Pakistan Journal of Engineering and Technology
ISSN (Print): 2664-2042; ISSN (Online): 2664-2050
Received: 2024-11-03
Accepted: 2024-12-20
https://doi.org/10.51846/vol7iss4pp151-158

PAKJET
Pakistan Journal of Engineering & Technology

Review

Cybersecurity for Smart Inverters: State-of-the-Art Review

Muhammad Irfan Habib

Department of Electrical Engineering Technology, National Skills University Islamabad, Islamabad 44310, Pakistan
Correspondence: Muhammad Irfan Habib (irfan.habib@nsu.edu.pk)

Abstract: As renewable energy sources such as solar panels and wind turbines become more common, smart inverters are being deployed in power grids. Inverters are required to convert direct current (DC), produced from solar panels or wind turbines, into alternating current (AC) so that they can be fed into the grid. However, smart technology is also associated with significant cybersecurity flaws that can undermine the integrity and reliability of energy systems. This study reviews the current state of the security of smart inverters. They have unique architectures that make their cybersecurity a difficult challenge. Smart inverters use many communication protocols. The unauthorized entry, malware threats, and data breaches will be discussed regarding their ramifications on grid stability and security. The study stresses the necessity of cyber-attack protective measures such as intrusion detection systems, data encoding, and continuous monitoring. SMART inverters protect measures. It also covers the importance of compliance requirements and the need for cybersecurity training for staff involved in the operations of these systems. This review aims to guide the stakeholders of the energy sector to enhance the cybersecurity of smart inverters through the synthesis of the recent research and the practices followed at the industry level.

Keywords:
Cybersecurity, Power Grid Security, Renewable Energy, Smart Inverters

1. Introduction

The distribution of electrical energy is getting revolutionized with the adoption of renewable energy sources and, in particular, photovoltaic solar energy and wind energy. The transition to digitalization has necessitated the use of smart technology for effective management of electrical systems. Effective smart inverters are an essential part of this transformation. Smart inverters are devices that convert direct current (DC) from a photovoltaic panel or wind generator to alternating current (AC) supplied in the electrical grid. Smart inverters can do a lot more than just convert and transfer energy to the grid by adjusting the frequency of the energy generated to match that of the grid. These allow the grid to support other grid components, continue monitoring grid performance, and interact with other grid components and structures, which improves the efficiency of the grid overall [1].

Advanced inverters that are integrated with distributed energy resources (DERs) in the power grid are intended to enhance the security and dependability of the grid, as shown in Fig. 1. The main functions of these inverters include voltage regulation, frequency support, and reactive power control, which guarantee power quality and a reliable electricity supply for steady integration of DERs. Modern power systems are becoming increasingly complex as they manage large amounts of data and communicate with the control systems on the grid as utilities and new challenges arise. Although this complexity offers many benefits, the cybersecurity risks associated with it should not be overlooked. Smart inverters are connected to the grid and perform tasks that can give rise to new security vulnerabilities [2]. In the same context, a study has been conducted by [3] on the challenges and opportunities of Industrial Revolution 4.0 in the renewable energy sector of Pakistan and stated that renewable energy is shifting away from conventional power and giving rise to the energy crisis and the greening of energy. The Industrial Revolution 4.0 enable renewable energy integration by smart grid and IoT-based stability of the system. Even without certainty, these technologies do make generating power easier and more reliable. Another study by [4] stated that the management of the surplus energy created by renewable hybrid systems is developed using smart contracts and a private blockchain. It also proposes a cluster communication architecture for improved DG performance and evaluates the system's efficiencies in various scenarios.

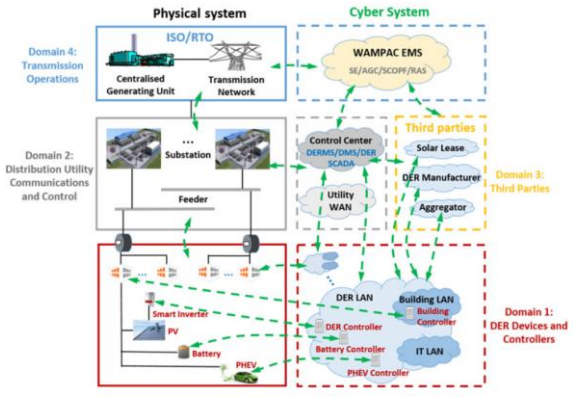

Figure 1. Proposed DER architecture [2].

2. Cybersecurity Challenges

The growing occurrence of cyberattacks is a cause of alarm for the security of advanced inverters and, subsequently, the power grid. As smart inverters are interlinked more with grids and communications with another grid, the possibility of malicious behavior increases along with vulnerability. Attacks on smart inverters can cause total power blackouts and grid failures, with dire consequences. Also, the attack can damage infrastructure-related activities that further affect the reliability and stability of the power grid [5].

2.1. Increased Attack Surface

Smart inverters have communication interfaces for communication between inverters and also between inverters and power grids. Though this connection is required for efficient management of the grid, it also creates more gaps, thus creating new cyber threat opportunities. People who hack computers, smartphones and other devices may try to take control of the inverter remotely. This can create problems in the grid using the inverter. The fact that smart inverters are generally complex devices, often employing multiple techniques and protocols, complicates security. This complication makes them more challenging to protect as now there are more attack surfaces that need protection [6].

2.2. Complexity of Systems

The incorporation of hardware, firmware, and communication protocols into one device, such as a smart inverter, makes it complicated. Implementing and managing all the security measures on every component is so complicated that the active participation of so many people becomes imperative. Moreover, a flaw in one section of the system may affect the whole gadget. As technology is getting upgraded too soon, at times security cannot be applied to the system. Due to this, the system is more vulnerable. This dynamic creates strong challenges for robust and full protection against threats [7].

2.3. Resource Constraints

Smart inverters can't provide strong security because of their limited computation and memory capacities, like advanced encryption and IDS (intrusion detection systems). Due to their lack of resources, they are easier to attack than more powerful ones. The smart inverter's limited capacity to accommodate extensive security features makes it easy prey for malicious actors and, therefore, vulnerable to a security breach that can disturb the grid [8].

3. Potential Cyber Threats

Smart inverters can face many cyber threats; each cyber threat can pose a direct risk of power instability and safety hazards. Recognizing these threats can enable the development of more effective strategies to prevent their occurrence. By identifying the probable weaknesses and various types of attacks, targeted measures and protection can be developed to ensure smart inverter reliability and, more importantly, the reliability of the power system as a whole. Updating software regularly and working on protective measures is useful to minimize threats.

3.1. Malware and Ransomware

Inverters can be attacked by malware, such as ransomware, which can cripple or destroy their operations. If ransomware attacks occur and lock the inverter systems, they would become unusable. Cybercriminals may request substantial monetary contributions or other support before granting access again. These demands can be so significant that they result in a cease-and-desist order. When the power grid is not reliable, it can lead to substantial losses in utility revenue and expenses to deal with the attack [5].

3.2. Unauthorized Access

Changing the smart inverter settings gives unauthorized access to the attackers which can hurt the grid stability and performance. When someone uses a generator or load without permission, it can cause faults such as normal frequency deviation, voltage imbalance and more. To make sure no such attacks happen, strong authentication and access controls must be implemented in order for unauthorized individuals and systems to change inverter settings. These protections help to maintain the quality of the electrical grid while preventing it from being targeted [9]. Fig. 2 shows the role of a typical smart inverter, and Fig. 3 shows functional elements of a Smart Inverter.

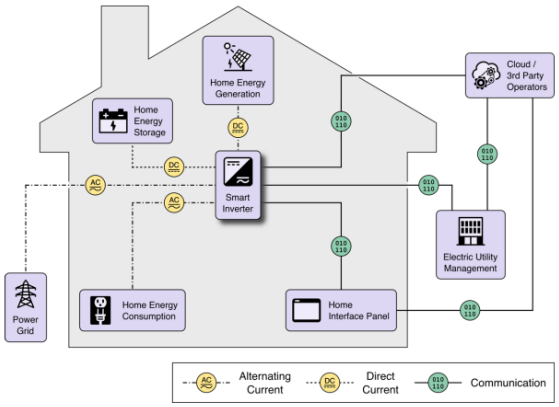

Figure 2. The role of a typical smart inverter [9].

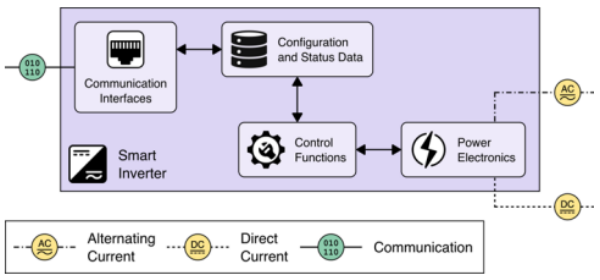

Figure 3. Functional elements of a smart inverter [9].

3.3. Data Breaches

The smart inverters gather and send a lot of data, such as how they operate and how well they perform, as illustrated in Fig. 4. If this data gets into the wrong hands, it can lead to breaches of privacy and malicious users taking advantage of vulnerable systems. It is essential to use encryption and secure channels to protect this information and prevent its hacking, as authentication details can prove to be risky [10].

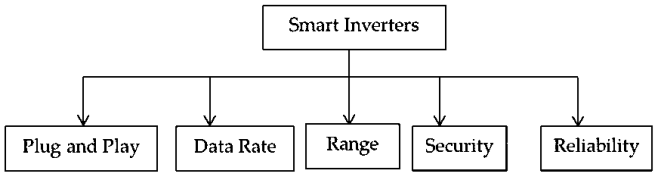

Figure 4. Features of a smart inverter [10].

3.4. Denial of Service (DoS) Attacks

Smart inverter communication channels can be hacked by Denial of Service (DoS) attacks that can flood these channels, preventing the sending or receiving of important information. When that happens, that can severely impact the normal operation of the grid, leading to outages and performance degradation. To reduce these types of risks, firewalls and encryption as well as infrastructure detection systems (IDS), need to be put into place. A power grid's communication channel must ensure that it does not allow malicious activities that may threaten the power grid's integrity, condition, and reliability [11]. In Fig. 5, an impact of Distributed Denial of Service (DDoS) attacks on the communication infrastructure of smart grids or microgrids can be seen as well as Fig. 6 shows a loss of connectivity between the primary and secondary control layers due to a DDoS attack.

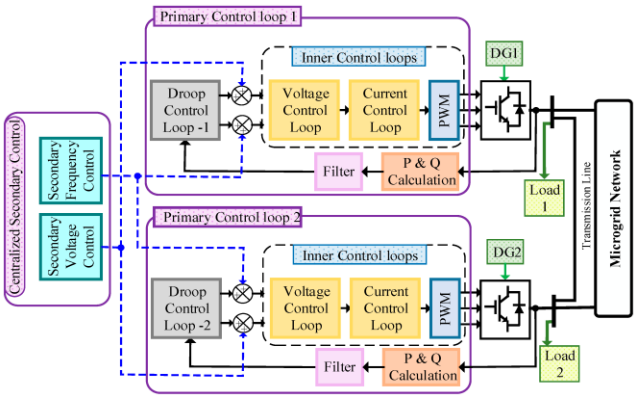

Figure 5. Impact of distributed denial of Service (DDoS) attacks on the communication infrastructure of smart grids or microgrids [11].

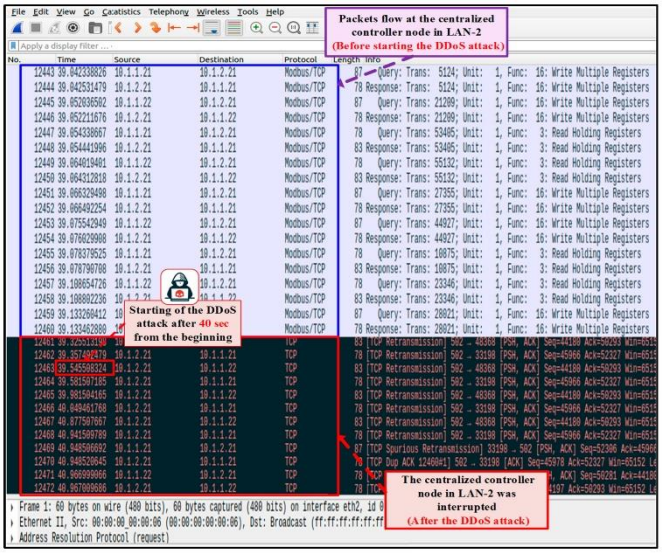

Figure 6. Loss of connectivity between the primary and secondary control layers due to a DDoS attack [11].

4. Existing Cybersecurity Measures

According to the increased cyber-attack threat against smart inverters, various methods of dealing with the same have been proposed and implemented to secure the inverter and enhance reliability in the power system. These are encryption of data, authentication, and secure communication of devices. Apart from that, intrusion detection systems (IDS) and regular updates detect and address gaps on a real-time basis. The smart inverter's security and resilience will increase based on these strategies and secure operation smart grid stability will be further ensured with the safe operation of smart inverters.

4.1. Authentication Mechanisms

Securing smart inverters properly is important to prevent unauthorized access to the power grid. Using multi-factor authentication helps to secure the authentication process. The safest approach for credential management is a process. However, policies like storing credentials that should be kept secret in encrypted form are good practices. Changing passwords and credentials regularly further reduces the risk of unauthorized access because even if the passwords or credentials have been hacked, they will not be secure. The above measures work together to fortify cyber threat defense [12] [13]. An illustration of the working of multifactor authentication is shown in Fig. 7. Also, Fig. 8 shows the flowchart of the self-security algorithm for smart inverters.

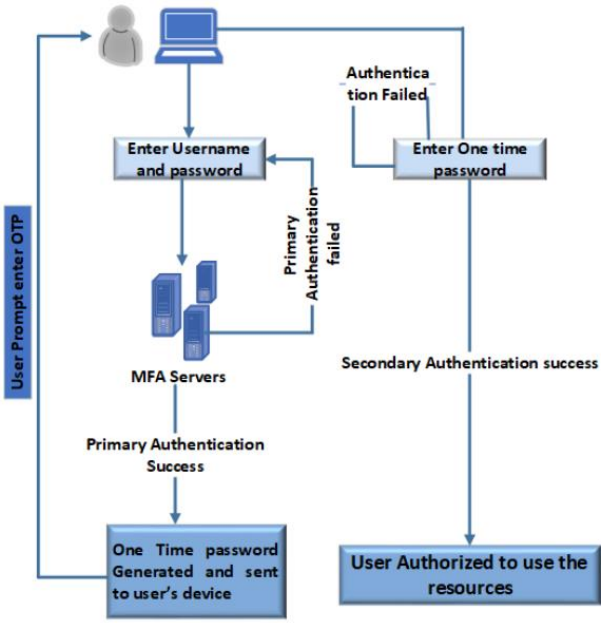

Figure 7. Working of multifactor authentication [12].

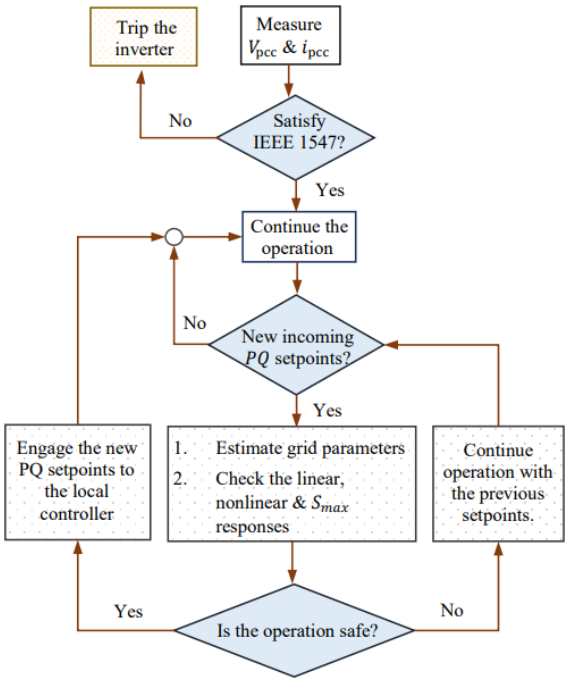

Figure 8. Flowchart of the self-security algorithm for smart inverters [13].

4.2. Software Updates and Patching

Smart inverter firmware and software need to be regularly upgraded and patched to fix existing vulnerabilities. Keeping the firmware and software updated can rectify known weaknesses that would otherwise be taken advantage of by hackers. Using automated processes to update an update optimizes the entire patching process and applying the security fix. By continuously strengthening the ability of smart inverters and keeping them resilient, the proposed method minimizes the chance of a successful attack due to the emergence of new weaknesses [14]. An illustration of a smart inverter firmware attack surface in a PV system has been shown in Fig. 9 and an experimental setup has been shown in Fig. 10.

The experimental setup environment makes sure that the smart inverter's firmware and software are patched and upgraded regularly to mitigate existing vulnerabilities. The current firmware and software versions are reviewed to determine the baseline of the evaluation. The On-Board Security Module (OSM) configures an automated way to update that checks for file changes, detects updates, and checks firmware integrity through static malware analysis and hash verification using software like PeStudio or custom Python code. Following the deployment of a security patch that fixes vulnerabilities, the automated update process begins, and the firmware is validated before being applied. To test the validity of the update, a mock cyber-attack is executed on the outdated firmware and then resilience tests are done on the update. The blockchain server checks whether issues causing the system to become faulty are resolved and whether its security status is normal. The OSM continuously monitors smart inverters at all times to ensure their resilience and protect them from evolving vulnerabilities to maximize the chances of a non-successful cyber-attack.

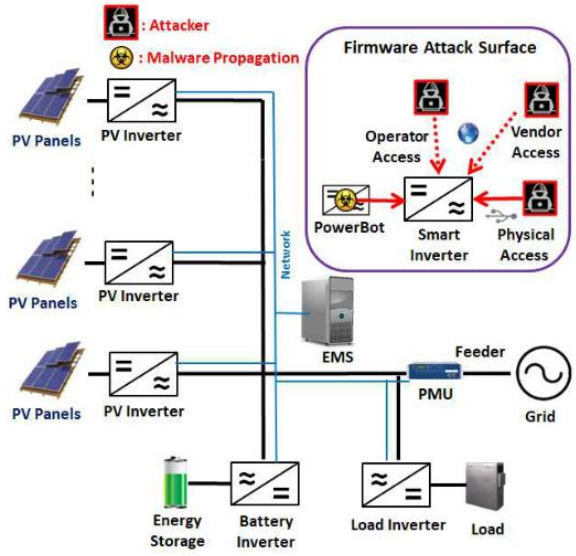

Figure 9. Smart inverter firmware attack surface in a PV system [14].

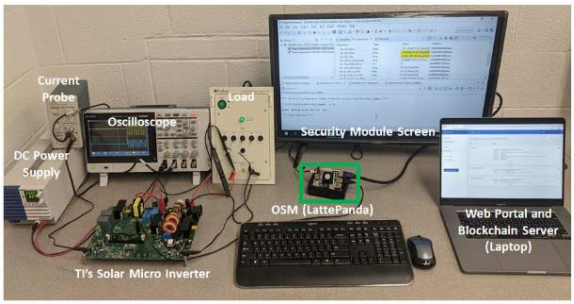

Figure 10. Experimental setup [14].

4.3. Network Segmentation

Network segmentation can be used to prevent smart inverters and other key assets from interacting with other parts of the network. This method allows the utility to confine the attack in a certain location of the energy grid and not let it spread to other points. Network segmentation boosts security by enabling easier monitoring and detection of suspicious activities. Since network segments are smaller, they can be easier to monitor. This makes it easier to spot threats on the electrical grid so the person in charge can respond in a more targeted and effective manner [15].

4.4. Data Encryption

When smart inverters pass any data, it should be encrypted to avoid data interception or access. End-to-end encryption means that even if data is captured, it is unreadable and unaltered unless the decryption key is available. This type of encryption protects the communication channel and stored messages from an attacker. To have strong security, only use end-to-end encryption for all transmission and storage of data [16]. The techniques for defending against various attacks on DER trust, including the use of encryption to ensure data integrity, client authentication, and data privacy, have been shown in Fig. 11.

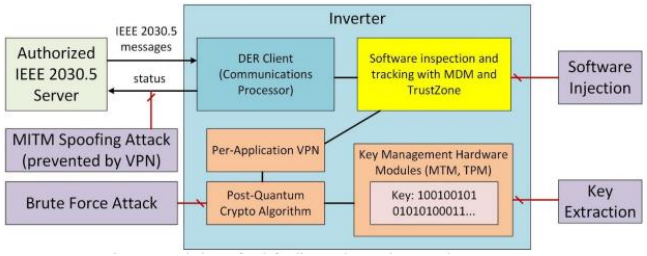

Figure 11. Techniques for defending against various attacks on DER trust, including the use of encryption to ensure data integrity, client authentication, and data privacy [16].

4.5. Intrusion Detection Systems (IDS)

In real-time, an Intrusion Detection System (IDS) aids in the identification of and response to threats on digital channels. Monitoring network traffic and examining patterns for suspicious activity or strange requests allows an IDS to quickly discover anomalies that could highlight a breach. Integrating IDS into smart inverters increases their capacity to detect and defend against attacks to further secure the overall system. This early recognition will aid in preventing any occurrence of blackouts or attacks on the power grid [17].

4.6. Cybersecurity Training

Utility staff must be educated on cybersecurity best practices to help lessen the chances of a security breach due to human error. Training programs should address various topics like how to spot phishing attempts, dealing with sensitive information safely, and what procedures to follow if a security incident occurs. If utility companies train their staff to recognize possible cybersecurity attacks and how to properly respond, then it can strengthen the vulnerabilities and possibly create a stronger power grid that is more secure [18].

5. Best Practices for Enhancing Cybersecurity

Smart inverters will have improved cybersecurity if best practices and industry standards are adopted. When utilities follow these established guidelines, they can take a more integrated and proactive approach to security. Use resources, including strong encryption, regular updates, user-access control, intrusion detection systems, network segmentation, and more security tools. Following standard practices helps smart inverters protect themselves against future threats. This supports ensuring the integrity of the power grid and a secure, reliable energy supply.

5.1. Holistic Security Approach

A resilient, holistic approach to security involving technology, organizational processes and human resources is essential for the security of critical assets. This means protecting the security of information through the use of technical solutions, primarily encryption, firewalls and intrusion detection systems, as well as behavior through measures that make the policies clear. Moreover, all staff of the organization must be educated and trained in regard to cybersecurity. The preparedness of the employees to handle cyber-attacks is vital. By incorporating these components, organizations can build a strong security framework that takes care of both technical and human factors [19].

5.2. Collaboration and Information Sharing

In order to tackle shared threats and vulnerabilities, universities, government agencies, and cybersecurity experts must unite. Working together and sharing information can help unearth new threats and solutions against them. By taking part in forums, intelligence networks, and cross-sector initiatives, they can pool expertise to reinforce defences and strengthen overall cybersecurity posture. Working together or collaborating helps to respond to existing threats or dangers. Also, it helps to predict future threats or risks, contributing to smart inverter systems and the power grid [2].

5.3. Regulatory Compliance

Ensuring an essential security standard for smart inverters requires operable requirements and standards from the industry. Adhering to developed standards, such as the IEEE's smart grid cybersecurity guidelines and the ISO/IEC 27001 framework for information security, vulnerability reduction is expected. The standards apply structured management and mitigating processes to the cybersecurity risks of the smart inverter. Furthermore, it also covers that the smart inverters will withstand cybersecurity threats. Organizations can improve the security of their smart grid systems with the help of such top frameworks that are recognized globally [20].

5.4. Continuous Monitoring and Improvement

Frequent security tests are important to keep up with evolving threats. Smart inverters must be continuously monitored and

regularly evaluated for security vulnerabilities and weaknesses. This ensures any security flaws are dealt with quickly to keep the system stable going forward. By carrying out regular security evaluations, utilities can adjust to changing new threats and enhance their defences to protect smart inverter infrastructure over a long period [21].

6. Discussion

In the digital world of today, organizations face many cyber threats that can compromise data and disrupt operations. To counter these threats effectively, a range of mitigation technologies has been developed. Intrusion Detection Systems (IDs), encryption, and network segmentation are three examples. This piece provides more information on these measures, including technical details and case studies, in relation to the analysis.

6.1. Intrusion Detection Systems (IDS)

6.1.1. Technical Details

Intrusion Detection Systems are important parts of cybersecurity plans. By monitoring network traffic, intrusion detection systems (IDS) generate alerts when suspicious activities are detected. There are two general types of IDS.

- Network-based IDS (NIDS): Monitors traffic across the entire network.
- Host-based IDS (HIDS): Monitors individual devices for suspicious activity [22].

6.1.2. Case Study

A good example of IDS effectiveness is in ICS (Industrial Control Systems). In a ransomware attack against ICS, it was seen that the organization uses an IDS to detect an unusual pattern due to an ongoing attack that happens. So, the organization quickly takes measures to stop any possible damage [23]. This shows how important IDS are for maintaining the integrity of operations.

6.2. Encryption

6.2.1. Technical Details

Encryption is an essential method of securing data by scrambling it so that only those with the proper knowledge, such as a password or key. Types of encryptions are:

- Symmetric Encryption: Uses the same key for both encryption and decryption.
- Asymmetric Encryption: Utilizes a pair of keys (public and private) for secure data exchange.

6.2.2. Case Study

The 2020 SolarWinds hack employed encryption to exploit vulnerabilities. Organizations that use strong encryption techniques manage to protect their data from being harmed in the data breach incident. This shows that encryption can help stop data theft from happening.

6.3. Network Segmentation

6.3.1. Technical Details

Network segmentation is the process of dividing a computer network into smaller parts. When an organization separates sensitive data and other computer systems, it reduces the lateral movement of attackers. Key strategies include:

- VLANs (Virtual Local Area Networks): Create distinct broadcast domains within the same physical network.
- Firewalls: Control traffic between segments based on predefined security policies.

6.3.2. Case Study

The ransomware attack on the Colonial Pipeline highlighted the need for network segmentation. Investigations found that attackers spread into systems by moving from IT to operational technology because of poor segmentation on networks. Implementing better segmentation may have limited the impact of attack [23-25]. This case shows how to use strategic network design to strengthen cyber resilience.

The landscape of threats is evolving and necessitates cybersecurity risk mitigation. Using IDS, applying encryption, and segmenting networks are some of the ways that can increase the security of an organization. Real-world case studies emphasize the significance of these measures, showcasing their power to prevent or mitigate cyber incidents' impact. Organizations need to regularly assess and modify cybersecurity strategies per the changes in the threat.

Table 1. Contributions of various authors to different sections.

Contribution	Authors	Year
Introduction	[1]	2021
Cybersecurity Challenges	[2]	2016
Cybersecurity Challenges	[3]	2021
Cybersecurity Challenges	[4]	2021
Malware and Ransomware	[5]	2024
Unauthorized Access	[6]	2022
Data Breaches	[7]	2024
Denial of Service (DoS) Attacks	[8]	2023
Intrusion Detection Systems	[9]	2024
Software Updates and Patching	[10]	2021
Data Encryption	[11]	2024
Network Segmentation	[12]	2021
Cybersecurity Training	[13]	2021
Holistic Security Approach	[14]	2021
Collaboration and Information Sharing	[15]	2023
Regulatory Compliance	[16]	2019
Continuous Monitoring	[17]	2021
Cybersecurity Challenges	[18]	2023
Best Practices for Enhancing Cybersecurity	[19]	2023
Best Practices for Enhancing Cybersecurity	[20]	2020
Best Practices for Enhancing Cybersecurity	[21]	2019
Intrusion Detection Systems	[22]	2007
Encryption	[23]	2024
Network Segmentation	[24]	2024

A summary of the author's contributions to various sections of the review article is presented in Table 1. The effect of advanced inverter functions, cybersecurity issues in distributed energy systems and the integration of smart grids with blockchain technology are among the topics covered in the contributions. The table also describes important cybersecurity threats like malware, ransomware, unauthorized access and data breaches. Additionally, it highlights some measures and best practices to address these solutions, which may include encryption, intrusion detection systems, and segmentation. A summary of discussions and findings on the cybersecurity of smart inverters and the reliability and stability of the power grid.

7. Conclusion

The study shows the need for enhanced security, and the threat of cyber-attacks is evolving continuously. With a greater emphasis on renewable energy, smart inverters are required not just to convert electricity but to help the grid to function properly. Dealing with these systems is extremely critical, comprising diverse technologies and protocols, and they often pose specific challenges requiring creative risk solutions.

The finding that comes from the study suggests areas for improvement. To prevent unauthorized access and data breaches, an advanced cybersecurity framework needs to be used, which includes an intrusion detection system and strong encryption. Assessing security regularly and monitoring them continuously is another way of adapting to new emerging threats. In addition to this, a culture of cybersecurity training for personnel can further strengthen the security of renewable energy management organizations.

It is critical to work with all stakeholders, such as manufacturers, regulators, and energy suppliers, to set up cybersecurity standards/best practices. Emphasizing cybersecurity in smart inverter design and operation of the energy sector will not only protect the overall infrastructure but also begin to form a level of trust amongst the general public in renewable energy. To ensure the sustainable development of renewable energy technologies and the security of their integration within the interconnected grid, cybersecurity needs to be built in proactively.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

[1] A. Mentens, H. R. Chamorro, V. A. Jacobs, D. Topolánek, J. Drápela, and W. Martinez, "Impact of advanced inverter functions on low-voltage power grids," *IET Energy Systems Integration,* vol. 3, no. 4, pp. 426-436, 2021.

[2] 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, no. 1, pp. 28-39, 2016.

[3] M. Hamza and A. M. Khan, "Challenges and opportunities of industrial revolution 4.0 in renewable energy sector of Pakistan: case study," *Pakistan Journal of Engineering and Technology,* vol. 4, no. 2, pp. 32-37, 2021.

[4] R. F. Ahmad, M. Siddique, K. Riaz, M. M. Hussain, and M. Bhatti, "Blockchain based secure energy trading mechanism for smart grid," *Pakistan Journal of Engineering and Technology,* vol. 4, no. 2, pp. 100-107, 2021.

[5] H. N. N. Naiho, O. Layode, G. S. Adeleke, E. O. Udeh, and T. T. Labake, "Addressing cybersecurity challenges in smart grid technologies: Implications for sustainable energy infrastructure," *Engineering Science & Technology Journal,* vol. 5, no. 6, pp. 1995-2015, 2024.

[6] N. D. Tuyen, N. S. Quan, V. B. Linh, V. Van Tuyen, and G. Fujita, "A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy," *IEEE Access,* vol. 10, pp. 35846-35875, 2022.

[7] S. Karumba, S. C.-K. Chau, H. Pearce, M. Ahmed, and H. Janicke, "Systematic Study of Cybersecurity Threats for Smart Inverters," in *Proceedings of the 15th ACM International Conference on Future and Sustainable Energy Systems*, 2024, pp. 669-675.

[8] A.-A. Bouramdane, "Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process," *Journal of Cybersecurity and Privacy,* vol. 3, no. 4, pp. 662-705, 2023.

[9] J. McCarthy, J. Marron, D. Faatz, D. Rebori-Carretero, J. Wiltberger, and N. Urlaub, "Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems," National Institute of Standards and Technology, 2024.

[10] M. K. Srinivasan, "Technological Perspective of Cyber Secure Smart Inverters Used in Power Distribution System: State of the Art Review," 2021.

[11] O. Ali, T.-L. Nguyen, and O. A. Mohammed, "Assessment of Cyber-Physical Inverter-Based Microgrid Control Performance under Communication Delay and Cyber-Attacks," *Applied Sciences,* vol. 14, no. 3, p. 997, 2024.

[12] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid," *Energies,* vol. 14, no. 18, p. 5894, 2021.

[13] M. Gursoy and B. Mirafzal, "Self-security for grid-interactive smart inverters using steady-state reference model," in *2021 IEEE 22nd Workshop on Control and Modelling of Power Electronics (COMPEL)*, 2021: IEEE, pp. 1-5.

[14] B. Ahn, G. Bere, S. Ahmad, J. Choi, T. Kim, and S.-w. Park, "Blockchain-enabled security module for transforming conventional inverters toward firmware security-enhanced smart inverters," in *2021 IEEE Energy Conversion Congress and Exposition (ECCE)*, 2021: IEEE, pp. 1307-1312.

[15] T. Hossen and B. Mirafzal, "A Study on Self-Security of Smart Inverters," in *2023 IEEE Kansas Power and Energy Conference (KPEC)*, 2023: IEEE, pp. 1-6.

[16] J. Obert *et al.*, "Recommendations for trust and encryption in DER interoperability standards," Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Kitu Systems …, 2019.

[17] K. Rayane, H. Abu-Rub, M. Shadmand, S. Bayhan, and A. Benalia, "Grid interactive smart inverter with intrusion detection capability," in *2021 IEEE 12th International Symposium on Power Electronics for Distributed Generation Systems (PEDG)*, 2021: IEEE, pp. 1-6.

[18] D. Tolossa, "Importance of cybersecurity awareness training for employees in business," *Vidya,* vol. 2, pp. 104-107, 2023.

[19] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, and N. Ghadimi, "A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future," *Electric Power Systems Research,* vol. 215, p. 108975, 2023.

[20] A. Marotta and S. Madnick, "Analyzing the interplay between regulatory compliance and cybersecurity (Revised)," 2020.

[21] K. Misbrener, "Cyberattacks threaten smart inverters, but scientists have solutions," *Solar Power World,* 2019.

[22] K. Scarfone, "Guide to Intrusion Detection and Prevention Systems (IDPS)," *NIST special publication,* 2007.

[23] E. Tari Yvonne, "Impact of ransomware on industrial control systems in the oil and gas sector: Security challenges and strategic mitigations," *Computer Science & IT Research Journal,* vol. 5, no. 12, pp. 2664-2681, 2024, doi: 10.51594/csitrj.v5i12.1759.

[24] C. I. Advanced Persistent Threat Compromise of Government Agencies, and Private Sector Organizations, "Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations." Cybersecurity and Infrastructure Security Agency (CISA) https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-352a (accessed 16 December 2024.

[25] F. J. Jaime, A. Muñoz, F. Rodríguez-Gómez, and A. Jerez-Calero, "Strengthening Privacy and Data Security in Biomedical Microelectromechanical Systems by IoT Communication Security and Protection in Smart Healthcare," (in eng), *Sensors (Basel),* vol. 23, no. 21, Nov 3 2023, doi: 10.3390/s23218944.