Renewable Energy and Cyber Threats: Safeguarding Solar Power Systems

Homam El-Taj
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
htaj@dah.edu.sa

Amena Khoja
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
amkhoja@dah.edu.sa

Dania Kamal
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
dskamal@dah.edu.sa

Fatima Alammari
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
fmalammari@dah.edu.sa

Joud Alkhowaiter
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
jialkhowaiter@dah.edu.sa

Layal Bogari
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
lybogari@dah.edu.sa

Renad Essa
Department of Cybersecurity
Dar Al-Hekma University
Jeddah, Saudi Arabia
rmessa@dah.edu.sa

2024 International Jordanian Cybersecurity Conference (IJCC) | 979-8-3315-1846-2/24/$31.00 ©2024 IEEE | DOI: 10.1109/IJCC64742.2024.10847288

***Abstract*— Solar energy systems play a significant role in sustainable energy production but face alarming risks due to cybersecurity vulnerabilities. This paper examines critical challenges, including encryption weaknesses, insecure authentication protocols, and insufficient intrusion detection mechanisms, with a specific focus on Operations Technology (OT) and Supervisory Control and Data Acquisition (SCADA) systems. Cyberattacks exploiting these systems can disrupt energy production, compromise data accuracy, and lead to severe environmental and economic consequences. The resilience of renewable energy infrastructure depends on proactive measures such as advanced encryption and real-time monitoring by stakeholders to address these cybersecurity risks. By securing these systems, stakeholders can safeguard the reliability and sustainability of renewable energy infrastructure, ensuring their continued growth in the face of evolving cyber threats.**

Keywords: Sustainable energy, Cybersecurity, Solar power, Operation Technology, Supervisory Control and Data Acquisition, and Cybersecurity risks

I. Introduction

Solar energy systems are vital for reducing carbon emissions and promoting environmental sustainability, making them a foundation of the global transition to renewable energy. As these systems increasingly rely on digital technologies, robust cybersecurity measures are essential to safeguard energy production and distribution. With the growing reliance on renewable energy systems, the risks of hacking, data breaches, and system manipulation have never been greater. Cyberattacks pose significant risks to solar energy systems and the broader energy sector, impacting both infrastructure and users. Key components, such as solar panels, inverters, batteries, and other critical technologies, are particularly vulnerable to these threats [27]. This paper examines the cybersecurity challenges faced by renewable energy systems, focusing on vulnerabilities at the intersection of cybersecurity and renewable energy protection. It also discusses the responsibilities of stakeholders in developing initial security programs and implementing long-term strategies. To mitigate these risks, it is crucial to integrate advanced digital security technologies with comprehensive cybersecurity strategies, addressing vulnerabilities swiftly and effectively. Critical systems like Operational Technology (OT) and Supervisory Control and Data Acquisition (SCADA) are especially susceptible to cyberattacks, underscoring the need for proactive protection. These systems are central to managing solar infrastructure, making their security a priority for the resilience of renewable energy networks. In conclusion, cybersecurity measures are not just protective tools; they are essential to the sustainability and resilience of solar energy systems. Securing these systems ensures their longevity and supports the broader goal of a sustainable future [22].

A. Solar System

The burning of fossil fuels is not only environmentally destructive but also unsustainable, necessitating a shift toward sustainable energy systems, particularly renewable sources such as solar and wind, for hydrogen production. To meet the 1.5°C climate target, a rapid and extensive transition away from fossil fuels is required, supported by legislative and technical approaches such as expanding renewable energy deployment and improving efficiencies across all sectors [3]. The socio-economic consequences, particularly the impacts on fossil-fuel-dependent communities, are complex and profound [3]. Furthermore, the adoption of these technologies introduces cybersecurity risks, particularly for microgrids. Vulnerabilities arise in communication networks, which can be exploited by cyberattacks, compromising the resilience and security of power systems. A thorough analysis and the development of robust cybersecurity solutions are essential to counter these challenges. Solutions must account for threats such as denial-of-service (DoS), distributed denial-of-service (DDoS), and false data injection attacks, which undermine the stability and sustainability of the system [4][5]. Figure 1 below demonstrates how the SCADA system is relevant. Just like the solar system's Lesson, the System of Complex Planetary Systems is relevant to cybersecurity systems and environmental sustainability.

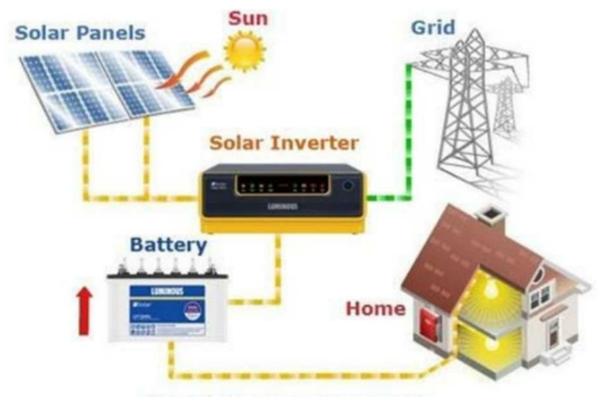

Fig. 1. Solar Energy System

A solar cell, primarily made from semiconductor materials like silicon, performs the photovoltaic (PV) process to convert sunlight into electrical energy. This occurs due to the photovoltaic (PV) process, where sunlight excites electrons, generating an electric current. The solar panel placed on the surface of a photovoltaic facility absorbs photons from sunlight, causing electrons to flow and generate an electric current. At this point, charge controllers play a critical role in managing the flow of electrical charge between the solar panel and the battery. They regulate the voltage and protect the system from both overcharging and excessive recharging, ensuring that the electrical charge moving to and from the cell is kept within safe limits. The voltage generator of 12-volt solar panels typically varies between 16 to 21 volts, depending on the battery characteristics. The battery's voltage is typically adjusted from 14 to 14.7 volts. Charge controllers regulate the voltage to protect the battery from excessive voltage, preventing overcharging. This is crucial because, without proper regulation, consumers could receive more electricity than the system is designed to manage, leading to potential damage [1].

Batteries, or accumulators, are components of photovoltaic systems responsible for retaining electricity generated from the solar panels for later use, such as at night. They are responsible for two tasks: saving excessive power when demand is low and providing power when the solar array cannot meet demand. On the other hand, inverters, which are part of the system, convert the direct current from the batteries into alternating current, which is required by the household appliances, and are connected directly to the battery terminal [1][2][7].

B. Cybersecurity

Cybersecurity prevents unauthorized access to networks or devices, ensuring protection of personal or organizational data from breaches, while also guaranteeing the availability, confidentiality, and integrity of information. The solar system's assets, including satellites and space infrastructure, represent valuable resources that require protection. A heightened level of awareness and concern will emerge if an attack affects a satellite. Cybersecurity plays a key role in maintaining the stability of space infrastructure by mitigating risks and reducing threats. Its primary goal is to safeguard astronaut safety and ensure the integrity of space missions.

II. Challenges

Solar-powered systems, particularly photovoltaic (PV) systems, face some of the highest security risks. These systems are notably more vulnerable due to the unpredictable nature of weather, which makes them "less reliable" compared to traditional power systems [8, 9]. Factors such as cloud cover, time of day, and seasonal fluctuations directly impact energy production, while environmental issues like infrastructure decay and dust particles' reduce system efficiency. This factor not only affects the physical performance of PV systems but also introduces cybersecurity vulnerabilities. Most PV systems are located in remote, expansive areas, making them more prone to physical security breaches if personnel are not adequately trained [6][10]. The high costs associated with training staff and relocating them to these locations further decrease physical security and increase the potential for attacks.

Additionally, the high level of integration among PV systems of varying grid sizes introduces extra vulnerabilities, including potential false data injection, man-in-the-middle attacks, and denial-of-service attacks [11][12]. Ensuring that these extensive and varied systems are encrypted sufficiently to maintain both security and performance remains a significant challenge.

A. Mitigation

A multi-layered approach is essential for addressing the challenges and security risks associated with solar-powered systems. The initial step involves mitigating environmental challenges through careful pre-planning and selecting the appropriate location for installation. Weather conditions and climate variations must also be taken into account when installing photovoltaic (PV) and solar-powered systems.

In addition, implementing access control and authentication protocols is crucial to mitigate attacks. This should be complemented by the employment of security personnel. Authentication protocols, such as biometrics, password authentication, token-based systems, and two-factor authentication, must be integrated with the site's physical security systems. This reduces the need for additional employees.

Moreover, it is essential that all employees receive training and are fully aware of the risks and challenges associated with the system [13].

To address the complexity of these systems, scalable solutions must be implemented. Several model-based strategies have been developed to mitigate the absence of sufficient encryption and effective intrusion detection systems (IDS) in PV installations.

Analytical models, such as dynamic watermarking [29], variation mode decomposition [30], isolation forest [31], and deep belief networks [32], are all examples of techniques developed against attacks on PV systems [11].

B. Impact

Since 1990, detailed studies have been conducted on dust deposition, with improved accuracy in experimental measurements. These studies have shown that many collectors experience a reduction in electrical and thermal performance after a short exposure to dust. El-Shobokshy and Hussein were pioneers in studying the effects of dust on photovoltaic (PV) cells in Saudi Arabia. Their research focused on how dust accumulation and its deposition density affect PV efficiency. The findings highlighted the significant impact of cement particles, showing that a cement dust deposition of 73 g/m² led to an 80% reduction in PV short circuit voltage [14]. In 2006, Eliminar et al. conducted a study in Egypt to examine the transmittance of glass under varying conditions [33]. They monitored 100 glass samples placed at different angles and orientations over a seven-month period, particularly following each nearby thunderstorm. This study also involved a detailed mineralogical examination of the dust accumulated on the transparent covers of the solar cells. The results indicated a noticeable decline in glass transmittance, which correlated with increased dust deposition density, ranging from 52.54% to 12.38%, as the dust density rose from 4.48 g/m² to 15.84 g/m² [14]. PV systems are vulnerable to cyberattacks due to their unpredictable behavior, which is influenced by environmental conditions. The integrity of the power grid can be jeopardized, and the misuse of timing and grid response can disrupt energy output. This can lead to economic loss, possible safety risks, and a major security risk to vital infrastructure. The physical security and monitoring of PV systems are particularly challenging because they are often spread across large, remote areas. Physical attacks on the infrastructure are more likely to occur when there are insufficient security measures, leading to equipment damage, theft, or tampering. Such incidents not only endanger worker and community safety but can also hinder energy production, resulting in repair costs. Monitoring remote systems effectively requires security staff to be trained, but the cost of relocating and training personnel in isolated areas can be prohibitively expensive. Insufficient monitoring increases the risk of security breaches, which could compromise system integrity and lead to interruptions in energy production through unauthorized access or manipulation of devices. In addition to these physical vulnerabilities, PV systems are also prone to cyber risks because of their reliance on Operational Technology (OT) and SCADA systems. These digital entry points create significant security concerns and impact the overall resilience of the system.

III. OT Attacks

Since OT and IOT are commonly used together, the attacks on both are similar [16]. Some of these attacks include the DDoS attacks and side-channel; we will discuss the most common attacks [15].

1) DDOS Attack

When A Distributed Denial-of-Service (DDoS) attack occurs when multiple compromised systems target a server or network, overwhelming it with traffic and preventing legitimate users from accessing the system. In such attacks, malware exploits the vulnerability of IoT devices, converting them into a botnet. The botnet then sends a high volume of requests, which can either slow down or completely shut down the system. Srivastava et al. categorized these IoT-based DDoS attacks by their impact on resource depletion, bandwidth availability, infrastructure, and fonts [28]. These attacks primarily affect the memory, CPU, and socket resources in an IoT environment and may also exploit existing network vulnerabilities or initiate attacks like Ping-of-Death.

Some DDoS attacks specifically target bandwidth consumption, usually by amplifying or broadcasting malformed packets. This can include UDP flood and ICMP flood attacks. Infrastructure-focused attacks also target IoT devices and their components, using their resources to deny user access. Additionally, Zero-day attacks, which exploit unknown software vulnerabilities before they are patched, are another common threat.

To prevent DDoS attacks, security solutions must be implemented across various IoT layers. At the perception layer, lightweight encryption mechanisms can protect against both DoS and DDoS attacks. At the network layer, protocols like IPv6, ESP, and AH can be used to ensure encryption and integrity verification. DTLS (Datagram Transport Layer Security) provides secure end-to-end communication and automatic certificate management. The middleware and application layers should incorporate access control, local or remote authentication, and machine learning models to enhance IoT security. Additionally, a monitoring and alerting system can be implemented to detect unusual traffic patterns and notify the administrator. Algorithms such as Double Heavy Hitters and Triple Heavy Hitters can help mitigate DoS attacks by filtering out malicious traffic and blocking attackers [17].

Real-life DDOS Attack: A notable instance of a botnet malware attack was the use of BlackEnergy in the attack that took down the Ukrainian power grid in December 2015 [16]. Initially identified in 2007 by Nazario, BlackEnergy was described as a basic botnet that used Hypertext Transfer Protocol (HTTP) and employed runtime encryption to avoid detection. The attack involved a network of compromised systems that targeted and disrupted the Ukrainian power grid, marking one of the first high-profile uses of the BlackEnergy malware.

2) Side Channel Attack

Most IoT devices send side-channel emissions signals, which can unintentionally reveal information about their internal operations. Attackers exploit these emissions to extract sensitive data, such as encryption keys, enabling them to carry out side-channel attacks. This concept is grounded in the idea that systems inherently leak information, which can be intercepted through methods like monitoring power consumption or detecting electromagnetic emissions. The authors have identified two primary types of side-channel attacks:

Timing Analysis Attacks –Timing analysis attacks involve comparing the timestamps of events defined as actions occurring over time. Attackers use specialized techniques to gather information about events, such as packet transmissions within an ecosystem. These attacks leverage differences in the timing of execution paths within the system to extract sensitive data.

Power analysis attacks: Approaching the power consumed by devices can be a great source of information for attackers. The attacker should be in a close location to the sensor node to measure its power consumption. There are two types of power analysis:

SPA – the power consumed by different cryptographic operations, and DPA – a type of analysis whereby the attacker

attempts to measure the consumed energy, including both cryptographic and non-cryptographic computation. [17]
A notable example comes from research conducted at the University of California, Berkeley, in 2018. Their thesis demonstrated the feasibility of power side-channel attacks on power grids. The research proposed that electromagnetic emissions from enterprise power grids could be exploited to autonomously develop access to and control power grid operations [17].

IV. SCADA

Supervisory Control and Data Acquisition (SCADA) systems form the foundation of control system architecture. These systems are designed to monitor and manage various processes, including distribution, manufacturing, oil and gas, pharmaceuticals, energy, and experimental facilities such as nuclear fusion [18][19]. SCADA systems are inherently complex, consisting of computers, network data transmission, and a graphical user interface for managing machines and processes at a high level.

When integrated with solar energy systems, SCADA introduces a range of multidimensional challenges involving cybersecurity, sustainability, and the shifting dynamics of renewable energy projects. As societies increasingly transition to renewable energy solutions, SCADA plays a critical role in ensuring a sustainable approach to managing these systems [23]

A. Software &Hardware Architecture

- In Industrial Control Systems (ICS), the SCADA hardware and software work together to monitor and control industrial operations. The SCADA software plays a key role in archiving data for analysis, offering a user-friendly interface, and analyzing data in real-time. PLCs and RTUs locally process data from sensors and other physical devices. Data transmission is supported by a robust communication infrastructure, while host computers running the SCADA software serve as the command center. This integrated system ensures operational efficiency and supports a dynamic industrial environment across various sectors.
- Figure 2 provides a detailed view of the SCADA system's operation through an Architecture Block Diagram [21], which organizes the devices and systems into five hierarchical levels:
-
- Level 0: Ground-level devices such as sensors and actuators interact directly with the physical environment, converting signals like temperature and light into electronic signals.
- Level 1: Programmable devices, such as PLCs (Programmable Logic Controllers) and RTUs (Remote Terminal Units), manage ground-level devices and connect to local area networks (LAN) and wide area networks (WAN) to enable efficient communication.
- Level 2: Computers connected to programmable devices oversee local control and facilitate the Human-Machine Interface (HMI).
- Level 3: These computers coordinate multiple plants, centralizing data for a unified system.
- Level 4: The central control level, where data analysis drives critical decisions, plays a crucial role in the decision-making process within the SCADA system [21].

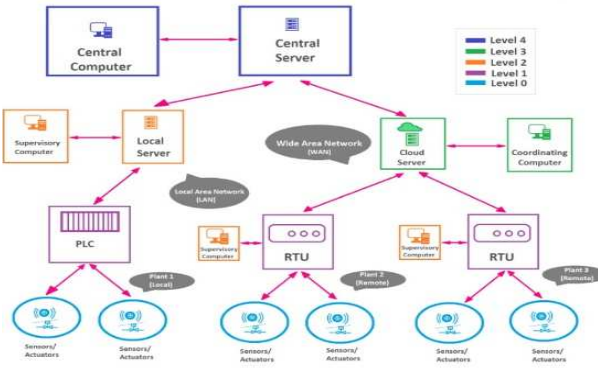

Fig. 2. SCADA System

B. Cybersecurity Challenges in Solar SCADA Systems

Integrating advanced software-development technologies into solar SCADA systems introduces significant security challenges [20]. As digital technologies continue to evolve, cyber risks such as unauthorized access, data breaches, and control system manipulation are becoming more prevalent. These systems are vulnerable to various types of attacks, including Denial of Service (DoS), replay attacks, cryptographic attacks, fragmentation attacks, and others [24].

A notable example of a successful cyberattack on SCADA systems occurred in 2015 in Ukraine, where spear phishing emails provided an entry point for attackers targeting the power grid. This attack indicates the cybersecurity vulnerabilities within SCADA systems, as hackers were able to access the network and cause nationwide power outages [25].

V. CONCLUSION

The shift toward renewable energy systems, particularly solar energy, not only represents a critical alternative to fossil fuels but also highlights humanity's commitment to a sustainable future. However, as these technologies evolve and integrate with SCADA architecture, they bring forth new and complex cybersecurity challenges. Vulnerabilities such as DDoS attacks, side-channel breaches, and system manipulation must be addressed to ensure the safety and reliability of these critical infrastructures. Real-world incidents, such as the 2015 Ukraine power grid cyberattack, serve as stark reminders of the urgent need to strengthen security protocols in renewable energy systems.

Addressing these risks requires a layered and comprehensive approach, combining cutting-edge technologies with a proactive focus on security. Tools such as machine learning algorithms, encryption protocols, and real-time monitoring systems are vital in protecting the integrity of solar SCADA systems. Equally important is the human factor—ensuring personnel are well-trained and fully equipped to anticipate and mitigate potential threats.

As the world transitions away from fossil fuels and embraces renewable energy, the emphasis on cybersecurity resilience will become increasingly important. By prioritizing security at every level of implementation, stakeholders can protect the essential infrastructures that power a sustainable future. The path forward requires not only technical innovation but also a collaborative commitment to addressing evolving threats, ensuring that the promise of renewable energy is realized safely and sustainably.

Acknowledgment

This research/project was funded by the Vice Presidency for Graduate Studies, Research and Business (GRB) at Dar Al-Hekma University, Jeddah. The authors, therefore, acknowledge with thanks GRB for technical and financial support.

References

[1] S. D. Riskiono, et al., “Implementation of the School Solar Panel System to Support the Availability of Electricity Supply at SDN 4 MESUJI TIMUR,” vol. 5, no. 1, pp. 34–34, Jan. 2021.

[2] R. Zakharchenko, “Photovoltaic Solar Panel for a Hybrid PV/Thermal System,” Solar Energy Materials and Solar Cells, vol. 82, no. 1-2, pp. 253–261, 2004, doi: 10.1016/j.solmat.2003.12.012.

[3] PT PLN, “Solar Levelized Cost of Energy Projection in Indonesia,” 2030.

[4] H. Dutta, et al., “Optimal Selection of Solar Tracking System in India: A Review,” 2030.

[5] R. A. Kemmerer, “Cybersecurity,” in 25th International Conference on Software Engineering, Proceedings., Portland, OR, USA, pp. 705-715, 2003, doi: 10.1109/ICSE.2003.1201257.

[6] J. White, “Cyber Threats and Cyber Security: National Security Issues, Policy and Strategies,” Global Security Studies, vol. 7, no. 4, 2016.

[7] N. D. Tuyen, et al., “A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power Systems Amid the Boom of Renewable Energy,” IEEE Access, vol. 10, pp. 35846–35875, 2022.

[8] A. Dagoumas, “Assessing the Impact of Cybersecurity Attacks on Power Systems,” Energies, vol. 12, no. 4, p. 725, 2019.

[9] H. Gunduz and D. Jayaweera, “Reliability Assessment of a Power System with Cyber-Physical Interactive Operation of Photovoltaic Systems,” International Journal of Electrical Power & Energy Systems, vol. 101, pp. 371–384, 2018.

[10] 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.

F. Harrou, B. Taghezouit, B. Bouyeddou, and Y. Sun, “Cybersecurity of Photovoltaic Systems: Challenges, Threats, and Mitigation Strategies: A Short Survey,” 2023.

[11] S. N. Vodapally and M. H. Ali, “Overview of Intelligent Inverters and Associated Cybersecurity Issues for a Grid-Connected Solar Photovoltaic System,” Energies, vol. 16, no. 16, p. 5904, 2023.

[12] F. A. Rahim, N. A. Ahmad, P. Magalingam, N. Jamil, Z. C. Cob, and L. Salahudin, “Cybersecurity Vulnerabilities in Smart Grids with Solar Photovoltaic: A Threat Modelling and Risk Assessment Approach,” International Journal of Sustainable Construction Engineering and Technology, vol. 14, no. 3, pp. 210–220, 2023.

[13] S. Ghazi and K. Ip, “The Effect of Weather Conditions on the Efficiency of PV Panels in the Southeast of UK,” Renewable Energy, Sep. 1, 2014. https://doi.org/10.1016/j.renene.2014.03.018.

[14] “Smart Grid Security: Attacks and Defense Techniques,” IET Research, 2022. Available at: https://ietresearch.onlinelibrary.wiley.com/doi/full/10.10

[15] R. Hallman, J. Bryan, G. Palavicini, J. Divita, and J. Romero-Mariona, "IoDDoS — The Internet of Distributed Denial of Service Attacks: A case study of the Mirai malware and IoT-based botnets," *U.S. Department of Defense, SPAWAR Systems Center Pacific*, San Diego, California, USA, 2017.

[16] T. Kuniyasu, T. Shigeyasu, and T. Shigeyasu, "Data Collecting System Based on CCN with Congestion Avoidance Routing on WSN," in *Proc. International Conference on Network-Based Information Systems*, 2018, pp. 311-316, doi: 10.1007/978-3-319-65521-5_24.

[17] A. Srivastava and A. Agarwal, “Emerging Technology IoT and OT: Overview, Security Threats, Attacks, and Countermeasures,” IJERT, vol. 10, no. 7, pp. 86–93, 2021.

[18] Loom Solar Private Limited, “Know about Important Facts and All Components of Solar Panels,” Medium, Jan. 12, 2018. Available: medium.com/@luminousestore/know-about-important-facts-and-all-components-of-solar-panels-19e28d69596f.

[19] A. Daneels and W. Salter, “What is SCADA?,” presented at the International Conference on Accelerator and Large Experimental Physics Control Systems, Trieste, Italy, 1999.

[20] A. Sami, “SCADA (Supervisory Control and Data Acquisition),” Technology Times, Jan. 14, 2019. Available: scada-supervisory-data-acquisition.pdf.

[21] V. M. Igure, S. A. Laughter, and R. D. Williams, “Security Issues in SCADA Networks,” Computers & Security, vol. 25, no. 7, 2006.

[22] M. N. Islam, “Simple Explanation About SCADA Architecture Block Diagram,” Voltage Lab, Feb. 2, 2022. Available: Simple Explanation About SCADA Architecture Block Diagram.

[23] C. Queiroz, A. Mahmood, and Z. Tari, “SCADA Sim—A Framework for Building SCADA Simulations,” IEEE Transactions on Smart Grid, vol. 2, no. 4, pp. 589–597, 2011, doi: 10.1109/TSG.2011.2162432.

[24] G. Yadav and K. Paul, “Architecture and Security of SCADA Systems: A Review,” International Journal of Critical Infrastructure Protection, vol. 34, p. 100433, 2021.

[25] N. Sayegh, A. Chehab, I. H. Elhajj, and A. Kayssi, “Internal Security Attacks on SCADA Systems,” in Third International Conference on Communications and Information Technology (ICCIT), Beirut, Lebanon, 2013, pp. 22–27, doi: 10.1109/ICCITechnology.2013.6579516.

[26] S. Ghosh and S. Sampalli, “A Survey of Security in SCADA Networks: Current Issues and Future Challenges,” IEEE Access, vol. 7, pp. 135812–135831, 2019, doi: 10.1109/ACCESS.2019.2926441.

[27] “What Is A Man-in-the-Middle (MitM) Attack?,” SentinelOne, Nov. 16, 2023. Available: https://www.sentinelone.com/cybersecurity-101/what-is-a-man-in-the-middle-mitm-attack-2/.

[28] N. D. Tuyen, et al., “A Comprehensive Review of Cybersecurity in Inverter-Based Smart Power System Amid the Boom of Renewable Energy,” IEEE Journals & Magazine, 2022. Available: https://ieeexplore.ieee.org/abstract/document/9745091.

[29] A. Srivastava and A. Agarwal, “Emerging Technology IoT and OT: Overview, Security Threats, Attacks, and Countermeasures,” ResearchGate, Jul. 7, 2021. Available: https://www.researchgate.net/profile/Aman-Srivastava26/publication/353233293_Emerging_Technology_IoT_and_OT_Overview_Security_Threats_Attacks_and_Countermeasures/links/60ee50fefb568a7098a9e180/Emerging-Technology-IoT-and-OT-Overview-Security-Threats-Attacks-and-Countermeasures.pdf.