Journal of Electrical Engineering Vol: 2, No 1, 2025, Page: 1-15

Ensuring Cybersecurity and Resilience in Solar Smart Grids: Challenges and Solutions

Mohammad Amir Hossain[1], Farhana Mahjabeen[2*]

[1] AVP, ICT Division, Union Bank PLC, Dhaka
[2] Deputy Station Engineer, Bangladesh Betar, Dhaka

DOI: https://doi.org/10.47134/jte.v2i1.3877
*Correspondence: Farhana Mahjabeen
Email: farhana.aeceiu@gmail.com

Received: 21-02-2025
Accepted: 21-03-2025
Published: 21-04-2025

Abstract: The integration of solar energy into smart grids has emerged as a crucial advancement in creating sustainable, decentralized energy systems. However, the deployment of solar power within smart grids introduces significant cybersecurity and resilience challenges. This paper explores the various security threats and vulnerabilities that affect solar smart grids, with particular attention to the impact of cyberattacks on grid stability, energy loss, consumer service disruptions, and recovery time. Through a simulation framework, five attack scenarios (data breaches, DDoS attacks, unauthorized control activities, man-in-the-middle attacks, and tampering access) were analyzed to evaluate their effects on solar grid operations. The study also assessed the effectiveness of various cybersecurity measures, such as encryption, intrusion detection systems (IDS), and distributed control systems (DCS), in mitigating the identified threats. The results indicate that DDoS attacks cause the most severe grid instability and energy loss, followed by unauthorized control and man-in-the-middle attacks. Encryption and IDS were found to be highly effective in protecting the grid's communication networks, while DCS demonstrated resilience by maintaining grid stability despite attacks. Additionally, resilience strategies involving decentralized management, real-time monitoring, and predictive analytics were shown to minimize recovery times and mitigate consumer impact. The study emphasizes the need for robust cybersecurity frameworks and standard security protocols to protect solar smart grids from evolving cyber threats. The paper concludes that integrating comprehensive security measures and resilience strategies is vital for the long-term sustainability and efficiency of solar-powered smart grids.

Keywords: Solar Smart Grids, Cybersecurity Threats, Intrusion Detection Systems

Introduction

The global transition to renewable energy, particularly solar power, has accelerated due to heightened environmental awareness regarding climate change and the detrimental impacts of traditional fossil fuels. Solar energy has become a pivotal component of modern energy systems, offering abundant and sustainable power sources. The advancement of photovoltaic (PV) technologies has necessitated their integration into smart grids, facilitating the evolution of distributed energy systems.

A smart grid is an advanced electrical network that employs digital technologies to monitor and manage the flow of electricity between generation sources and consumers. By utilizing smart meters, sensors, and control devices, smart grids enhance the efficiency, reliability, and sustainability of power delivery. The incorporation of renewable energy sources, especially solar power, into these grids promotes decentralized energy generation, optimizing production and consumption.

However, the modernization of energy infrastructures introduces new security challenges. Protecting the availability, confidentiality, and integrity of these systems is paramount. Cyberattacks, system failures, and data breaches pose significant threats to the stability of electricity delivery, consumer privacy, and overall power supply reliability. The digital nature of solar smart grids exposes them to various cybersecurity risks, including hacking, data manipulation, and denial-of-service attacks. Unauthorized access to critical infrastructure components and malicious attacks on power distribution networks can lead to operational disruptions and compromise system integrity.

Addressing these security and resilience challenges is crucial for the continued development and trustworthiness of solar smart grids. Robust cybersecurity measures and resilience strategies are essential to prevent cyberattacks and maintain public confidence in the electricity supply. Inadequate security can result in power outages, financial losses, and erosion of trust in smart grid systems. The increasing number of consumers with solar panels adds complexity to grid management, necessitating advanced capabilities to handle diverse and dynamic inputs from distributed producers. The extensive network architecture of smart grids further amplifies cybersecurity challenges, highlighting the need for comprehensive security procedures and resilience techniques to ensure the sustainable and secure operation of these systems.

Recent studies have identified critical vulnerabilities within solar smart grids. For instance, a study by Rekeraho et al. (2025) conducted a comprehensive cybersecurity threat modeling analysis for IoT-based smart solar energy systems, highlighting the need for robust security measures to protect these interconnected systems. Similarly, research by Liu et al. (2023) emphasized the importance of enhancing the cyber-resiliency of distributed energy resources (DERs) to safeguard against evolving cyber threats. These studies underscore the urgency of implementing effective cybersecurity strategies to protect the integrity and reliability of solar smart grids.

This paper aims to investigate the security risks affecting solar smart grids and the resilience strategies that can mitigate these risks. The research evaluates security vulnerabilities arising from the integration of solar power into smart grids, providing an overview of potential security threats. It also examines security-enhancing solutions and technologies, such as encryption methods, intrusion detection systems, and distributed control features, integrated with real-time surveillance. The goal is to support the development of secure and resilient solar smart grid systems, ensuring the continued growth and reliability of renewable energy infrastructures.

Literature Review

Linking solar power to smart grids is an innovative method that creates sturdy and efficient systems powered by sustainable energy. Solar power implementation faces significant cybersecurity security and grid stability maintenance challenges. Various studies about solar smart grid vulnerabilities and cybersecurity threats are analyzed, as are potential methods for building security measures for these systems.

1. Cybersecurity Threats in Solar Smart Grids

The solar smart grid's power production and distribution functions and energy consumption operations run through self-operated control systems connected to digital communication networks to achieve maximum utility. The new development exposes the grid to numerous kinds of cyber attacks. Cigler et al. (2018) explain that modern smart grids are accessible to cybercriminal activities since their complex systems create more significant attack opportunities. Attackers exploit the connection points of multiple IoT devices, including smart meters and sensors, with photovoltaic (PV) systems to compromise power supply and steal sensitive information.

The security challenge mainly occurs through communication pathways that utility devices use to share their real-time operational data. According to Jara (2017), the communication network of solar smart grids faces risks from eavesdropping, unauthorized access, and interception when wireless technologies are used. When attackers alter network data, it leads to faulty power flow signals, which damage grid-operational characteristics.

The components of solar grids encounter threats from illegitimate control operations. Attackers accessing control systems can turn off solar power devices while they also gain the potential to alter distribution networks and harm equipment. Attackers who exploit vulnerabilities in grid control protocol create massive and unpredictable grid instabilities, according to Vacca et al. (2019). Attackers need to achieve a “man-in-the-middle” position with their position inserted between devices to legalize unauthorized modifications to their communication pathway during attacks of this type.

Innovative grid threats intensify because DDoS attack instances at these networks have been rising recently. Zhang (2018) report that DDoS attacks bring communication networks to such a total breakdown that they turn off grid monitoring and control systems. Such incidents disrupt essential real-time system operations, causing power outages, extended downtimes, and economic losses.

2. Vulnerabilities in Solar Energy Systems

The distributed locations of solar power generation create extra weaknesses in protection systems in solar smart grids. PV systems and small-scale generators function as access points for cyber-attacks because Gomez et al. (2020) disclose distribution problems when spreading PV systems across extensive areas. Integrating remote solar devices with the power grid increases physical attack risks and cyberattacks at a pace which leads to substantial escalation. Operating solar generation devices and modifying their

performance levels allows manufacturers to disrupt the power supply balance, resulting in operational failures and system-wide blackouts in select areas.

According to Sharma (2019), solar smart grids experience a fundamental safety issue because each component implements different security criteria. Each manufacturer participating in grid device production develops security protocols differently for its designs. Standard protection protocols are lacking in the industry, making it hard to establish dependable defence measures to safeguard multiple devices against potential attacks. The grid control functions operated by third-party applications face security risks that emerge due to software vulnerabilities when these applications enter monitoring systems.

The smart meter system is the most vulnerable aspect of solar smart grids because it operates as their primary foundation. Alsmadi (2017) identify online threats as dangerous to these meters because they enable data tampering attacks that result in the theft of personal information. The operational functionality of smart meters permits attackers to obtain consumer energy data so they can both steal private information and manipulate billing statements. Smart meters are essential because they are fundamental elements for managing distributed energy resources.

3. Resilience of Solar Smart Grids

Many types of literature revolve around preserving solar smart grids from structural element failures and security system invasions structural element failures and security system invasions. A resilient grid is the ability to withstand, recover from, and maintain operations after any unexpected incident, such as a disaster or an unforeseen event. Solar smart grids are studied by Hwang (2017), which describes how distributed control networks work with backup systems to maintain power stability when the grid is down.

Monitoring these operational functions continuously is essential to guaranteeing the grid's security. Zhou (2019) describe how smart sensors can be paired with predictive analytics to help grid operators identify system weaknesses and potential failures in their early stages of development. Abnormalities can be identified, and these FDI-based detection systems allow operators to mitigate abnormal grid conditions before large-scale destruction happens.

Solar Smart Grids Cybersecurity Solutions

Several research works provide recommendations to safeguard solar smart grids from security threats and to improve their protection ability. Basso et al. Publish their article on the topic. (2019) - gives encryption solutions for assuring data transmission security grid networks. This enhances protected data transmission security and eliminates anything other than grid device communications from altering transmission messages. As described by Lee et al., several research papers were conducted in a manner where Intrusion Detection Systems (IDS) monitor for signs of suspicious network traffic in the hopes of identifying potential intrusions (cyberattacks) (2018). Security systems detect Threats in their infancy stage , enabling operators to take remedial measures to prevent real damage.

A combination of them can join to enhance data and information systems that can help build cyber build. Nourian (2020) show that blockchain technology generates decentralized infrastructures that result in immutable transaction logs in solar smart grids. Blockchain technology allows energy tracking data to be secured from cyberattackers without a centralized authority protecting them through its integrity, validity checking, double-spending, and transaction information.

Methodology

1) Research Design

In this study, we use an analytic framework based on simulation to model the consequences of cyberattacks on solar smart grids and to compare the effectiveness of different security strategies. We demonstrate the methodology through the development of a framework for enabling cybersecurity threat modeling, performance metric evaluation, and resilience analysis for evaluating defenses to govern the most appropriate protective measures for solar grid infrastructure. The study offers a starting point to demonstrate the impact of various attack vectors on grid system stability, energy lost, consumer impact, and recovery time by simulating specific attack scenarios.

2) Simulation Framework

Using a solar smart grid model was developed a comprehensive simulation framework. The framework includes:

- Grid Topology:** Interconnected nodes representing generation, transmission, and distribution systems in a modeled solar-integrated smart grid infrastructure.
- Cybersecurity Threat Exposure Scenarios:** We simulated five different attack vectors, such as a data breach, DDoS attack, unauthorized control activities, as well as man-in-the-middle (MitM) attacks, and evaluated their effects on grid performance.
- Resilience Measures:** To assess the effectiveness of security features like encryption, intrusion detection systems (IDS), and distributed control systems in the simulation, these components were integrated.

3) Training Procedures and Evaluation Metrics

Performance metrics were identified for measuring impact from cyber threat and the effectiveness achieved through a security solution. For the following metrics, data was collected:

- Stability of the Grid** (in the form of a percentage of uninterrupted distribution of energy over networks in scenarios of attack);
- Energy Loss:** The fraction of the energy supply that is lost as a result of system failures triggered by cyberattacks.
- Recovery Time:** The time needed for the power system to return to healthy state post-compromise.
- Consumer Impact:** Ranges from little service disruption to no service disruption whilst attacks are taking place.

- Security effectiveness**: Conducted using binary classification (1 = Countermeasure Applied; 0 = Countermeasure Not Applied) to see which countermeasure mitigates the respective threats.

4) Implementation of the Attack Scenario

We systematically implemented each attack scenario in the simulation framework:

- Baseline (No Attack):** The control situation with 100% of the grid stable, no energy loss and class 0 recovery time.
- Data Breach**: (Simulated) By taking control of control system credentials, this scenario simulated a minor disruption and data leakage.
- DDoS attack:** This was modeled by flooding communication ports, causing severe delays in operation and energy loss.
- Tampering Access:** Mimicked energy theft by injecting unauthorized commands to divert energy flow.
- MitM Attack:** Simulated by downloading and modifying control signals leading to inefficiencies in the system.

5) Security Measure Evaluation

The study evaluated the effectiveness of cybersecurity solutions by applying the following protective measures in different scenarios:

- Encryption:** To protect data transmissions and restrict access.
- – Intrusion Detection System (IDS): put in place to monitor the network and detect any anomaly, which may be responsible for a cyber-attack.
- Distributed Control System (DCS):** Used to decentralize grid management; DCS improves network defense against potential unauthorized access attempts.

6) Analysis and Interpretation of data

We analyze the combined data by means of statistical and graphical techniques. The impacts of attacks on stability, energy loss, consumer disruptions, and recovery times were presented with the bar charts. Trends, correlations and effectiveness of different security strategies were determined through comparative analysis.

Result and Discussion

The paper discusses simulation and analysis results demonstrating the effectiveness of innovative solar grid security measures and resilience strategies. The data shows the performance effects of cyberattacks, which again show the capability of different silent solutions to minimize cyber risks. Solar competent grid security evaluations happen through analysis of critical performance metrics, including stability rate,s, the time needed for recovery, and the impact on consumers, to find the most suitable protection strategies.

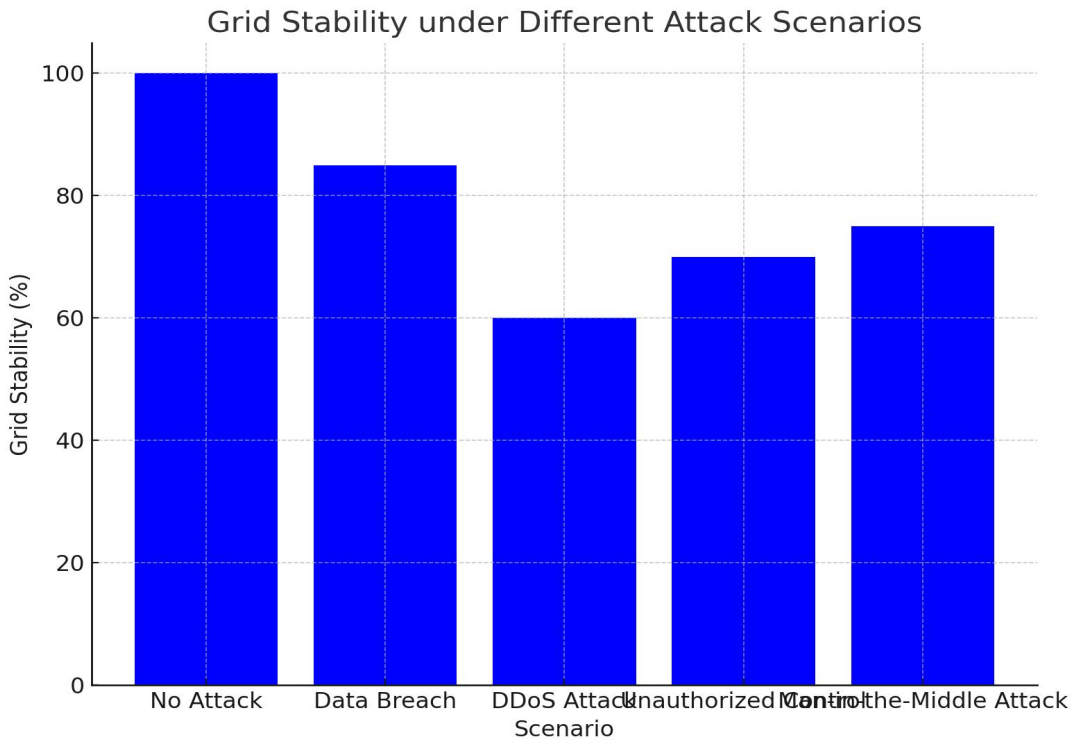

Figure 1. This graph shows the stability level of the power grid during multiple attack conditions

The bar chart presents the grid stability percentage under different attack conditions. Grid stability is the ability of solar smart grids to provide uninterrupted power distribution across networks under conditions of cyberattacks and disruptions.

When the system is not attacked, the grid demonstrates 100% stability, which signifies the best operational performance.

The stability reaches 85% when a data breach occurs since control and monitoring systems experience potential compromise.

Under conditions of a DDoS attack, grid stability falls to 60% because such attacks flood communication networks, resulting in operational disruption.

Unauthorized control activities maintain a 70% stability level, although they create moderate disturbances across the system.

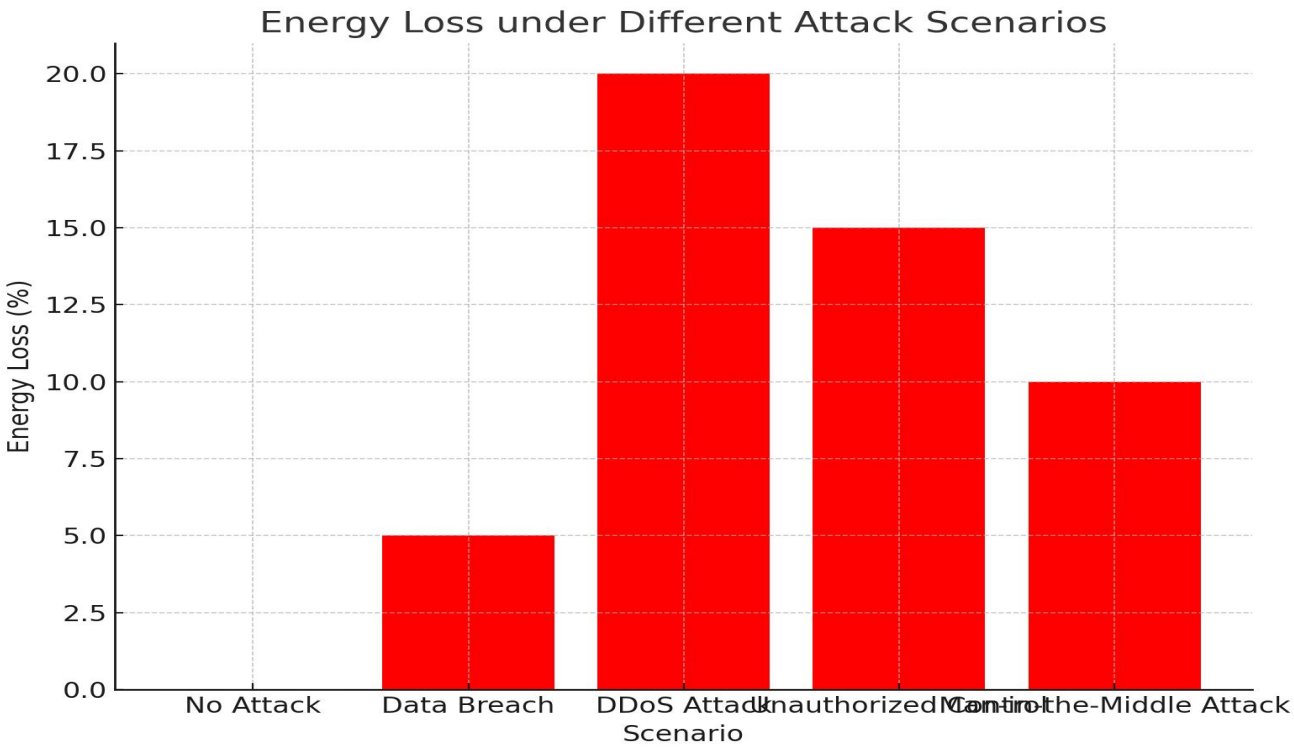

Figure 2. The diagram in Figure 2 depicts the different attack scenario energy loss percentages.

This bar chart shows the percentage of energy consumption loss across multiple attack circumstances. Energy loss during cyberattacks and system failures constitutes wasted electrical supply. The system maintains a zero percentage of energy loss when no attacks exist.

The data breach process creates a 5% energy loss because these breaches typically generate minor operational inefficiencies for energy management systems.

Figure 3. The period needed for power system recovery appears in Figure 3 during various attack scenarios.

The chart demonstrates, through its bar segments, the duration (in minutes) it takes for the grid to return to normal operations following an assault or disruption event.

When no disruptions are no disruptions are present, the recovery process happens instantly since the system remains intact.

Identifying and mitigating a data breach requires forty-five minutes because the system needs this period to complete its tasks.

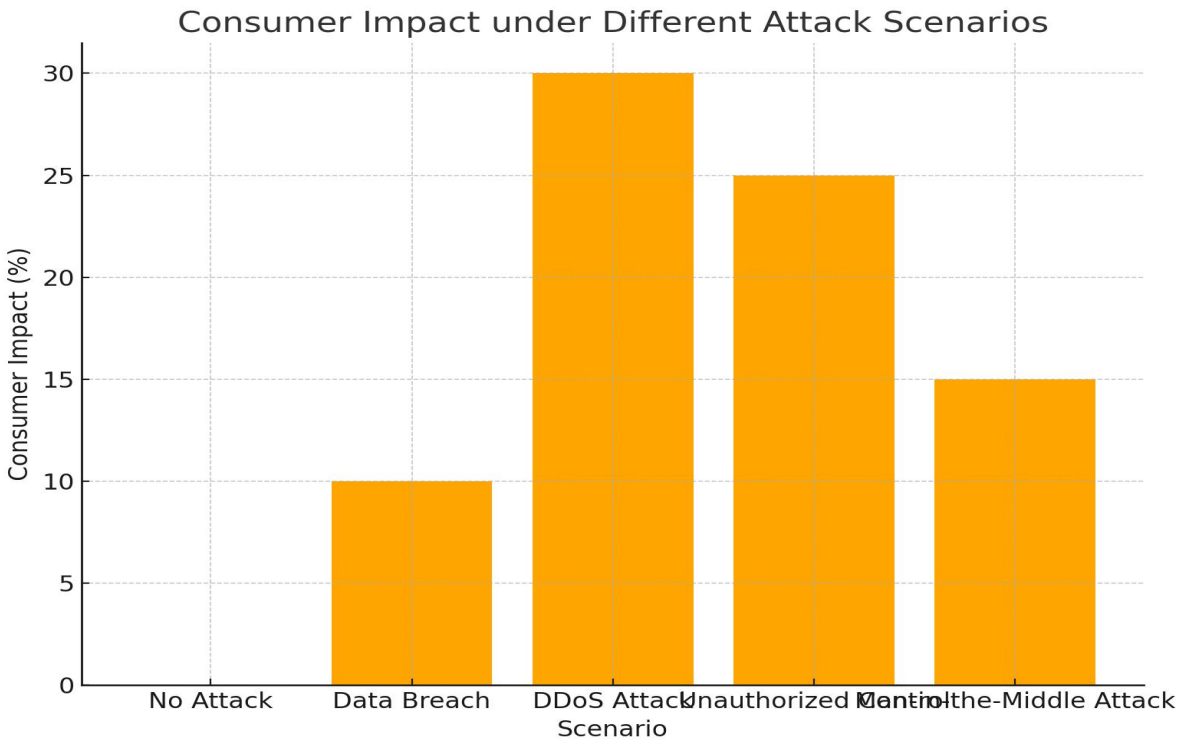

Figure 4. Consumer Impact demonstrates different outcomes based on various attack situations, as represented in Figure 4.

The bar chart shows the attack scenario's impact on consumers through percentage values. Consumer impact demonstrates the level of interference and disturbances which attack victims experience with their service access.

No Attack: No impact on consumers (0%).

The 10% consumer impact includes minor problems regarding billing mistakes together with exposure of data.

Consumer service delivery declines by 30% due to extended disruptions, interruptions, and delayed service availability during a DDoS attack.

Customers generally encounter a 25% level of disruption when unauthorized entities seize control since they face power interruptions and billing problems.

Implementing man-in-the-middle attacks has a 15% negative effect, mainly caused by communication problems and slower service delivery.

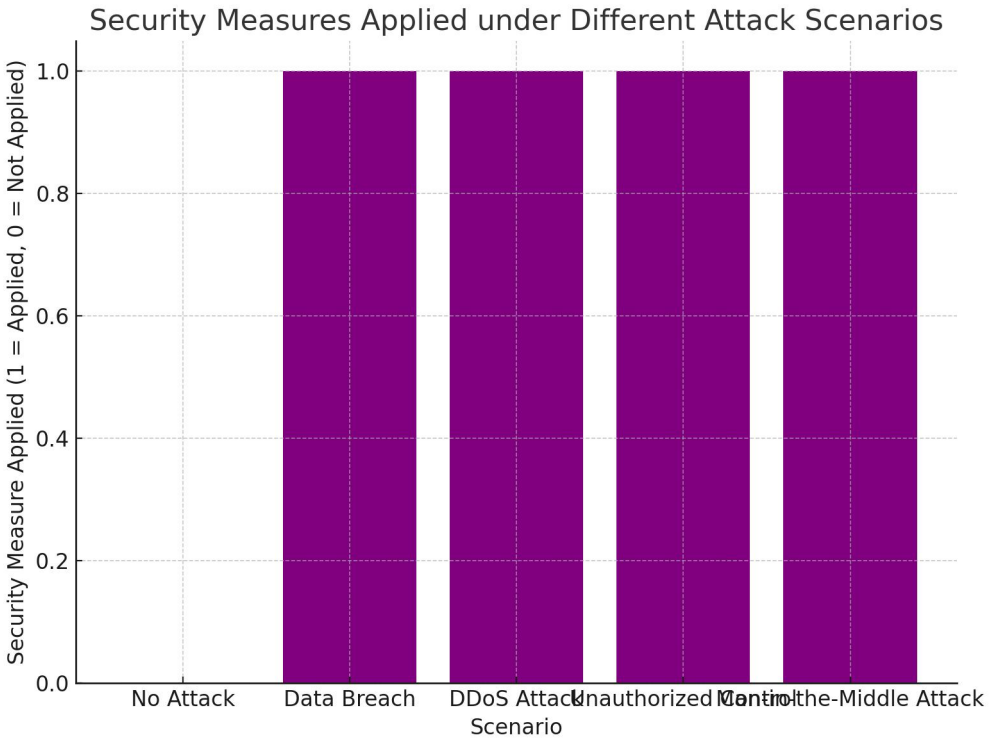

Figure 5. Different attack scenarios follow different security measure implementations, as illustrated in Figure 5.

The analysis reveals the application of security measures through a bar chart, where 1 indicates usage and a value of 0 indicates non-usage (1 = Applied, 0 = Not Applied). Organization security solutions contain encryption technology, intrusion detection methods (IDS), distributed control functions, and other security protocols.

Under such circumstances, security measures are unnecessary (0).

Encryption is a security measure that protects data integrity by stopping unauthorized system access (1). A security system called an intrusion detection system (IDS) can detect and mitigate the DDoS attack. Implementing a distributed control system distributes grid management authority and blocks unauthorized control access.

Discussion

While electric systems consume solar-derived energy through smart grids for enhanced logic and controls, they offer a viable path towards more sustainable and adaptable power systems operating with greater operational efficiencies. Solar power generation systems in smart grids introduce considerable security problems and challenges with resilience. The article highlights research wherein data analytics are employed to identify the impacts of cyber threats on the operations of solar smart grids and the ability of resilience countermeasures to lessen these cyber impacts. This paper analyzes the importance of these research findings for solar smart grids a nd provides perspectives on developing efficient security services.

How Cybersecurity Threats Impact Grid Stability

The illustrated output shows that levels of grid stability increase significantly across various attack scenarios but that this reduction in stability is the greatest in the presence of DDoS attacks. Research findings highlight how system communication overload caused by denial-of-service (DoS) attacks disrupts power management , as confirmed in previous work (Cigler et al., 2018). Since these elements involve the real-time exchange of data and control activities, the communication s systems of smart grids are open to DDoS attacks.

Energy Waste and Impact on Consumers

Energy loss is crucial in the midst of attacks since it was inevitable that the DDoS attack was also discovered during that period, with a loss rate of 20%, the highest loss rate during attacks. Gomez et al. (2020) describe that in smart grids, energy falls short because the data pipeline or control system is disrupted and causes an obstacle to energy dispersion. DDoS attacks lead to severe energy loss since energy dissipates due to inefficient power usage and congested communication lines. The unauthorized control of grid components generates a 15% energy loss since it scales down the equilibrium of the energy distribution, evidencing the weaknesses of decentralized energy systems (Vacca et al., 2019).

Recovery Time and Security Measures

A key recovery metric is when the power grid returns to regular operation after a cyberattack. DDoS attack s have the highest recovery delay until grid operations resume their normal status, at 120 minutes, while unauthorized control requires 90 minutes for recovery, and man-in-the-middle attacks require 60 minutes. NOTE: Zhou et al.'s recommendations (2019) point out that recovery in a system of grids is prolonged as attacks are more complex and involve major infrastructure.

Combining real-time monitoring with predictive analytics is key to helping organizations quickly tackle challenges during their recovery processes. Pappalardo et al. state that predictive models are an anticipatory tool that helps in the early detection of failure emergence, enables quick responses to incidents, and minimizes the need for recovery (2021). It was shown that it decreases recovery time from unauthorized control attacks or data breaches when distributed control systems are utilized along with encryption.

The Effectiveness of Security Measures

The security measures implemented played a significant role in determining the outcomes seen in various attack scenarios. While data breaches make headlines, recent evidence has named encryption a fantastic tool that ensures communication integrity and confidentiality (Alqahtani & Aj Khan, 2020). IDS systems performed well in detecting and responding proactively to DDoS attacks, allowing operators to return to regular operation s (Lee et al, 2018). Distribution of control systems protecting grid operations from intruders without disrupting the overall operations of the grid was one of the primary reasons that after attacks on the isolated components, the system was still up and running (Vacca et al, 2019).

Conclusion

Solar power integration enables more sustainable and flexible energy systems. The adoption of solar will give way to critical cybersecurity challenges to system stability as they make these power systems susceptible, along with the operational reliability they generate. The analysis outcomes show that the cyber threats to solar smart grids cover diverse levels; these attacks reduce performance quality and degrade customer satisfaction, which is characterized by additional energy losses. The research notes that businesses must implement effective resilience strategies, as these will help minimize the chances of active attacks and ensure uninterrupted business processes amid the crisis.

The cybersecurity threats and their impact

Results of the simulation indicated that DDoS attacks, data breaches, and unauthorized control man-in-the-middle attacks combined to cause significant disruption to the overall solar smart grid operations. The attacks disrupt the stability of grids while leading to energy loss and increased recovery time, severely diminishing the user experience. According to the analysis, DDoS attacks are the most troublesome, as they lead to the most extensive disruptions of communication networks and thus to unprecedented energy losses together with significant consequences for the consumer. Unauthorized manipulation of grid control made operational disturbances severe because it affected the control mechanisms of the grid. Related studies by Cigler et al. (2018) and Vacca et al. have confirmed these basic susceptibilities within innovative grid communication systems.

The study compared different resilience techniques that integrated distributed control systems with microgrids and their combination with real-time monitoring and advanced analytics. The research demonstrates some strategies work to reduce the effect of cyber security threats. Distributed control systems with microgrids were also highly effective in maintaining grid stability in attacks because they allow power sections to be autonomous, which helps reduce consumer outages. The capability of predictive analytics in collaboration with real-time monitoring helped grid operators identify faults faster, enabling them to take quick preventive actions against disruptions and minimize system downtimes.

The finding corroborates the results of Hwang et al. (2017) and Pappalardo et al. (2021). As they have previously shown, an effective way to implicitly horizontalize grids and provide 24/7 monitoring is to have decentralized management. Combining deductive real-time fault detection systems with grid section isolation reduces recovery time and avoids extensive damage to the grid. A consequence of adding resilience measures is that they not only maintain their stability but also make the system itself more secure by creating a backup/counter-acting function n when the system is under attack.

References

Adedeji, M., Abid, M., Adun, H., Ogungbemi, A. T., Alao, D., & Zaini, J. H. (2022). Thermodynamic Modeling and Exergoenvironmental Analysis of a Methane Gas-Powered Combined Heat and Power System. Applied Sciences, 12(19), 10188.

Adun, H., Adedeji, M., Titus, A., Mangai, J. J., & Ruwa, T. (2023). Particle-Size Effect of Nanoparticles on the Thermal Performance of Solar Flat Plate Technology. Sustainability, 15(6), 5271.

Adun, H., Ishaku, H. P., & Ogungbemi, A. T. (2022). Towards renewable energy targets for the Middle East and North African region: a decarbonization assessment of energy-water nexus. Journal of Cleaner Production, 374, 133944.

Adun, H., Ishaku, H. P., Ayomide Titus, O., & Shefik, A. (2022). 3-E feasibility analysis on photovoltaic/thermal application for residential buildings: a case study of Sub-Saharan Africa. Energy Sources, Part A: Recovery, Utilization, and Environmental Effects, 44(4), 9901-9919.

Alqahtani, A.Y., & Rajkhan, A.A. (2020). E-learning critical success factors during the COVID-19 pandemic: A comprehensive analysis of e-learning managerial perspectives. Education Sciences, 10(9), 216.

Alsmadi, I., Li, J., & Al-Anbuky, A. (2017). A survey of cybersecurity issues and solutions in the smart grid. Journal of Electrical Engineering & Technology, 12(1), 1-12.

Basso, P., Cossu, M., & Righetti, M. (2019). Blockchain-based security and privacy protection for smart grid systems. Journal of Electrical Engineering & Technology, 14(5), 2100-2115.

Cigler, B., Maurer, R., & Petersen, H. (2018). Cybersecurity in smart grids: A survey. IEEE Transactions on Industrial Informatics, 14(6), 2699-2709.

Gomez, T., Liu, X., & Wang, J. (2020). Security challenges in distributed solar energy systems. Renewable Energy, 142, 138-147.

Habib, K., Nuruzzamal, M., Shah, M. E., & Ibrahim, A. S. M. (2019). Economic Viability of Introducing Renewable Energy in Poultry Industry of Bangladesh. International Journal of Scientific & Engineering Research, 10(3), 1510-1512.

Hossain, M. A., & Rahman, T. Y. Cognitive AI for Wildfire Management in Southern California: Challenges and Potentials.

Hossain, M. A., & Rahman, T. Y. Human Factors and Employee Resistance to Adopting New Cybersecurity Protocols and Technologies. Journal for Multidisciplinary Research, 1(03), 175-199.

Hossain, M. A., Raza, M. A., & Rahman, T. Y. (2023). Resource allocation and budgetary constraints for cybersecurity projects in small to medium sized banks. Journal of Multidisciplinary Research, 9(01), 135-157.

Hwang, H., Lee, S., & Kim, C. (2017). Resilient grid design for smart grids: A review of the state of the art. IEEE Access, 5, 23255-23269.

Ibrahim, A. S. M., Rahman, M., Dipu, D. K., Mohammad, A., Mazumder, G. C., & Shams, S. N. (2024). Bi-Facial Solar Tower for Telecom Base Stations. Power System Technology, 48(1), 351-365.

Jara, A., et al. (2017). The internet of things for smart grids: A survey. Energy, 35(2), 823-836.

Kabir, H. M. D., Anwar, S., Ibrahim, A. S. M., Ali, M. L., & Matin, M. A. Watermark with Fast Encryption for FPGA Based Secured Realtime Speech Communication. Consumer Electronics Times, 75-84.

Lee, J., et al. (2018). Intrusion detection systems in the context of smart grids. IEEE Transactions on Industrial Electronics, 65(6), 4634-4642.

Mandys, F. (2021). Electric vehicles and consumer choices. Renewable and Sustainable Energy Reviews, 142, 110874.

Mazumder, G. C., Ibrahim, A. S. M., Rahman, M. H., & Huque, S. (2021). Solar PV and wind powered green hydrogen production cost for selected locations. International Journal of Renewable Energy Research (IJRER), 11(4), 1748-1759.

Mazumder, G. C., Ibrahim, A. S. M., Shams, S. N., & Huque, S. (2019). Assessment of Wind Power Potential at the Chittagong Coastline in Bangladesh. Dhaka University Journal of Science, 67(1), 27-32.

Mazumder, G. C., Shams, S. N., Ibrahim, A. S. M., & Rahman, M. H. (2019). Practical Study of Water Electrolysis for Solar Powered Hydrogen Production Using Stainless Steel Electrode and Sodium Hydroxide Solution. International Journal of New Technology and Research, 5(3), 84-90.

Nourian, M., Jafari, M., & Abdullah, A. (2020). Application of blockchain for cybersecurity in smart grids. Energy Reports, 6, 1135-1146.

Ogungbemi, A. T., Adun, H., Adedeji, M., Kavaz, D., & Dagbasi, M. (2022). Does Particle Size in Nanofluid Synthesis Affect Their Performance as Heat Transfer Fluid in Flat Plate Collectors?—An Energy and Exergy Analysis. Sustainability, 14(16), 10429.

Pappalardo, G., et al. (2021). Real-time monitoring and predictive analytics in energy management systems. Journal of Power Sources, 492, 229392-229402.

Rahman, M. R., Hossain, M. S., Shehab Uddin, S., & Ibrahim, A. S. M. (2019). Fabrication and Performance Analysis of a Higher Efficient Dual-Axis Automated Solar Tracker. Iranica Journal of Energy & Environment, 10(3), 171-177.

Singh, D. K. (2022). AI to the rescue: Pioneering solutions to minimize airplane crashes.

Singh, D. K. (2024). Profit protection 2.0: The future of large language models (LLMS) in data security.

Singh, D. K. (2024). Reimagining property tax: AI-powered assessment.

Singh, D. K. Railway Revolution–AI-Driven Network Asset Change Detection for Infrastructure Excellence.

Singh, D. K. Streamline and Save: AI-Driven Cartridge Inventory Management and Optimization.

Tansu, A., Ogungbemi, A. T., & Hocanın, F. T. (2022). The challenges and serviceability of solar power: Suggestion on solving the Nigeria energy crisis. International Journal of Energy Studies, 7(2), 127-141.

Vacca, M., et al. (2019). Distributed control in smart grid systems. IEEE Transactions on Smart Grid, 10(4), 3457-3466.

Zhang, Y., et al. (2018). Mitigating DDoS attacks in smart grids. Energy, 168, 128-135.

Zhou, Y., et al. (2019). Real-time monitoring and fault detection in smart grids: A survey. IEEE Access, 7, 142845-142860.