International Journal of Applied Power Engineering (IJAPE)
Vol. 10, No. 3, September 2021, pp. 207~216
ISSN: 2252-8792, DOI: 10.11591/ijape.v10.i3.pp207-216

Problems and analysis directions in smart grid technology and their potential solutions

Manoj Saini[1], Shagufta Khan[2], Rajeev Gupta[3], Shivani Singh[4], Pooja Upadhyay[5], Shivangi Soni[6]
[1,2]SEECE, Galgotias University, Gr. Noida, Uttar Pradesh, India
[3,4,5,6]GCET, Gr. Noida, Uttar Pradesh, India

Article Info

Article history:

Received Jan 26, 2021
Revised Mar 9, 2021
Accepted Jun 17, 2021

Keywords:

Communication infrastructure
Core technology
Information and communication technology
Information infrastructure
Privacy and security

ABSTRACT

The idea of smart grid (SG) technology has revolutionized the traditional power system and has made it more efficient, robust and reliable in a number of ways. SG networks are recently upgraded networks of associated objects of information and communication technology (ICT) and core technology. Many active research areas have been developed to achieve the goals and planned requirements of the transfer of power systems from the traditional grid to the SG. Despite the significant characteristics of SG, future research needs to resolve numerous problems relating to core and ICT technology. This analysis paper identifies the challenges facing SG growth, potential research directions and also proposes possible solutions to some of these challenges, thus achieving the SG goals and planned requirements.

Corresponding Author:

Shagufta khan
School of Electrical, Electronics & Communication Engineering
Galgotias University
Plot No. 2, Yamuna Expy, Opposite Buddha International Circuit
Sector 17A, Greater Noida, Uttar Pardesh, India
Email: engg.manojsaini@gmail.com

1. INTRODUCTION

The security of functioning innovation technologies which are one of the center parts of the smart grid (SG) structure, meaning to make the entire situation more trustworthy, unbending, versatile, and insightful energy utility, is an approaching issue that should be understood rapidly. Once more, with the expanded mix of operational technology gadgets with other existing system applications and correspondence, the spine is making both the clients and the energy utilities to profoundly investigate the protection and security issues of the network [1]. The security oppositions in the center operational technology like supervisory control and data acquisition (SCADA), industrial control systems, and advanced metering infrastructure (AMI) have been concentrated in detail and depicted in area 2.1 of this paper [2], [3].

To understand the previously mentioned areas, one of the fundamental foundations is smart metering that keeps a track of all the 2-way flow of energy and communication throughout the entire power grid as compared to the traditional grid. Although, in spite of such advanced technological integrity, there are certain drawbacks and challenges in the metering networks that are still under discussion and need to be arrested quickly. An attack on a smart grid network can potentially showdown or shutdown the entire power grid, and halt the energy utility systems. It will also affect the utility as well as the end users. In the accompanying subsection, we examined recent survey papers related to pointed issues and pointed out the distinctive highlights of our work. SG innovation has been utilized in its activity to incorporate new data and correspondence advances to improve creation, dispersion, and energy utilization and to all the more likely

deal with the connection between vitality providers and their end clients [4]. The commitment of incorporating the new data and correspondence innovations, all the more especially Smart Grid, into the power conveyance arrangement is a problem for keen networks. To be sure, smart meters assume a significant job in the change of the power dissemination arranged into keen matrices [5]. They empower customers to follow their utilization continuously to all the more likely realize their power charges all the more precisely [6].

Although SG shows up as a considerable answer for vitality suppliers and their purchasers, they represent significant security [7]. This issue worries about the security of the information traded between Smart Grid's and system administrators since this information traded between the two members convey touchy data as respects the age of utilization solicitations for expended amounts [8], as a result of their sending in a system that isn't generally secure, this information is probably going to be captured, controlled and adulterated by an assailant who can assault the conduct of SG frameworks and debilitate their legitimate working, for example, the distortion of vitality utilization bills [9].

Our methodology is a contributor to the above-mentioned problem. It especially approaches the security of sensitive data traded between SG's and system appropriation directors in opposition to any investigation for their divulgence when they are sent in the system. The suggested method is to give protection ensured key understanding security conspire that plans to furnish any traded correspondence with an adaptability capacity permitting it to display variable and eccentric practices to secure it against assaults on their substance and offer higher degree of protection.

These days, because of the expanding populace, there is popularity for sustainable power sources and this interest is expanding because of rising vitality costs and worldwide natural changes as shown in Figure 1. The current power matrix depends vigorously on customary petroleum derivative-based power age units which are very nearly eradicated. Transferring electrical vitality from these age units over the dispersion lines to the clients in the present-day power framework acquires huge force misfortunes. Likewise, numerous ordinary petroleum derivative-based power age units present perils, e.g., risks from atomic force plants. In this manner, there is a worldwide push to change the power age by moving ceaselessly from petroleum derivative-based plants and shifting towards renewable energy resources. By utilizing renewable energy resources, CO_2 discharge can be around the world diminished.

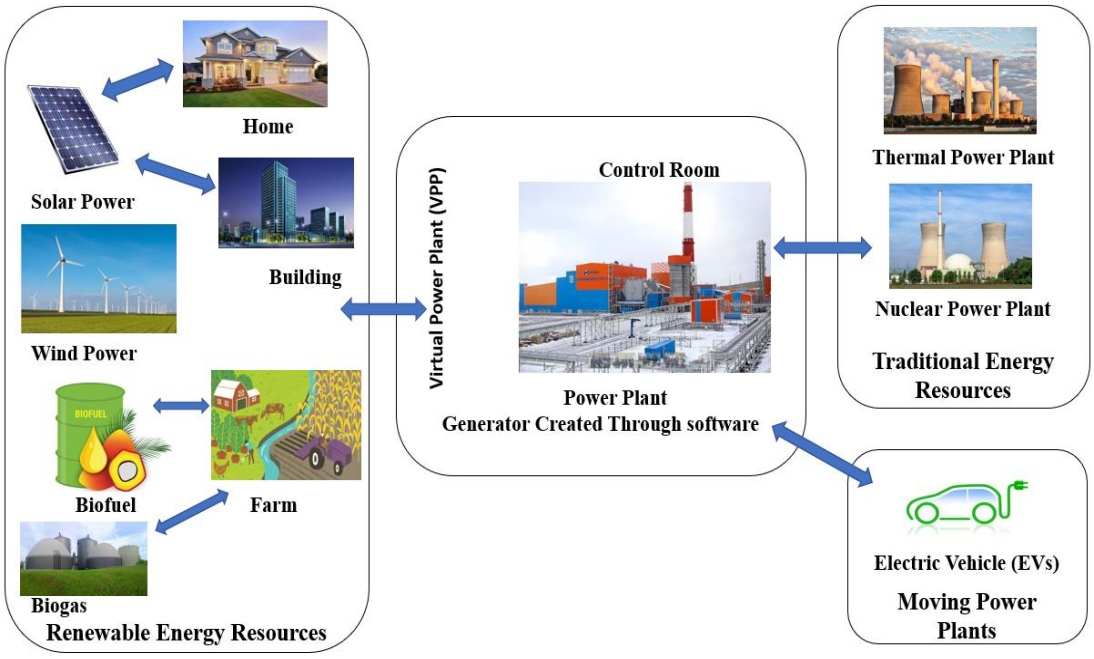

Figure 1. Normal virtual power plant, which joins distinctive energy assets through concentrated programming [5]

According to the IEEE Grid Vision 2050, the essential any expectation of the SG is to have the control and automation estimates spread over the force framework to allow beneficial and strong bidirectional power stream [10]. This is recognized through the compromise of information and

communication technology (ICT) into the power network which makes it a sort of digital actual framework (CPS) [11]. The dynamic blend between the certified and virtual universes opened an enormous gateway of expected headways, counts, and responds in due order regarding be made and completed in the SG, for instance, passed on data dealing with and mechanized thinking [12].

With its promising advancements, the SG network will reform our general public, economy, and condition. Enormous and little partnerships anticipated the SG innovations developing business sectors and raced to be the first to convey. In any case, security perspectives have assumed the lower priority inside this surge. With the presentation of the broadly shifted ICT segments, the weakness of the SG has been undermined hugely. This shaped an immense worry over the unwavering quality and the security of the ever-needed SG with huge dangers extending from monetary to strength viewpoints. In this way, a few exploration endeavors have been led toward the security expansion of the savvy lattice by initially understanding the diverse weakness focuses and by proposing appropriate and solid arrangements either on the digital or the physical layer. These endeavors came in light of the ever-expanding digital physical assaults on SG.

2. RESEARCH CONTENT AND METHODOLOGIES USED

2.1. Understanding the smart grid with respect to security & privacy aspect

The information technology (IT) and operational technology (OT) frameworks are being robotized for successful administration of the electrical grid and related system approaches, as shown in Figure 2. The IT tasks are helped out through an inflexible and made sure information correspondence network at different areas including the Information Technology for Operation Technology stations. In this situation, the accessibility of the OT frameworks can be kept up with an IT/OT intermingling through a made sure about correspondence channel.

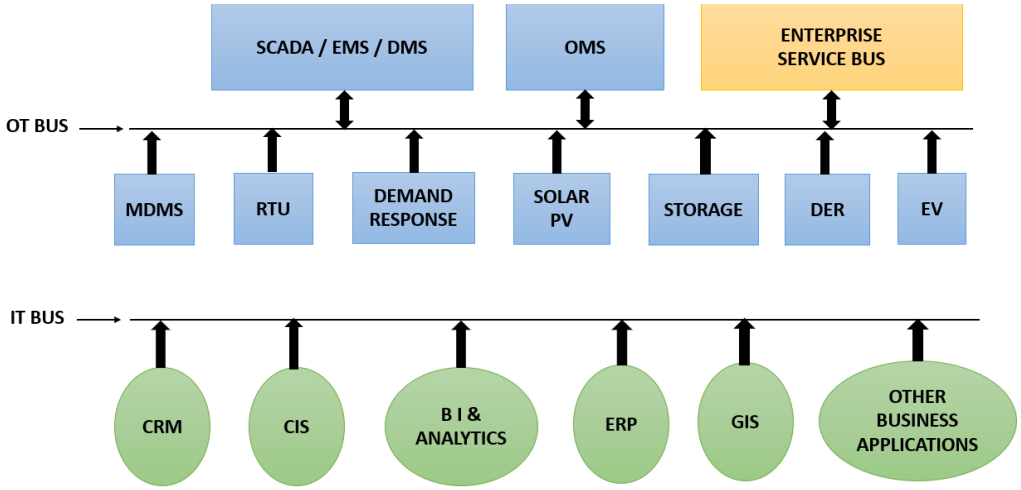

Figure 2. IT and OT operations under smart grid rule

Since the IT frameworks are presented to the Internet, they are more helpless against digital assaults and accordingly the Operational Technology frameworks are associated in an isolated way. For the endeavor application mix, the data as information must be shared in the middle of the Information Technology and Operational Technology frameworks through an ESB.

2.2. Challenges in security domains of the smart grid infrastructure

2.2.1. Attacks, type of attackers and vulnerabilities in operational technology systems

Smart grid aims to accomplish three main objectives: 1) accessibility of continuous power force according to client prerequisites 2) trustworthiness of conveyed data and 3) secrecy of client's information. With cutting edge innovations into play the force the board has become streamlined however the whole IT empowered network has gotten helpless against various sorts of assaults. These dangers may offer admittance to the lawbreakers to assault the correspondence organization and bargain the classification and information uprightness of the data that influences the customers with a power outage [13]. The distinctive assault variations in the OT frameworks are given beneath in Figure 3.

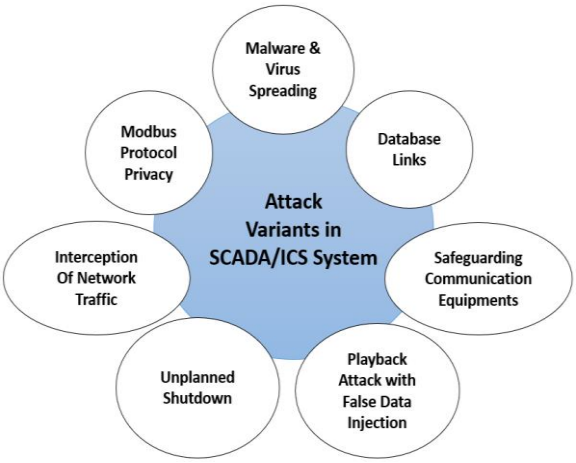

Figure 3. Assault variants in SCADA or industrial control systems framework

Types of attackers:
- The moral programmers who've no goal to hurt the framework and their thought process are to increase a standing among the associates.
- Clients at home may get vindictive and take a stab at hacking to truly close down their home meters.
- Cybercriminals who attempt to risk the meter the board framework through the public web.
- Disappointed representatives who submit inadvertent errors to influence the frameworks and at last become an assailant.

The vulnerable attack surfaces are as follows [14]:
- Checking Modbus messages.
- Postponing reaction messages proposed for the experts.
- Assaulting a machine with the best possible ports.
- Sending dependable data to every conceivable location to gather gear data.
- Closing out an ace and controlling at least one field gadget.
- Replaying valid recorded messages back to the pro control network.
- Sending bogus messages to endpoint gadgets.

2.2.2. Vulnerable attack surfaces of AMI

There are several vulnerable attack surfaces of AMI:
- AMI architecture.
- Communication system.
- Data manipulation & tampering techniques: 1) physical tampering, 2) data hacking.

The two significant correspondence frameworks transcendent in the smart metering system [15]: (i) public internet, as shown in Figure 4, and (ii) RF mesh networks, as shown in Figure 5.

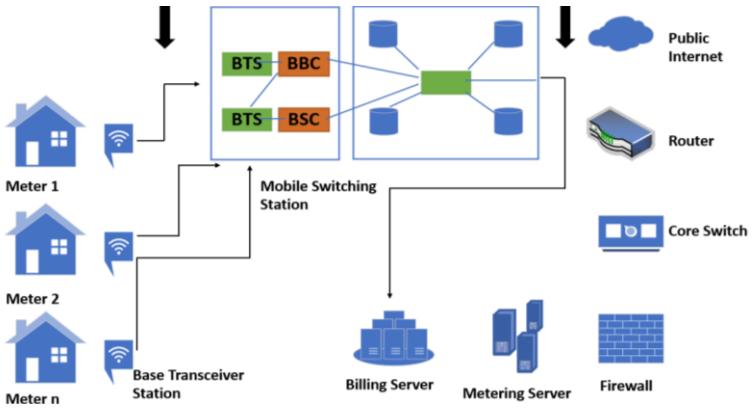

Figure 4. Weak points of smart meter correspondence utilizing public web

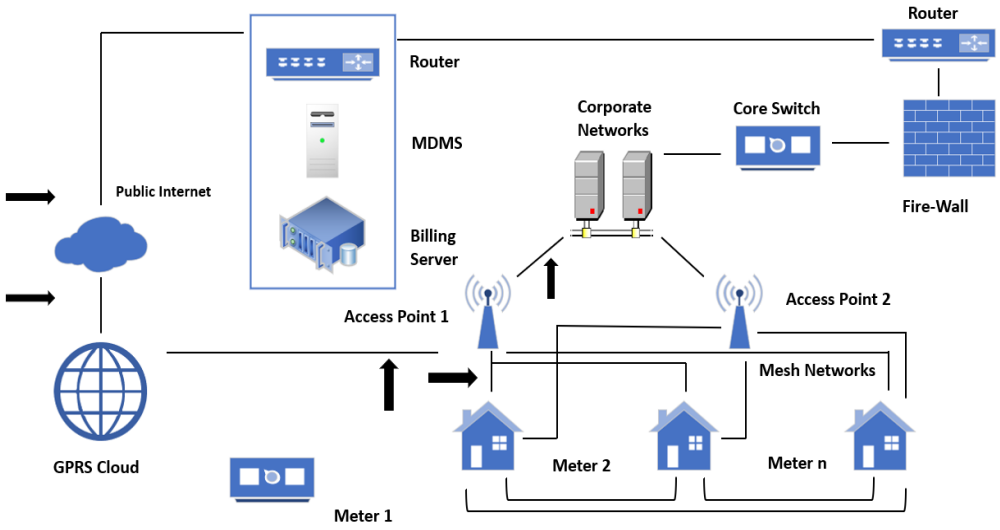

Figure 5. Weak points of smart grid communication utilizing radio frequency mesh network

2.2.3. Existing work on security, privacy and open research issues of smart grid metering networks

Proposed ideas in Table 1:

- An exhaustive perspective on security and protection concerns.
- Detailed classification of smart grid assaults.
- A complete report for security and privacy objectives and relating solutions.
- Future research paths.

Table 1. Comparison with other existing surveys

Reference marking	Security issues	Privacy issues	Real attack incidents	Threat to system level security	Thefts or threats via services	Threats to privacy	Papers covered
[16]	Yes	No	No	Yes	No	No	2008-12
[17]	Yes	Yes	No	Yes	Limited	Limited	2010-14
[18]	Yes	Yes	No	No	Limited	Limited	2010-16
[19]	No	No	No	No	No	No	2008-15
[20]	Yes	No	No	Yes	No	No	2009-16
[21]	Yes	Yes	No	No	Limited	Yes	2007-14
[22]	No	Yes	No	No	No	Limited	2008-15
[23]	Yes	Yes	No	No	Limited	Limited	2007-14
[24]	No	No	No	No	Limited	Limited	2010-15
[25]	No	No	No	No	Limited	Limited	2010-18
Suggested [26]	Yes	Yes	Yes	Yes	Yes	Yes	2010-18

2.2.4. Solution idea proposed for scalable and efficient authentication scheme for secure SG communications

To give a successful complete answer for the security of the SG conduct against any examination of their exposure during use as Table 2, we recommend another way to deal with guaranteed secure correspondence between smart grid and vitality providers as Figure 6. To do this, we have divided our solution in 4 stages, *Setup-> *Identification-> *Authentication-> *Password Change.

Table 2. Security analysis

Security properties	Paper [27]	Paper [28]	Paper [29]	Paper [30]	Suggested
Protection against forgery attack	Yes	No	No	Yes	Yes
Protection against replay attack	No	Yes	No	Yes	Yes
Protection against password guessing attack	No	No	Yes	No	Yes
Protection against a man-in-the-middle attack	No	Yes	No	Yes	Yes
Protection against session key security	Yes	Yes	Yes	Yes	Yes
Perfect forward secrecy	No	Yes	Yes	Yes	Yes
Protection against insider attack	Yes	No	No	No	Yes
Smart meter anonymity	No	No	Yes	Yes	Yes

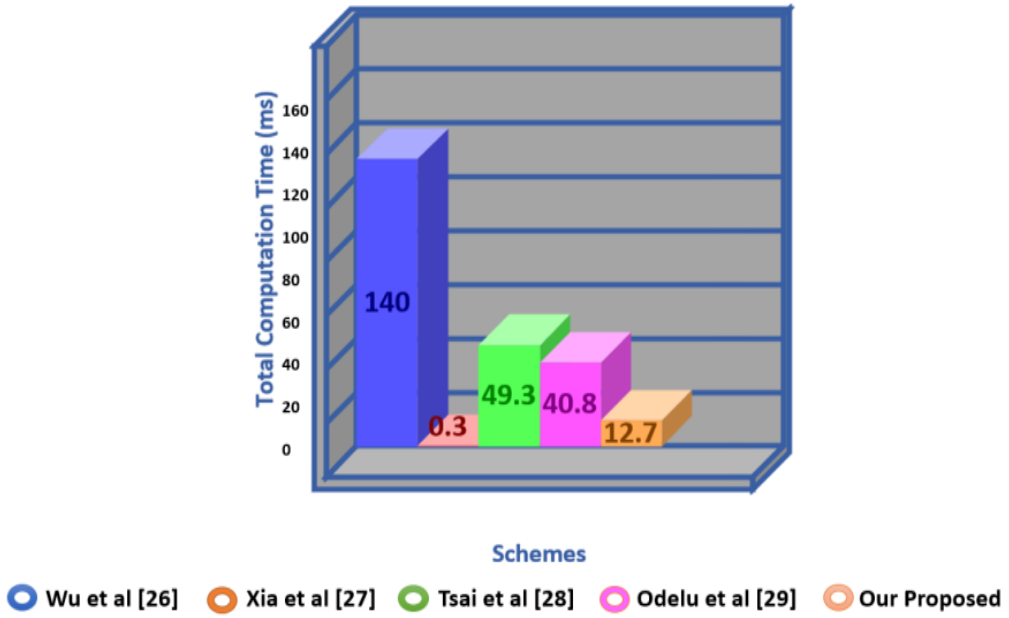

Figure 6. Correlation of our solution with different arrangements regarding computation costs

2.3. Comparison with related survey articles

Broad earlier work has inspected the combination of dispersed energy resources and renewable energy resources into the SG as shown in Figure 7. A few exceptional diary concern cases have been distributed on the mix of renewable energy resources into the SG, see for example, [31]. Additionally, a few books have been distributed on this theme [32]-[34]. Corresponding to these earlier articles, we give a forward-thinking outline of the correspondence perspectives emerging from the reconciliation of renewable energy resources into the SG as shown in Figure 8.

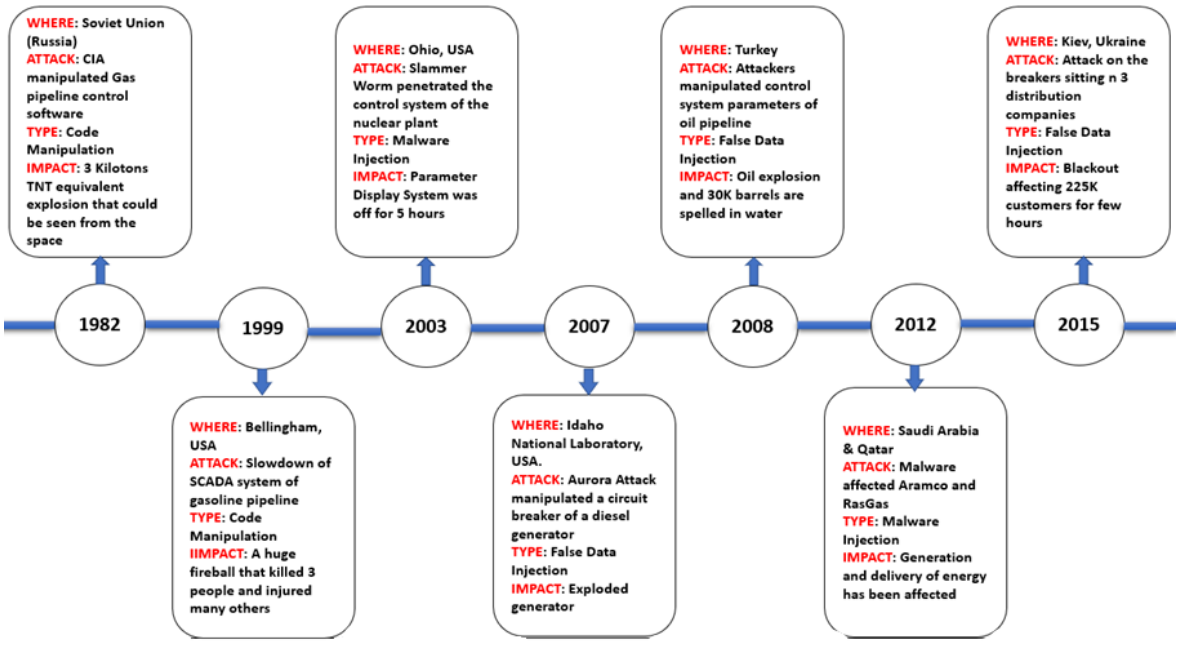

Figure 7. A timetable of the major digital-physical assaults in the vitality business segment

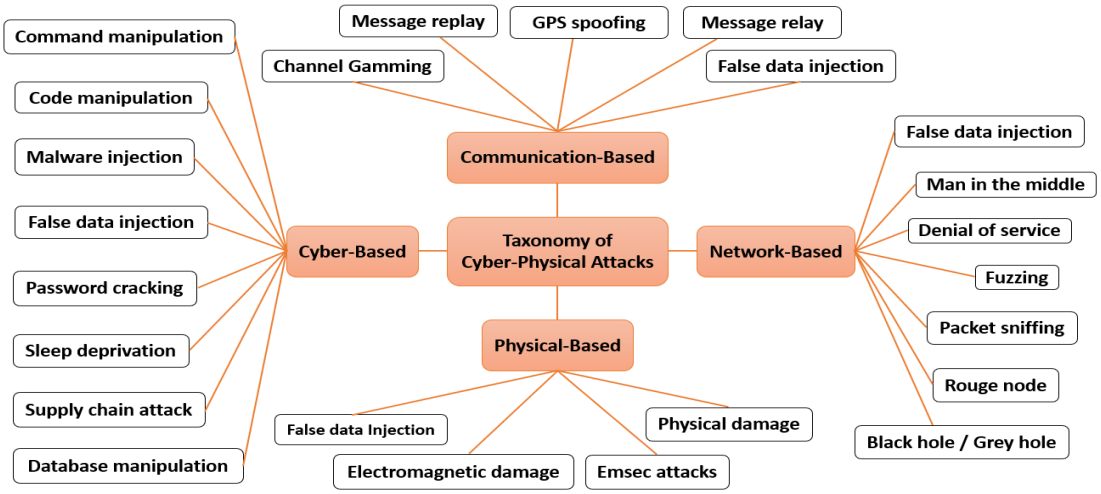

Figure 8. The scientific categorization of digital physical assaults as per their conveyance strategy

3. FUTURE SCOPES

3.1. Security and privacy aspects in SG

SG is one of the crucial components in the distribution and reconciliation of energy. The security domain of the SG infrastructure which is an integral part of the SG framework has certain challenges and needs to be resolved quickly. There are still these concerns, despite the advanced features of Demand Management Infrastructure, which are still undergoing controversy due to the connection of large no. of heterogeneous devices. SG invention is a great achievement for both energy providers and users, giving them advantage to perform more accurate estimations of energy, analyze their utilization, and in this manner control their power bills. In any case, this cutting-edge innovation also quickly raises various kinds of assaults that can unfavorably influence the activity of the grid by distorting power utilization information.

3.2. Integration of SG with renewable energy resources

Expanding energy costs, losses in the customary framework, hazards from atomic electricity generation, and worldwide natural changes are inspiring a change of the traditional methods of creating power. Worldwide, there is a craving to depend on renewable energy resources more than non-renewable ones for power production. The power lattice is by and by advancing towards an insightful network, the purported SG. One of the significant objectives of things to come in SG is to move towards 100% power generation from renewable sources, i.e., towards a 100% sustainable grid. In any case, the divergent, discontinuous, and normally broadly topographically circulated nature of renewable energy resources convolutes the joining of renewable energy resources into the SG. Additionally, singular renewable energy resources have by and large lower limit than regular non-renewable energy source plants, and these renewable resources depend on a wide range of various advancements.

4. CONCLUSION

The need to resolve the privacy and security issue of smart grid infrastructure is an issue that needs to be resolved as quickly as possible because the flow of data is very sensitive and also because of the need for a sustainable future. The conventional power networks worldwide of today will change to the cutting-edge keen lattices in the coming future. Notwithstanding, the achievement of SG metering system relies upon its security properties. Another essential component of SG metering system is the customer's privacy, i.e., how to total purchasers' information without unveiling their own and touchy data. Hence, security and protection in power lattice are considered as a rising exploration topic, which merits examination. This review examines an exhaustive overview on security and protection research in SG metering systems. We examine the genuine digital assaults episodes in the force business and related applications. Also, we research definite danger scientific classification including framework level, robbery of administration, and protection/secrecy dangers that have prompted the security and protection necessity in SG metering systems. Additionally, we present and think about the preferences and weaknesses of cutting edge existing most forward-thinking arrangements, at that point finish this paper by calling attention to the future examination issues. The work done in this paper is also on the SG security framework in its running condition. In our proposed method, we have turned to the utilization of light cryptographic natives.

REFERENCES

[1] R. K. Bhatia and V. Bodade, "Smart grid security and privacy: Challenges, literature survey and issues," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 4, no. 1, Jan. 2014.

[2] J. Liu, Y. Xiao, S. Li, W. Liang and C. L. P. Chen, "Cyber security and privacy issues in smart grids," in *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981-997, Fourth Quarter 2012, doi: 10.1109/SURV.2011.122111.00145.

[3] P. Ganguly, M. Nasipuri and S. Dutta, "Challenges of the existing security measures deployed in the smart grid framework," *2019 IEEE 7th International Conference on Smart Energy Grid Engineering SEGE*, Oshawa, ON, Canada, pp. 1-5, 2019, doi: 10.1109/SEGE.2019.8859917.

[4] M. H. Rehmani, M. Reisslein, A. Rachedi, M. Erol-Kantarci and M. Radenkovic, "Integrating renewable energy resources into the smart grid: Recent developments in information and communication technologies," in *IEEE Transactions on Industrial Informatics*, vol. 14, no. 7, pp. 2814-2825, Jul. 2018, doi: 10.1109/TII.2018.2819169.

[5] M. Emmanuel and R. Rayudu, "Communication technologies for smart grid applications: A survey," *Journal of Network and Computer Application*, vol. 74, pp. 133-148, 2016, doi: 10.1016/j.jnca.2016.08.012.

[6] Seong Cheol Kim, Papia Ray and S. Surender Reddy, "Features of smart grid technologies: An overview," *ECTI Transaction Electrical Engineering Electronic Communication*, vol. 17, no. 2, pp. 169-180, 2019, doi: 10.37936/ecti-eec.2019172.215478.

[7] I. Colak, S. Sagiroglu, G. Fulli, M. Yesilbudak and C.-F. Covrig, "A survey on the critical issues in smart grid technologies," *Renewable Sustainable Energy Reviews*, vol. 54, pp. 396-405, 2016, doi: 10.1016/j.rser.2015.10.036.

[8] P. Kumar, Y. Lin, G. Bai, A. Paverd, J. S. Dong and A. Martin, "Smart grid metering networks: A survey on security, privacy and open research issues," in *IEEE Communications Surveys & Tutorial*s, vol. 21, no. 3, pp. 2886-2927, thirdquarter 2019, doi: 10.1109/COMST.2019.2899354.

[9] A. K. Das and S. Zeadally, "Chapter 13- data security in the smart grid environment," *Pathways to a Smarter Power System*, pp. 371-395, Jan. 2019, doi: 10.1016/B978-0-08-102592-5.00013-2.

[10] IEEE Standars Associations, "Smart grid research: Power IEEE grid vision 2050, reference model," *IEE-PES*, 30 Apr. 2013.

[11] M. Faheem, S. B. H. Shah, R. A. Butt, B. Raza, M. Anwar, M. W. Ashraf, Md. Ngadi and V. C. Gungor, "Smart grid communication and information technologies in the perspective of industry 4.0: Opportunities and challenges," *Computer Science Review*, vol. 30, pp. 1-30, 2018, doi: 10.1016/j.cosrev.2018.08.001.

[12] X. Yu and Y. Xue, "Smart grids: A cyber–physical systems perspective," in *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058-1070, May 2016, doi: 10.1109/JPROC.2015.2503119.

[13] F. Ye, Y. Qian and R. Q. Hu, *Smart grid communication infrastructures: Big data, cloud computing, and security*, USA: Wiley IEEE Press, 304 pages, Aug. 2018.

[14] C. Peng, H. Sun, M. Yang and Y. Wang, "A survey on security communication and control for smart grids under malicious cyber attacks," in *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1554-1569, Aug. 2019, doi: 10.1109/TSMC.2018.2884952.

[15] T. Mehra, V. Dehalwar and M. Kolhe, "Data communication security of advanced metering infrastructure in smart grid," *2013 5th International Conference and Computational Intelligence and Communication Networks, Mathura*, India, pp. 394-399, 2013, doi: 10.1109/CICN.2013.87.

[16] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Computer Networks*, vol. 57, no. 5, pp. 1344-1371, 2013, doi: 10.1016/j.comnet.2012.12.017.

[17] N. Komninos, E. Philippou and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," in *IEEE Communications Surveys & Tutorial*s, vol. 16, no. 4, pp. 1933-1954, Fourthquarter 2014, doi: 10.1109/COMST.2014.2320093.

[18] S. Tan, D. De, W. Song, J. Yang and S. K. Das, "Survey of security advances in smart grid: A data driven approach," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 397-422, Firstquarter 2017, doi: 10.1109/COMST.2016.2616442.

[19] D. Alahakoon and X. Yu, "Smart electricity meter data intelligence for future energy systems: A survey," in *IEEE Transactions on Industrial Informatics*, vol. 12, no. 1, pp. 425-436, Feb. 2016, doi: 10.1109/TII.2015.2414355.

[20] H. He and J. Yan, "Cyber-physical attacks and defenses in the smart grid: A survey," *IET Cyber Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016, doi: 10.1049/iet-cps.2016.0019.

[21] S. Finster and I. Baumgart, "Privacy-aware smart metering: A survey," in *IEEE Communications Surveys & Tutorials*, vol. 17, no. 2, pp. 1088-1101, Secondquarter 2015, doi: 10.1109/COMST.2015.2425958.

[22] M. R. Asghar, G Dan, D. Miorandi and I. Chlamtac, "Smart meter data privacy: A survey," in *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820-2835, 2017, doi: 10.1109/COMST.2017.2720195.

[23] R. R. Mohassel, A. Fung, F. Mohammadi and K. Raahemifar, "A survey on advanced metering infrastructure," *International Journal of Electrical Power & Energy Systems*, vol. 63, pp. 473-484, 2014, doi: 10.1016/j.ijepes.2014.06.025.

[24] Y. Kabalci, "A survey on smart metering and smart grid communication," *Renewable and Sustainable Energy Reviews*, vol. 57, pp. 302-318, 2016, doi: 10.1016/j.rser.2015.12.114.

[25] Y. Wang, Q. Chen, T. Hong and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," in *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3125-3148, May 2019, doi: 10.1109/TSG.2018.2818167.

[26] A. Ahmad, M. H. Rehmani, H. Tembine, O. A. Mohammed and A. Jamalipour, "IEEE access special section editorial: Optimization for emerging wireless networks: IoT, 5G, and smart grid communication networks," in *IEEE Access*, vol. 5, pp. 2096-2100, 2017, doi: 10.1109/ACCESS.2017.2655238.
[27] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," in *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 375-381, Jun. 2011, doi: 10.1109/TSG.2011.2120634.
[28] J. Xia and Y. Wang, "Secure key distribution for the smart grid," in *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1437-1443, Sept. 2012. doi: 10.1109/TSG.2012.2199141.
[29] J. Tsai and N. Lo, "Secure anonymous key distribution scheme for smart grid," in *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906-914, Mar. 2016, doi: 10.1109/TSG.2015.2440658.
[30] V. Odelu, A. K. Das, M. Wazid and M. Conti, "Provably secure authenticated key agreement scheme for smart grid," in *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1900-1910, May 2018, doi: 10.1109/TSG.2016.2602282.
[31] M. H. Rehmani, M. Erol Kantarci, A. Rachedi, M. Radenkovic and M. Reisslein, "IEEE access special section editorial smart grids: A hub of interdisciplinary research," in *IEEE Access*, vol. 3, pp. 3114-3118, 2015, doi: 10.1109/ACCESS.2016.2516158.
[32] Q. C. Zhong and T. Hornik, "Control of power inverters in renewable energy and smart grid integration," *Wiley IEEE Press*, 2013.
[33] A. S. Musleh, G. Chen and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," in *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218-2234, May 2020, doi: 10.1109/TSG.2019.2949998.
[34] H. Hammami, S. B. Yahia and M. S. Obaidat, "Scalable and efficient authentication scheme for secure smart grid communication," *IET Networks*, vol. 9, no. 4, pp. 165-169, Jul. 2020, [Online]. Availaible: doi: 10.1049/iet-net.2019.0225.

BIOGRAPHIES OF AUTHORS

Manoj Saini, Research Scholar, School of Electrical, Electronics & Communication Engineering, Galgotias University, Gr. Noida. Uttar Pradesh, India, M-Tech: Electrical Engineering (Power System), D.C.R.U.S.T, Murthal, Sonipat, in 2011, B.E.: Electrical Engineering, C.R.S.C.E, Murthal, Sonipat, Haryana, in 2009. Currently working as Assistant Professor in Electrical Engineering Department, Galgotias College of Engineering and Technology, 1, Knowledge Park, Phase II, Greater Noida, Uttar Pradesh 201306, Since 01 Dec 2014 to till date. Research Area: Renewable Energy Generation, Power system and Energy Auditing, Teaching Experience: 7 years

Shagufta Khan, Assistant Professor, School of Electrical, Electronics & Communication Engineering, Galgotias University, Gr. Noida. Dr. Shagufta Khan received the Ph.D. degree in electrical engineering from Delhi Technological University, Delhi, India. She is currently an Assistant Professor with the School of Electrical, Electronics and Communication Engineering, Galgotias University, Greater Noida, India. Her research interests include power systems and renewable energy.

Rajeev Gupta, Student, Pursuing Bachelor of Technology in Electrical Engineering from Galgotias College of Engineering and Technology, Knowledge Park, Phase-II, Greater Noida (201306), Uttar Pradesh, India.

Shivani Singh, Student of Electrical Engineering at Galgotias College of Engineering and Technology, Knowledge Park, Phase-II, Greater Noida (201306), Uttar Pradesh, India.

Pooja Upadhyay, Student, Bachelor of Technology in Electricals at Galgotias College Of Engineering and Technology, 1, Knowledge Park, Phase-II, Greater Noida (201306), Uttar Pradesh, India.

Shivangi Soni, Student of Electrical Engineering at Galgotias College of Engineering and Technology, Knowledge Park, Phase-II, Greater Noida (201306), Uttar Pradesh, India.