Journal of Modern Technology
Vol. 01, No. 02, Dec 2024, pp. 106-120.

Homepage: https://review.journal-of-modern-technology.com

Strengthening Resilience: A Brief Review of Cybersecurity Challenges in IoT-Driven Smart Grids

Alireza Zabihi [1], Mohammad Parhamfar [2*], Maryam Khodadadi [3]
[1] PhD Scholar, Department of Electrical Engineering and Intelligence Systems, University of Coimbra, Portugal. E-mail: alireza.zabihi@student.uc.pt , ORCID: https://orcid.org/0000-0003-4800-5583

[2*] Independence Researcher and Entrepreneur, Iran, Website: www.parhamfar.com , E-mail: drparhamfar@gmail.com , ORCID: https://orcid.org/0000-0002-3442-8270

[3] Electronic Expert in Innovation Ultra Tech Gmbh, Iran. E-mail: khodadadimaryam999@gmail.com

Article Info

Article history:

Received: Oct 05, 2024
Revised: Nov 02, 2024
Accepted: Nov 10, 2024
First Online: Nov 25, 2024

Keywords:

Internet of Things (IoT)
Artificial intelligence (AI)
Smart grids,
Data analytics
Operational efficiency
cybersecurity

ABSTRACT

While efficiency and real-time monitoring have significantly improved with the integration of Internet of Things (IoT) devices into smart grids (SGs), new cybersecurity vulnerabilities have also been brought about by this process. This study examines the security risks associated with IoT-enabled SGs, emphasizing the possibility of cyberattacks that could interfere with grid operations or compromise sensitive data, as well as the use of IoT in certain industries, IoT standards, and the significance of individual protocols. These days, SG cybersecurity is essential to ensuring the global security of our energy networks. Presenting a thorough overview of the security issues, risks, and potential solutions for Internet of Things-based SGs is the aim of this paper. Our research focuses on network vulnerabilities, security needs, and cyber-attacks in SG applications to assess their effects on the network and provide guidance for future paths in cyber-security development.

Corresponding Author:

E-mail address: drparhamfar@gmail.com (Mohammad Parhamfar)

1. INTRODUCTION

Internet of thing (IoT) enabled smart grids (SGs) face major cybersecurity challenges that require advanced secure data transmission systems like blockchain to overcome [1]. The paper discussed cybersecurity challenges, threats, and solutions for IoT-enabled SGs [2]. SG systems are critical infrastructures that are vulnerable to cyber-attacks, which can have severe consequences such as national security deficits, disruption of public order, loss of life, or large-scale economic damage. - There is an ongoing research effort in industry, government, and academia to enhance the cybersecurity of SGs [3]. Ref [4] provided a security pyramidal method that is used in a digital substation use case to detect vulnerabilities and attacks in IoT-enabled SGs. Cyber-attacks pose a serious threat to IoT-SGs and can have far-reaching effects, including compromises to national security, disturbances of public order, fatalities, or substantial economic losses.

Cyber risks, including malware and other harmful activities, can be successfully detected and mitigated in SGs through the use of machine learning (ML) algorithms [5]. The integration of Internet of Things (IoT) devices and technologies within SGs may provide novel security and privacy obstacles. More work needs to be done to develop enhanced guidelines for communication between gadgets and SGs, even as technology advances to assure safe communication is under consideration [6]. Incorporating IoT equipment with SGs may improve surveillance, asset management, and smart decision-making throughout energy generation, transmission, distribution, and consumption [7]. In [8], the study seeks to present a comprehensive overview of security risks and approaches, as well as suggest potential research objectives for SG protection. Reference [9] offered a thorough analysis of the risk landscape with an emphasis on hazards and mitigation mechanisms for SG-IoT devices. IoT technologies can transform conventional power grids into more effective and smarter energy grids [10]. Providing the safe and dependable transfer of data across connected devices while preserving the resilience of the grid and averting cyberattacks or illegal access is a major concern in the application of IoT-SGs, while ref [11], mentioned implementing SGs can have major positive effects on the economy and society. In order to facilitate the modernization of the power system, concerns about cyber safety and confidentiality are brought about by improved communication and the emergence of SGs.

The objective of [12] is to provide recommendations for safety protocols and requirements, such as blockchain technology, to improve user identification, reliability of data, and privacy safeguards in the IoT. This will increase the safety and stability of device-to-device connections.
Difficulties in IoT standardization include protocols for communication, verification, cooperation, and stringent rules [13]. To enhance transaction safety, this paper evaluates blockchain innovation, confidentiality and security procedures, and efficiency requirements for mobile payment platforms. The fundamental goal of IoT is linking all devices to the network. Each object and device in the IoT have a sensor and is connected to an IoT infrastructure [14].

Several factors directly involved include routing information, storage, handling of increasing data volume, risk of obsolescence due to rapid technology advancements, lack of appropriate safety and security standards, and disregard for safety during development stages [15]. While references [16-18] focus on IoT-based cyber-physical systems, a crucial aspect of improving IoT-based cyber-physical systems for immediate detection is ensuring identification algorithms balance speed and accuracy, while minimizing computing costs to prevent delays and maintain system efficiency. Fig 1 demonstrates the application of IoT in various industries.

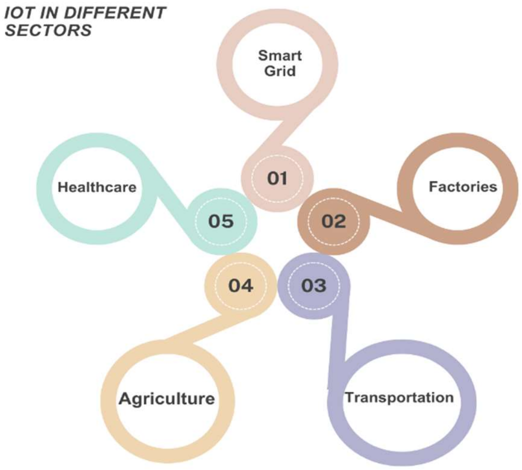

Fig 1. Application of IoT in some sectors.

Taking into account the interconnected elements discussed above, the goal of this article is to present a brief literature review of cybersecurity in IoT within smart grid systems in order to identify the primary research avenues, highlight knowledge gaps, and offer suggestions for addressing particular security issues and emerging trends. The article is organized around three primary questions in order to give a comprehensive summary of the subject.

- *What are the primary sources, publications, publishers, key words and how has scientific literature evolved recent years?* This first query focuses on the connections between the players engaged in the creation and dissemination of scientific research and the ways in which the cybersecurity space in IoT and smart grids has changed over time. Researchers looking for suitable sources or collaborating to locate pertinent content may find this information to be helpful. We used science mapping methodologies in the chosen database (ScienceDirect and webofscience) to gather this type of data.
- *What research avenues are the most well-known in the area?* Research opportunities in the areas of technology, operations, and protocols related to cybersecurity in the IoT are numerous. Consequently, future research orientations might be greatly influenced by closely examining the field into essential research streams. In this work, we used term clustering to accomplish this purpose.
- *What are present-day research developments and gaps in the literature, and how have studies changed over time?* The primary research areas for cybersecurity in IoT for SGs are covered in this question, which also identifies shortcomings and future work directions. To highlight the hottest subjects and areas in need of additional study, we performed a content assessment.

2. RESEARCH GROWTH AND FOCUS AREAS

The first part of this research is based on keywords in articles between 2020 and 2024. Based on fig 2, the visualization highlights the interconnected concepts of smart grids. It emphasizes the critical roles of cybersecurity, IoT, and deep learning in enhancing energy management and operational efficiency. The importance of interoperability and emerging technologies like blockchain and smart meters in addressing cybersecurity challenges and fostering a secure, efficient, and sustainable energy future is underscored.

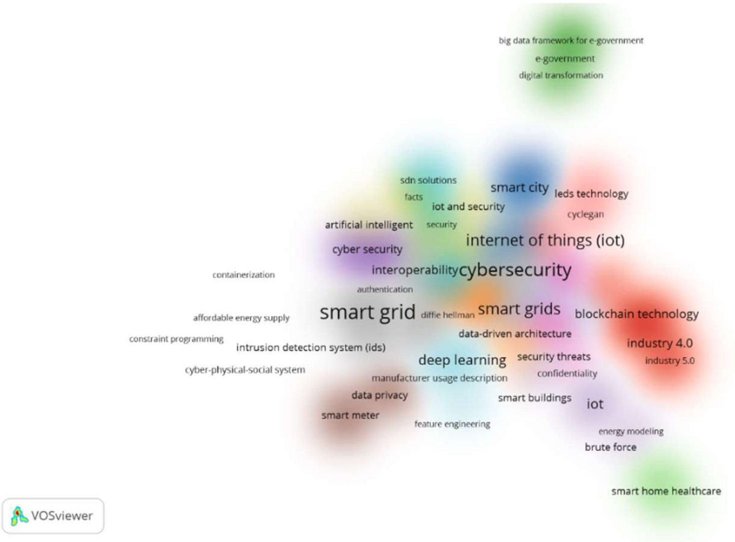

Fig 2. The significant keywords in this area between 2020 and 2024, based on ScienceDirect articles.

According to fig 3, utilizing data from Web of Science, the bar graph illustrates the publishing trends of various types of articles on cybersecurity in SGs from 2017 to 2024. Nearly 5,000 articles are being published each year, showing a peak in publications from 2018 to 2021. Nevertheless, there is a noticeable decrease in publications in 2023 and 2024, possibly indicating a shift in the field's concerns or research focus. This trend highlights the evolving nature of cybersecurity research in smart grids and underscores the crucial need to continuously explore new threats and defenses, ensuring the topic remains consistently vital throughout this period.

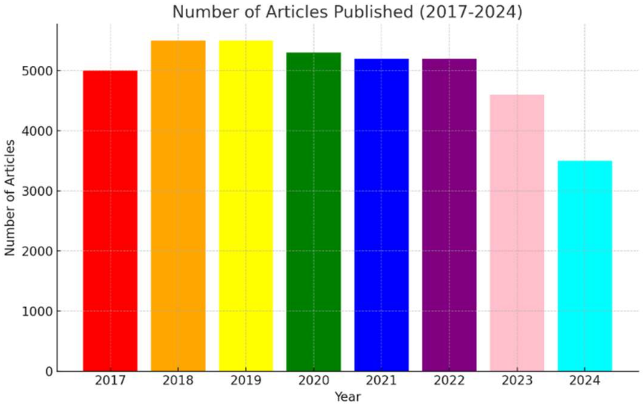

Fig. 3: The number of different types of articles and year publications in cybersecurity in SGs between 2017 and 2024 based on Web of Science (https://www.webofscience.com).

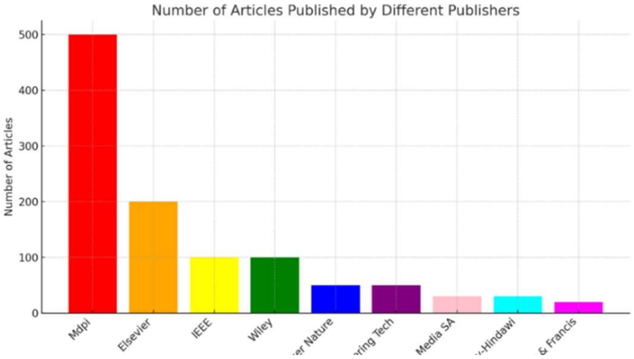

Fig. 4: The number of publications from some famous publishers in this area between 2017 and 2024 based on Web of Science (https://www.webofscience.com).

Fig 4 depicts the number of publications by various publishers. MDPI has the most articles, surpassing other publishers like Elsevier, IEEE, and Wiley by a large margin. Other publishers, such as Taylor & Francis and Frontiers Media, have significantly fewer publications in contrast.

3. CHALLENGES AND ISSUES

There are some challenges in the application of IoT in SGs, such as numerous SG network components exchanging massive amounts of data on a regular basis in order to optimize generation, consumption, and distribution [19-20], smart meters, phasor measurement units, plug-in hybrid electric vehicles, and remote terminal units [2]. Table 1 lists the challenges.

Table 1. Challenges and issues in the application of IoT.

Component	Challenges
Smart Meter	Vulnerable to jamming, wiretapping, stealthy attacks, replay attacks, and physical access, leading to incorrect billing, privacy violations, and unauthorized power use.
Phasor Measurement Units (PMU)	Susceptible to message delays, spoofing, and replay attacks, which can disrupt critical decision-making processes such as power cut-offs and event detection.
Plug-in Hybrid Electric Vehicle	Prone to pricing information manipulation and denial of service (DoS) attacks, leading to incorrect or lost pricing data for vehicle owners.
Remote Terminal Unit (RTU)	Can be hijacked through denial-of-service attacks, causing delays in real-time data exchange and leading to incorrect control center decisions.

4. SGS FRAMEWORK BASED ON IOT

The IoT in SGs enhances real-time monitoring and automation of power distribution systems by connecting key components such as power plants, renewable energy sources, transmission lines, and consumers. This interconnectivity allows for improved energy management, load balancing, and fault detection, while also enabling efficient integration of renewable energy sources. However, the increased connectivity introduces significant cybersecurity risks, including potential attacks on critical infrastructure components, necessitating robust security protocols to ensure the grid's reliability and safety. The objective of [53] is to examine the crucial role of IoT in enhancing the reliability and efficiency of smart grids through significant advancements and practical applications. On the other side, there are various energy resources [54]-[55], like photovoltaic (PV) [56]-[57], hydropower [58], but the integration of diverse energy resources, such as PV and hydropower, into IoT-driven smart grids is essential for strengthening resilience against cybersecurity challenges, as it enhances grid stability and efficiency while necessitating robust security measures to protect against potential threats to the interconnected systems [59]-[60]. Fig 5 illustrates an architecture of IoT-SGs.

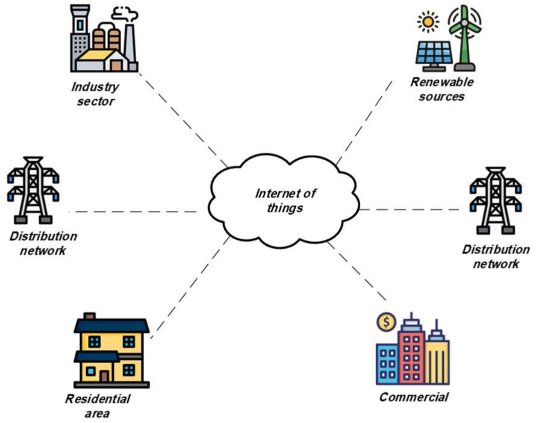

Fig. 5: IoT-based SGs structure.

5. COUNTERACTIONS FOR CYBERATTACKS

The use of software-based controls alone is no longer adequate to protect systems from a wide range of attack vectors. For computer systems to be managed and secured efficiently, a thorough understanding of hardware platforms is becoming more important. It is now crucial to not only comprehend how software program's function but also ensure the integrity of the entire processing chain, including lesser-known hardware elements like chipsets, input/output interfaces, and peripherals. Securing intelligent grid systems poses numerous challenges due to the wide distribution of assets across large geographic areas. Effective cyber defense strategies must protect all aspects of SG systems by incorporating a combination of proactive, real-time intrusion prevention and detection (IPS/IDS) systems, enhanced through ML and artificial intelligence (AI) [20], [2], [3]. Other key techniques include network segmentation, controlled wireless access, and robust authentication, authorization, and certification protocols. These defense solutions must be scalable, resilient, and adaptive, ensuring that they protect SG operations without disrupting legitimate functions.

To apply IoT in this domain, there are some advantages and challenges which are displayed in Fig 6. According to reference [12], this article reviewed the IoT Global Standard Initiative (IoT-GSI), so table 2 lists the standards and important aspects in each protocol.

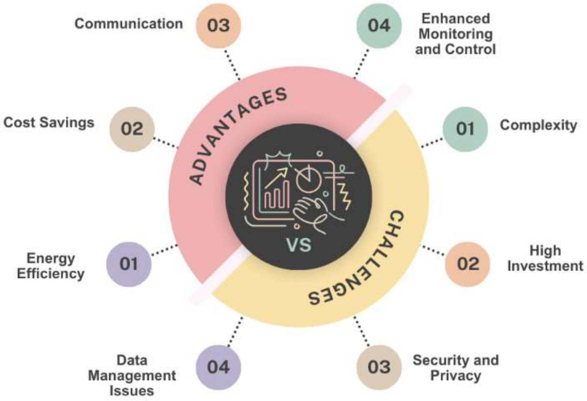

Fig. 6: Pros and cons of implementation of IoT in the domain.

Table 2. IoT standards.

Standard/Protocol	Description	Importance
ITU-T Y.2060 Recommendation	Defines the IoT reference model with four layers: application, service/application support, network, and device. It outlines general and specific security capabilities for these layers.	Provides a structured approach to IoT security by detailing capabilities at each layer, ensuring comprehensive protection of IoT systems.
ITU-T Y.2061 Recommendation	Focuses on Next Generation Networks (NGN) and Machine Oriented Communications (MOC), addressing security aspects like identity verification, authorization, data security, and device access.	Enhances the security of NGN and MOC environments, which are crucial for IoT communication and data exchange.
IETF RFC 4919, 4944	Proposes standards for IPv6 in limited systems using header compression and encapsulation. LoWPAN6 enables IPv6 deployment in low-power, resource-constrained devices.	Facilitates IPv6 communication in resource-limited environments, crucial for expanding IoT networks with efficient data transfer.

IETF RFC 6550	The RPL routing protocol for Low-Power and Lossy Networks (LLNs) with minimal security requirements and various security modes (insecure, pre-installed, authenticated).	Provides flexible routing for LLNs, balancing minimal security with effective data transmission, essential for IoT networks.
ONS (Object Naming Service)	A standard for object naming and routing requests in distributed systems, building on domain name system (DNS) with enhanced features for global object naming.	Ensures reliable and efficient routing of requests in distributed IoT systems, improving communication and object management
OASIS MQTT Standard	A lightweight publish/subscribe messaging protocol for IoT with stages for initialization, encryption, publication, and decryption. Provides confidentiality even if the broker is compromised.	Ideal for constrained environments due to its simplicity and lightweight design, crucial for secure and efficient IoT communication.
IEEE 1888.3 Standards	Security standards for Pervasive Green Control Networks (PGCN), covering data protection, integrity, confidentiality, authentication, and access control.	Ensures robust security for energy-efficient IoT networks, addressing data protection and access control in diverse applications.
Stream Control Transmission Protocol (SCTP)	A reliable transport layer protocol supporting message-based communication, multi-homing, and resistance to various attacks	Enhances communication reliability and security in IoT applications by providing message-oriented transfer and multi-path support
Trusted Computing Group (TCG)	Provides security mechanisms such as Trusted Platform Module (TPM), Remote Trust Update (RTU), and secure storage for IoT applications	Offers comprehensive security solutions for IoT devices, ensuring secure boot, firmware updates, and protection of sensitive data.
Mobile IP Protocol	Enables node mobility over IPv4 networks, allowing devices to maintain their IP address while moving between different networks.	Facilitates continuous connectivity for mobile devices, supporting applications that require seamless mobility and uninterrupted communication.
Host Identity Protocol (HIP)	Separates identity and location in communication, enabling mobility and multi-homing while enhancing security and privacy.	Supports seamless mobility and secure communication by separating identity from location, enhancing trust and reducing attack risks.

Another solution is applying blockchain to enhance security. Blockchain innovation strengthens safety through the development of a decentralized and secure record, guaranteeing that activities are transparent, accessible, and immune to unauthorized changes. One cutting-edge area of investigation in the realm of IoT security is the use of blockchain-based technology for creating intelligent agreements and safeguarding IoT-based devices [22]. Potential uses of this technology, which is mainly linked to cryptocurrencies like Bitcoin, are being investigated on the Internet of Things sector. By developing intelligent agreements, cutting complexity and costs, and enhancing safety and transparency, it can improve the effectiveness of mobile payment solutions and safeguard transactions [23]. However, the reference [24] mentioned that mobile payments can be enhanced in security and efficiency to safeguard against fraud and various security threats.

ITU-T Y.2060, IETF RFC 6550, and OASIS MQTT are just a few examples of the standards and protocols that offer vital frameworks for protecting IoT systems in SGs through reliable data transfer, device management, and effective communication. However, these shortcomings are frequently brought on by the demand for real-time reactions, limited device capabilities, and insufficient handling of emerging cyber threats. These protocols may have issues with scalability, latency, and complete defense against complex, persistent cyberattacks in the setting of SGs.

In addition to demonstrating the potential of blockchain for decentralized financial systems and financial inclusion, the study in [25] indicated how using a private Ethereum blockchain on Amazon Web Services (AWS) for an electronic payment system improved security and efficiency, decreased fraud risk, and facilitated faster, more transparent transactions. Comparably, research in [26] presented how well a secure electronic health framework built on blockchain may ensure tamper-proof health data and enhance security by means of permanent information hashing. Table 3 presents summary of relevant documents in the area.

Table 2. Summary of relevant documents in the area.

Ref	**Main Topic**	**Main Finding**	**Limitation**
[27]	IoT Cybersecurity	SGs are becoming more digitally connected, which creates a number of cybersecurity risks and concerns. In order to guarantee the worldwide security of energy infrastructures, cybersecurity is essential.	A key limitation in IoT cybersecurity for smart grids is the lack of standardized security protocols across diverse devices.
[28]	Intrusion Detection	The paper presents a novel intrusion detection system that analyzes the DNP3 protocol to detect malicious activity in IoT-based SGs.	The intrusion detection system must be improved in order to decrease false positives and increase the precision of classification, and the protocol.
[1]	SG Security	IoT-enabled smart grids must overcome significant cybersecurity obstacles with the use of cutting-edge, secure data transport technologies like blockchain.	Scalability issues.
[3]	SG Security	The paper analyzes cyber-security threats and potential solutions for IoT-enabled SGs.	Lack of comprehensive frameworks that integrate both cybersecurity measures and operational protocols
[29]	SG Security	Because of the special qualities of smart grid systems, cybersecurity is an essential concern for these systems.	It is difficult to implement universal security measures in smart grid networks due to variation, delay limits, bandwidth, and adaptability.
[4]	SG Security	It explains about how IoT is integrated into SG systems and examines the features and structures of SGs.	The emphasis on theoretical models has a drawback in that it might not adequately address real-world

			implementation issues in IoT-enabled SG scenarios.
[5]	SG Security	By offering a decentralized, impenetrable infrastructure for data storage and transactions, blockchain technology offers a viable way to improve the security and privacy of SGs.	A limitation is the intricacy of integrating ML, 5G, and blockchain technologies into current SG infrastructures; this may necessitate a large outlay of funds and specialized knowledge.
[7]	SG Security	The technology and architectures involved, as well as security considerations and applications, are reviewed in this article on IoT integration with SGs.	Risk associated with using the internet for tracking and handling IoT devices in SGs.
[9]	SG Security	In addition to offering a thorough grasp of threat vulnerabilities and mitigation strategies, the study makes recommendations for future research focuses on threats in SGs IoT.	Lack of standardized protocols for threat mitigation frameworks
[30]	SG Security	The convergence of cloud computing, IoT, and smart grids introduces new cybersecurity risks that need to be addressed.	Complexity of managing security across multiple platforms, as integrating cloud computing
[10]	SG Security	The study makes the case that cutting-edge technologies like blockchain, AI, and ML are required to get past the current obstacles and constraints facing IoT-enabled smart energy grid systems in order to increase their effectiveness, resilience, and dependability.	High implementation cost
[31]	Cybersecurity Challenges	This study examines the cybersecurity issues that arise when IoT and communication networks are integrated into SGs.	Vulnerability of communication protocols.
[32]	SG Security	To enable uniform security testing of smart grids without causing any disruptions to the actual grid, a digital twin's technique is suggested.	Complexity and high cost of developing and maintaining accurate digital representations of the physical systems, which can be resource-intensive and time-consuming.
[33]	IoT-enabled SGs	Bidirectionally energy transfer between service providers and customers is made possible by SGs.	Dependence on Connectivity

The cybersecurity challenges and innovations in IoT-enabled SGs are mentioned [27,33]. Reference [27] highlighted the increased digital connectivity of SGs and the resultant cybersecurity risks, emphasizing the lack of standardized security protocols as a major limitation, while [28] introduced a novel intrusion detection system focused on the DNP3 protocol but points out the need to reduce false positives for improved accuracy. The necessity for advanced data transport technologies, like blockchain, while noting scalability issues are discussed in [1]. Ref [3] analyzed the diverse cybersecurity threats and the absence of comprehensive frameworks integrating security measures with operational protocols. The unique characteristics of SGs that complicate the implementation of universal security measures are underscored [29].

The author of [4] examined the theoretical focus of IoT integration into SGs, suggesting that real-world implementation issues may not be adequately addressed. Although reference [5] presented blockchain as a solution for SG security but warns of the high costs and complexity in integrating new technologies. Ref [30] explored the cybersecurity risks posed by the convergence of cloud computing and IoT within SGs, stressing the challenges of managing security across multiple platforms. A digital twin technique for non-disruptive security testing, acknowledging the resource-intensive nature of maintaining accurate digital models is proposed in [32]. In [33], authors focused on bidirectionally energy transfer between service providers and customers is made possible by SGs. Potential research avenues are listed in table 4.

Table 4. Potential research avenues.

Topic	Research Avenue
Intrusion Detection Systems	Develop advanced algorithms for real-time threat detection.
Blockchain Integration	Explore blockchain applications for secure data transactions in smart grids.
ML Applications	Investigate ML techniques for anomaly detection in smart grid environments.
Security Protocols	Create frameworks for assessing cybersecurity risks in smart grid infrastructures.
Privacy Preservation	Research methods for ensuring user privacy in smart grid data management.
Incident Response Strategies	Develop comprehensive incident response plans tailored for smart grid environments.
Cloud Security in SGs	Examine cybersecurity problems and potential remedies for merging cloud computing and SGs.
Resilience and Recovery	Investigate techniques for increasing resilience and recovering from threats in SGs.
IoT Device Management	Research effective management and security measures for IoT devices in SG systems.

The primary purpose of the research is to improve SG cybersecurity by investigating communication protocols and standards, with the problem being the grids' sensitivity to IT-related assaults due to their reliance on Information and Communication Technology (ICT) [34]. By combining sophisticated information acquisition, algorithms for forecasting, AI diagnostics, and optimal power flow efficiency, the proposed framework aims to develop a comprehensive energy management system for smart grids that improves security, efficiency, and flexibility [35]. It also addresses real-world challenges with implementation like infrastructure integration and training requirements. Achieving the integration of these latest developments with the current infrastructure is a major problem that can call for considerable money and particular training. In order to achieve secure and effective load management in IoT networks for quickly urbanizing smart cities, the main objective of [35] is to develop an AI-enhanced Multi-Stage Learning-to-Learning (MSLL) approach using the MMS transformer model. This will improve predicted load accuracy while addressing issues related to privacy and security. In this context, efficiently integrating various operational and societal factors is crucial for managing the complex and rapidly changing information that characterizes smart city networks.

The goal of [36] is to enhance the stability prediction of IoT-driven SGs using advanced ML models, with the challenge being the need for effective hyperparameter optimization to achieve superior predictive accuracy and reliability. Another aspect is agriculture, reference [37] focused in this area, and it also explored the difficulties with multi-class classification and feature dimensions, the suggested intelligent Intrusion Detection System seeks to enhance agricultural data security by detecting cyberattacks on the Internet of Agriculture Things using cutting-edge techniques like Dynamic Kernel Partial Least Squares (DKPLS) and Kernel Extreme Learning Machine (KELM). The goal of the suggested structure in [38] is to balance safety with excellence of service while autonomously mitigating dangers in Cyber Physical Systems via self-adapting safeguards. Nevertheless, one drawback is that the model's efficacy may differ depending on the intricacy and variability of the system's surroundings and facilities modifications. In [39], authors offered a thorough overview of ML and data analytics applications to address SG issues and improve consumer confidence, data security, and overall electrical system reliability. A constraint exists in that the efficacy of the suggested remedies can rely on the distinct obstacles and diverse settings encountered by distinct utilities, hence complicating the extrapolation of conclusions to the whole power industry. Although [40] introduced a significant aspect and topic in security, while the suggested approach has a drawback in that real-time performance in dynamic SG systems may be impacted by its heavy reliance on complicated deep learning (DL) models and blockchain technology, which could result in considerable processing complexity and delays. Nonetheless, a significant constraint of [41] is its extensive depiction of cybersecurity alternatives and the contrasting evaluation of security methodologies for intelligent grid systems.

The main goal of [42] is to investigate cybersecurity threats to smart home environments and develop an IoT-based intrusion detection and prevention system to enhance the security of home automation devices, however the limitation of the protocols mentioned, such as Hypertext Transfer Protocol (HTTP), Secure Shell(SSH), Telnet, and File Transfer Protocol (FTP), is that they can be vulnerable to brute force attacks and other exploits due to weak password policies and inadequate security measures, making them susceptible to unauthorized access and data breaches. Tightiz et al. [43] investigated the applicability of the metaverse via a variety of scenarios and incorporate it into the design of SGs. Given the complexity of both ecosystems, one issue of this connection is guaranteeing the safety and confidentiality of data exchanged between SGs and the metaverse. Ref [44] focused on application of IoT in control and monitoring, while one of the limitations in this field can be scalability and interoperability. The complexity of merging disparate devices, sensors, and systems from various vendors rises with the amount and variety of IoT devices. The fact that these devices frequently adhere to disparate communication protocols and standards makes it difficult to guarantee smooth system compatibility. This may reduce the efficacy of control and tracking, resulting in ineffectiveness, sluggish execution of data, or insufficient insight into the current condition of the grid.

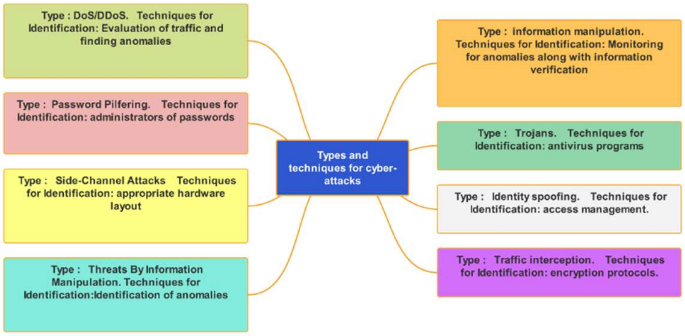
Type : DoS/DDoS. Techniques for Identification: Evaluation of traffic and finding anomalies
Type : Password Pilfering. Techniques for Identification: administrators of passwords
Type : Side-Channel Attacks Techniques for Identification: appropriate hardware layout
Type : Threats By Information Manipulation. Techniques for Identification:Identification of anomalies
Types and techniques for cyber-attacks
Type : information manipulation. Techniques for Identification: Monitoring for anomalies along with information verification
Type : Trojans. Techniques for Identification: antivirus programs
Type : Identity spoofing. Techniques for Identification: access management.
Type : Traffic interception. Techniques for Identification: encryption protocols.

Fig 7. Types, and identification approach for Cyber-attacks.

There are some references which concentrated on cybersecurity, like [45-52]. According to Fig 7, it outlines various types and techniques for identifying cyber-attacks. Key types including Denial of Service or Distributed Denial of Service (DoS/DDoS) attacks [45], which involve evaluating traffic to find anomalies, and password pilfering [46], which targets password administrators. Additionally, ide-Channel attacks [47] exploit hardware layouts, while Information Manipulation [48, 49] focuses on monitoring anomalies through verification processes, trojans [50], other notable techniques include identity spoofing [51] for access management and traffic interception [52] emphasizing the importance of encryption protocols.

6. CONCLUSION

The generation, delivery, and consumption of electricity are all made more efficient by the SG by communication technology. This system relies heavily on the IoT, which makes it possible for a wide range of smart devices--from end users to generating plants--to be connected. Nevertheless, there are a number of security flaws brought about by the IoT's connection with the SG. Numerous potential assaults have been found by research, including ones that might even cut off customers' access to energy and cause billing system disruptions, or identity theft via smart meters. These security flaws demonstrate the necessity of strong security measures to safeguard the infrastructure of the IoT-enabled SG. Security is a critical concern due to the integration of communication technologies, which introduces potential vulnerabilities. So, this review article can help researchers to find the research gaps, approaches in detection cyberattacks, limitation in recent studies, protocols, research avenue in this area.

To ensure the effective implementation and integration of IoT devices within the SG, it is essential to address these security challenges comprehensively. This includes developing and deploying advanced security measures to protect against identity theft, replay attacks, and other threats that could disrupt SG's operation and customer service.

DECLARATIONS

Conflict of Interest: The authors declare that there is no conflict of interests.

Funding: This research received no external funding.

Availability of data and materials: No data is available in this article.

Publisher's note: The Journal and Publisher remain neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

[1] Goudarzi, Arman, Farzad Ghayoor, Muhammad Waseem, Shah Fahad, and Issa Traore. "A survey on IoT-enabled smart grids: emerging, applications, challenges, and outlook." *Energies* 15, no. 19 (2022): 6984. DOI: https://doi.org/10.3390/en15196984

[2] Ouaissa, Mariya, and Mariyam Ouaissa. "Cyber security issues for iot based smart grid infrastructure." In *IOP Conference Series: Materials Science and Engineering*, vol. 937, no. 1, p. 012001. IOP Publishing, 2020. DOI: 10.1088/1757-899X/937/1/012001

[3] Gunduz, Muhammed Zekeriya, and Resul Das. "Cyber-security on smart grid: Threats and potential solutions." *Computer networks* 169 (2020): 107094. DOI: https://doi.org/10.1016/j.comnet.2019.107094

[4] Abraham, Doney, Sule Yildirim Yayilgan, Mohamed Abomhara, Alemayehu Gebremedhin, and Fisnik Dalipi. "Security and Privacy Issues in IoT-Based Smart Grids: A Case Study in a Digital Substation." *Holistic Approach for Decision Making Towards Designing Smart Cities* (2021): 57-74. DOI: https://doi.org/10.1007/978-3-030-85566-6_4

[5] Abraham, Doney, Sule Yildirim Yayilgan, Mohamed Abomhara, Alemayehu Gebremedhin, and Fisnik Dalipi. "Security and Privacy Issues in IoT-Based Smart Grids: A Case Study in a Digital Substation." *Holistic Approach for Decision Making Towards Designing Smart Cities* (2021): 57-74. DOI: https://doi.org/10.1007/978-3-030-85566-6_4

[6] Dalipi, Fisnik, and Sule Yildirim Yayilgan. "Security and privacy considerations for IoT application on smart grids: Survey and research challenges." In *2016 IEEE 4th international conference on future internet of things and cloud workshops (FiCloudW)*, pp. 63-68. IEEE, 2016. DOI: 10.1109/W-FiCloud.2016.28

[7] Kirmani, Sheeraz, Abdul Mazid, Irfan Ahmad Khan, and Manaullah Abid. "A survey on IoT-enabled smart grids: technologies, architectures, applications, and challenges." *Sustainability* 15, no. 1 (2022): 717. DOI: https://doi.org/10.3390/su15010717

[8] Wang, Wenye, and Zhuo Lu. "Cyber security in the smart grid: Survey and challenges." *Computer networks* 57, no. 5 (2013): 1344-1371. DOI: https://doi.org/10.1016/j.comnet.2012.12.017

[9] Kumar, Ranjit, Rahul Gupta, and Sunil Kumar. "IOT security on Smart Grid: threats and mitigation frameworks." *ECS Transactions* 107, no. 1 (2022): 14623. DOI: 10.1149/10701.14623ecst

[10] Abir, SM Abu Adnan, Adnan Anwar, Jinho Choi, and A. S. M. Kayes. "IoT-enabled smart energy grid: Applications and challenges." *IEEE access* 9 (2021): 50961-50981. DOI: 10.1109/ACCESS.2021.3067331

[11] Liu, Jing, Yang Xiao, Shuhui Li, Wei Liang, and CL Philip Chen. "Cyber security and privacy issues in smart grids." *IEEE Communications surveys & tutorials* 14, no. 4 (2012): 981-997. DOI: 10.1109/SURV.2011.122111.00145

[12] Shahinzadeh, Ghazaleh, Hossein Shahinzadeh, and Sudeep Tanwar. "Security and Privacy Issues in the Internet of Things: A Comprehensive Survey of Protocols, Standards, and the Revolutionary Role of Blockchain." In *2024 8th International Conference on Smart Cities, Internet of Things and Applications (SCIoT)*, pp. 59-67. IEEE, 2024. DOI: 10.1109/SCIoT62588.2024.10570131

[13] Abed, Ali Kamil, and Angesh Anupam. "Review of security issues in Internet of Things and artificial intelligence-driven solutions." *Security and Privacy* 6, no. 3 (2023): e285. DOI: https://doi.org/10.1002/spy2.285

[14] Available online: https://www.ibm.com/blogs/internet-of-things/what-is-the-iot/. "What is the Internet of Things? " (accessed on 20 May 2024).

[15] Kimani, Kenneth, Vitalice Oduol, and Kibet Langat. "Cyber security challenges for IoT-based smart grid networks." *International journal of critical infrastructure protection* 25 (2019): 36-49. DOI: https://doi.org/10.1016/j.ijcip.2019.01.001

[16] Khan, Samee Ullah, Ijaz Ul Haq, Noman Khan, Amin Ullah, Khan Muhammad, Huiling Chen, Sung Wook Baik, and Victor Hugo C. de Albuquerque. "Efficient Person Reidentification for IoT-Assisted Cyber–Physical Systems." *IEEE Internet of Things Journal* 10, no. 21 (2023): 18695-18707. DOI: 10.1109/JIOT.2023.3259343

[17] Hamdan, Salam, Sufyan Almajali, Moussa Ayyash, Haythem Bany Salameh, and Yaser Jararweh. "An intelligent edge-enabled distributed multi-task learning architecture for large-scale IoT-based cyber–physical systems." *Simulation Modelling Practice and Theory* 122 (2023): 102685. DOI: https://doi.org/10.1016/j.simpat.2022.102685

[18] Javed, Safdar Hussain, Maaz Bin Ahmad, Muhammad Asif, Waseem Akram, Khalid Mahmood, Ashok Kumar Das, and Sachin Shetty. "APT adversarial defence mechanism for industrial IoT enabled cyber-physical system." *IEEE Access* 11 (2023): 74000-74020. DOI: 10.1109/ACCESS.2023.3291599

[19] Bashir, Channi, "IoT-Based Smart Grid Security Challenges," in Renewable Energy Optimization, Planning and Control: Proceedings of ICRTE (2022):261-273. 2023.

[20] Wang, Wenye, and Zhuo Lu. "Cyber security in the smart grid: Survey and challenges." *Computer networks* 57, no. 5 (2013): 1344-1371.DOI: https://doi.org/10.1016/j.comnet.2012.12.017

[21] Bekara, Chakib. "Security issues and challenges for the IoT-based smart grid." *Procedia Computer Science* 34 (2014): 532-537. DOI: https://doi.org/10.1016/j.procs.2014.07.064

[22] Moradi, Jalal, Hossein Shahinzadeh, Hamed Nafisi, Gevork B. Gharehpetian, and Mahdi Shaneh. "Blockchain, a sustainable solution for cybersecurity using cryptocurrency for financial transactions in smart grids." In *2019 24th Electrical Power Distribution Conference (EPDC)*, pp. 47-53. IEEE, 2019. DOI: 10.1109/EPDC.2019.8903713

[23] Zanjani, S. Mohammadali, Hossein Shahinzadeh, Jalal Moradi, Zohreh Rezaei, Bahareh Kaviani-Baghbaderani, and Sudeep Tanwar. "Securing the internet of things via blockchain-aided smart contracts." In *2022 13th International Conference on Information and Knowledge Technology (IKT)*, pp. 1-8. IEEE, 2022. DOI: 10.1109/IKT57960.2022.10039016

[24] Surekha, Nayak, Rangasamy Sangeetha, Chellasamy Aarthy, Rajamohan Kavitha, and R. Anuradha. "Leveraging blockchain technology for internet of things powered banking sector." In *Blockchain based Internet of Things*, pp. 181-207. Singapore: Springer Singapore, 2022. DOI: https://doi.org/10.1007/978-981-16-9260-4_8

[25] Aliyu, Ahmed Abubakar, and Jinshuo Liu. "Blockchain-Based Smart Farm Security Framework for the Internet of Things." *Sensors* 23, no. 18 (2023): 7992. DOI: https://doi.org/10.3390/s23187992

[26] Gorelova, Anastasiia, and Santiago Meliá. "Applying a healthcare web of things framework for infertility treatments." In *International Conference on Web Engineering*, pp. 426-431. Cham: Springer International Publishing, 2022. DOI: https://doi.org/10.1007/978-3-031-09917-5_30

[27] Ouaissa, Mariya, and Mariyam Ouaissa. "Cyber security issues for iot based smart grid infrastructure." In *IOP Conference Series: Materials Science and Engineering*, vol. 937, no. 1, p. 012001. IOP Publishing, 2020. DOI: 10.1088/1757-899X/937/1/012001

[28] Yin, Xiao Chun, Zeng Guang Liu, Lewis Nkenyereye, and Bruce Ndibanje. "Toward an applied cyber security solution in IoT-based smart grids: An intrusion detection system approach." *Sensors* 19, no. 22 (2019): 4952. DOI: https://doi.org/10.3390/s19224952

[29] Shapsough, Salsabeel, Fatma Qatan, Raafat Aburukba, Fadi Aloul, and A. R. Al Ali. "Smart grid cyber security: Challenges and solutions." In *2015 international conference on smart grid and clean energy technologies (ICSGCE)*, pp. 170-175. IEEE, 2015. DOI: 10.1109/ICSGCE.2015.7454291

[30] Mavroeidakos, Theodoros, and Vasilis Chaldeakis. "Threat landscape of next generation IoT-enabled smart grids." In *Artificial Intelligence Applications and Innovations. AIAI 2020 IFIP WG 12.5 International Workshops: MHDW 2020 and 5G-PINE 2020, Neos Marmaras, Greece, June 5–7, 2020, Proceedings 16*, pp. 116-127. Springer International Publishing, 2020. DOI: https://doi.org/10.1007/978-3-030-49190-1_11

[31] Ustun, Taha Selim, and SM Suhail Hussain. "A review of cybersecurity issues in smartgrid communication networks." In *2019 International Conference on Power Electronics, Control and Automation (ICPECA)*, pp. 1-6. IEEE, 2019. DOI: 10.1109/ICPECA47973.2019.8975629

[32] Atalay, Manolya, and Pelin Angin. "A digital twins approach to smart grid security testing and standardization." In *2020 IEEE International Workshop on Metrology for Industry 4.0 & IoT*, pp. 435-440. IEEE, 2020. DOI: 10.1109/MetroInd4.0IoT48571.2020.9138264

[33] Saleem, Yasir, Noel Crespi, Mubashir Husain Rehmani, and Rebecca Copeland. "Internet of things-aided smart grid: technologies, architectures, applications, prototypes, and future research directions." *IEEE Access* 7 (2019): 62962-63003. DOI: 10.1109/ACCESS.2019.2913984

[34] Muhammad, Mamdouh, Abdullah S. Alshra‘a, and Reinhard German. "Survey of Cybersecurity in Smart Grids Protocols and Datasets." *Procedia Computer Science* 241 (2024): 365-372. DOI: https://doi.org/10.1016/j.procs.2024.08.049

[35] El Maghraoui, Adila, Hicham El Hadraoui, Younes Ledmaoui, Nabil El Bazi, Nasr Guennouni, and Ahmed Chebak. "Revolutionizing smart grid-ready management systems: A holistic framework for optimal grid reliability." *Sustainable Energy, Grids and Networks* (2024): 101452. DOI: https://doi.org/10.1016/j.segan.2024.101452

[36] Alkanhel, Reem Ibrahim, El-Sayed M. El-Kenawy, Marwa M. Eid, Laith Abualigah, and Mohammed A. Saeed. "Optimizing IoT-driven smart grid stability prediction with dipper throated optimization algorithm for gradient boosting hyperparameters." *Energy Reports* 12 (2024): 305-320. DOI: https://doi.org/10.1016/j.egyr.2024.06.034

[37] Zidi, Kamel, Khaoula Ben Abdellafou, Ahamed Aljuhani, Okba Taouali, and Mohamed Faouzi Harkat. "Novel intrusion detection system based on a downsized kernel method for cybersecurity in smart agriculture." *Engineering Applications of Artificial Intelligence* 133 (2024): 108579. DOI: https://doi.org/10.1016/j.engappai.2024.108579

[38] Chehida, Salim, Eric Rutten, Guillaume Giraud, and Stéphane Mocanu. "A model-based approach for self-adaptive security in CPS: Application to smart grids." *Journal of Systems Architecture* 150 (2024): 103118. DOI: https://doi.org/10.1016/j.sysarc.2024.103118

[39] Mitra, Somalee, Basab Chakraborty, and Pabitra Mitra. "Smart meter data analytics applications for secure, reliable and robust grid system: Survey and future directions." *Energy* 289 (2024): 129920. DOI: https://doi.org/10.1016/j.energy.2023.129920

[40] Kumar, Prabhat, Randhir Kumar, Ahamed Aljuhani, Danish Javeed, Alireza Jolfaei, and AKM Najmul Islam. "Digital twin-driven SDN for smart grid: A deep learning integrated blockchain for cybersecurity." *Solar Energy* 263 (2023): 111921. DOI: https://doi.org/10.1016/j.solener.2023.111921

[41] Paul, Bishowjit, Auvizit Sarker, Sarafat Hussain Abhi, Sajal Kumar Das, Md Firoj Ali, Md Manirul Islam, Md Robiul Islam et al. "Potential smart grid vulnerabilities to cyber attacks: Current threats and existing mitigation strategies." *Heliyon* 10, no. 19 (2024). DOI: 10.1016/j.heliyon.2024.e37980

[42] Bhardwaj, Akashdeep, Salil Bharany, Anas W. Abulfaraj, Ashraf Osman Ibrahim, and Wamda Nagmeldin. "Fortifying home IoT security: A framework for comprehensive examination of vulnerabilities and intrusion detection strategies for smart cities." *Egyptian Informatics Journal* 25 (2024): 100443. DOI: https://doi.org/10.1016/j.eij.2024.100443

[43] Tightiz, Lilia, L. Minh Dang, Sanjeevikumar Padmanaban, and Kyeon Hur. "Metaverse-driven smart grid architecture." *Energy Reports* 12 (2024): 2014-2025. DOI: https://doi.org/10.1016/j.egyr.2024.08.027

[44] Alomar, Madani Abdu. "An IOT based smart grid system for advanced cooperative transmission and communication." *Physical Communication* 58 (2023): 102069. DOI: https://doi.org/10.1016/j.phycom.2023.102069

[45] Cai, Tianyang, Tao Jia, Sridhar Adepu, Yuqi Li, and Zheng Yang. "ADAM: an adaptive DDoS attack mitigation scheme in software-defined cyber-physical system." *IEEE Transactions on Industrial Informatics* 19, no. 6 (2023): 7802-7813. DOI: 10.1109/TII.2023.3240586

[46] Khan, Rafiullah, Peter Maynard, Kieran McLaughlin, David Laverty, and Sakir Sezer. "Threat analysis of blackenergy malware for synchrophasor based real-time control and monitoring in smart grid." In *4th International Symposium for ICS & SCADA Cyber Security Research 2016*, pp. 53-63. BCS, 2016. DOI: 10.14236/ewic/ICS2016.7

[47] Zhang, Yicheng, Carter Slocum, Jiasi Chen, and Nael Abu-Ghazaleh. "It's all in your head (set): Side-channel attacks on {AR/VR} systems." In *32nd USENIX Security Symposium (USENIX Security 23)*, pp. 3979-3996. 2023. DOI:

[48] Su, Junhong, Junhao Chu, Qifeng Yu, and Huilin Jiang. "Seventh Symposium on Novel Photoelectronic Detection Technology and Applications." In *Proc. of SPIE Vol*, vol. 11763, pp. 1176301-1. 2021.

[49] Rajasekaran, James Ranjith Kumar, Balasubramaniam Natarajan, and Anil Pahwa. "Modified Matrix Completion-Based Detection of Stealthy Data Manipulation Attacks in Low Observable Distribution Systems." *IEEE Transactions on Smart Grid* 14, no. 6 (2023): 4851-4862. DOI: 10.1109/TSG.2023.3266834

[50] Liu, Mengxiang, Fei Teng, Zhenyong Zhang, Pudong Ge, Mingyang Sun, Ruilong Deng, Peng Cheng, and Jiming Chen. "Enhancing cyber-resiliency of DER-based smart grid: A survey." *IEEE Transactions on Smart Grid* (2024). DOI: 10.1109/TSG.2024.3373008

[51] Ramadan, Mohammed, Ghada Elbez, and Veit Hagenmeyer. "Verifiable Certificateless Signcryption Scheme for Smart Grids." In *2023 7th International Conference on System Reliability and Safety (ICSRS)*, pp. 181-189. IEEE, 2023. DOI: 10.1109/ICSRS59833.2023.10381069

[52] Gunduz, Muhammed Zekeriya, and Resul Das. "Cyber-security on smart grid: Threats and potential solutions." *Computer networks* 169 (2020): 107094. DOI:

[53] Zabihi, Alireza, and Amirhossein Shafiei Alavijeh. "Enhancing Reliability and Efficiency in Power Systems: The Role of IoT in Optimizing Smart Grids."

[54] Zabihia, Alireza, and Mohammad Parhamfar. "Empowering the grid: toward the integration of electric vehicles and renewable energy in power systems." *International Journal of Energy Security and Sustainable Energy* 2, no. 1 (2024): 1-14.

[55] Peng, Li, Alireza Zabihi, Mahdi Azimian, Hadis Shirvani, and Farhad Shahnia. "Developing a robust expansion planning approach for transmission networks and privately-owned renewable sources." *IEEE access* 11 (2022): 76046-76058. DOI: 10.1109/ACCESS.2022.3226695

[56] Zabihi, Alireza, Mohammad Parhamfar, SSSR Sarathbabu Duvvuri, and Milad Abtahi. "Increase power output and radiation in photovoltaic systems by installing mirrors." *Measurement: Sensors* 31 (2024): 100946. DOI: https://doi.org/10.1016/j.measen.2023.100946

[57] Zabihi, Alireza, Iman Sadeghkhani, and Bahador Fani. "A partial shading detection algorithm for photovoltaic generation systems." *Journal of Solar Energy Research* 6, no. 1 (2021): 678-687. DOI: 10.22059/jser.2021.310010.1171

[58] Sree, P. Bhavya, K. Balaji, Naveen Banoth, and Mohammad Parhamfar. "A Light Weight Mobile Net SSD Algorithm based dentification and Detection of Multiple Defects in Ceramic Insulators." *Journal of Modern Technology* (2024): 59-74.

[59] Patthi, Sridhar, VB Murali Krishna, Lokeshwar Reddy, and Sairaj Arandhakar. "Photovoltaic String Fault Optimization Using Multi-Layer Neural Network Technique." *Results in Engineering* (2024): 102299. DOI: https://doi.org/10.1016/j.rineng.2024.102299

[60] Bhatraj, Anudeep, Elad Salomons, and Mashor Housh. "An optimization model for simultaneous design and operation of renewable energy microgrids integrated with water supply systems." *Applied Energy* 361 (2024): 122879. DOI: https://doi.org/10.1016/j.apenergy.2024.122879