IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES

ISSNPRINT23191775Online23207876

Research paper

UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

Securing the Smart Grid with IoT-Based Energy Monitoring and Challenges of Data Security

Rakhi Kamra[1], Annu Dagar[2], Dr. Pankaj Gupta[3]

[1]Assistant Professor, Department of Electrical and Electronics Engineering, Maharaja Surajmal Institute of Technology, New Delhi, Delhi, Pin Code: 110058, India.
[2]Assistant Professor, Department of Electrical and Electronics Engineering, Maharaja Surajmal Institute of Technology, Indira Gandhi Delhi Technical University for Women, New Delhi, Delhi, Pin Code: 110058, India.
[3]Assistant Professor, Department of Electronics and Communication Engineering, Indira Gandhi Delhi Technical University for Women, New Delhi, Delhi, Pin Code: 110006, India.
E-mail: rakhikamra@msit.in

Abstract

The development of smart grids, supported by IoT technologies, is an epochal moment in the population's lives: this time brings new possibilities for energy control and management, which is characterized by increased efficiency, reliability, and integration of renewable energy sources. But masses of IoT in smart grid framework present vast information security issues such as issues to information protection, vulnerability to cyber assaults, and worries regarding information honesty. This paper focuses on the importance of IoT-based energy monitoring systems in smart grids, as stressing their cost and efficacy in managing power flows and boosting grid reliability and renewable integration. It methodically assesses the vulnerabilities of such interdependent systems related to data security, along with the technological and regulatory difficulties associated with protecting sensitive materials and ensuring the resilience of such systems in the face of cyber threats. Based on the analysis of the contemporary literature and case studies, this research paper assesses advanced encryption technologies, strong authentication procedures, privacy-preserving methods, and the impact of emerging technologies such as blockchain in developing smart grids' security posture. This reality is highlighted by the study's findings, which underline holistic security in the face of technical solutions, regulatory frameworks and industry practices working to manage risks and secure smart grids from emerging cyber threats. The paper provides a valuable contribution to the ever-evolving discussion surrounding security on the smart grid by providing a host of information and recommendations for stakeholders to understand the challenges that characterize IoT technology applications in energy systems governance and data protection.

Keywords: *Smart Grids, Internet of Things (IoT), Energy Monitoring, Data Security, Cybersecurity in Energy Systems, IoT Security.*

ISSNPRINT23191775Online23207876

Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

1. Introduction to Smart Grids and IoT

Smart grids mark a breakthrough in energy systems by combining modern information and communication technology with conventional electrical networks, thus resulting in a more efficient, reliable, and environmentally-friendly power supply network. In contrast to traditional networks which are linear and passive, smart grids have dynamic nature in addition to active operations that enable them to handle two-way energy flows and simultaneous data transfers[1,2]. This up to date infrastructure supports latest technologies in terms of communication and control that facilitates the process of generation, transmission and consumption of electricity.

The value of smart grids is how the principle itself can fix some of the toughest issues hindering traditional energy systems, from ageing infrastructure to rising demand, energy wastefulness, and renewable integration. Digital technology is integrated into smart grids that increase reliability on the grid due to better detection of faults and the autonomic restoration properties[3]. They also improve efficiency through efforts to reduce energy losses and maximize the use of assets. In addition to smart grids contribute to sustainability by supporting integration of renewable energy sources, like wind and solar power, that are also connecting electrical automobiles[4,5]. At the center of the evolution revolution that is smart grid lies the Internet of Things (IoT) which unlocks a level of connectivity and intelligence never before achieved[6]. The IoT devices and sensors are incorporated with the grid from generation sources up to the end users premises that collects and transmits the data in real time. This omnipresent system of linked devices allows utilities and grid operators to have never seen before level of visibility and control over the energy system.

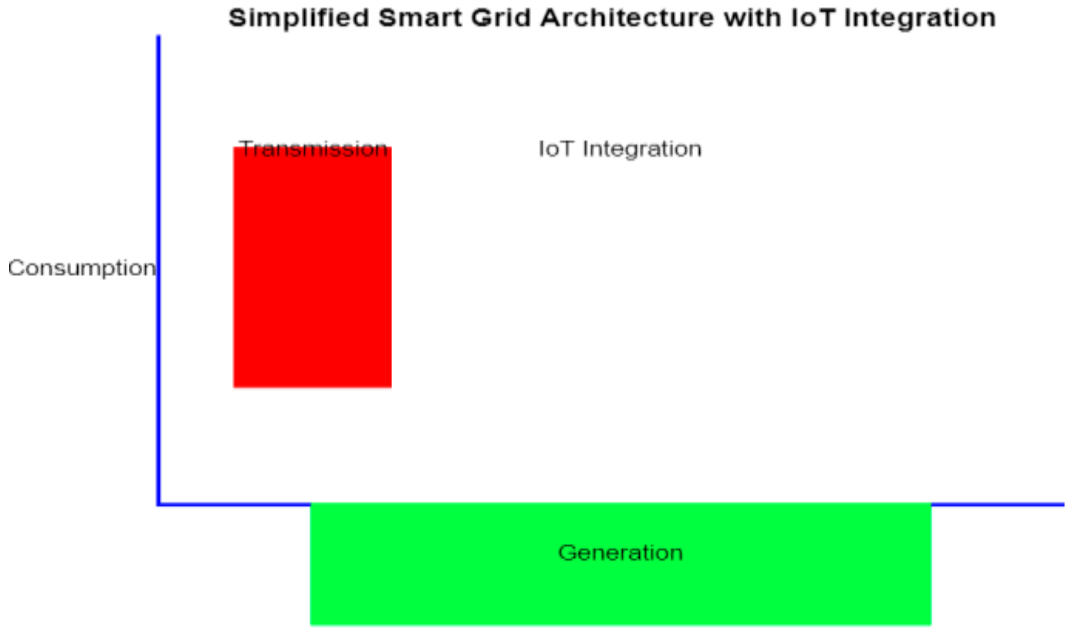

Figure.1: Smart Grid Architecture with IoT Integration

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

A modern smart grid architecture representation with IoT (Internet of Things) devices implemented in Figure 1 is shown in the figure. While these are the highlights, this illustrative figure captures the crucial aspects which outline a smart grid's fundamental components and layers constituting them, while at the same time, placing emphasis on digital technologies and IoT devices that further improve its functionality.In this depiction, the smart grid is divided into three distinct components, each represented by a rectangular block: He illustrated "Generation", "Transmission" and, "Consumption". The term "Generation", however, refers to the different means of power generation, which includes conventional power stations and alternative energy options[7]. The "Transmission" element is the vital layer that enables efficient carry electricity across long distances, where it can be received by consumers[8]. At the same time, the "Consumption" section captures the interest of end-users or consumers who use electricity for a number of purposes. Important to note, the figure includes an extra layer labeled as "IoT Integration" which sits in-between the 'Transmission' and 'Consumption' parts. This layer ensures the integration of IoT machines and sensors into the smart grid framework[9]. These IoT devices form the basis of fast, real time data exchange between the agent and the grid. They provide advanced functionalities, including energy monitoring and load optimization within the grid and dynamically responding to energy demand[10].

IoT technologies enable several key applications within smart grids:

Smart Metering: This enables dynamic pricing, better demand response, and improved consumer involvement because of the IoT-enabled smart meters that measure energy consumption and report it in real-time[11]. The consumer is able to keep track on the consumption of energy so that they can modify their behavior and minimize on wastage of costs in terms of energy.

Demand Response: IoT devices allow demand response programs as they automatically decrease the consumption of energy by appliances and systems in accordance with the signals from utility firm, especially when there is a peak demand[12]. This is aimed at harmonizing supply and demand, preventing grid congestions, and thus avoiding the usage of costly peaking power plants.

Distributed Energy Resource Management: The spread of DERs, such as rooftop solar panels and residential batteries, is an important factor that acts as the driving force for IoT technologies for managing these resources[12]. They facilitate the aggregation, optimization, and cohesive management of DERs, further enhancing flexibility in grids and opening doors for ancillary services.

2. Benefits of IoT-Based Energy Monitoring

The initial and most prominent advantages that IoT-based energy monitoring brings for smart grids include improvement in grid efficiency, backing up the resilience of quality of service, and assisting in renewable energy sources integration. One of the major advantages is energy flow optimizations,

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

which IoT-based monitoring systems minimize waste and extraordinary increase the balance between the supply and demands of energy[13]. This is done through the utilization of real-time data gathering and analysis, which ensures that energy distribution is adjusted accordingly in order to keep up with immediate needs and ultimately boost overall grid capacity.

Secondly, IoT-related technologies are significantly better in grid reliability and resilience. This set of systems is highly important in the detection of faults and abnormalities within the grid that enables operators to have an early response to potential distortions[14,15]. This quick reaction ability reduces the effect of such events to keep the grids stable and avoid large and significant outages. The resilience offered through IoT systems makes it possible for the grid to survive and bounce back from different challenges, such as those posed by physical, cyber and environmental threats[16]. Also, it should be noted that IoT energy monitoring serves a major role in the integration of renewable energies to the grid. With the help of these monitoring systems, it is possible to collect relevant information that is important for adequately managing the variable nature of renewable energy; this includes accurate and real-time representation of energy production from renewable sources, as well as information on consumption patterns[17,18]. This allows the grid operators to make effective decisions on energy transmission, which helps them ensure smooth and a consistent energy supply despite the growing dependence on non-renewable sources. Smooth incorporation of renewable power into the grid does not only support the goal for sustainability but also contributes to the decrease of carbon emissions, representing a big leap in the direction of cleaner energy systems' transition.

3. Challenges of Data Security in IoT-Based Smart Grids

The application of IoT-based technologies to smart grids provides many advantages, but it also creates a number of challenges in the field of data protection: first, about the issues of personal data confidentiality, next, vulnerability to cyber attacks and finally integrity and reliability of data. Data Privacy Concerns in the collection of confidential information through IoT devices later become a major issue. Smart meters and IoT sensors collect highly granular data on consumer energy consumption patterns, inadvertently exposing private data including details about the types of individuals' daily routines and lifestyles[19,20]. The danger of incorrect use, such as data theft or unauthorized access cannot be underestimated and the need for good data protection is an essential part of upholding security and integrity. Consumer data protection against unauthorized access is fundamental in preserving trust for smart grid technologies and ensuring that government privacy regulations are respected.

The IoT-based smart grids are highly dependent and are at risk of Cyber Attacks since they are

ISSNPRINT23191775Online23207876
UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

interconnected. Every connected device is another opening to exploit and search for vulnerabilities in the grid, enlarging the attack surface. In addition, cyber-attack on smart grid can lead to many repercussions including the power failure and compromised data. The negative influence on the grid stability and security are significant, which calls for sophisticated cybersecurity instruments to defend against advanced threats. The above-mentioned risks can be addressed by ensuring communication channels are secure and access controls are kept strict.

SIA challenges are many times higher while it comes to IoT-based smart grids, where data integrity and reliability from the large amount of connected IoT devices play a crucial role in operational decisions[21]. Data tampering or corruption is possible by either malicious attacks or technical misfortunes that constitute some major threats. The maintenance of the integrity of data is not something that should be overlooked because it could interfere with the proper functioning of the smart grid, such as energy distribution management and demand response strategies. One of the important practices that ensure enforcing secure data transmission protocols and regular data validation processes are essential for sustaining the reliability of provided IoT-generated data.

4. Solutions and Best Practices for Enhancing Data Security

Improving data security within the IoT-enabled smart grids necessitates a holistic approach which involves the use of cutting-edge encryption methods, strong authentication procedures, privacy preserving techniques, secure anonymization and auditing in addition to adherence to industry standards.

AIA techniques serve a critical purpose in the transmission of sensitive data on IoT devices, considering that most IoT devices have little processing power. To ensure that these devices have adequate resources to execute the processes, developers create lightweight encryption methods whereby they offer robust security. Technologies like ECC provide a tradeoff between computational efficiency and security, such that messages that are transmitted from devices to the central system cannot be compromised through tampering or divulging confidential information. The use of these encryption methods ensures to keeps the confidentiality and integrity of the sensitive information that moves through the network.

Effective Identity of the Devices and Users are very Important in verifying the authenticity of devices and users, respectively for authorizing them within the smart grid network. The strong authentication protocols assist in the minimization of unauthorized access and ensuring that only those devices and users, who have the right credentials interact with the infrastructure connected to the grid system. Techniques like mutual authentication- where both the device and the network authenticate each other- and proper use of digital certificates is made sure to have a high level of

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

security. This inhibits the action of rogue actors who can disguise as legitimate devices and corrupting the function of the grid.

Privacy issues can be addressed through Data Anonymization and Privacy-Preserving Techniques whereby after collecting the data from IoT devices, it is anonymised. These approaches anonymize or encrypt personally identifiable information from collected data so that the latter could be used for analysis without revealing any personal information. Methods like differential privacy make it less possible to detect particular customers but help learn patterns of energy consumption. This technique enables users to use data for optimization and strategic planning without disrespecting individual anonymity.

Security audits are a necessity for clients and businesses, and mandatory compliance with the industry standards and regulatory requirements is needed to maintain a strong security position. Ongoing security assessments enable to identify the weaknesses and gaps therein in the security infrastructure of smart grid, so that strengthening measures can be adopted beforehand. Following standards, such as NIST guidelines for smart grid cybersecurity will ensure future protection of the grid from constantly developing threats. The implementation of rules brings attention to the utility's focus on consumer data protection, and ensuring the smart grid ecosystem's credibility.

5. Case Studies and Emerging Technologies

Smart Grid Project in Chattanooga, Tennessee: This is evidenced by the fact that one of the most successful IoT-based smart grid implementation cases can be observed from the Chattanooga smart grid project managed by the Electric Power Board (EPB) of Chattanooga. Under this project a high speed fiber optic based network with a smart grid technology enabled to serve more than 170,000 households and business units. AmFee distinguished itself through the use of sophisticated encryption and systems that help in the constant monitoring of cyber threats that improved grid reliability, reducing outage times. In the project, the level of security that was designed against threats from data and their theft could coexist with complex smart grid functions that became a model to be followed by other such projects in other countries.

Sweden's Smart Grid Consortium: In Sweden, a consortium involving utility firms, tech providers, and learning establishments worked in collaboration in establishing a smart grid project targeting at improving the efficiency of energy and the integration of poised sources. The project used secure communication protocols, strict authentication mechanisms and tools and technologies to protect data exchange within the grid. Through the implementation of the latest cybersecurity solutions by consortium, significant security breaches were addressed effectively showing the benefits of sharing

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

data through collaborative techniques to address security of smart grids.

Emerging Technologies

Blockchain for Secure Transactions: Such a security of data has the potential to increase data integrity and security in the smart grid ecosystem through blockchain technology. Blockchain guarantees the integrity of energy trading processes since it makes transactions reliable, transparent, and tamper-proof. For instance, the blockchain technology can secure all transactions in peer-topeer energy trading platforms that allow consumers to purchase and sell renewable energy directly. Its relatively decentralized nature greatly mitigates the risk of breach attacks on centralized data or unauthorized access.

Artificial Intelligence (AI) and Machine Learning (ML): AI and ML technologies have changed the mode of monitoring and managing Smart Grids, as well as in the realms of cybersecurity. These technologies forecast and identify abnormalities in real-time and can detect cyber threats before they damage or destroy any system. For example, AI-enabled systems can identify patterns in the network traffic, meanwhile to detect abnormal activities that may indicate to be a cyberattack and quickly respond to it. Further, ML algorithms can improve encryption practices and authentication procedures, changing dynamically in response to new hazards, keeping the grid safe.

The use of these case studies and emerging technology applications show how some of the innovative approaches being used globally to deal with data safety challenges in IoT-based smart grid systems. They also emphasize the need of implementing new modern security techniques and ability of future technologies to protect the grid against cyberattacks, making it reliable and preserving privacy of client data. With the further evolution of a smart grid, these technologies will be instrumental in improving their security framework, thus making them more resistant to attacks and capable of handling energy demands of tomorrow.

6. Results and Discussions

Figure.2 presents a comparative assessment of available secure encryption protocols that can suit IoT (Internet of Things) devices. The figure provides insights into the four encryption ECC (Elliptic Curve Cryptography) in terms of their application to IoT devices utilizing minimal processing power. As depicted on the graph, shown are bars representing computational overhead cost to each encryption method. On the one hand, computational overhead refers to the extra burden of encryption and is a critical factor for IoT devices with limited resources; Lower bars in the chart denote encryption methods having lower cost of computation, which are more favorable to low-powered devices. The second essential parameter shown in fig. 4 is energy consumption. It represents a scaled-up figure showing the power consumption for each encryption method during the

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

process of data encryption and decryption. In the figure, energy used in encryption refers to bars that represent each encryption. Low bars represent efficient encryption methods used for IoT devices that work on batteries or with power acquired through energy harvesting. The figure below provides a comparison of the methods of three encryption techniques that used with IoT devices in terms of efficiency. This is based on the computational overheads and energy consumption metrics that are analyzed below. A lightweight encryption method that requires less computing power and costs less energy is seen as more appropriate for IoT devices with resource restrictions.

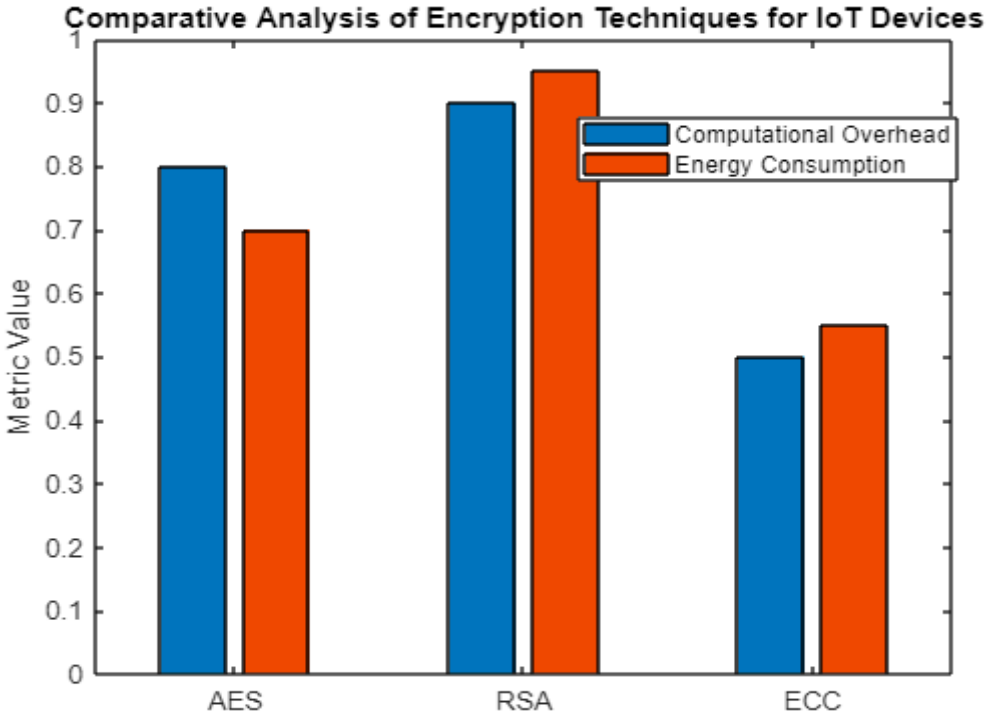

Figure.2: Comparative Analysis of Encryption Techniques for IoT Devices

Figure.3. presents the perspectives of AI and ML applied to detecting anomalies in IoT-driven smart grids in the figure below. The figure below depicts the main mechanism through which the AI and ML algorithms analyze data gathered by IoT devices, allowing them to find an unusual pattern or anomalies in smart grid operation. The graph shows a simple illustration of information from IoT sensors in the smart grid. Time units are on the x-axis that denote the order of occurrence of data points while sensor readings or data values are shown along the y-axis. In the case of the presented example, the exhibited data is in the form of a sinusoidal pattern that could possibly represent normal functioning. The blue dots on the scatter plot represent data points that show normal operation. These data points are clustered around the normal pattern, meaning that they correspond with the pattern followed during the normal working behavior of the smart grid. These data can be classified as such as learning examples for AI and ML algorithms that determine the normal operation. Anomalies or irregularities are shown on the graph with red 'X' markers. These ones can

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

be indicators of strange processes or abnormal data structures detected using AI and ML algorithms.

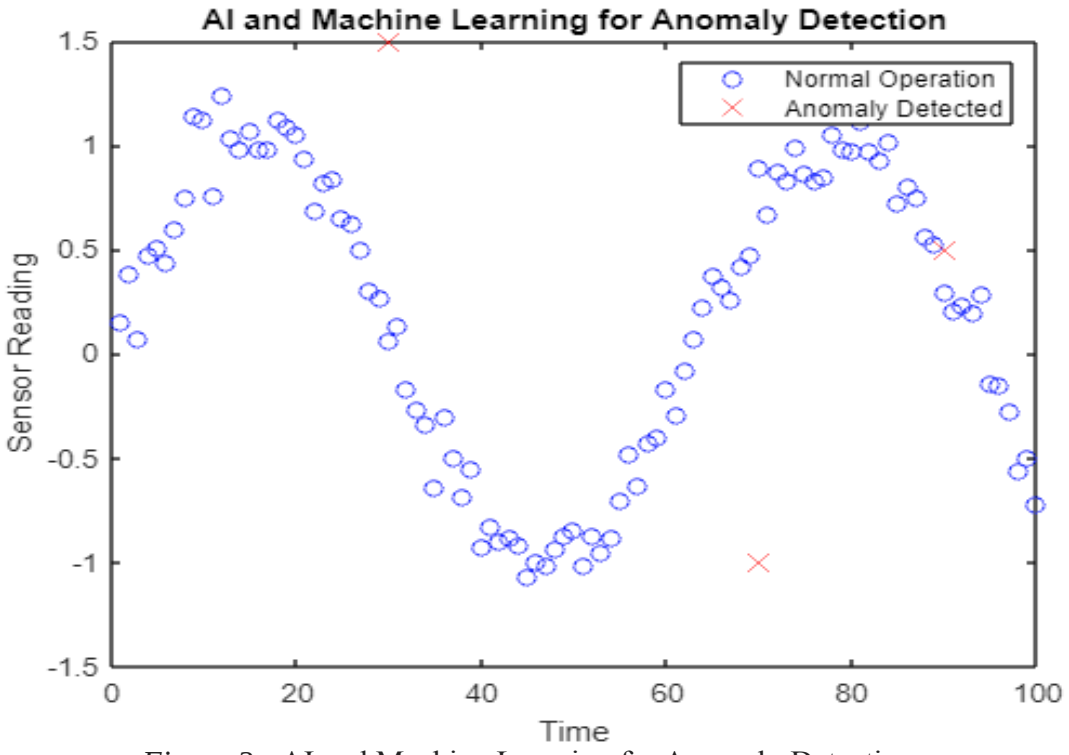

Figure.3: AI and Machine Learning for Anomaly Detection

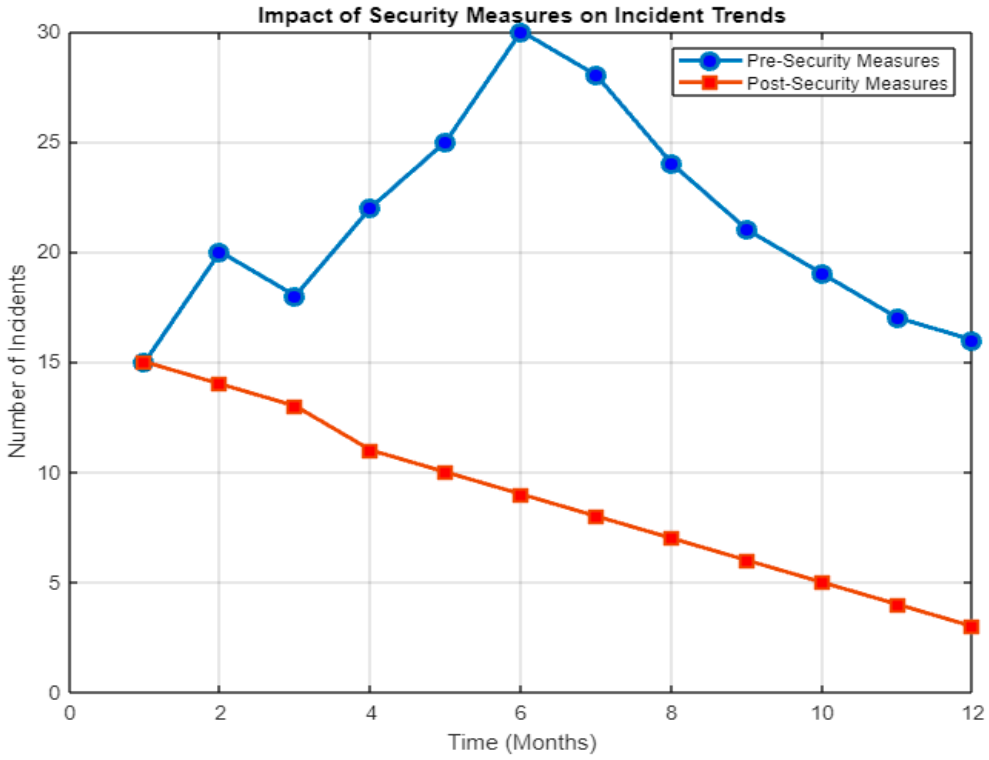

Figure.4: Impact of Security Measures on Incident Trends

The algorithms in real-time sense the incoming data and detect deviations from learned normal behavior at all times. Whenever an anomaly is found, its sign is a red "X" on the plot. The algorithms are used to facilitate proactive responses when there is an anomaly detected by both AI and ML. Answers to these questions could be by alerting grid operators or automatic actions aimed

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

at responding to the issue identified. The figure does not show what the specific response actions look like but shows that quick anomaly detection is needed.Figure.4. presents a line chart that provides a visual representation of the impact of security measures on the trends of security incidents within IoT-based smart grids over a defined time period. This diagrammatic chart, therefore, is an illustrative way of providing a broad array of how the advanced security measures have impacted on the ways in which the dynamics of security incidents are affecting the smart grid environment. The coordinate chart consists of the X-axis, representing time, and typically designed as months, and the Y-axis measuring the number of security occurrences that happened during a specific period.Two distinct lines are featured on the chart: On the "Pre-Security Measures," illustrated with blue circles joined with a continuous line, and the "Post-Security Measures," symbolized through red squares connected by a continuous line. The latter evidences the historical pattern of incident trends prior to the universal use of security measures; sometimes this trend can show fluctuations or can be monotony-increasing. On the other hand, the second refers to the latter, which points to trends after introducing changes to security measures and ideally shows a decrease in the number of incidents or stabilization of trends, reflecting the degree of effectiveness of measures. Securement annotations are strategically placed on the timeline that accompany signposts in the history of security, like when encryption is installed or regular health-checks automated. These annotations indicate critical moments on the part of implementing security measures that set an example for the analysis made. This part of the paper addresses key results and learnings regarding IoT-based smart grids discussed in the findings section. It contains a diagram of the smart grid architecture fitted with IoT gadgets that emphasizes on digital technology as a cornerstone for improving grid performance. Moreover, a comparative analysis assesses encryption technologies that can fit the devices used in the IoT environment, which helps make informed decisions regarding safety implementation. The practical effectiveness of the security measures or their impact can be shown through the comparison of the historical trends of the security incidents before and after certain improvements are made. An additional result-driven visualization further strengthens the impact of the security measures on incident trends and boosts the overall grasping of study results in IoT-oriented smart grids.

7. Conclusion

In conclusion, the implementation of IoT-driven smart grid is a progressive step in the development of energy systems providing better performance, safety and renewable source integration. Nevertheless, the potential realization of these benefits is inherently linked to the management of mammoth issues in data security. This work has identified certain core areas that

ISSNPRINT23191775Online23207876
Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

should be protected and secured, these include information security in protecting both the sensitive information and keeping the grid safe from cyberattacks as well as the integrity and reliability of data for smart grids. The identification of the advanced encryption techniques, strong authentication measures, data anonymity procedures, and regular security audits and compliance standards have reveals the way out in dealing with data security risks. These solutions, on top of this, solve current weaknesses and provide a means to ensure the resilient functioning of smart grids from emerging threats. In addition, the major potential of technologies which can be defined as emerging ones namely blockchain, artificial intelligence (AI), and machine learning (ML) in the improvement of data safety and grid management has been pointed out promising development focus. Such technologies provide advanced means of transaction security, cyber threats anticipation and counteraction, grid optimization etc., thus revealing prospects of smart grids' dynamic development provided strong data security.

References

1. N. Pramudhita, R. A. Asmara, I. Siradjuddin and E. Rohadi, "Internet of Things Integration in Smart Grid," *2018 International Conference on Applied Science and Technology (iCAST)*, Manado, Indonesia, 2018, pp. 718-722, doi: 10.1109/iCAST1.2018.8751518.
2. Xi Chen, Jianming Liu, Xiangzhen Li, Limin Sun and Yan Zhen, "Integration of IoT with smart grid," *IET International Conference on Communication Technology and Application (ICCTA 2011)*, Beijing, 2011, pp. 723-726, doi: 10.1049/cp.2011.0763.
3. S. Sidid and S. Gaur, "Smart grid building automation based on Internet of Things," *2017 Innovations in Power and Advanced Computing Technologies (i-PACT)*, Vellore, India, 2017, pp. 1-4, doi: 10.1109/IPACT.2017.8245201.
4. L. Bagherzadeh, H. Shahinzadeh, H. Shayeghi, A. Dejamkhooy, R. Bayindir and M. Iranpour, "Integration of Cloud Computing and IoT (CloudIoT) in Smart Grids: Benefits, Challenges, and Solutions," *2020 International Conference on Computational Intelligence for Smart Power System and Sustainable Energy (CISPSSE)*, Keonjhar, India, 2020, pp. 1-8, doi: 10.1109/CISPSSE49931.2020.921219
5. E. Esenogho, K. Djouani and A. M. Kurien, "Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect," in *IEEE Access*, vol. 10, pp. 4794-4831, 2022, doi: 10.1109/ACCESS.2022.3140595.
6. J. Zhao, M. -M. Xiang, X. Song, C. Tian and Y. Yang, "The Application and Threat of the Internet of Things in the Smart Grid," *2020 2nd International Conference on Applied Machine Learning (ICAML)*, Changsha, China, 2020, pp. 339-343, doi: 10.1109/ICAML51583.2020.00075.
7. N. Singh and P. Paliwal, "Planning and monitoring of smart grid Architecture using Internet of Things," *2022 IEEE 6th International Conference on Condition Assessment Techniques in Electrical Systems (CATCON)*, Durgapur, India, 2022, pp. 12-16, doi: 10.1109/CATCON56237.2022.10077659.

ISSNPRINT23191775Online23207876

Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

8. Miao Yun and Bu Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," *2010 International Conference on Advances in Energy Engineering*, Beijing, China, 2010, pp. 69-72, doi: 10.1109/ICAEE.2010.5557611.
9. S. A. Alharthi, P. Johnson and M. A. Alharthi, "IoT architecture and routing for MV and LV smart grid," *2017 Saudi Arabia Smart Grid (SASG)*, Jeddah, Saudi Arabia, 2017, pp. 1-6, doi: 10.1109/SASG.2017.8356507.
10. Ghasempour, A. Internet of Things in Smart Grid: Architecture, Applications, Services, Key Technologies, and Challenges. *Inventions* 2019, *4*, 22. https://doi.org/10.3390/inventions4010022
11. M. Antolić, D. Vučinić, S. Nikolovski and Z. Baus, "Smart Grid Architecture Based on Active Demand Approach," *2016 International Conference on Smart Systems and Technologies (SST)*, Osijek, Croatia, 2016, pp. 49-54, doi: 10.1109/SST.2016.7765631.
12. M. F. Khan, A. Jain and A. Paventhan, "An approach to Internet of Things network deployment for smart grid applications," *2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)*, Chennai, India, 2017, pp. 1664-1669, doi: 10.1109/WiSPNET.2017.8300044.
13. Z. Hameed, F. Ahmad, S. u. Rehman and Z. Ghafoor, "IoT Based Communication Technologies to Integrate and Maximize the Efficiency of Renewable Energy Resources with Smart Grid," *2020 International Conference on Computing and Information Technology (ICCIT-1441)*, Tabuk, Saudi Arabia, 2020, pp. 1-5, doi: 10.1109/ICCIT-144147971.2020.9213730.
14. A. N. Babadi, S. Nouri and S. Khalaj, "Challenges and opportunities of the integration of IoT and smart grid in Iran transmission power system," *2017 Smart Grid Conference (SGC)*, Tehran, Iran, 2017, pp. 1-6, doi: 10.1109/SGC.2017.8308847.
15. Y. Feng, X. Lin and Z. Yu, "Internet of Things in Power Systems: A Bibliometric Analysis," *2023 26th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, Rio de Janeiro, Brazil, 2023, pp. 1427-1432, doi: 10.1109/CSCWD57460.2023.10152802.
16. F. Beligianni, M. Alamaniotis, A. Fevgas, P. Tsompanopoulou, P. Bozanis and L. H. Tsoukalas, "An internet of things architecture for preserving privacy of energy consumption," *Mediterranean Conference on Power Generation, Transmission, Distribution and Energy Conversion (MedPower 2016)*, Belgrade, 2016, pp. 1-7, doi: 10.1049/cp.2016.1096.
17. S. Das and G. Panda, "An Initiative Towards Privacy Risk Mitigation Over IoT Enabled Smart Grid Architecture," *2020 International Conference on Renewable Energy Integration into Smart Grids: A Multidisciplinary Approach to Technology Modelling and Simulation (ICREISG)*, Bhubaneswar, India, 2020, pp. 168-173, doi: 10.1109/ICREISG49226.2020.9174557.
18. S. K. Viswanath *et al.*, "System design of the internet of things for residential smart grid," in *IEEE Wireless Communications*, vol. 23, no. 5, pp. 90-98, October 2016, doi: 10.1109/MWC.2016.7721747.
19. A. Meloni and L. Atzori, "A cloud-based and RESTful Internet of Things platform to foster Smart Grid technologies integration and re-usability," *2016 IEEE International Conference*

ISSNPRINT23191775Online23207876

Research paper UGC CARE Listed (Group-I) Journal Volume11, Iss11, November-2022

on Communications Workshops (ICC), Kuala Lumpur, Malaysia, 2016, pp. 387-392, doi: 10.1109/ICCW.2016.7503818.

20. M.E. El-hawary, "The smart grid state of the art and future trends", *ElectricPower Compon. Syst.*, vol. 42, 2014.
21. N.A. Hidayatullah and D.E.J. Sudirman, "Desain dan aplikasi internet of thing (iot) untuk smart grid power system", *VOLT - Jurnal Pendidikan Teknik Elektro*, vol. 2, no. 1, pp. 35-44, 2017.