCADA security.

The authors have implemented the SCADA based protection scheme which performs an autonomous protection to mitigate the system disturbances. They have first implemented the stealthy cyber-attack which compromised the SCADA controller followed by data integrity attack on the system generator. Next, they perform the impact analysis during the attack followed by performance evaluation of IDS tools. The authors found that both Snort and Bro were effective in detecting the attacks within an acceptable time frame, although they did not find significant differences in the performance of the two IDS tools.

The research results provide evidence that IDS tools can be used to protect SCADA systems from cyber threats and highlight the need for further research to understand the differences more fully between IDS tools and to identify the best IDS for SCADA security. The results of the paper can be used to improve the security of critical infrastructure such as the power grid, which is increasingly reliant on SCADA systems and vulnerable to cyber threats. The paper also suggests some future research directions for the field.

### Article 159

The paper titled "A Study of Linear Programming and Reinforcement Learning for One-Shot Game in Smart Grid Security" presents an analysis of the interactions between attackers and defenders in a one-

shot game in smart power systems. The authors investigate solutions for one-shot games using linear programming and reinforcement learning techniques, and use game theory to model the interactions between the attacker and defender. The paper demonstrates the proposed game on both a 6 bus system and an IEEE 30 bus system, and analyzes the optimal solutions obtained.

The authors first use linear programming to design a one-shot game with multi-line-switching attack and solve it. They also use reinforcement learning to design a game with single-line-switching attack and solve it. The pay-off and utility/reward of the game is calculated based on the generation loss due to the attack initiated by the attacker. The defender's defense action is also considered while evaluating the pay-off from both the attacker's and defender's action. The linear programming based solution gives the probability of choosing the best attack actions against different defense actions. The reinforcement learning based solution gives the optimal action to take under the selected defense action.

Overall, the paper provides a framework for modeling and analyzing the interactions between attackers and defenders in smart power systems using game theory and machine learning techniques. The results of the study may be useful in helping to improve the security of smart grids by providing insight into the potential vulnerabilities of the systems and by finding optimal strategies for each player. The use of game theory and machine learning techniques in this context may also help to identify emergent areas of vulnerabilities in smart grid security that need further exploration.

## Article 160

In this paper, the authors have presented a literature review on the topic of security of grid-interactive smart inverters. The authors have highlighted the vulnerabilities of these devices to cyber-attacks, and the potential consequences of such attacks, which include asymmetrical and abnormal operation, excessive power injection, equipment destruction and large-scale blackouts. The authors also discussed the state-of-the-art system-level and device-level cyber-defense measures that can be used to protect these devices and have provided an analysis of the advantages and drawbacks of each technique.

The authors have emphasized the significance of device-level self-security and its advantages for grid-interactive inverters, as this can minimize the concerns about malicious attacks and achieve safer operation under such attacks. They have also provided recommendations for future studies to improve the self-security system of grid-interactive smart inverters and make them more secure.

In conclusion, the authors have presented a comprehensive literature review on the topic of security of grid-interactive smart inverters, highlighting the vulnerabilities of these devices to cyber-attacks and the potential consequences of such attacks. They have also discussed the various techniques that have been proposed to protect these devices and have provided an analysis of the advantages and drawbacks of

each technique. The paper highlights the importance of protecting these devices from cyber-attacks and the potential consequences of not doing so and provides information and suggestions on how to mitigate these risks.

## Article 161

The paper titled "Mitigating Event Confidentiality Violations in Smart Grids: An Information Flow Security-Based Approach" presents a theoretical approach to mitigate event confidentiality violations in smart grids. The authors argue that the tight coupling between physical and cyber systems in smart grids can lead to violations of the confidentiality of system commands, which can ultimately lead to integrity and availability attacks. To address this problem, the authors propose an information flow security-based approach that can be used to mitigate these types of issues.

The proposed solution is based on the concept of self-obfuscating systems, which can prevent cyber command disclosure through inherent physical observations. The authors provide mathematical formulas for calculating replacement solutions, which can be used to obscure the original command from external observation. Additionally, the authors describe a cyber algorithm that can be used to calculate alternative event placements for a given initial placement, which can be integrated with the overall control algorithm of the system to provide a secure way of protecting the sensitive system settings and the system topology from unauthorized disclosure.

The authors also discuss the potential applicability of their approach to different types of smart grid systems and network topologies and provide examples to illustrate their ideas. The research results have the potential to impact the field of smart grid security by proposing a new approach to addressing event confidentiality violations and providing a theoretical foundation to support it. The results are presented in a clear and understandable way, it is easy to follow, and the results provided are both clear and impactful.

## Article 162

The research paper presents a proposed information and communication technology (ICT) framework for a smart grid system that utilizes big data analytics and cloud computing to assist the local control centers in dealing with large amounts of data. This proposed ICT framework aims to provide price forecast to customers and energy forecast to the utility company. However, public cloud and transmission over the internet may be vulnerable in terms of security, especially with regards to privacy preservation and authentication.

To address these security concerns, the authors propose an identity-based signcryption (IBSC) security scheme. The proposed IBSC scheme provides confidentiality, nonrepudiation, and data integrity by performing simultaneously the functions of encryption and digital signature. Additionally, the authors also present identity-based signature and key distribution as extended applications from the IBSC scheme. The security and performance of the proposed IBSC scheme are analyzed, and the efficiency of the scheme is demonstrated with an implementation using modified Weil pairing over an elliptic curve.

The proposed ICT framework and the IBSC security scheme are aimed to improve the efficiency of the energy management, enhance the security and improve customers experience by providing forecast of energy prices. However, the paper does not mention the potential impact of these results on the field of smart grid systems or the industry in general. The paper presents the proposed solution and its characteristics but doesn't provide detailed information on data collection, sample size, and statistical analysis methods used to evaluate the performance and security of the proposed IBSC scheme, which is important for assessing the validity and generalizability of the proposed solution.

## Article 163

The paper "The Design of Information Security Protection Framework to Support Smart Grid" discusses the challenges faced by State Grid Corporation of China in the construction of a strong and secure smart grid. The authors propose a comprehensive security model and framework that addresses these challenges and is based on an active defense approach. The proposed model includes several elements such as strategy, management, and technology, which are used to identify security risks, analyze requirements, and implement security measures. The proposed framework includes several components such as safety technology measures, business security and optimization, and operational security and optimization.

The authors proposed an information security protection model and framework that can be used to support the construction of a strong and secure smart grid by State Grid Corporation of China, with the focus of protecting the confidentiality, integrity, and availability of smart grid information systems and infrastructure. The paper also presented a methodology for the implementation of information security protection framework, which guides the business systems in every aspect of smart grid to implement information security protection works from the points of technology, management, and operation.

The paper suggests an information security protection model and overall information security protection strategy considering the characteristics of China Smart Grid and the new information security protection requirements, and also proposes an information security protection framework to support the information security protection in smart grid, but the paper doesn't mention how it will impact the organization or the industry. The research results presentation is clear, in that it presents the design of an information security protection model and framework, but it does not provide any information about

the impact or implications of the proposed model and framework, or about how it has been validated or tested.

## Article 164

The paper titled "Security by Design for the Smart Grid: Combining the SGAM and NISTIR 7628" presents an approach for integrating the European Smart Grid Architecture Model (SGAM) and the NISTIR 7628 model into the development process for security assessments of smart grid systems. The authors argue that combining these models is necessary for interoperability between the US and European smart grid systems, and for creating a more effective security analysis framework. The paper provides a five-step process for integrating the methodology into the development process and describes the advantages and limitations of this approach. Additionally, the paper also briefly mentions the use of Monte Carlo simulation method to estimate the reliability indices of a smart grid system by simulating the actual process and the random behavior of the system.

The authors suggest that by combining these two models, experts from both US and European smart grid systems will be able to reuse the SGAM model and its benefits, and vice versa encourage the European stakeholders to use the particularly useful security analysis framework from NIST. They claim that the proposed approach will increase the overall availability and dependability of the smart grid infrastructure and its basic components, it will also help to decrease costs associated with integrating the different components, and it will help to improve the level of protection required for different scenarios of the components. However, it is important to note that these impacts assumed that the proposed approach is implemented correctly, and the simulation method is accurate, but the paper did not provide any concrete evidence or data to support these claims.

Overall, the paper provides a valuable contribution to the field of smart grid security by proposing an approach for integrating existing models and methodologies for security analysis.

## Article 165

The paper presents a novel architecture for securing smart grid systems by making use of software-defined networking (SDN) and Long-term Evolution (LTE) technology. The proposed architecture uses a specialized SDN controller called Flow Visor for slicing the smart grid network and forwarding AES-128 encrypted metering data to ensure the confidentiality, authentication, authorization, and availability of the data. The authors also use LTE to send 24-hour metering sum to the utility for comparison with the last 24 readings received via SDN switches, ensuring integrity and non-repudiation.

To evaluate the performance of the proposed architecture, the authors set up a testbed using Mininet and NS-3 and conducted a simulation of the smart grid system. They collected data from the simulation and compared it with existing solutions. They found that the proposed architecture is more effective than existing solutions in terms of security and performance and is flexible enough to be easily adopted in any smart grid. The authors conclude that their proposed architecture addresses serious security threats in a cost-effective manner and provides a good balance of cost-effectiveness and security.

The paper also conducts a literature review and analysis on the previous research to back their findings and the experiment they did to evaluate the security benefits of the proposed architecture. The research methodology used in the paper is a simulation-based approach which enables the authors to evaluate the reliability indices of the proposed architecture by simulating the actual process and random behavior of the smart grid system. The research results of the above paper indicate that the proposed architecture for smart grid security, which combines software-defined networking (SDN) and Long-term Evolution (LTE) technology, addresses security threats in a cost-effective manner and provides a good balance of cost-effectiveness and security.

## Article 166

The paper presented a study on the security and reliability of smart grid wireless communications systems. The study proposed a scheme to secure the communications between the consumers' smart meters and the gateway, as well as between the gateway and the aggregator, by encoding the data over multiple communication time slots. The scheme aimed to decrease the outage probability and increase the secrecy of the system. The performance of the proposed scheme was evaluated through simulation results, which were compared to a scheme where the same data packet is transmitted over multiple time slots. The results showed that the proposed scheme performed better in terms of both security and reliability.

The simulation results also indicated that the active attacks, in the form of jamming signals, had a significant impact on the system's security and reliability. As the jamming power increased, the secrecy and link rates of the legitimate system decreased. Additionally, the results indicated that the proposed encoding scheme had a positive impact on the total cost paid by the utility due to energy-demand estimation errors. The proposed scheme resulted in a lower cost compared to the case where the same data packet is transmitted over multiple time slots. The results also showed that there is an optimal value of the parameter x, which is used to weight the mean of a consumer's average energy demand, that minimizes the energy-demand estimation-error cost.

In conclusion, the study proposed a scheme to secure the smart grid wireless communications systems and evaluated its performance through simulation results. The results showed that the proposed scheme improves the security and reliability of the system and has a positive impact on the total cost paid by the utility due to energy-demand estimation errors. The study also highlighted the impact of active attacks on the system and the importance of considering the energy-demand estimation-error cost in the design of smart grid wireless communications systems.

## Article 167

The proposed research in this paper aims to develop a secure scheme for a Home Area Network (HAN) in a smart grid system using a Cloud of Things (CoT) infrastructure. Smart grids are power systems that consist of communication infrastructure, IT systems, advanced actuators, and advanced monitoring building blocks for a smart city. The devices powered in smart homes have embedded systems in appliances. They are sensor-based and network-enabled and commonly referred to as Internet of Things (IoT). A Cloud of Things (CoT) virtualizes the IoT and provides monitoring and control. The CoT services in the home area network will enable a collection of applications that will use real-time data from these appliances.

The proposed scheme aims to address various security issues that can arise in a HAN such as replication attacks, Sybil attacks, man-in-the-middle attacks, and scalability, while also addressing other practical security requirements for the HAN. The proposed architecture and security mechanism for the HAN based on CoT and its security features are discussed in detail in the paper, which provides a general overview on the proposed scheme and its possible implementation. The proposed scheme is designed to be simple to implement, flexible and can work both with and without a cloud infrastructure.

In summary, this paper proposes a secure scheme for a Home Area Network (HAN) in a smart grid system using a Cloud of Things (CoT) infrastructure. It addresses various security issues that can arise in a HAN such as replication attacks, Sybil attacks, man-in-the-middle attacks, and scalability, while also addressing other practical security requirements for the HAN. The proposed architecture and security mechanism for the HAN based on CoT and its security features are discussed in detail in the paper, which provides a general overview on the proposed scheme and its possible implementation.

## Article 168

The research paper "Adaptive Security and Privacy in Smart Grids: A Software Engineering Vision" presents an overview of the security and privacy challenges faced by smart grids and the need for

adaptive security and privacy measures to address them. The paper begins by discussing the unique features of smart grids that make them vulnerable to security and privacy threats, such as the increased interfaces and access to services and information. The paper then argues that traditional security and privacy measures are not sufficient to address these threats, and that adaptive security and privacy measures, which can monitor and adapt to changing conditions at runtime, are necessary to effectively protect smart grids.

The paper then outlines the technical and implementation details of how to achieve adaptive security and privacy in smart grids, including decision-making and multi-objective optimization techniques. It also describes the use of causal networks, fuzzy or probabilistic reasoning, decision theory, and machine learning, but it does not provide any details on how these methods were implemented, how the data was collected, how the experiments were designed, how the data was analyzed. The paper also reviews the published reports by NIST and other research papers to provide an overview of the current state of knowledge on the topic.

The paper concludes by identifying areas for further research, such as the monitoring and analysis of security and privacy requirements at runtime, the use of runtime asset models to track changes in assets, and the use of contextual integrity frameworks to protect privacy in smart grids. Overall, this research paper provides a thorough overview of the security and privacy challenges faced by smart grids.

## Article 169

The research paper entitled "Security Challenges in the Integration of IoT with WSN for Smart Grid Applications" focuses on the challenges and risks associated with integrating Internet of Things (IoT) and Wireless Sensor Networks (WSN) in Smart Grid applications. The authors argue that this integration can help to transform existing power grids into more reliable and cost-efficient systems. The primary methodology used in the paper is simulation and the authors propose a solar energy harvesting system that can be used in a Smart City Framework, where buildings in a community are equipped with solar panels and can share energy according to decisions made by a control station.

The paper describes a proposed system for integrating IoT with WSN in the context of Smart Grid applications, which can lead to more efficient use of energy, better management of power generation and consumption, and ultimately, improved reliability and reduced costs. The authors also discuss the security challenges that arise in this context and suggest ways to address them, such as protecting personal information and secret documents stored and transmitted through the cloud as part of the IoT and WSN infrastructure and identifying the chances of occurrence of faults in the long running cable of the grid from the control station itself without human help.

In summary, the paper presents a cost-effective Smart Grid model using distributed renewable energy generators that helps meet the local power demands while protecting secret details and avoiding cyber-physical security risks. The authors propose a solar energy harvesting system that can be used in a Smart City Framework, where buildings in a community are equipped with solar panels and can share energy according to decisions made by a control station. The proposed system can result in a more efficient use of solar energy and better management of power generation and consumption in communities, which can improve reliability and reduce costs.

## Article 170

This paper presents an overview of the smart grid and the issues surrounding the security of its cyber-physical components. The motivation for this topic arises from the current transition of the power grid to an advanced, two-way communication and distributed generation of renewable energy smart grid. Due to the fact that the power grid's infrastructure, systems, and applications were not designed to easily integrate the IT network, architectural vulnerabilities arise leading to physical and cyber security risks. The paper outlines an overview of smart grid infrastructure, cyber security approaches to smart grid security and challenges.

The smart power grid is based on the integration of information and communication technology with power automation devices, equipment, etc. and renewable energy technologies in order to offer and guarantee power quality to consumers. This leads to complex systems that introduce new dependencies and vulnerabilities making it difficult to develop strategic and efficient methods for protecting data, securing control and communication networks. The paper discusses the challenges associated with matching electricity generation to consumer needs and how the smart grid aims to solve these problems through communication and information technologies, which offer a better situational awareness to control centers and utilities of the grid's state.

The paper also highlights the security challenges associated with the integration of the power grid with communication and information systems. It is expected that the heterogeneous, diverse and complex components integrated in the grid will create a series of vulnerabilities. Moreover, power grid is the backbone of society maintaining all vital domains that are crucial to economic stability and social well-being, and by introducing communication and information systems into the equation, the smart grid will be exposed to cyber-physical attacks with the intention of accessing crucial information or even causing physical disasters. The paper suggests several security measures and countermeasures to mitigate these risks, such as upgrading the communication infrastructure, and developing algorithms that can handle communication constraints and choose adequate protocols to power grid.

Article 171

The paper "An Overview of Cyber Security for Smart Grid" presents a review of the current state of research on cyber security for smart grids. The paper highlights the key security concerns that arise in the context of smart grids and discusses various cyber-attack models and defense strategies that can be used to mitigate these risks. The paper argues that as the smart grid system is becoming more popular, the cyber security becomes increasingly important for power industry, since traditional power grid is mainly based on private networks which do not need substantial cyber security concern.

The paper begins by reviewing the traditional power system security framework and then introduces the emerging cyber security issues in smart grids. It then presents some typical cyber-attack models and countermeasures against cyber-attacks. The paper explains that cyber-attacks can undermine the availability, integrity, and confidentiality of smart grids, and can have negative and severe impacts on the smart grid. It also highlights the importance of identifying and mitigating potential security vulnerabilities in order to ensure the safe and reliable operation of these systems.

Overall, the paper provides a comprehensive overview of the cyber security challenges associated with smart grids and the research that has been done in this area. It highlights the need for further research and development in this field in order to ensure the safe and reliable operation of smart grids. The paper also emphasizes the importance of identifying and mitigating potential security vulnerabilities in order to ensure the safe and reliable operation of these systems. It could be a useful resource for researchers and practitioners in the field of cyber security and smart grids.