Journal Homepage: -www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI:10.21474/IJAR01/15959
DOI URL: http://dx.doi.org/10.21474/IJAR01/15959

RESEARCH ARTICLE

SECURITY ANALYSIS OF SMART GRIDS

Derya Betul UNSAL[1,2,3]

1. Assistant Professor, Graduate Institute of Natural and Applied Sciences, Department of Energy Science and Technology Engineering, Cumhuriyet University, Sivas, Türkiye.
2. Cumhuriyet University, Renewable Energy Research Center (CUYEM), Sivas, Türkiye.
3. Cumhuriyet University, Coordination of Sustainability Office, Sivas, Türkiye.

Manuscript Info

Manuscript History
Received: 30 October 2022
Final Accepted: 30 November 2022
Published: December 2022

Key words:-
Security, Cybersecurity, Smart Grids

Abstract

A kind of electricity networks in which various processes are carried out, energy measurements are made with smart meters and there are renewable energy sources and other efficient energy sources called Smart Grids. These grids are; consists of generation, transmission and distribution systems. For the smooth operation of it, the conditions of communication, flexibility of control system and smartness of distribution are required. Smart grids can be attacked simply by the penetration of voltage source converters. These attack types include caller ID attack, website, email, IPand, etc. Attacks occur when the attacker acts on behalf of another person or program by forging data. The attacker could be like another person, another computer, another device, etc. can behave like Smart grids have a communication network that spans large areas. Therefore, every component of smart grids can become active in attacks. Network traffic status should be regularly monitored to detect, recognize, control, and evaluate attacks. However, the network must also have the potential to heal itself in the face of attacks.

Introduction:-

There are numerous issues associated with the introduction of smart grids. These issues include power fluctuations, voltage imbalance, frequency mismatch, and transition management [1-2]. As a result of the unrestricted movement of renewable energy sources, power oscillations occur.

The source of voltage imbalance is excessive loads on minor voltage decreases. The intermittent, unpredictable imbalance between local generation and consumption is a concern for distribution networks. In order to integrate renewable energy into power grids, networks must be controlled with considerably greater care using smart grid technology [3].

Control will be effective if intelligent grids are observable, predictable, manageable, and flexible. Machine Learning (ML) is a technique for learning and predicting based on available data received by a computer system. In smart grids, it is the process of processing large amounts of data to obtain useful production information. Without the extraction of useful information, the obtained information has little to no value. In an IoT-based system, Machine Learning is entrusted with sifting through the massive amounts of data created. The smart grid system (SG), which

Corresponding Author:- Dr. Derya Betul Unsal
Address**:-** Assistant Professor, Graduate Institute of Natural and Applied Sciences, Department of Energy Science and Technology Engineering, Cumhuriyet University, Sivas, Türkiye.

is determined by the data gathering, analysis, and decision-making phases, is effectively terminated. With these stages, intelligent grids function as intended. It comprises of a variety of algorithms that analyze the given data based on a variety of instructions to generate predictions or judgments. Machine Learning; It detects network intruders at future phases of optimal scheduling, power generation, fault detection, adaptive control, sizing, consumption, cost, and data breach. Machine Learning can be implemented in software such as the power plant model validation tool (PPMV) and the free flight risk assessment tool (FRAT). In next generation energy systems, the ML prediction technique is mostly utilized in the renewable energy industry.

Cyber Security of Smart Grids:

Cyberattacks; management of power flow, voltage stability, and frequency regulation, etc. It can occur on sensors, load collectors, and smart meters in a mobile distribution network to decrease energy consumption. By limiting the flow of information, disconnecting connections, or altering communication metrics, channels can lead to the shutdown of a system via a variety of means.

Virtually every member of contemporary society uses the internet in all fields. It is now impossible to live without the internet, including for social media, banking, and health. With the expansion of the internet, attacks began occurring online rather than in the actual world. Cybersecurity is defined as a computer-based discipline that incorporates technology, people, data, and processes to protect operations from unwanted access or attacks. Cybercrime is described as a variety of crimes committed through the use of various forms of communication to instill fear in others, damage or destroy property [4]. Malware is used by cybercriminals to launch cyberattacks. Malware is executed on computers, smartphones, computer networks, and other electronic devices. Malware was originally created for simple objectives. Consequently, it was simpler to detect. Such software is classified as classical malware. Today, malicious software that is more destructive and potent than classic malware is known as malware of the new generation. This malware can readily circumvent security software and firewalls. Malware of the latest generation; they utilise many processes at once and employ a variety of tactics to conceal themselves and remain in the system. This malware contains detecting methods. Signature-based, behavior-based, heuristic-based, model-checking-based, deep learning-based, cloud-based, mobile device-based, and Internet of Things-based detection approaches [5].

Cyber Systems Vulnerabilies:

As a result of the inaccessibility of the utilities caused by cyber assaults, there may be a decline in demand. The smart grid network can enhance the existing electrical system, making it more secure and resistant to a variety of threats. Awareness of consumers; A complete and simple security mechanism for smart grids that contains all the necessary elements for identifying and tracking threats requires extensive study that cannot be attained by service alone. Due to the need for established aid, services, and safeguards, consumers must be properly informed of the risks, costs, and benefits of these assistance, services, and safeguards. Controlling a big number of computers necessitates a large number of access points. This is a really challenging task [6]. Smart Grids (SG) comprise of tools used to follow the necessity for an electrical network's flow. Such tools grant attackers broad access. Unknown and novel technology; because firewalls and their limitations are unknown, it contains numerous advancements that only attackers can see. Therefore, it is simple to identify ways around faults. Standards and regulations; It enables multiple smart grid systems to work together, share computers and data, and utilize compatible system components. To ensure interoperability, smart grid components are safeguarded by rules and standards. The implementation requirements of freshly made decisions also contribute to the lack of security. Teams; they work in many aspects of smart grids. Errors and a lack of collaboration between teams also lead to errors and gaps in computer security. IP hardware; software compatibility on the PC. It is however susceptible to cyber threats such as DoS (Denial-of-service) attack and FDI (False Data Injection).

Figure 1 depicts the division of SGs into generation, transmission, distribution, service providers, and consumers. According to several disciplines of study, power management and communication technologies should be able to tackle any difficulties that may arise in the SG [7].For an effective SG system, the functioning principles of all power electronics parts integrated into the network must be thoroughly analyzed [8]. Stable and efficient energy transmission to the end user is essential for the construction of a reliable network. If it is implemented, energy efficiency and the utilization of local renewable energy sources will grow, and the ideal grid system will be realized through the reduction of transmission losses [9].

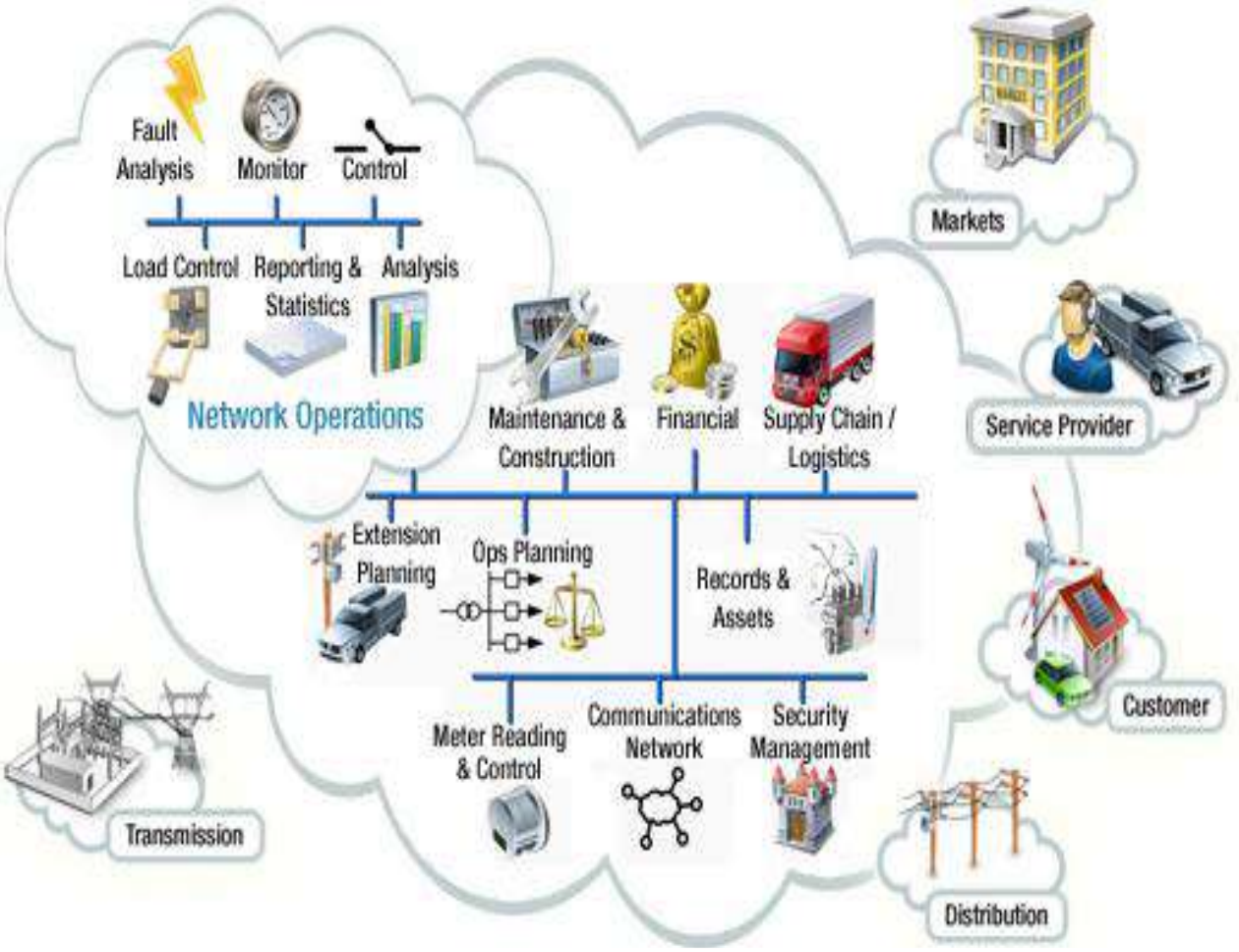

Fig. 1:- Smart Grid NIST model.

The use of Wifi, TCP, IP, and other operating systems by smart grids makes the infrastructure more susceptible to attack. Therefore, the infrastructure of smart grids must be risk- and attack-proof. The power grid plans and eliminates the defense against cyber attack threats.

Communication Vulnerabilities: in the Smart Grid The infrastructure data of smart grids is dependent on internet protocols with vulnerabilities that can be exploited to launch network-based assaults. TCP/IP is used to connect to the Internet for ordinary purposes and not to connect to control centers. Due to the misconfiguration of other networks, Internet networks are directly or indirectly linked to the smart grid. The ICCP protocol for data sharing between control centers includes security issues.

Smart Grid Software Vulnerabilities: Smart grids are vulnerable to assault because smart meters can be remotely upgraded. Attackers can individually dim the counters or control them from the command center. Software defects can be used to exploit these vulnerabilities. If network components are accessible, they may serve as an entry point for an attacker.

Smart Grid Vulnerabilities for Privacy: The two-way connection between smart meters put in consumers' houses and electricity companies creates these vulnerabilities.

Smart Grid Physical Weaknesses: In smart grids, it is impossible to offer physical safety for physical assets. Installing smart meters in houses, buildings, and distant regions makes them vulnerable to multiple physical attacks. Therefore, detection approaches using inhibitory solutions must be developed.

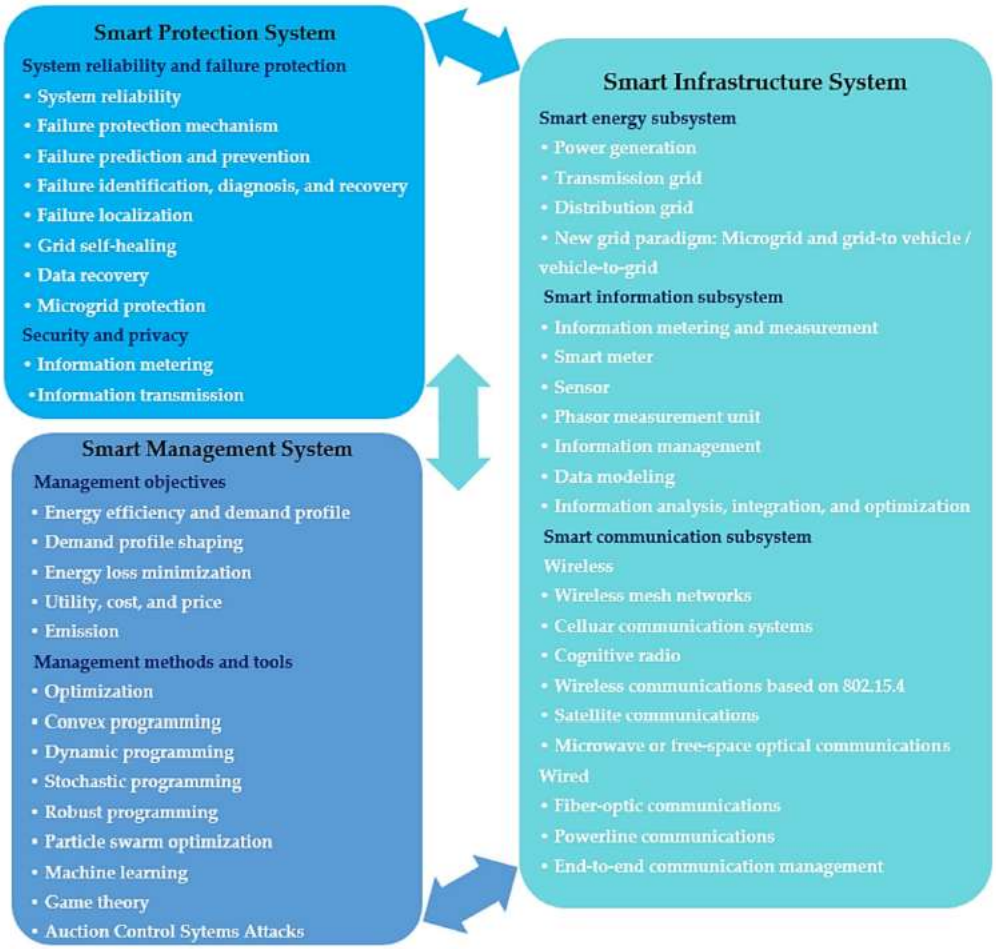

Fig.2:- SG Cyber-Security Basic Infrastructure.

Figure 2 illustrates the security relationship of SGs[10].As indicated in Figure 2, cybersecurity can be categorized into three distinct systems. Listed under smart infrastructure system are intelligent energy, information, and communication systems. They must work in conjunction with İntelligent management system and protection system assist. Existing cybersecurity solutions struggle to satisfy the requirements of SG communication systems. This study examining, it is clear that traditional cybersecurity approaches and algorithms have been researched, and that there are separate studies on cyber risk power and communication.

Solutions for important vulnerabilies:

Malware, False Data Injection Attack, DDoS and DoS, Phishing, SQL Injection, Man in the Middle, Cryptojacking, Zero Day Exploit, Passwords Attack, Eavesdropping Attack, Supply Chain Attack, Ransomware, Credential Stuffing, Internet of Things, and Cross-Site Scripting are the most common forms of cyber attacks. This paper examines the most prevalent of these threats, including DoS Attacks and False Data Injection Attacks. A. DoS Attacks DoS attacks are service denial attacks. It is a perilous form of attack that allows the attacker to seize control of the availability of services. DoS can seize control of numerous infected systems, such as Internet Control Message Protocol (ICMP), and bring about system failure [9]. Important resources belonging to registered users can be obtained with these assaults.

DoS attacks target electronic systems and protocols, effectively stopping all communication routes. A DoS attack can cause the communication network to become overloaded, limiting user access. With DDoS attacks, the attacks are pre-planned. DoS attacks can eliminate communication in intelligent networks [10]. A distributed denial of service (DDoS) attack occurs when the attacker has access to multiple network channels and is constantly prepared

to launch an assault against another system. In distributed DoS (DDoS) attacks, a system is simultaneously attacked by multiple computers. DDoS assaults can be carried out in numerous ways.

Volumetric DDoS:
The goal of volume-based DDoS assaults is to overwhelm entire data centers with traffic. These DDoS attacks eat the bandwidth of the entire data center's networks. Some of these attacks are Internet Control Message Protocol (ICMP) flood, User Datagram Protocol (UDP) flood, IP/ICMP Fragmentation, and IPsec flood.

Protocol DDoS:
Protocol DDoS attacks take use of all protocol weaknesses. These vulnerabilities are challenging to locate and replace, and the process takes time. Application Layer Distributed Denial of Service: Also known as Layer 7 (L7) DDoS assaults. It is a sort of attack designed to penetrate the top layer of major Internet networks, such as HTTP GET. Additionally, it harms servers in comparison to other network layers.

In malicious injection attacks (FDIA), the attacker can tamper with the network operator's state prediction procedures and deceive them. It can also be regarded the deadliest cyber attack due to the fact that it leads to progressively poor decision making throughout smart grid networks and therefore to significant cyber attacks. Depending on the intruder's goal, the FDIA can have a variety of comparable effects, including energy theft and network devastation [11].

Physically Based FDIA:
Typically, these assaults are designed to monitor control and security devices. By modifying the firmware of any processor-based device, FDIA can be implemented. There are a limited number of such vulnerable gadgets.

Cyber-Based FDIA:
These are attacks in which the adversary gains access to the control system and its vital applications. Their mission is to make the system functional and useful.

Conclusion and Suggestions:-

For Ddos Vulnerabilites:
DoS attacks target the sum of the data sent to the system, not the system's primary data. Such assaults can be prevented without collateral damage by implementing measures such as bolstering data verification, addressing the various services of network resources, enhancing network infrastructures, and conducting routine network monitoring. Authentication and encryption mechanisms are also among the available alternatives. However, certain techniques employed to block these assaults may degrade service quality or even create an attack vector. This requires a successful installation of the mechanism.

For FDIA Preventative Measures:
In these methods, load calculation is crucial. Regular research must be conducted to improve algorithm precision and computational speed in order to reduce energy consumption, lower computational costs, and improve the algorithm's performance.

Avoid Authentication: This approach has been effective for preventing FDIA. However, its ability to thwart DoS assaults has not been demonstrated [12]. This is due to data congestion.

Public Key Cryptography: This is an additional way for detecting cyber assaults in smart power systems. Such techniques may be realizable with the integration of smart meters and smart inverters with ICT elements. ways of encryption for the FDIA; Rivest-Shamir-Adleman (RSA), Elliptic Curve Encryption (ECC), public key encryption, and data authentication encryption [13] are some of its common names. To identify the private key, a code with a known, robust decryption algorithm and error correction mechanism is selected. The name of this system is the McEliece System.

Trust-Based Strategies: Trust value mechanism is an additional preventative approach for smart grids. Using a model that measures the level of trust, this strategy identifies malicious nodes. [14] This is the Hash algorithm. Once the rogue node has been located, the administration center is notified and it is destroyed. When a sensor node is assigned to a new group, the trust value is transmitted back to the administration center. Consequently, the

confidence value is taken as the starting confidence value of the cluster's nodes. This method is an FDIA prevention strategy.

Despite the fact that numerous solutions are proposed for FDIA and DDOS assaults, when the working stages of cyber security are applied in smart networks, cyber attacks will not occur, and smart networks will be protected from cyber attacks. When the security flaws in cyber attacks are considered and worked on, unique solutions must be developed for each security vulnerability. With these security measures, cyber attacks on intelligent networks are averted and the systems function properly. When the forms of cyber attacks are analyzed in depth, these attack types are well-known and early detection enables the implementation of preventative measures.

References:-

[1] M.Amin, F.F.M. El-Sousy, G.A.A.Aziz, K.Gaber and O.A.Mohammed, ‘‘CPS Attacks Mitigation Approaches on Power Electronic Systems With Security Challenges for Smart Grid Applications: A Review’’ IEEE, vol. 9, March 2021.
[2] R.Khan, N.Islam, S.K.Das, S.M.Muyeen, S.I.Moyeen, MD.F.Ali, Z.Tasneem, MD.R.Islam, D.K.Saha, MD.F.R.Badal, H.Ahamed and K.Techato, ‘‘Energy Sustainability–Survey on Technology and Control of Microgrid, Smart Grid and Virtual Power Plant’’ IEEE, vol. 9, August 2021.
[3] H.A.H.Hassan, A.Pelov and L.Nuaymi, ‘‘Integrating Cellular Networks, Smart Grid, and Renewable Energy: Analysis, Architecture and Challenges’’ IEEE, vol. 3, December 2015.
[4] W.A.Al-Khater, S.Al-Maadeed, A.A.Ahmed, A.S.Sadıq and M.K.Khan, ‘‘Comprehensive Review of Cybercrime Detection Techniques’’ IEEE, vol. 8, August 2020.
[5] B.X.Yu and Y.Xue, ‘‘Smart Grids: A Cyber–Physical Systems Perspective’’ IEEE, vol. 104, no. 5, May.2016.
[6] H.A.H.Hassan, A.Pelov and L.Nuaymi, ‘‘Integrating Cellular Networks, Smart Grid, and Renewable Energy: Analysis, Architecture, and Challenges’’ IEEE, vol. 3, December 2015.
[7] N.Javaid, G.Hafeez, S.Iqbal, N.Alrajeh, M.S.Alabed and M.Guizani, ‘‘Energy Efficient Integration of Renewable Energy Sources in the Smart Grid for Demand Side Management’’ IEEE, vol. 6, December 2018.
[8] N.D.Tuyen, N.S.Quan, V.B.Linh, V.V.Tuyen and G.Fujita, ‘‘A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy’’ IEEE, vol. 10, April 2022.
[9] Z.Wang, L.Li, H.Sun, C.Zhu and X.Xu, ‘‘Dynamic Output Feedback Control of Cyber-Physical Systems Under DoS Attacks’’ IEEE, vol. 7, December 2019.
[10] Unsal, D.B.; Ustun, T.S.;Hussain, S.M.S.; Onen, A. EnhancingCybersecurity in Smart Grids: FalseData Injection and Its Mitigation.Energies 2021, 14, 2657. https://doi.org/10.3390/en14092657.
[11] A. Kovacevic, N. Putnik and O. Toskovic, ‘‘Factors Related to Cyber Security Behavior’’ IEEE, vol. 8, July 2020.
[12] M.I.Oozer and S.Haykin, ‘‘Cognitive Dynamic System for Control and Cyber-Attack Detection in Smart Grid’’ IEEE, vol. 7, June 2019.
[13] M.E.Kantarcı and H.T.Mouftah, ‘‘Energy-Efficient Information and Communication Infrastructures in the Smart Grid: A Survey on Interactions and Open Issues’’ IEEE, 2015.
[14] O. Aslan and R.Samet, ‘‘A Comprehensive Review on Malware Detection Approaches’’ IEEE, vol. 8, Jan. 2020.