Smart Grid

Subjects: Automation & Control Systems

Contributor: George Suciu, Aristeidis Farao, Giorgio Bernardinetti, Ivan Palamà, Mari-Anais Sachian, Alexandru Vulpe, Marius-Constantin Vochin, Pavel Muresan, Michail Bampatsikos, Antonio Muñoz, Christos Xenakis

Traditional power grid models are based on a central system for generating and distributing energy and have undergone significant changes in recent years. The integration of the latest generation of technologies, rare in critical infrastructure such as the Internet of Things (IoT), has facilitated the evolution to a more dynamic and connected power grid model now known as the Smart Grid (SG). SG's contributions result from introducing a mutual flow of information between manufacturers and customers, from which both can benefit. This flow enables fine-grained consumption measurements reported to each energy service provider in near real-time to provide consumers with up-to-date price data or control a utility that contains the grid's energy load in real-time according to actual demand, allowing utilities to perform accurate demand response procedures by anticipating high demand peaks, avoiding and mitigating power outages, and distributing the load on available generators. On the other hand, consumers can take part in programs that reduce electricity consumption in the event of rising energy prices while using home-generated (renewable) electricity (such as the so-called microgrid).

Keywords: smart energy ; smart grid ; IoT ; policy ; security

1. Introduction

The above measurement model is called Advanced Metering Infrastructure (AMI) [1]. Technically speaking, this infrastructure consists of several interconnected elements that collect home-measured consumption data, later passed to the power company via an aggregation point. Part of this information is analyzed through Meter Data Management Systems [2]. As a result, further control procedures for the system include industry and information technology equipment (integrated throughout the infrastructure) and correct usage of devices and resources by all involved parties. The architecture for capturing measurement information from IoT devices and consistently controlling power generation contributes to the development of cybersecurity attacks that can compromise resource availability and thus network stability. Access control is essential to manage permissions for all users, processes, and heterogeneous devices that interact continuously within the infrastructure in this complex environment. Therefore, it is imperative to consider the full range of requirements for this scenario to apply the available solutions accurately and propose hybrid access control mechanisms with integrated security monitoring mechanisms.

2. Authorization in Smart Grid (SG)

2.1. Definition and Participants

The focus is on the importance of authorizing and monitoring the security status of the participating entities within a SG network. The main SG components are the Utility, the Smart Meter (SM) and the Aggregator. The Utility is responsible for billing by computing the total consumption of a customer at the end of a billing period. The SM is placed within a house or building, and its purpose is to collect the readings of the electricity consumption. The Aggregator represents the binder between the Utility and the SMs. It is responsible to sum all the readings received by SMs and transmit the results to the Utility. In this way, data become available without putting too much load on the Utility. In general, SG's main goal is to provide a dynamic two-way information exchange between Utility companies and their customers contributing towards a smart and sustainable energy management. However, in such cases, the main challenges that a SG has to exceed are related to scalability [3], trust [4] and interoperability [4]. Thus, divergent information and operational technologies have to cooperate for achieving interconnection of various mechanisms.

There are many ways to cope with the aforementioned challenges including but not limited to policy-based management. Thus, policy specification languages are utilized to communicate the various authorization policies in numerous access control applications with complicated policies. A well-known as well as commonly used language in SG ecosystems is the XACML [5], which is used to construct complex authorization policies [6]. The entities that participate under the policy

manner are the following: (i) Policy Enforcement Point (PEP): this is responsible for performing the decision requests, receives policy updates and accordingly translates them, as well as enforces the decisions that stem from each policy. (ii) Policy Decision Point (PDP): this assesses the applicable policy against other relevant policies and attributes providing the decision outcome to PEP. (iii) Policy Information Point (PIP): this acts as a source of attribute values to make a policy decision. (iv) Policy Administration Point (PAP): this provides the authoring and the maintenance of a policy or a set of policies. As it could be observed, in the SG ecosystem the participating entities own numerous titles. For instance, a Utility in a domain may also be a PDP. That leads to the fact that the different roles can be allocated to an entity being hardcoded in a device. **Figure 1** shows the involved entities and the flows between them.

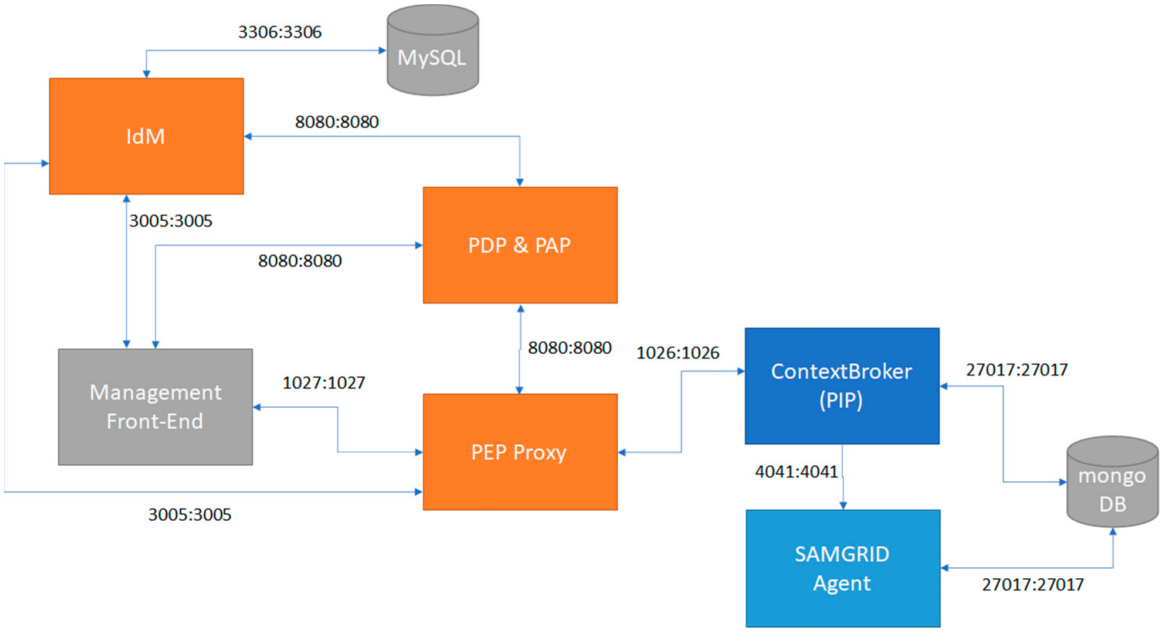

Figure 1. Illustration of participants in the authorization component of SAMGRID.

2.2. Motivating Examples

The focus is on the most notorious cyber-attacks in critical infrastructure that occurred in recent decades to gain a better understanding of the presented notions. The approach aims to emphasize not only the security flaws that enable cyberattacks in critical infrastructures, but also how a malicious actor can take advantage of various vulnerabilities and launch attacks. Moreover, the following examples come from real-life events that shocked involved governments, citizens and stakeholders, also these are explained in brief providing valuable insights.

Stuxnet was a directed cyberwarfare attack against the Iranian nuclear program. It was first uncovered in 2010; however, it has been reported that it was in development since at least 2005. The attackers' approach relied on delivering the worm via USB sticks and local networks. Stuxnet infected both Windows PCs and also controllers. However, its behavior against the controllers was totally different, picking controllers from a specific manufacturer. Once Stuxnet identified its targeted controller then it went through an intricate process of fingerprinting to make sure that it was the target. When it met the requirements, Stuxnet's dropper loaded rogue code to the controller. The code injection enables Stuxnet to stealthily launch its code, letting legitimate code continue correctly working. The rogue code periodically worked. When the attack time came, the rogue code took control without letting the legitimate controller code understand. Finally, during the attack, the genuine code of the controller was knocked out [7].

Another infamous example is **BlackEnergy**, which is the first reported successful cyberattack on a power grid. On 23 December 2015, the attack occurred, managing to disrupt three energy distribution companies in Ukraine and temporarily stop the electricity supply to the end users. In particular, the attacking group that mounted the attack utilized spear-phishing emails attaching malicious Excel documents with macros infecting computers in a targeted network. Additionally, it obtained the credentials and hijacked the Supervisory Control and Data Acquisition (SCADA) systems to ultimately switch off certain substations. At the same time, the attackers flood the call centers with automated telephone calls, preventing the affected utilities from receiving outage reports from their customers (end-users) confronting the response effort [8][9].

Additionally, a well-known attack is **GreyEnergy** targeting critical infrastructure organizations in Central and East Europe in 2018. It is widely known that the malware used during this attack bears many similarities to the one used in the

BlackEnergy attack (see above). The attacking group that was responsible for this cyber-attack used two ways to achieve the intrusion into the organization's network. One the one hand, the first weapon they used was through the *GreyEnergy mini*, which is a first-stage backdoor that works without the demand of administrative privileges- the attackers searched for public-facing web services running on servers that were connected on the targeted network. Once it was finished, the attackers started mapping and scanning the network, as well as collecting credentials to obtain administrator privilege. Then, they were capable of initiating the main malware. In particular, the attackers targeted servers with high uptime, and workstations used to control industrial and control system environments. Additionally, they utilized command and control services to establish communication among their computers (malicious network) and the compromised machines (targeted network). On the other hand, the second way to end the targeted network was via spear phishing emails that bear with them malicious attachments.

The cyberattacks in industrial control systems (ICS) are not a cybersecurity issue that belongs to the past, in 2020 a ransomware encrypted data in **Düsseldorf Hospital** and then demanded ransom to unlock it. During this attack, the first death by ransomware was reported. Particularly, the ransomware compromised the digital infrastructure that the hospital relies on to organize its processes forcing the cancellation of many operations and other procedures. The ransomware entered the University Hospital Düsseldorf's network through a widely known vulnerability in a Citrix application [10]. Apart from this attack, in 2021 **Colonial Pipeline**—the largest fuel pipeline in the U.S.A.—shut down for five days due to a ransomware attack [11]. Herein, the attackers managed to compromise the targeted network utilizing a VPN account. They found the related credentials inside a batch of leaked passwords on the dark web [12][13].

Apart from the aforementioned attacks, it is also mandatory to analyze the different attack stages to complete a cyberattack in ICS. At this point, it is mentioned that the most well-known frameworks that provide the necessary steps for an attack. On the one hand, there is the Cyber Kill Chain framework [14][15] that provides seven steps that attackers have to fulfill to achieve their objectives, the steps are the following: (i) Reconnaissance; (ii) Weaponize; (iii) Delivery; (iv) Exploitation; (v) Installation; (vi) Command and Control and (vii) Actions on objectives. On the other hand, there is the MITRE ATT&CK framework [15][16] that provides 14 steps, which the attackers have to follow to accomplish their attack. The steps for this are the following: (i) Reconnaissance; (ii) Resource Development; (iii) Initial Access; (iv) Execution; (v) Persistence; (vi) Privilege Escalation; (vii) Defense Evasion; (viii) Credential Access; (ix) Discovery; (x) Lateral Movement; (xi) Collection; (xii) Command and Control; (xiii) Exfiltration and (xiv) Impact. Both frameworks follow the same pattern. The primary difference between the aforementioned frameworks is that the MITRE ATT&CK framework is a list that consists of tactics and techniques; it is noted that it does not propose a specific order of operation. However, the Cyber kill Chain proposes a well-defined sequence of events.

2.3. Security and Functional Requirements

As it could be observed, SG is an ecosystem that inherits risks that are directly related not only to the participating SG components (Smart Meter, Aggregator, Utilities), but also to the inadequate security controls implemented by handlers to these. This leads to the conclusion that security and functional requirements need to be declared for a scheme that aims to provide authorization and security monitoring features. Since the functional and security requirements of a SG ecosystem have been extensively expressedherein, the light is shed on requirements related to security and functionality being dedicated to authorization. In particular, the requirements were formulated intending to meet high demands of SG stakeholders. At the end, it is noted that the ensuing requirements were expressed adopting a security by design approach.

2.3.1. Security Requirements

Since the security among a SG ecosystem depends not only on the devices (e.g., vulnerabilities), but also on the poor security practices that are established for authentication and authorization purposes, a kit of standard security requirements were expressed applied to it [5][17][18][19][20][21].

S1.Data confidentiality: Data exchanged within a SG ecosystem should be available only to SG components with the respective privilege.

S2.Data integrity and authenticity: Data exchanged among the participating SG components should be safeguarded against alteration and replication; thus, these should be capable of verifying the origin of the acquired data.

S3.Accountability: Devices, handlers/employees and end-users should be accountable for their actions.

S4.Non-repudiation: Devices, handlers and end-users should not be able to deny their actions.

S5.Physical protection: All electronic devices that participate in a SG ecosystem should contain protection mechanisms to prevent being tampered by adversaries with physical access.

2.3.2. Functional Requirements

Apart from the security requirements, a SG ecosystem consists of processes that demand specific functionalities to be enabled. Analyzing herein, it is expressed that the functional requirements applying a security by design approach but understanding the stakeholders demands [17][18][19][20][21].

F1.Time consuming: As it is well known, the SG concept aims to support real-time services to its end-user. Thus, the implemented application for authentication, authorization, policy updating should not consume much time and deplete the available sources.

F2.Scalability: A SG ecosystem should consist of applications that are capable of handling the numerous fluctuations of grid's size (e.g., nodes can join and leave a grid) without negatively affecting their performance.

F3.Delegated access control: Any application access must be authenticated and authorized by a security policy, and the granting decisions must be made relying on a trusted party.

F4.Authorization: Any access to applications must be authorized according to a security policy.

F5.Authentication: Requesters should be authenticated before accessing any application.

3. Security Authorization Approaches

Although the literature proposes different authorization methods and mechanisms for the SG ecosystem, to the best of the knowledge, this is the first paper that proposes the seamless work of an opinion dynamics approach together with an individual Authorization mechanism. Herein, it is an extension to the paper "FI-WARE authorization in a Smart Grid scenario" written by George Suciu, Cristiana Istrate, Mari-Anais Sachian, Alexandru Vulpe, Marius Vochin, Aristeidis Farao and Christos Xenakis, which has been published in the proceedings of the 4th Global Internet of Things Summit (GioTS) in 2020. Some of the extensions of the work include: (i) an elaborated description of security and functional requirements that should be accomplished by a proposed solution for authorization purposes in SG ecosystem; (ii) a proposal of an opinion dynamics approach that works together with the initial version of the Authorization element proposed in [7]; (iii) a summary of several performance evaluation experiments performed to analyze different aspects of the module demonstrating the impact that the proposed solution has in terms of performance and efficiency and (iv) an analysis related to the security features of SAMGRID. Parts of the work presented in [7] are reused in the current paper.

Security interoperability known as one of the most challenging research areas within the field of critical infrastructures by International Organizations such as the NIST, and IEEE. Therefore, diverse technologies (sensors, meters, actuators and so on) and various communication systems (WiMAX, Wi-Fi, ZigBee, 3G cellular and so on) as well as different domains must cooperate in a unified ecosystem to provide the ability of performing critical actions. These actions, involving the control of user's sensitive information (e.g., electrical consumption) performed across the different elements of the SG may be (i) tampered by malicious actors if data are not completely protected, or (ii) disrupted due to missing standardization and interoperability mechanisms. The design of secure authorization and interoperability mechanisms is a complex process as specified in [22][23]. It is stated that the interconnection between systems that were not originally envisioned to interoperate may pose unanticipated problems, not just in operation, but in data availability, resolution, and format; it may also cause significant delays in the primitive operations.

A solution for providing a decentralized SG in a secure manner using blockchain is presented in [24]. In respect to Electricity Theft Detection, in [25] two solutions based on supervised learning are proposed. The first solution addresses class imbalanced problems solving, perform feature extraction and then use a deep learning-based system to classify electricity consumers. The second solution is a Synthetic Minority Oversampling Technique Edited Nearest Neighbor (SMOTEENN) system. [26] improves the security of existing SCADA systems within smart grids using a cyber-physical digital signature scheme. In [27], Advanced Metering Infrastructure (AMI), which is an important component of an IoT based Smart Grid is analyzed separately and secured based on evolutionary game theory. Ref. [28] proposed a middleware architecture based on RBAC, Policy Enforcement Points (PEPs) and Policy DecisionPoints (PDPs) to collect data streams from several sources connected to the AMI in a standardized format. In [29], a solution based on the usage of PEPs and PDPs has been proposed to interconnect large distributions, involving technologies of different infrastructures, manufacturers and vendors. In [30], a data-centric access control framework for smart grids that follow the

publish/subscribe model has been analyzed, adopting an Attribute-Based Authorization Policy. In [31], an authorization mechanism for monitoring and reduction in resource consumption by using resource trading contribution, implemented on blockchain technology, has been designed. The proposed system provides secure data access and storage together with controller functions transfers among householders.

The main limitation of the related state of the art is that these solutions are not able to cope with the dynamic environment of SG, since they are based mainly on RBAC. Even more, the above solutions do not offer any implementation details, nor performance evaluations through simulations.

Itron's OpenWay Riva [32] is a commercial communication platform that offers well-defined points of interoperability between customer and utility systems, greatly simplifying and reducing integration costs and issues.

4. Opinion Dynamics Approaches

Smart Grid is one of the largest applications of the Internet of Things, the revolution of the Internet and machine-to-machine (M2M) communications. While SG offers many well-known benefits and new opportunities, their distributed nature and two-way information flow between consumer and producer enables a multitude of new attacks against smart grid infrastructure. Given the potentially extremely severe consequences that these attacks could have (e.g., environmental hazards/pollution, rendering hospitals or security defenses inoperable, suspension of economic activities) it is important to note that these attacks are likely to have a significant impact on the environment. Therefore, it is evident that it is imperative to develop anomaly/intrusion detection techniques and systems.

Traditional Intrusion Detection Systems (IDS) are only a first line of defense in attempting to identify anomalous behavior at very specific points in the infrastructure and are tailored to specific types of communication standards or data types, which is not sufficient to track the wide range of attack vectors that could be used against an SG environment. One of the most interesting and innovative cybersecurity innovations in the SG scenario is the usage of the Opinion Dynamics as a distributed detection technology to evaluate the security status of the SG environment. The Opinion Dynamics method proposes to aggregate the coverage of multiple detection systems strategically deployed on the infrastructure under a common distributed framework, which permanently correlates all detected malicious patterns and anomalies and learns from them.

The study and modeling of opinion propagation in a network through the interactions of its agents originated a few decades ago. French in 1956 was one of the first researchers who focused on opinion dynamics [33]. Subsequently, De Groot formalized one of the simplest and most famous dynamic models of opinions in 1974 [34]. Since then, the interest of the research community has gradually increased and according to the nature of the context under consideration the format of the different opinions expressed by the agent and the purpose of interaction, the dynamics of opinions have taken different forms [35][36][37].

Opinion Dynamics can be used in the SG cybersecurity context to design a multi-agent advanced detection system [19][20][21][38], which is one of the main defense threats in the field of SG cybersecurity [39]. In [17], an intrusion detection scheme Opinion Dynamics-based was initially proposed under a theoretical perspective. From a practical point of view, in [20] its ability to detect and monitor attacks in an industrial testbed was demonstrated; in [39], it also showed its contributions to the Smart Grid scenario, and in [21] to the Industrial IoT, also known as IIoT, scenario. This is possible because the opinion dynamics can include anomalous indicators (i.e., equipment and communication link compromises) as the main indicators (opinions), which also include the integration of external IDS.

References

1. Ghosal, A.; Conti, M. Key management systems for smart grid advanced metering infrastructure: A survey. IEEE Commun. Surv. Tutor. 2019, 21, 2831–2848.
2. Rendroyoko, I.; Setiawan, A.D. Development of Meter Data Management System Based-on Event-Driven Streaming Architecture for IoT-based AMI Implementation. In Proceedings of the 2021 3rd International Conference on High Voltage Engineering and Power Systems (ICHVEPS), Bandung, Indonesia, 5 October 2021; IEEE: Piscataway, NJ, USA, 2021; pp. 403–407.
3. Bolgouras, V.; Ntantogian, C.; Panaousis, E.; Xenakis, C. Distributed key management in microgrids. IEEE Trans. Ind. Inform. 2019, 16, 2125–2133.

4. Karopoulos, G.; Ntantogian, C.; Xenakis, C. MASKER: Masking for privacy-preserving aggregation in the smart grid ecosystem. Comput. Secur. 2018, 73, 307–325.
5. Farao, A.; Veroni, E.; Ntantogian, C.; Xenakis, C. P4G2Go: A Privacy-Preserving Scheme for Roaming Energy Consumers of the Smart Grid-to-Go. Sensors 2021, 21, 2686.
6. Suciu, G.; Istrate, C.I.; Vulpe, A.; Sachian, M.A.; Vochin, M.; Farao, A.; Xenakis, C. Attribute-based access control for secure and resilient smart grids. In Proceedings of the 6th International Symposium for ICS & SCADA Cyber Security Research 2019, Athens, Greece, 10–12 September 2019; pp. 67–73.
7. Suciu, G.; Istrate, C.; Sachian, M.A.; Vulpe, A.; Vochin, M.; Farao, A.; Xenakis, C. FI-WARE authorization in a Smart Grid scenario. In Proceedings of the 2020 Global Internet of Things Summit (GIoTS), Dublin, Ireland, 3 June 2020; IEEE: Piscataway, NJ, USA; pp. 1–5.
8. Langner, R. Stuxnet: Dissecting a cyberwarfare weapon. IEEE Secur. Priv. 2011, 9, 49–51.
9. FireEye. Cyber Attacks on the Ukrainian Grid: What You Should Know. 2015. Available online: https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/fe-cyber-attacks-ukrainian-grid.pdf (accessed on 17 May 2022).
10. Kaspersky. BlackEnergy APT Attack in Ukraine. Available online: https://www.kaspersky.com/resource-center/threats/blackenergy (accessed on 17 March 2022).
11. Wired. The Untold Story of a Cyberattack, a Hospital and a Dying Woman. Available online: https://www.wired.co.uk/article/ransomware-hospital-death-germany (accessed on 17 March 2022).
12. Nbc News. Colonial Announces Pipeline Restart, Says Normal Service Will Take ‘Several Days’. Available online: https://www.nbcnews.com/tech/security/colonial-announces-pipeline-restart-says-normal-service-will-take-seve-rcna917 (accessed on 17 March 2022).
13. Hackers Breached Colonial Pipeline Using Compromised Password. Available online: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password (accessed on 17 March 2022).
14. Farao, A.; Panda, S.; Menesidou, S.A.; Veliou, E.; Episkopos, N.; Kalatzantonakis, G.; Mohammadi, F.; Georgopoulos, N.; Sirivianos, M.; Salamanos, N.; et al. SECONDO: A platform for cybersecurity investments and cyber insurance decisions. In Proceedings of the International Conference on Trust and Privacy in Digital Business, Bratislava, Slovakia, 14–17 September 2020; Springer: Cham, Switzerland, 2020; pp. 65–74.
15. The Cyber Kill Chain. Available online: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed on 17 March 2022).
16. Yadav, T.; Rao, A.M. Technical aspects of cyber kill chain. In Proceedings of the International Symposium on Security in Computing and Communication, Kochi, India, 10 August 2015; Springer: Cham, Switzerland, 2015; pp. 438–452.
17. Rubio, J.E.; Alcaraz, C.; Lopez, J. Preventing advanced persistent threats in complex control networks. In Proceedings of the European Symposium on Research in Computer Security, Oslo, Norway, 11–15 September 2017; Volume 10493, pp. 402–418.
18. Mitre Att&Ck. Available online: https://attack.mitre.org/ (accessed on 17 March 2022).
19. Nisioti, A.; Loukas, G.; Laszka, A.; Panaousis, E. Data-driven decision support for optimizing cyber forensic investigations. IEEE Trans. Inf. Forensics Secur. 2021, 16, 2397–2412.
20. Rubio, J.E.; Roman, R.; Alcaraz, C.; Zhang, Y. Tracking apts in industrial ecosystems: A proof of concept. J. Comput. Secur. 2019, 27, 521–546.
21. Rubio, J.E.; Roman, R.; Lopez, J. Integration of a threat traceability solution in the industrial internet of things. IEEE Trans. Ind. Inform. 2020, 16, 6575–6583.
22. Gopstein, A.; Nguyen, C.; O’Fallon, C.; Hastings, N.; Wollman, D. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0; NIST Special Publication; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2021.
23. Alcaraz, C.; Lopez, J. Secure interoperability in cyber-physical systems. In Cyber Warfare and Terrorism: Concepts, Methodologies, Tools, and Applications; IGI Global: Hershey, PA, USA, 2020; pp. 521–542.
24. Hasankhani, A.; Hakimi, S.M.; Bisheh-Niasar, M.; Shafie-khah, M.; Asadolahi, H. Blockchain technology in the future smart grids: A comprehensive review and frameworks. Int. J. Electr. Power Energy Syst. 2021, 129, 106811.
25. Javaid, N.; Gul, H.; Baig, S.; Shehzad, F.; Xia, C.; Guan, L.; Sultana, T. Using GANCNN and ERNET for Detection of Non-Technical Losses to Secure Smart Grids. IEEE Access 2021, 9, 98679–98700.

26. Yang, H.; Liu, S.; Fang, C. Model-based secure load frequency control of smart grids against data integrity attack. IEEE Access 2020, 8, 159672–159682.
27. Boudko, S.; Aursand, P.; Abie, H. Evolutionary Game for Confidentiality in IoT-enabled Smart Grids. Information 2020, 11, 582.
28. Veichtlbauer, A.; Engel, D.; Knirsch, F.; Langthaler, O.; Moser, F. Advanced metering and data access infrastructures in smart grid environments. In Proceedings of the Seventh International Conference on Sensor Technologies and Applications (SENSORCOMM) 2013, Barcelona, Spain, 25–31 August 2013; pp. 63–68, ISBN 978-1-61208-296-7.
29. Alcaraz, C.; Lopez, J.; Wolthusen, S. Policy enforcement system for secure interoperable control in distributed smart grid systems. J. Netw. Comput. Appl. 2016, 59, 301–314.
30. Duan, L.; Liu, D.; Zhang, Y.; Chen, S.; Liu, R.P.; Cheng, B.; Chen, J. Secure data-centric access control for smart grid services based on publish/subscribe systems. ACM Trans. Internet Technol. (TOIT) 2016, 16, 1–7.
31. Alcarria, R.; Bordel, B.; Robles, T.; Martín, D.; Manso-Callejo, M.Á. A blockchain-based authorization system for trustworthy resource monitoring and trading in smart communities. Sensors 2018, 18, 3561.
32. “OpenWay Riva”, Itron. Available online: https://blogs.itron.com/tag/openway-riva/ (accessed on 17 March 2022).
33. French, J.R., Jr. A formal theory of social power. Psychol. Rev. 1956, 63, 181.
34. DeGroot, M.H. Reaching a consensus. J. Am. Stat. Assoc. 1974, 69, 118–121.
35. Dong, Y.; Zhan, M.; Kou, G.; Ding, Z.; Liang, H. A survey on the fusion process in opinion dynamics. Inf. Fusion 2018, 43, 57–65.
36. Noorazar, H. Recent advances in opinion propagation dynamics: A 2020 survey. Eur. Phys. J. Plus 2020, 135, 1–20.
37. Grabisch, M.; Rusinowska, A. A Survey on Nonstrategic Models of Opinion Dynamics. Games 2020, 11, 65.
38. Lopez, J.; Rubio, J.E.; Alcaraz, C. A resilient architecture for the smart grid. IEEE Trans. Ind. Inform. 2018, 14, 3745–3753.
39. Gunduz, M.Z.; Das, R. Cyber-security on smart grid: Threats and potential solutions. Comput. Netw. 2020, 169, 107094.