IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023

DOI: 10.17148/IJARCCE.2023.125228

Cyber Security and Privacy Issues in Smart Grids

Arpita Mahadev Belekar[1], Lovelesh N.Yadav[2], Neehal B.Jiwane[3]

Student, Computer Science & Engineering, Shri Sai College of Engineering &Technology , Bhdrawati, India[1]

Head Of Department , Computer Science & Engineering, Shri Sai College Of Engineering & Technology, Bhdrawati, India[2]

Asst.prof, Computer Science & Engineering, Shri Sai College Of Engineering & Technology, Bhdrawati, India[3]

Abstract: smart grid is a promising power delivery infrastructure included with communique and statistics technologies. Its bi-directional communique and power float permit each utilities and customers to monitor, predict, and control strength usage. It additionally advances energy and environmental sustainability thru the integration of significant dispensed energy assets. Deploying any such green electric powered machine has considerable and far-achieving monetary and social blessings. nevertheless, improved interconnection and integration also introduce cybervulnerabilities into the grid. Failure to cope with those issues will hinder the modernization of the prevailing electricity machine. In order to build a reliable smart grid, a top level view of relevant cyber protection and privacy troubles is presented. based totally on contemporary literatures, numerous capability research fields are discussed on the give up of this paper.

Keywords: smart grid, SCADA; AMI, security, privacy

I. INTRODUCTION

while generation and innovation hold to modernize enterprise, our electric strength machine has been maintained in the same manner for decades. The growing load and intake needs growth power complications, along with voltage sags, black outs, and overloads. meanwhile, the present day electric network contributes substantially to carbon emissions. the us' power system on my own takes up forty% of all nationwide carbon dioxide emissions . Considering each monetary and environmental hobbies, huge changes should be made to such an risky and inefficient system. therefore, many countries (e.g., U.S., european, Canada, China, Australia, South Africa, and so on.) at the moment are modernizing their energy grids [42]. They accept as true with that they now not simplest require reliability, scalability, manageability, and extensibility, but also that they must be comfortable, interoperable, and fee-powerful. Such an electric infrastructure is called a "smart grid."usually speaking, the clever grid is a promising power transport infrastructure that is incorporated with two-manner communication and electricity flows. thru superior sensing technology and manage strategies, it may seize and analyze

II. OVERVIEW OF SMART GRID

A. FEATURES

In 2007, the U.S. countrywide strength generation Laboratory (NETL) [6] identified seven important traits for modern strength grid design. Later in 2009, the U.S. department of energy (DOE) merged two of them (self-heals and resists assault) and restated the layout functions and benefits for smartgrid as follows :

enabling knowledgeable Participation with the aid of clients: in contrast to traditional electricity structures, clients are higher informed through a -manner communique era. The complete clever grid becomes an lively electricity marketplace that permits clients to shift load and to generate and store strength based on close to real-time costs and other financial incentives. via bidirectional electricity glide, clients also are able to promote surfeit stored strength back to the grid whilst the rate is high

Accommodating All era and garage alternatives: The clever grid now not simplest contains remote centralized energy generation, but additionally adopts numerous and significant allotted power aid (DER) (e.g., solar, wind, or geothermal strength) through bendy community structure and dispensed management. This concept is proposed to relieve peak load, to support returned-up energy all through emergencies, and to fulfill the grid's growing according with the herbal surroundings, society, and the economy. three) enabling New merchandise, offerings, and Markets: New services and products are essential components of the smart grid that may sell low-cost and green solutions for all power uSers. by

DOI: 10.17148/IJARCCE.2023.125228

the usage of customer-oriented "smart home equipment" or wise digital gadgets (IEDs), for instance, clients or authorized provider companies can remotely manage IEDs' energy usage. Markets act as coordinators dealing with a sequence of independent grid parameters, such as time, ability.

supplying the electricity nice for the variety of needs: strength fine includes elements like voltage flicker, voltage quantity, short-term interruptions, and many others. distinctive customers can also have awesome energy best requirements (e.g., industrial vs. residential customers). to meet a specific customer's electricity utilization, the clever grid ought to meet a extensive range of power nice needs in terms of architectural designs and settlement concerns.

B ARCHITECTURE

To date, the architectural framework and implementation standards of the smart grid are still under investigation by the academic [7], [8], [16], industrial [1], [17], [18], [30], and government sectors [2], [4], [6]. Although there are various designs for the grid architecture, almost every case follows the common reference model [4] proposed by the U.S. National Institute of Standards and Technology (NIST). LIU et al.: CYBER SECURITY AND PRIVACY ISSUES IN SMART GRIDS.

C KEY COMPONENTS

AMI (advanced Metering Infrastructure): AMI is an integration of more than one technologies that provides shrewd connections among customers and system operators [5]. principal packages include clever meters, HAN, meter recordscontrol structures (MDMS), and operational gateways (as proven in Fig. 2) [5]. it's far designed to help consumers know the near-actual-time charge of strength and accordingly to optimize their power utilization as a consequence [4], [5]. It additionally enables the grid acquire treasured data about customers' strength intake in order to make certain the reliability of the electric electricity machine

verbal exchange Protocols and standards: The communication standards for the energy enterprise were evolved by five main agencies which includes the IEEE, the IECN(worldwide Electro-technical fee), and the DNP3 (allotted network Protocol) users organization [37]. The maximum universal protocols for SCADA conversation systems are IEC 60870-five and DNP3 [37]. The IEC protocol is typically used in Europe for communique between MTU and RTUs in SCADA systems [38], [39]. The DNP3, that's derived from IEC 60870-five and identified by way of the IEEE 1379 widespread, is broadly utilized in Asia and North the us [38], [39]. IEC 61850 has now been released to support greater better skills together with a peer-to-peer communication mode for area devices [39]. it may be appeared as a successor to the DNP3 [29]. IEC 62351 [41] is a widespread that specifies protection constraints and issues of the above conversation protocols and standards. It consists of 8 parts. the first elements present an creation to its background and a thesaurus of terms. part-3 specifies the security requirements for TCP/IP profiles in IEC 60870 and IEC 61850. specially, it describes the TLS (transport degree protection) configuration for cozy interactions [29], [38], [41]. part-four addresses MMS (production Message Specification, ISO 9506) protocol security within the IEC 61850 preferred. especially, the MMS will work with the TLS to comfy communications [38]. no longer all additives are required to adopt this comfy mechanism [38]. part-5 focuses on the safety of serial verbal exchange in IEC 60870 and DNP3. It indicates that the TLS (transport Layer safety) encryption mechanism may be applied for serial communique to allow confidentiality and integrity [38]. As for the authentication, the serial version can only deal with replay, spoofing, amendment, and some DoS assaults [38]. It can not prevent eavesdropping, traffic analysis, or repudiation due to its constrained computing functionality. however, it can be included by means of alternate techniques, including VPNs or "bump-in-the-cord" (a scheme that use an IPSec device as a firewall to filter unwanted programs from the net) technology, depending upon the skills of the devices and communications involved [38]. relevant key control measures are also defined on this eleme

III. CYBER SECURITY ISSUES ON SMART GRID

he conventional electricity delivery gadget makes a speciality of developing system to enhance integrity, availability, and confidentiality. till these days, modern-day verbal exchange technologies and device had been generally seemed as helping the energy enterprise's reliability.however,increased connectivity is turning into more essential to the cyber security of the power device. In a huge feel, the cyber safety of the power enterprise covers all IT and communications problems that affect the operation of electricity transport systems and the management of the utilities [3]. particularly, securing the energy grid prevents, prepares for, protects in opposition to, mitigates, responds to, and recovers from surprising cyber activities or herbal screw ups [3]. Wei et al. [30] pointed out that the development of a cozy clever grid would come across the following 4 demanding situations:

DOI: 10.17148/IJARCCE.2023.125228

1) The power transport system has new communication necessities in phrases of protocols, put off, bandwidth,and price. averting early obsolescence is critical in smart grid protection improvement.

2) Many legacy devices were utilized in strength automation structures for many years. most of them most effective recognition on a positive functionality and for that reason lack enough reminiscence area or computational capability to cope with protection issues. Integrating the prevailing legacy system into the clever grid without weakening their control performance is a task. three) Networking within the cutting-edge energy grid uses heterogeneous technologies and protocols along with ModBus [50], ModBus+ [50], ProfiBus (procedure subject Bus) [51], ICCP (Inter-manipulate center verbal exchange Protocol), DNP3 [37], and many others. however, most of them had been designed for connectivity with out cyber security. four) modern-day energy systems are typically proprietary structures that offer precise performances

A. Device issues

gadgets like percent (Programmable Logical Controllers), RTUs, and IEDs are widely deployed in energy delivery systems to permit administrators to carry out preservation or to dispatch functionalities from a far flung vicinity [30]. This function also permits malicious customers to manipulate the tool and disrupt regular operations of the grid, inclusive of shutting down going for walks devices to disconnect power offerings or tampering with sensing information to misguide the decisions of the operators [30]. The authors in [53] mentioned any such cyber vulnerability, wherein an attacker may want to transfer-off masses of tens of millions of smart meters with far off off switches. although no agreed solutions are proposed in gift standards and policies, some endorsed countermeasures in [53] can be considered in similarly discussions. For the gadgets, the IEEE 1686- 2007 widespread has detailed protection necessities. but, enjoy suggests that usual IEDs are far from complying with this standard. As described in desk II, ability security troubles can also gift within the packages of clever meter, customer interfaces, and PHEVs. As for the meter tool, a traditional physical meter can be modified via reversing the inner usage counter (aka. meter inversion) or be manipulated to control the calculation of the electric waft [14]. Addressing this hassle can also require.

hardware assist. we will therefore not recognition on its solutions on this paper. except, statistics aggregation is generally perceived as a primary function for the clever meter. numerous algorithms [60], [61] have been proposed to save you the meter statistics from being compromised. Authors in [61] analyzed the tradeoff between security and efficiency and designed algorithms for consistent with-hop and give up-to-cease communique protocol respectively. They used AES-CCM with 128 bit shared key to encrypt the line between the meter and the gateway, which showed their protocol is reliable and energy efficient (according to their experiment effects)

B Networking issue

potential protection issues of networking in smart grids specially consciousness on problems of the net, wireless networks, and sensor networks. similar to the net, more than one networking technologies can be applied for the clever grid, which includes fiber optics, land mobile radio (LMR), 3G/4G (WiMax), RS-232/RS-485 serial links, WiFi, and so forth [27]. Which one will be used relies upon at the necessities of the grid surroundings and is an open difficulty inside the development of smart grid verbal exchange standards. For stressed out networks, sun et al. [28] claimed that Ethernet Passive Optical Networks (EPON) could be a promising answer for the clever grid broadband get entry to networks because of the following metrics: 1) backward compatibility, 2) low-fee fiber deployment and maintenance, and 3) minimal protocol overhead. EPON additionally has been appeared as subsequent-generation Gigabit-Ethernet by way of IEEE 802.3ah popular.

C Dispatching and management tools

smart grid can be regarded as a mixture of several micro grids [11]. each micro grid operates autonomously within its local SCADA device and interacts with others like “Island capability” or “Islanding.” meanwhile, all micro grids could be managed by a central master SCADA device wherein every neighborhood SCADA acts as a slave controller offering strength associated records to the vital controller. This framework guarantees reliability of the smart grid and accordingly has been authorised by way of the IEEE-1547 trendy. traditionally, those SCADA structures are remoted and managed by way of authorized employees. maximum of them lack real-time manipulate and monitoring capabilities [32]. until recently, GPS time-stamped (in milliseconds) phasor size units (PMUs) offered atechnique to this hassle. To deal with the clock synchronization problem in the disbursed context, the NTP (network Time Protocol) and the IEEE 1588 standard are used inside the current SCADA gadget [40]. This accelerated interoperability, however, makes them more available to public users, which unavoidably increases the risk of the gadget being compromised as follows: 1) Take down the server: If the IP of the SCADA server and the community course are recognised to the attacker, the server may be without difficulty taken down or shutdown by the conventional denial of carrier mistakes or by way of sincerely deleting the gadget documents. Denial of service may be performed if the TCP/IP can be flooded.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 5, May 2023
DOI: 10.17148/IJARCCE.2023.125228

Deleting the files may be finished by hacking the consumer passwords or having access to the bodily system. these assaults can cause a primary danger to destiny offerings as properl. 2) Gaining control over the gadget: that is accomplished with the aid of planting a Trojan or by way of backdoor entry into the machine registries. that is the very best scale of safety chance, with the aid of which a false alarm and manipulated controls can be generated and despatched to RTUs inflicting large scalecollapses.

3) Stealing company data: these problems arise if the employer protection level is negative and the software program architecture used is not particularly capable. The company statistics can be stolen from the database for the internal rivalry among the competing provider providers

IV. CONCLUSION

This paper specifically gives a top level view of cyber safety and privateness problems inside the clever grid. in step with present studies, we may finish that almost each thing related to IT era in the smart grid has ability vulnerabilities because of inherent security risks inside the preferred IT environment.

The paper also offers future studies instructions. Cyber safety and privateness troubles inside the smart grid are new areas inside the fields of power industry, electric engineering, and laptop technological know-how. more in-depth studies is needed to increase this sort of promising power grid within the near future.

ACKNOWLEDGEMENT

This work was also supported in part by the National Science Foundation (NSF) under grants CCF-0829827, CNS0716211, CNS-0737325, and CNS-1059265. Prof. Liang's work is supported in part by the National High Technology Research and Development Program of China (863 plan) under 2011AA040101, the National Fundamental Research 973 Program of China under 2010CB334705,the Natural Science Foundation of China under 61174026, 60725312 and the Knowledge Innovative Program of The Chinese Academy of Sciences under KGCX2-EW-104-2. Prof. Chen's work is supported in part by The National Fundamental Research 973 Program of China under Grant 2011CB302801 and Macau Science and Technology Development Fund grant number 008/2010/A1

REFERENCES

[1] Cisco Systems, Inc., "Internet protocol architecture for the smart grid," White Paper, Jul. 2009, available at:http://www.cisco.com/web/strategy/docs/energy/CISCO IP INTEROP STDS PPR TO NIST WP.pdf.
[2] U.S. DOE, "Smart grid system report," White Paper, Jul. 2009, available at:http://www.oe.energy.gov/SGSRMain 090707 lowres.pdf.
[3] U.S. NIST, "Guidelines for smart grid cyber security (vol. 1 to 3)," NIST IR-7628, Aug. 2010, available at: http://csrc.nist.gov/ publications/PubsNISTIRs.html#NIST-IR-7628.
[4] U.S. NIST, "NIST framework and roadmap for smart grid interoperability standards, release 1.0," NIST Special ublication 1108, Jan. 2010, available at: http://www.smartgrid.gov/standards/roadmap.
[5] U.S. NETL, "Advanced metering infrastructure," White Paper, Feb. 2008, available at: http://www.smartgrid.gov/white papers.
[6] U.S. NETL, "A systems view of the modern grid," White Paper, Jan. 2007, available at: http://www.smartgrid.gov/white papers.
[7] A. Clark and C.J. Pavlovski, "Wireless networks for the smart energy grid: application aware networks," in: Proc. International MultiConference of Engineers and Computer Scientists 2010 Vol II (IMECS 2010), Hong Kong, Mar. 2010.
[8] J. Gadze, "Control-aware wireless sensor network platform for the smart electric grid," IJCSNS International Journal of Computer Science and Network Security, vol. 9, no. 1, Jan. 2009, pp. 16-26.
[9] D. Dvian and H. Johal, "A smart grid for improving system reliability and asset utilization," CES/IEEE 5th International Power Electronics and Motion Control Conference, Shanghai, China, Aug. 2006, pp. 1-7.
[10] G.N. Srinivasa Prasanna, A. Lakshmi, S. Sumanth, V. Simha, J. Bapat, and G. Koomullil, "Data communication over the smart grid," in: IEEE International Symposium on Power Line Communications and Its Applications (ISPLC 2009), Dresden, 2009, pp. 273-279.
[11] H. A. Khan, Z. Xu, H. Iu, and V. Sreeram, "Review of technologies and implementation strategies in the area of smart grid," in: The 10th Postgraduate Electrical Engineering and Computing Symposium, IEEE WA Section, Perth, Australia, Oct. 2009.
[12] A. Cavoukian, J. Polonetsky, and C. Wolf, "SmartPrivacy for the smart grid: embedding privacy into the design of electricity conservation," Identity in the Information Society, Springer Netherlands, ISSN: 1876- 0678, Apr. 2010.

DOI: 10.17148/IJARCCE.2023.125228

[13] S. Spoonamore and R.L. Krutz, "Smart grid and cyber challenges - national security risks and concerns," March 2009, avaliable online: http://www.whitehouse.gov/files/documents/cyber/.

[14] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," IEEE Security and Privacy, vol. 7, no. 3, May/Jun. 2009, pp. 75-77.

[15] Idaho National Laboratory, "Common cyber security vulnerablilities observed in control system assessments by the INL NSTB program," Idaho National Laboratory Technical Report (INL/EXT-08-13979), Nov. 2008, available at: http://www.inl.gov/scada/publications.

[16] C. Wei, "A conceptual framework for smart grid," in: Power and Energy Engineering Conference (APPEEC 2010), Chengdu, China, Mar. 2010, pp. 1-4.

[17] A.R. Metke and R.L. Ekl, "Smart grid security technology," in: Innovative Smart Grid Technologies (ISGT 2010), Gaihersburg, MD, Jan. 2010, pp. 1-7.

[18] W.Y. Chu and Dennis J.H. Lin, "Communication strategies in enabling smart grid development," in: The 8th International Conference on Advances in Power System Control, Operation and Management (APSCOM 2009), Hong Kong, China, Nov. 2009, pp. 1-6.

[19] W. Shireen and S. Patel, "Plug-in hybrid electric vehicles in the smart grid environment," in: 2010 IEEE PES Transmission and Distribution Conference and Expositoin, New Orleans, LA, Apr. 2010, pp. 1-4.

[20] K. Moslehi and R. Kumar, "A reliability perspective of the smart grid," IEEE Trans. Smart Grid, vol. 1, no. 1, Jun. 2010, pp. 57-64.

