International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 09 Issue: 04 | Apr 2022 www.irjet.net p-ISSN: 2395-0072

Cyber Security Issues in Smart Grids

Turkei Aldarrai[1], Dr. Abdalla Ismail [2]

[1] Graduate Student, Dept. of Electrical Engineering, Rochester Institute of Technology, Dubai, UAE
[2]Professor, Dept. of Electrical Engineering, Rochester Institute of Technology, Dubai, UAE

Abstract - *Cybersecurity for the smart grid is essential to ensure the resiliency of the supply and delivery of electrical power. Cybersecurity for the utility's electrical grid monitoring and control systems provides the actions required to preclude the unauthorized use of, denial of service to, modification to, disclosure of, loss of revenue from, or destruction of, critical system or informational assets. Cyber attacks and viruses have caused power disruptions, and malware has caused factories to manufacture bad products and even destroy product components.*

In this paper we will review the fundamental cybersecurity issues in modern smart grid environment. This includes the different types of security threats, Common Vulnerabilities, and Security Standards, Regulations, and Guidance.

Key Words: **Cybersecurity, Electrical Power, Smart Grid, Cyber attacks, Security Standards.**

1. INTRODUCTION

With strong arrangements that develop the proficiency of standard Electric Grids, Smart Grid innovation is going to change the current industry. The Smart Grid is a computerized interchanges-based energy dispersion organization. The rising burden and utilization requests entangle power issues. For instance, the interest has expanded, and issues like power outages, over-burdens, and voltage hangs have emerged, as well as the flow of electrical organization discharging basic fossil fuel byproducts and, above all, managing digital assaults [1]. The United States is liable for up to 40% of all carbon dioxide discharges from power frameworks, which is unsafe for the climate. The Smart Grid is supposed to further develop proficiency, dependability, and accessibility by coordinating modern advances, for example, availability and expanded handling power [2]. The Smart Grid likewise gives a framework that is connected to two-way correspondence and power streams. The Smart Grid is an efficient innovation that acquires heritage power age methods like gaseous petrol, petroleum products, and coal, as well as environmentally friendly power sources like breeze turbines and sun-based power [3]. The Smart Grid is perceived for disseminating and involving power in an efficient way to an organization of smart grid gadgets, transformers, and gear. Agreeable, since it utilizes two-way correspondence to accomplish these points, though the heritage matrix framework just purposes one-way correspondence [4].

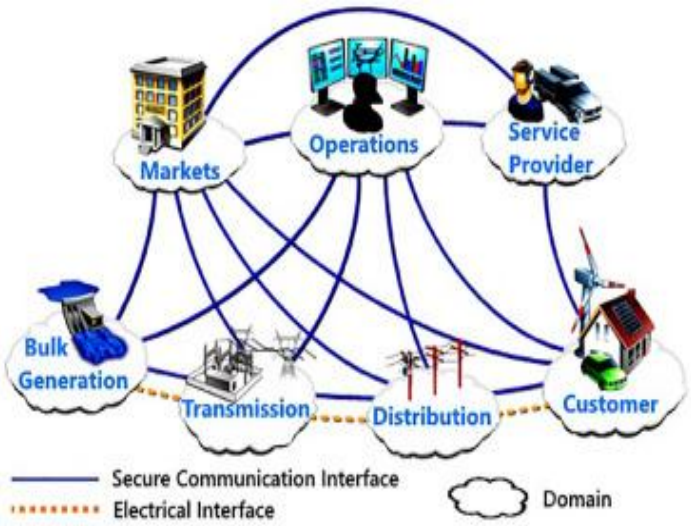

Fig -1: Domains of Small Grid

The Smart Grid furnishes clients with expedient and better administrations with a decreased response time delay, permitting the energy issue to be actually tended to [5]. Notwithstanding, Smart Grid innovation isn't without imperfections and difficulties, the most genuine of which is the powerlessness to get the most significant resource: information. The purposes behind this are that the Smart Grid framework will regularly trade data since delicate information might be put away there [6]. Since different gadgets, both business and private, will be associated through a progression of organizations to impart and give security to the organizations utilizing different methodologies, network protection in the Smart Grid is a pivotal action [7]. These are troublesome hardships that will be tended to through a writing survey in which an assortment of safety arrangements will be evaluated and broken down to give answers for complex security issues [8].

2. ISSUES RELATED TO OPERATION OF SMALL GRID

The actual power framework and the digital arrangement of data and correspondence advancements are inseparably connected in a smart grid, presenting huge security issues. Smart grid security issues should be addressed for the framework to be dependable, protected, proficient, and stable [9]. To keep up with the security of the inexorably tremendous and complex powerful brilliant lattice climate, present safety efforts are either unimportant, not

reasonable, deficiently versatile, incongruent, or basically lacking, and should be supplanted by new and modern arrangements [10]. A smart grid is comprised of actual power framework parts as well as a digital framework foundation, which incorporates programming, equipment, and correspondence needs. Power will move from mass-creating plants to end clients in a run-of-the-mill brilliant network design. Data stream, then again, will happen in two ways, i.e., at the gadget level for coordination and among administrators and specialist co-ops for productive and upgraded control [11].

Therefore, both digital and actual framework security are basic in a brilliant network, and considering security challenges in the digital domain and the actual power framework independently can't catch the whole picture. Coming up next are a portion of the digital actual brilliant matrix's security concerns [12]:

- The brilliant matrix's actual parts
- Control applications and control focus
- The digital frameworks for brilliant network activity and arranging are strong, dependable, and proficient [9].
- The connection between digital assaults and the ramifications for actual frameworks
- The shields are set up to lessen the perils presented by digital dangers [13]

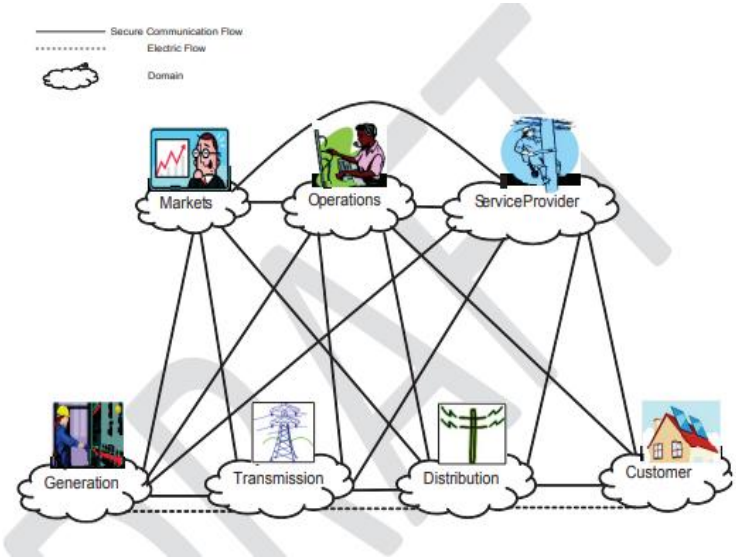

Fig -2: Small Grid Architecture

3. CYBER SECURITY ISSUES IN SMART GRID

These are a few likely normal dangers to Smart Grids that could be compelling. There are various perils that Smart Grids might confront, and these dangers might hurt companies as well as standard clients [14]. These perils might address significant threats to individual security, for example, touchy data about clients, which might be in danger of being taken or the firm being closed down forever. These risks are not restricted to web clients; they additionally influence clients at home, where assailants might endeavor to assemble individual data [15].

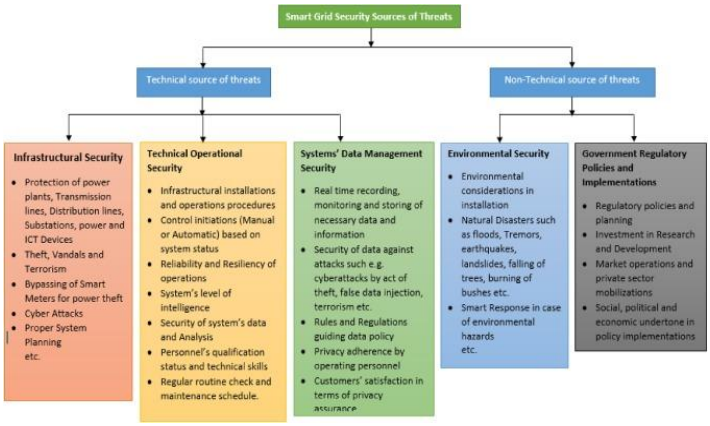

Fig -3: Small Grid Security sources of threats

3.1 Phishing

Since phishing is so easy to direct, it very well may be the initial phase in putting clients and organizations at risk. Programmers could take advantage of data from purchasers, for example, bills or installment receipts that were not as expected disposed of, and utilize this data, along with social designing, to get fundamental data about the firm, for this situation, data about the power provider [16].

Then again, the representative might confront different risks inside the firm, for example, fake messages or correspondences that seem, by all accounts, to be certifiable messages, in which the worker might enter individual data that could prompt a hack [17]. These perils are probably going to hurt a Smart Grid client, as giving data to obscure sources and without knowing the consequences of these dangers could monetarily affect clients. Notwithstanding, is it an important concern while managing safety efforts against phishing assaults?

3.2 Denial-of-Service

The Denial-of-Service (DoS) attack is an essential one, and any assault against accessibility is a DoS assault. On account of the Smart Grid, the main administrations for Smart Grids are accessible, suggesting that the Smart Grid might be exposed to a Denial-of-Service attack. The availability association for the Smart Grid should be secure and solid. Since the Smart Grid utilizes appropriated compositional frameworks to spread associations with endless gadgets over a more extensive area, the association should be trustworthy and secure [18]. On the off chance that a dispersed forswearing of-administration (DDoS) assault is

sent off against the Smart Grid, it will be seriously hurt [19]. Refusal of-Service assaults jam the channel and are a successive way to deal with focus on the OSI-actual Models and information connect layers. Programmers might actually change the MAC address and utilize a programmer's instrument like "Tidal wave Backdoor" to secure secondary passage admittance to the organization, permitting them to overpower PCs with customary organization demands [20]. Moreover, while the OSI-Model incorporates different security conventions at the Network and Transport layers, like TCP, SSL, and IPv6, the conventions are as yet weak when utilized in Smart Grid network design. In any case, the (DoS) assault will generally be done at the Application layer of the OSI Model since the Application layer takes into consideration information transmission and gathering, however, in the Smart Grid, a (DoS) attack can keep the correspondence framework from answering different gadgets [21].

3.3 Malware Spreading

The principal danger to the Smart Grid is the multiplication of malware, which is a major issue. The aggressors can make malware that can be utilized to contaminate both the association's frameworks and its gadgets [22]. The aggressor can impact the working of gadgets or frameworks by circulating malware, permitting the assailants to get access to and secure delicate data.

3.4 Eavesdropping and Traffic Analysis

Spoofing Parodying assaults incorporate listening in and traffic examination. By observing organization traffic, the assailant can get delicate data [23]. The Smart Grid will be helpless against this danger because of its gigantic organization; the Smart Grid has many organization hubs, making it hard to keep up with the gadgets associated with the greater organization. The Smart Grid gives the most serious risk of information robbery, which is a critical issue in information security all over the planet [24].

4. CASE STUDY

Smart grids have long been a crucial component of energy networks, incorporating a variety of instruments such as computers science technology and linked gadgets. It has aided in the optimization of energy production, distribution, consumption, and storage [25]. The advent of computers and complicated technologies to modernize electric grids has resulted in security breaches, resulting in cyber-attacks that exploit computer weaknesses to enter networks [26]. Wind turbines, concentrated solar power plants, photovoltaic panels, and possibly even plug-in hybrid vehicles are examples of energy renewable resources where this occurs. For example: The Power Substation Cyber Attack That Shook the World. In December 2015, a powerful framework in the area of Ukraine went down for six hours. As indicated by Wired's full report on Ukraine's power network hack, the blackout was expected to be a cyberattack that caused the gadgets that course power and change voltages to separate from the fundamental framework. Despite the fact that Ukraine's power framework network was appropriately portioned from the control place networks utilizing firewalls, the telecommuters were all the while signing into the SCADA network without legitimate confirmation strategies [27]. The aggressors figured out how to invade the organization utilizing Malware, assembled insight, and eventually captured the VPN certifications to get to the SCADA network that controlled the power matrix. The programmers who struck the power habitats in Ukraine the principal affirmed hack to bring down a power lattice - - weren't entrepreneurs who simply chanced upon the organizations and sent off an assault to test their capacities; as indicated by new subtleties from a broad examination concerning the hack, they were talented and secretive specialists who painstakingly arranged their attack over numerous months, first doing observation to concentrate on the organizations and siphon administrator certifications, then sending off a synchronized attack in a very much arranged dance [28].

Lee is a previous digital fighting tasks official for the US Air Force and is a fellow benefactor of Dragos Security, a basic foundation security organization. "As far as refinement, the vast majority generally malware," he says. "To me what makes refinement is coordinated factors and arranging and tasks and what's happening during its length. Furthermore, this was profoundly modern." Ukraine rushed to blame Russia for the attack [29]. Lee avoids ascribing it to any entertainer yet says there are clear depictions between the different periods of the activity that propose various degrees of entertainers dealt with various pieces of the attack. This raises the likelihood that the assault could host included cooperation between totally various gatherings perhaps cybercriminals and country state entertainers.

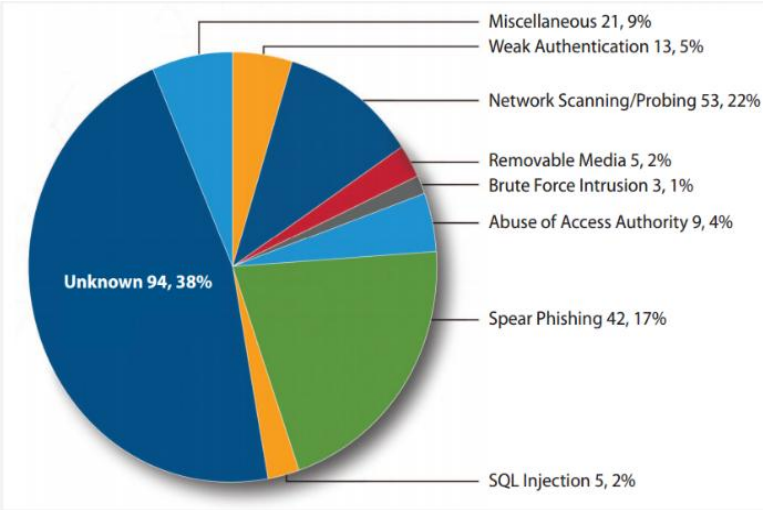

Fig -4: Percentage of Cyber Security attacks on Smart Grids

5. SOLUTIONS

5.1 Encryption

Encryption is the technique for encoding information so that it can't be perused. At the point when you utilize a VPN to associate with the web, your association is encoded, which demonstrates that assailants would possibly get strange code assuming they caught your information stream [30]. Encryption can be considered a kind of mystery code. A code is a strategy through which your information is mixed, and there is a code that lets you decipher the message. The most recommended VPN organizations use AES 256-digit encryption, which is the most elevated encryption grade available [31].

5.2 Malware Protection

Malware insurance is expected for the Smart Grid on the grounds that the installed frameworks and broadly useful frameworks that are associated with it should be gotten and watched from digital assaults. The primary explanation that firmware is secure is that it is simply presented to run programming that is obtained by the creator and requires a creation key to prove the product, while universally useful specific from outsider applications, for example, antivirus programming, which is continually updated [32].

5.3 Authentication

According to the creators, keeping up with a confirmation and controlling access are the main pressing issues, and the character ought to be approved utilizing solid validation instruments. A "stowed away deny strategy" might be utilized while connecting with the framework, as well as utilizing the arrangement to permit client admittance to just explicit clients, in carrying out validation [33]. The strategy gives safety efforts to the association, and the inferred deny strategy can be invaluable in light of the fact that typical clients will have changing authorizations, permitting the Manager to see every one of extra information connected to projects while the staff has obliged admittance to information [34].

5.4 Malware Protection

Malware insurance is expected for the Smart Grid on the grounds that the inserted frameworks and universally useful frameworks that are associated with it should be gotten and monitored from digital assaults [35]. The principal reason that firmware is secure is that it is simply presented to run programming that is acquired by the creator and requires a creation key to validate the product, though broadly useful specific form outsider application, for example, antivirus programming, which is continually refreshed [36].

5.5 Network Security

When using a wireless internet, such as the Internet, a Virtual Private Network adds an extra layer of protection. Because data may be at threat when using public network infrastructure, the employs a range of security mechanisms, including encryption and the protection of any data transmitted all across network. VPNs are also utilized for communication because they provide a secure channel [37].

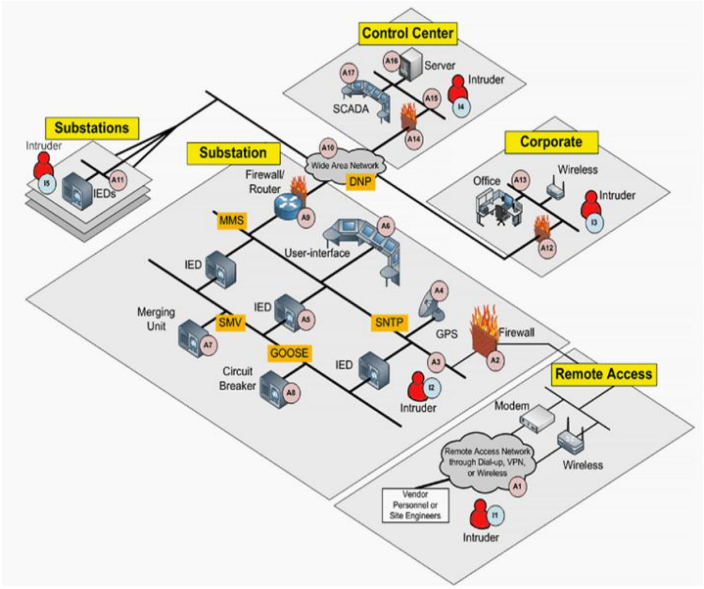

Fig -5: Network Security in cyber-attack ubstation

5.6 Remote Access VPN

The remote monitoring VPN connects to an organization's private network via a public network, such as the internet. After establishing authentication, customers will use smart phones or desktop computers to connect to the VPN gateway. If the credentials are correct, the security can validate access and get access to information stored on the vpn connection [38]. These resources, which include business software and papers, are exclusively available to users of the organization.

6. CONCLUSION

Smart Grids are more equipped and useful than standard methods power matrices as far as ability and creation since they are harmless to the ecosystem, use a lot of sustainable power sources, and are safer. Also, the review recognized expected benefits as well as weaknesses related to the Smart Grid. As far as the general advantages of utilizing a Smart Grid, it will give a more extensive range of safety, with various ways and methods to tackle a portion of the digital assault troubles. Be that as it may, while performing studies, various papers have proposed the security advantages and weaknesses associated with Smart Grids. Pretty much every

exploration paper has suggested that the Denial-of-Service assault is the most hazardous soft spot for Smart Grids. Since Smart Grids are based on top of organizations, attacking the organization would stop the Smart Grid. Although the Smart Grid will save the help's accessibility with various degrees of safety, embracing a Virtual Private Network (VPN) for more scrambled transmission would be the most ideal decision for security. Different gadgets are connected over wide geological region networks represent an issue for Smart Grids. The most troublesome test is getting little gadgets with regard to the more extensive foundation. By offering a conveyed and encoded record that is unchangeable to changes made by terrible hubs or assailants, blockchain innovation could help with the goal of safety challenges.

REFERENCES

[1] C.-C. Sun, A. Hahn, and C.-C. Liu, "Cyber security of a power grid: State-of-the-art," International Journal of Electrical Power & Energy Systems, vol. 99, pp. 45-56, 2018.

[2] G. Austin, "Corporate cybersecurity," in Cybersecurity in China, ed: Springer, 2018, pp. 65-79.

[3] A. Milovanov, "Intelligent Solar Energy Devices Cybersecurity System," Physical Optics Corporation 2019.

[4] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, and H. 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.

[5] J. Yao, "Cybersecurity of demand side management in the smart electricity grid," Ph. D. dissertation, Dept. Elect. Eng., Lehigh Univ., Bethlehem, PA, USA, 2017.

[6] 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.

[7] P. P. Biswas, H. C. Tan, Q. Zhu, Y. Li, D. Mashima, and B. Chen, "A synthesized dataset for cybersecurity study of IEC 61850 based substation," in 2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm), 2019, pp. 1-7.

[8] Y. Yan, Y. Qian, H. Sharif, and D. Tipper, "A survey on cyber security for smart grid communications," IEEE Communications Surveys & Tutorials, vol. 14, pp. 998-1010, 2012.

[9] E. L. Webb, "The Internet of Things: Cybersecurity, Insurance, and the National Power Grid," Nat. Resources & Env't, vol. 30, p. 35, 2015.

[10] A. Qureshi, "Cybersecurity in physically entangled networks."

[11] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," Computer networks, vol. 169, p. 107094, 2020.

[12] B. E. Camachi, L. Ichim, and D. Popescu, "Cyber security of smart grid infrastructure," in 2018 IEEE 12th International Symposium on Applied Computational Intelligence and Informatics (SACI), 2018, pp. 000303-000308.

[13] J. Johnson, J. R. Hoaglund, R. D. Trevizan, and T. A. Nguyen, "PHYSICAL SECURITY AN D CYBERSECURITY OF ENERGY STORAGE SYSTEMS."

[14] N. U. Ibne Hossain, M. Nagahi, R. Jaradat, C. Shah, R. Buchanan, and M. Hamilton, "Modeling and assessing cyber resilience of smart grid using Bayesian network-based approach: a system of systems problem," Journal of Computational Design and Engineering, vol. 7, pp. 352-366, 2020.

[15] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," IEEE Communications Surveys & Tutorials, vol. 14, pp. 981-997, 2012.

[16] I. Fette, N. Sadeh, and A. Tomasic, "Learning to detect phishing emails," in Proceedings of the 16th international conference on World Wide Web, 2007, pp. 649-656.

[17] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," IEEE Wireless Communications, vol. 24, pp. 88-98, 2017.

[18] J. Johnson, I. Onunkwo, P. Cordeiro, B. J. Wright, N. Jacobs, and C. Lai, "Assessing DER network cybersecurity defences in a power-communication co-simulation environment," IET Cyber-Physical Systems: Theory & Applications, vol. 5, pp. 274-282, 2020.

[19] J. Hull, H. Khurana, T. Markham, and K. Staggs, "Staying in control: Cybersecurity and the modern electric grid," IEEE Power and Energy Magazine, vol. 10, pp. 41-48, 2011.

[20] D. Moore, C. Shannon, D. J. Brown, G. M. Voelker, and S. Savage, "Inferring internet denial-of-service activity," ACM Transactions on Computer Systems (TOCS), vol. 24, pp. 115-139, 2006.

[21] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," IEEE Security & Privacy, vol. 8, pp. 81-85, 2010.

[22] T. S. Gopal, M. Meerolla, G. Jyostna, P. R. L. Eswari, and E. Magesh, "Mitigating Mirai malware spreading in IoT environment," in 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 2226-2230.

[23] J. Sakhnini, H. Karimipour, A. Dehghantanha, R. M. Parizi, and G. Srivastava, "Security aspects of Internet of Things aided smart grids: A bibliometric survey," Internet of things, vol. 14, p. 100111, 2021.

[24] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," Computer networks, vol. 57, pp. 1344-1371, 2013.

[25] L. James, "Making cyber-security a strategic business priority," Network Security, vol. 2018, pp. 6-8, 2018.

[26] A. Sajadi, L. Strezoski, V. Strezoski, M. Prica, and K. A. Loparo, "Integration of renewable energy systems and challenges for dynamics, control, and automation of electrical power systems," Wiley Interdisciplinary Reviews: Energy and Environment, vol. 8, p. e321, 2019.

[27] J. Hong, C.-C. Liu, and M. Govindarasu, "Integrated anomaly detection for cyber security of the substations," IEEE Transactions on Smart Grid, vol. 5, pp. 1643-1653, 2014.

[28] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," The Electricity Journal, vol. 30, pp. 30-35, 2017.

[29] D. E. Whitehead, K. Owens, D. Gammel, and J. Smith, "Ukraine cyber-induced power outage: Analysis and practical mitigation strategies," in 2017 70th Annual Conference for Protective Relay Engineers (CPRE), 2017, pp. 1-8.

[30] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," Future Internet, vol. 13, p. 39, 2021.

[31] W. F. Boyer and S. A. McBride, "Study of security attributes of smart grid systems-current cyber security issues," Idaho National Laboratory (INL) 2009.

[32] Z. El Mrabet, N. Kaabouch, H. El Ghazi, and H. El Ghazi, "Cyber-security in smart grid: Survey and challenges," Computers & Electrical Engineering, vol. 67, pp. 469-482, 2018.

[33] C. W. Crews, "Cybersecurity and Authentication: the marketplace role in rethinking anonymity–before regulators intervene," Knowledge, Technology & Policy, vol. 20, pp. 97-105, 2007.

[34] J. Qi, A. Hahn, X. Lu, J. Wang, and C.-C. Liu, "Cybersecurity for distributed energy resources and smart inverters," IET Cyber-Physical Systems: Theory & Applications, vol. 1, pp. 28-39, 2016.

[35] S. Ndichu, S. McOyowo, H. Okoyo, and C. Wekesa, "A Remote Access Security Model based on Vulnerability Management," International Journal of Information Technology and Computer Science, vol. 12, pp. 38-51, 2020.

[36] P. D. Ray, R. Harnoor, and M. Hentea, "Smart power grid security: A unified risk management approach," in 44th Annual 2010 IEEE international Carnahan conference on security technology, 2010, pp. 276-285.

[37] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber, "A network security monitor," Lawrence Livermore National Lab., CA (USA); California Univ., Davis, CA (USA ...1989.

[38] J. Steinberg and T. Speed, SSL VPN: Understanding, evaluating, and planning secure, web-based remote access: Packt Publishing Ltd, 2005.

BIOGRAPHIES

Turkei Aldarrai is a graduate of Electrical Engineering from the Higher Colleges of Techology, Dubai, UAE. Currently pursuing his Master's degree in Electrical Engineering, specializing in Smart Grids at Rochester Institute of Technology (RIT), Dubai Campus.

Dr. Abdalla Ismail is a professor of Electrical Engineering at Rochester Institute of Technology, Dubai, UAE. He received his Ph.D. in Electrical Engineering from the University of Arizona, USA. He has over 35 years of experience in higher education, teaching, research and management. He was the Associate Dean of Faculty of Engineering and member of the President Technical Office at UAE University. His education and research interests are in intelligent control systems, smart energy and grids, and renewable energy. He published over one hundred and ten technical papers and two co-authored books. He has participated in several higher education quality assurance and accreditation programs boards and committees in the UAE and other GCC countries. He received several prizes and awards including the Emirates Energy Award, IEEE Millennium award, and Fulbright scholarship.