IJEEP

INTERNATIONAL JOURNAL OF ENERGY ECONOMICS AND POLICY

EJ EconJournals

ISSN: 2146-4553

International Journal of Energy Economics and Policy

ISSN: 2146-4553

available at http: www.econjournals.com

International Journal of Energy Economics and Policy, 2026, 16(2), 1113-1119.

EJ EconJournals

Prioritizing Risks and Challenges in Smart Grid Implementation: An Analytical Hierarchy Process (AHP) Approach

Muataz Al Hazza[1], Lana Sakhrieh[2], Maissa Farhat[3], Ahmad Sakhrieh[1]*

[1]Department of Mechanical Engineering, School of Engineering and Computing, American University of Ras Al Khaimah, Ras Al Khaimah, UAE, [2]School of Science, Faculty of Health and Life Sciences, Coventry University, CV1 5FB Coventry, United Kingdom, [3]Department of Electrical and Electronics Engineering, School of Engineering and Computing, American University of Ras Al Khaimah, P.O. Box 10021 Ras Al Khaimah, UAE. *Email: ahmad.sakhrieh@aurak.ac.ae

Received: 21 October 2025 **Accepted:** 27 January 2026 **DOI:** https://doi.org/10.32479/ijeep.22938

ABSTRACT

As energy demand increases daily due to economic growth and population expansion, smart grid technology has emerged as an essential innovation for modern power systems. These grids integrate digital technologies, enabling real-time monitoring, control, and enhanced energy efficiency. However, deploying smart grids faces significant challenges, including cybersecurity threats, data privacy concerns, power theft, and communication infrastructure issues. This study prioritizes these challenges using the Analytical Hierarchy Process (AHP). The AHP results highlight the varying contributions of factors to smart grid risks. Cybersecurity emerges as the most critical factor (49.9%), emphasizing its role in preventing disruptions. Power theft (23.1%) significantly impacts economic and operational aspects, while data security and privacy (20%) underscore the need for robust safeguards. Communication infrastructure issues (7%) affect operations, and battery failure is identified as the least critical risk. A consistency check confirms the reliability of judgments with a Consistency Ratio (CR) below 10%. These findings help prioritize and mitigate risks effectively in smart grid systems

Keywords: Energy, Risks, Smart Grid, Analytical Hierarchy Process
JEL Classifications: Q40, L94, C44

1. INTRODUCTION

The economic growth, population growth, and rapid urbanization lead to the need for an effective solutions. One of these new approaches is by utilizing smart grids. Smart grids have emerged as one of the innovation in the modern power systems. This digital integration allows a real-time monitoring, analysis, and control of the energy supply chain, which improves efficiency, reduces energy consumption, and lowers costs (Sun et al., 2011). A smart grid is an advanced system that integrates electricity generation, distribution, and consumption, incorporating renewable energy sources and energy storage to improve efficiency and reduce environmental impact. Smart grids offer significant benefits, including improved efficiency, reliability, sustainability, and reduced energy consumption and carbon emissions. In the Gulf Cooperation Council (GCC) countries, there is a recognition that over-dependence on oil-based resources poses long-term risks to energy security. Consequently, GCC nations are diversifying their economies and increasing investments in renewable energy projects, with significant targets set for 2030-2040 (IRENA, 2018; KAPSARC, 2017). In the energy-intensive Gulf region, smart grids are critical for enhancing energy efficiency and reducing carbon emissions. For instance, Saudi Arabia’s National Renewable Energy Program (NREP) aims to generate 50% of its electricity from renewable sources by 2030, relying on smart grid technologies to ensure stability and reliability (IRENA, 2022). Similarly, Qatar has adopted advanced metering infrastructure (AMI), distribution automation, and demand response programs to manage energy use and reduce peak demand (Qatar

General Electricity and Water Corporation [KAHRAMAA], 2023). Kuwait is also advancing with AMI technologies introduced by Ericsson to optimize utility operations and IoT applications, slated for completion by 2024 (Lewis et al., 2023). In Oman, AMI has been identified as a key driver of economic benefits (Okedu and Al Salmani, 2019). Meanwhile, the UAE's Dubai Electricity and Water Authority (DEWA) has deployed over two million smart meters as part of its Smart Dubai initiative, empowering customers to monitor and manage their energy and water consumption efficiently (Lewis et al., 2023).

However, deploying smart grids in GCC countries is still early, and some challenges are facing, such as regulatory gaps, limited awareness, and insufficient technological infrastructure (Okedu and Al Salmani, 2019). Successful implementation requires collaboration between governments, utilities, and technology providers. However, transitioning from traditional to smart grids also introduces risks related to data privacy and cybersecurity. For instance, smart meters generate sensitive data that must be protected. Therefore, conducting comprehensive risk assessments is crucial to identify potential vulnerabilities and implement strategies to safeguard stakeholders (Sun et al., 2011).

Many researchers have extensively investigated and analyzed the risks and challenges of implementing smart grid technology. Khalid et al. (2024) highlight key challenges in smart grid realization, including limited user acceptance, reduced operational flexibility under high renewable penetration, and regulatory frameworks not suited to decentralized systems. They emphasize increased complexity in power system planning, operation, and installation, along with the lack of standardized metrics to assess smart grid progress. Critical research gaps in standardization, interoperability, and contingency management—especially black-start procedures—are identified as major risks to grid reliability and resilience. Abbas (2024) claim that the integrating information technology into smart grids has significantly transformed the energy sector by enhancing efficiency and sustainability; however, this integration simultaneously introduces serious cybersecurity challenges that threaten grid reliability, data privacy, and system resilience.

Another researcher (Bouramdane, 2023) focused on the critical role of cybersecurity in smart grids, addressing the growing challenges posed by digital threats. They emphasize using decision-making frameworks like the multi-criteria decision-making analytical hierarchy process to evaluate and optimize security measures.

Naiho et al. (2024) examine cybersecurity challenges in smart grid technologies, focusing on their implications for sustainable energy infrastructure. They highlight risks arising from ICT integration, including data breaches and security failure. The study underscores the potential of emerging technologies like blockchain to ensure secure, resilient smart grid development. Other researchers, Laha et al. (2024), claimed that the Internet of Everything (IoE) advances smart grids to meet growing energy needs but brings significant cybersecurity challenges.

Cyberattacks on smart grids often combine digital and physical methods, targeting critical components such as the Advanced Metering Infrastructure (AMI) (Kim et al., 2022). However, attackers can exploit transmission and storage vulnerabilities to compromise data privacy, alter meter measurements, or disable communication networks. Such breaches can lead to power shortages, operational inefficiencies, and broader infrastructure failures (Wei et al., 2018). Weak AMI designs also expose smart meters to attacks like meter spoofing and fraud, exacerbating system disruption risks (Ghiasi et al., 2023).

Simmhan et al. (2011) highlight that while cloud-based systems enhance efficiency in data management for smart grids, they also pose significant compliance challenges due to the geographically distributed nature of data processing. Moreover, Tchao et al. (2021) point out that while cloud computing integration enhances smart grid capabilities, it also introduces challenges such as data loss, account hijacking, and storage inefficiencies due to mismanagement. Another researcher, Joseph (2015) adds that unauthorized access, often enabled by malware or weak security controls, threatens the operational integrity of smart grids. Similarly, SaberiKamarposhti et al. (2024) emphasize that maintaining data anonymity remains a persistent issue, posing ongoing challenges to protecting consumer privacy in smart grid systems.

Liu et al. (2022) identify a critical challenge in managing demand response technologies used in smart grids to optimize electricity usage, noting that these technologies are vulnerable to tampering, leading to significant disruptions in power systems. Kataray et al. (2023) further emphasize integrating renewable energy into smart grids, highlighting synchronization challenges and the high costs associated with resource availability.

Hasan et al. (2022) examine smart grid communication networks and electric vehicles' role in empowering distributed generation. They study communication features, sustainable integration strategies, and intelligent grid technologies, providing recommendations to resolve challenges and guide researchers toward enhancing modern energy systems. Another researcher, Ghorbanian et al. (2019) investigated the critical role of advanced communication infrastructures in smart grids for delivering efficient, reliable, and sustainable electricity. They also explore the integration of IoT and cloud computing integration and discuss standardization, applications, and future research opportunities in smart grid communication systems.

Raza et al. (2022) highlighted that power theft remains a significant issue in smart grids, often achieved through manipulating energy consumption data, creating substantial supply-demand gaps, particularly in countries like Pakistan. Mohanty et al. (2022) emphasize that battery degradation is another critical concern in smart grid systems utilizing electric vehicles, as repeated charging and discharging cycles reduce efficiency and operational longevity. Additionally, Raza et al. (2022) note that equipment failures in transmission and distribution systems further exacerbate these challenges, necessitating enhanced maintenance and monitoring practices.

Mittra et al. (2021) studied power theft and negligence in fault detection, two critical vulnerabilities in smart grids. They explore modern technologies like IoT and Blockchain to enhance the distribution system. Moreover, they highlighted issues such as transformer health, line faults, theft, and billing malpractices while proposing improved methods to modernize traditional equipment and practices.

Wu et al., 2024 mentioned that rechargeable batteries face significant performance challenges under extreme conditions like high-altitude drones, ocean exploration, and polar expeditions. This review explores failure mechanisms related to ionic/charge transfer, material/interface evolution, and electrolyte degradation. They highlight different engineering solutions, including electrode materials design, electrolyte modification, and component optimization, and conclude with perspectives on advancing battery performance under harsh environmental conditions.

Kappagantu and Daniel (2018) point out that managing the vast amounts of data generated by sensors, meters, and controllers in smart grids is a persistent challenge. Data collection, analysis, and storage issues can significantly hinder the grid's overall performance. To ensure the efficiency, resilience, and long-term sustainability of smart grids, addressing these risks through comprehensive risk assessments and strategic mitigation measures is imperative.

2. RESEARCH METHODOLOGY

The methods selected for this research study were a combination of a comprehensive literature review with the implementation of the Analytical Hierarchy Process (AHP) as one of the multi-criteria decision-making (MCDM) techniques to prioritize the risk elements considering different conflicting criteria using pairwise comparison. Figure 1 shows the detailed steps of the research.

Step 1: Data collections

The data collection and analysis in this study were conducted with the involvement of experts in the field of smart grids and energy systems to ensure the accuracy and reliability of the findings. The Analytical Hierarchy Process (AHP) method was applied with the participation of professionals and researchers specializing in smart grid implementation, cybersecurity, and risk management. These experts contributed to the pairwise comparisons, ensuring that the weight assignment in the AHP matrix reflects real-world risk perceptions. However, the final Pairwise matrix, was a compination between the experts opinion and the literature review as shown in Table 1 that summarizes the authors, years, and associated risks and challenges.

Step 2: Filtering the risk factors

The selection of the five risk factors in Step 2 of the methodology was based on a comprehensive literature review and expert input to ensure that the most critical challenges in smart grid implementation were prioritized. The initial list of risks was gathered from various studies, highlighting multiple challenges in smart grids. To refine this list, experts in the field, including researchers and professionals specializing in energy systems and risk management, were consulted to identify the most relevant and impactful risks for smart grid deployment. Based on Table 1, the risks and challenges can be listed as follows:

1. Cybersecurity
2. Data Security and Privacy
3. Power Theft

Figure 1: Research methodology

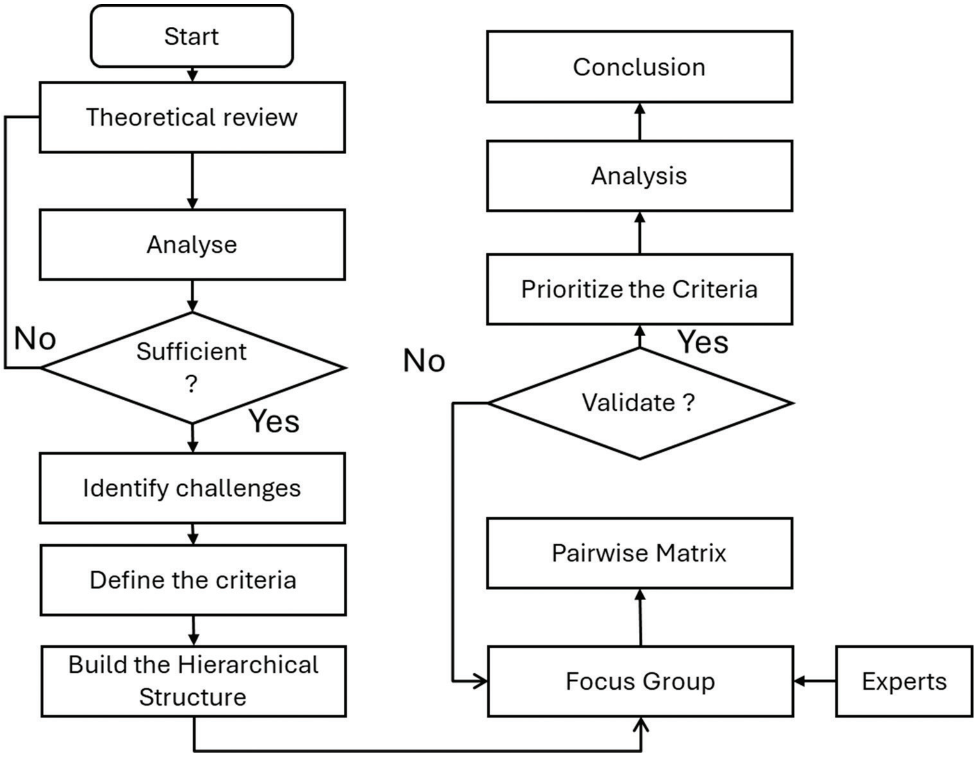


Table 1: Summary of the literature review

Author(s) name	Year	Risk and challenges
Khalid	2024	Susceptibility to cybersecurity threats, including data manipulation and operational disruptions
SaberiKamarposhti et al.	2024	Persistent challenges in protecting consumer data anonymity
Wu et al.	2024	Addressing battery failure mechanisms under extreme conditions
Abbas	2024	highlights cybersecurity in smart grids, showcasing Robust Principal Component Analysis's effectiveness in detecting and mitigating cyber threats.
Naiho et al.	2024	This study highlights cybersecurity challenges in smart grids, emphasizing advanced measures, collaboration, and emerging technologies.
Bouramdane	2023	cybersecurity's critical role in smart grids, emphasizing decision-making frameworks and AI techniques for enhanced protection.
Ghiasi et al.	2023	Operational risks from meter spoofing and fraud
Kataray et al.	2023	Synchronization issues and high costs in renewable energy integration
Mohanty et al.	2022	Battery degradation reduces efficiency and operational longevity
Liu et al.	2022	Vulnerabilities in demand response technologies causing disruptions
Raza et al.	2022	Power theft causing supply-demand gaps,
IRENA	2022	Ensuring grid stability and reliability while integrating renewable energy
Kim et al.	2022	Weak AMI designs expose systems to spoofing and fraud attacks.
Kahramaa	2022	Enhancing efficiency and reducing peak demand using AMI and demand response
Hasan et al.	2022	explores smart grid communication, EV integration, challenges, and solutions for sustainable energy systems.
Mittra et al.	2021	analyzes power theft and fault detection, proposing IoT and Blockchain for modernizing distribution system solutions.
Tchao et al.	2021	Data loss, account hijacking, and storage inefficiencies in cloud integration
Gündüz and Daş	2020	Exploitation of communication channel weaknesses via jamming and zero-day vulnerabilities
Okedu and Al Salmani	2019	The economic potential of AMI, despite regulatory gaps and limited awareness
Ghorbanian et al.	2019	explores smart grid communication infrastructures, addressing architectures, technologies, IoT, cloud computing, and future research.
Kappagantu and Daniel	2018	Data theft compromises integrity, availability, and confidentiality
El Mrabet et al.	2018	Vulnerabilities in AMI systems leading to power shortages and inefficiencies
Wei et al.	2018	Data transmission vulnerabilities in AMI systems lead to network issues
Lewis et al.	2023	Introducing AMI technologies to enhance IoT-based utility operations
Joseph	2015	Operational threats from malware and weak security controls
Sun et al.	2011	Risks of data privacy and cybersecurity in smart grids
Simmhan et al.	2011	Compliance challenges in geographically distributed data processing

4. Communication Infrastructure Issues
5. Battery Failure

These risks will then be prioritized using the analytical hierarchy process (AHP) method, and recommendations on best practices to overcome these challenges will be proposed.

Step 3: AHP Implimentation

To minimize bias in the AHP weight assignment, two steps were conducted: the pairwise comparisons inputs were conducted based on experts feedback in smart grids, cybersecurity, and risk management to reduce individual subjectivity and the consistency check was performed using the consistency ratio (CR) to validate the logical coherence of the pairwise comparisons. The pairwise comparison matrix was developed based on insights obtained from expert focus groups. These focus groups enabled validation, critical reflection, and augmentation of the study outcomes. A focus group can consist of any number that the researcher defines as a group, from three to 12 participants being common (Graham and Bryan, 2022). However, in our research we select three particpint and one focus group is enough due to that the research are focusing only on the challenges of smaryt grids. Participants were selected from a pool of experienced professionals in related fields within the UAE. The primary objective of the focus groups was to ensure the relevance, clarity, and practical usefulness. Participants were asked to review the preliminary problem template, rank the relative importance of each identified challenge and then developed the pairwise matrix. Based on the pairwise matrix, Cybersecurity (F1) emerged as the most critical risk, receiving the highest weight across all comparisons. This indicates that the stakeholders view cybersecurity threats as the top priority due to their potential to disrupt grid functionality, manipulate data, and compromise sensitive systems. Data Security and Privacy (F2) and Power Theft (F3) also scored relatively high, reflecting concerns about protecting consumer data and preventing unauthorized energy usage. Communication Infrastructure Issues (F4) and Battery Failure (F5) ranked lower, suggesting that while important, they are less immediate compared to the top three risks. Table 2 shows the factors code, and Table 3 clarifies the pairwise matrix.

Based on the results in Table 3, Factor F5 was identified as having a low priority and was subsequently excluded from further calculations. This decision was made to enhance the accuracy, stability, and reliability of the overall analysis by focusing on the more impactful factors. Therefore, the pairwise matrix is presented in Table 3.

The normalized pairwise matrix reveals the relative contributions of key factors to the overall risk landscape, highlighting their varying levels of priority. As shown in Table 4, the Cybersecurity emerges as the most critical factor, with a weight of 0.499, underscoring its essential role in preventing systemic disruptions and data breaches. Following this, data security and privacy rank second at 0.200, reflecting the urgent need for robust measures to protect sensitive information. With a weight of 0.231, power theft closely follows, emphasizing its economic and operational impacts. While communication infrastructure issues contribute

Table 2: Coaded factors

Code	Factor
F1	Cybersecurity
F2	Data Security and Privacy
F3	Power Theft
F4	Communication Infrastructure Issues
F5	Battery Failure

Table 3: Pairwise matrix

Criteria	F1	F2	F3	F4
F1	1.000	3.000	3.000	5.000
F2	0.333	1.000	0.500	5.000
F3	0.333	2.000	1.000	3.000
F4	0.200	0.200	0.333	1.000

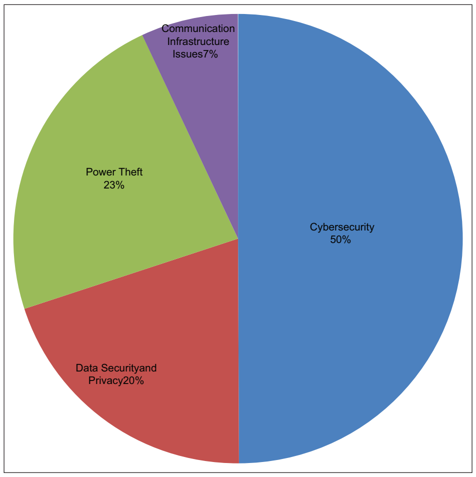
Table 4: Priority results

Criteria	F1	F2	F3	F4	Priority
F1	0.536	0.484	0.621	0.357	0.499
F2	0.179	0.161	0.103	0.357	0.200
F3	0.179	0.323	0.207	0.214	0.231
F4	0.107	0.032	0.069	0.071	0.070

Table 5: Consistency check

λmax	4.22878	CI	0.07626
n	4	CR	0.084734

Figure 2: Risk priority



a lower weight of 0.070, they remain significant for ensuring seamless smart grid operations. Lastly, battery failure is viewed as the least immediate risk, suggesting its impact is less critical compared to the other factors. This distribution underscores the varied focus areas required to manage the overall risk effectively.

These results is presented in Figure 2.

The last step was checking the consistency. The Analytical Hierarchy Process (AHP) consistency check ensures the reliability, stability, and logical coherence of pairwise comparisons. The results of the AHP method indicate a λmax of 5.383216 for a matrix size n = 5, yielding a Consistency Index (CI) of 0.07626 and a Consistency Ratio (CR) of 0.084734. Since the CR is less than (10%), the pairwise comparisons made in the matrix are consistent and reliable, these results is shown in Table 5. This suggests that the judgments used to prioritize the factors, including Cybersecurity, Data Security and Privacy, Power Theft, Communication Infrastructure Issues, and Battery Failure, were logical and coherent. The results can thus confidently guide decision-making in effectively addressing and mitigating smart grid risks.

3. RESULTS AND DISCUSSION

The Analytical Hierarchy Process (AHP) used in the prioritization of risks and challenges in smart grid implementation is displayed in Table 4. Cybersecurity was identified as the most critical factor, with a priority weight of 0.499, accounting for most of the overall concern. The second critical factor was power theft (0.231), followed by Data security and privacy (0.200), and less significantly, communication infrastructure issues (0.070) and battery failure.

The findings strongly highlight digital vulnerabilities within the smart grid ecosystem, which aligns with global prioritization concerns in which cybersecurity and data privacy are commonly highly pressing challenges in utilizing interconnected energy systems.

Identified factors' impact on key dimensions of smart grid implementation are emphasized as per the analysis:

- Cybersecurity (0.499): Cybersecurity's prominence as a risk factor illustrates the need for critical safeguarding against cyberattacks with the ability to disrupt grid operations, compromise sensitive data, and lead to economic losses. Ransomware attacks targeting energy sectors are an example of recent incidents highlighting this concern's magnitude and its effects on infrastructure and public trust.
- Power Theft (0.231): Power theft is a concern of high significance despite being viewed as a traditional issue, specifically in areas of weaker enforcement mechanisms. This affects revenue recovery and grid efficiency, which highlights the need for advanced metering infrastructure (AMI) to mitigate this risk.
- Data Security and Privacy (0.200): This priority emphasizes safeguarding consumer data and ensuring that regulations such as GDPR or other national legislation are followed. Violations can result in legal penalties, impairment to reputation, and a decline in customer adoption.
- Communication Infrastructure Issues (0.070): Reliable communication networks allow for real-time data transfer, and operational controls are therefore a crucial aspect of smart grids. Any communication infrastructure challenges, specifically in remote or underserved areas, could negatively affect smart grid deployment and performance.
- Battery Failure: Although not of the highest significance, battery failure remains a relevant concern, especially considering energy storage becomes integral to renewable energy integration. This issue can be dealt with through improving battery technologies and maintenance protocols.

The analysis shows possible interdependencies between the factors. By lowering network vulnerabilities, for example, resolving communication infrastructure problems might indirectly improve cybersecurity. Strong data security and privacy frameworks can also support initiatives to reduce cybersecurity threats. It is imperative to recognize these interdependencies to create comprehensive plans that handle many risks simultaneously.

Risk prioritization in smart grid installation emphasizes how important it is for various parties involved to collaborate to tackle these issues. Governments and regulators are responsible for establishing enforceable cybersecurity and data protection standards, ensuring that these frameworks can guide utilities and technology providers to ascertain that smart grid ecosystem complies with national and international policies. Considering the entities in charge of implementing these requirements, utilities and energy firms are equally significant. They have implemented significant investments in advanced metering systems, grid management technology, and secure communication infrastructure to improve resilience and lower vulnerabilities. In addition, technology providers contribute to creating solutions through research, allowing for resolutions involving secure communication protocols and next-generation battery technologies. Effective cooperation between various parties ensures a unified strategy for reducing risks and overcoming obstacles in deploying smart grids.

In order to rectify the possible risks effectively, targeted strategies can be implemented, including enhancing cybersecurity through regular penetration testing to safeguard the grid against potential threats, advanced encryption protocols, and continuous monitoring systems. Strictly following data protection regulations and employing anonymization techniques can secure sensitive consumer information and mitigate data privacy concerns. Tamper-resistant smart meters and the use of AI-based analytics can guard against power theft and unauthorized energy usage. Improving network hardware, implementing backup systems, and guaranteeing dependable connectivity—especially in isolated and underserved areas—can help address communication infrastructure problems. Finally, investments in cutting-edge battery technologies, like solid-state batteries, combined with predictive maintenance programs to reduce failure rates, can increase the dependability of energy storage systems. These all-encompassing tactics are necessary to create a smart grid ecosystem that is secure, efficient, and sustainable smart grid ecosystem.

The findings are in line with global smart grid priorities, particularly in regions with advanced deployments like the United States and Europe, where cyber security and data privacy make up the majority of the discourse. However, in nations with high non-technical losses, like parts of South Asia and Africa, the comparatively high ranking of power theft reflects particular regional challenges.

4. CONCLUSIONS

The study underscores the importance of the key challenges in the deployment of smart grids to ensure their effective integration and operation. The analytical Hierarchy Process (AHP) was implemented to prioritize these challenges. The results show that cybersecurity emerged as the most critical challenge, highlighting the need for robust safeguards against digital vulnerabilities that could compromise grid functionality and data integrity. Data security and privacy ranked second, emphasizing protecting consumer information while adhering to legal and ethical standards. Though a traditional issue, power theft still poses significant economic and operational risks, particularly in regions with weaker enforcement mechanisms. While communication infrastructure issues and battery failures are of lower priority, their significance remains undeniable in ensuring seamless and reliable grid operations. The interdependencies between these factors reveal the importance of a holistic approach to risk management, where improvements in one area, such as communication infrastructure, can enhance other aspects like cybersecurity.

Battery failure was deprioritized in this study because the impact of failure varies significantly based on the type of battery used in smart grid applications. Different battery chemistries, such as lithium-ion, lead-acid, or solid-state batteries, exhibit varying levels of efficiency, degradation rates, and resilience under different operating conditions. Some advanced battery technologies are designed with enhanced durability and management systems, reducing the overall risk of failure. Additionally, other risks, such as cybersecurity threats and power theft, were found to have a more immediate and widespread impact on smart grid reliability.

To effectively mitigate these risks, the study recommends targeted strategies, including enhanced cybersecurity measures, adherence to data protection standards, tamper-resistant technologies for power theft prevention, improved communication protocols, and advancements in battery technologies. Collaborative efforts among governments, utilities, and technology providers are critical to achieving a secure, efficient, and sustainable smart grid ecosystem.

These findings align with global priorities while also reflecting regional effects, offering a comprehensive framework to guide smart grid implementations in diverse contexts. By addressing these challenges strategically, stakeholders can realize the full potential of smart grids in transforming energy systems for a sustainable future.

5. ACKNOWLEDGEMENT

The authors are very grateful to the Office of Research and Sustainability at the American University of Ras Al Khaimah for supporting this research

REFERENCES

Abbas, A.K. (2024), Cybersecurity challenges in smart grids: A focus on information technology. Journal of Electrical Systems, 20(6S), 1394-1407.

Bouramdane, A.A. (2023), Cyberattacks in smart grids: Challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. Journal of Cybersecurity and Privacy, 3(4), 662-705.

El Mrabet, Z., Kaabouch, N., El Ghazi, H. (2018), Cyber-security in smart grid: Survey and challenges. Computers and Electrical Engineering, 67, 469-482.

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

Ghorbanian, M., Dolatabadi, S.H., Masjedi, M., Siano, P. (2019), Communication in smart grids: A comprehensive review on the existing and future communication and information infrastructures. IEEE Systems Journal, 13(4), 4001-4014.

Graham, D., Bryan, J. (2022), How many focus groups are enough: Focus groups for dissertation research. Vol. 7. Wisconsin: Faculty Focus.

Gündüz, M.Z., Daş, R. (2020), Cyber-security on smart grid: Threats and potential solutions. Computer Networks, 169, 107094.

Hasan, M.K., Habib, A.A., Islam, S., Balfaqih, M., Alfawaz, K.M., Singh, D. (2022), Smart grid communication networks for electric vehicles empowering distributed energy generation: Constraints, challenges, and recommendations. Energies, 16(3), 1140.

Hossain, M.R., Oo, A.M., Ali, A.B. (2010), Evolution of Smart Grid and Some Pertinent Issues. In: 20th Australasian Universities Power Engineering Conference (AUPEC).

International Energy Agency (IEA), IRENA. (2022), Renewables Policies Database. Paris: International Energy Agency.

IRENA. (2018), Accessible Finance for Renewable Energy Projects in Developing Countries. Abu Dhabi: IRENA.

Joseph, A. (2015), Smart grid and retail competition in India: A review on technological and managerial initiatives and challenges. Procedia Technology, 21, 155-162.

Kappagantu, R., Daniel, S.A. (2018), Challenges and issues of smart grid implementation: A case of Indian scenario. Journal of Electrical Systems and Information Technology, 5(3), 453-467.

KAPSARC (King Abdullah Petroleum Studies and Research Center). (2017), GCC Energy System Overview. Arabia Saudi: KAPSARC.

Kataray, T., Nitesh, B., Yarram, B., Sinha, S., Cüce, E., Shaik, S., Vigneshwaran, P., Roy, A. (2023), Integration of smart grid with renewable energy sources: Opportunities and challenges - A comprehensive review. Sustainable Energy Technologies and Assessments, 58, 103363.

Khalid, M. (2024), Smart grids and renewable energy systems: Perspectives and grid integration challenges. Energy Strategy Reviews, 51, 101299.

Kim, Y., Hakak, S., Ghorbani, A.A. (2022), Smart grid security: Attacks and defence techniques. IET Smart Grid, 6(2), 103-123.

Laha, S.R., Pattanayak, B.K., Pattnaik, S., Hosenkhan, M.R. (2024), challenges associated with cybersecurity for smart grids based on IoT. In: Intelligent Security Solutions for Cyber-Physical Systems. London: Chapman and Hall, CRC. p191-202.

Lewis, R.,S., Mamatha, S., Tilva, S.S., Maimoona, S. (2023), Advanced metering infrastructure (AMI) using IoT. International Journal of Innovative Science and Research Technology, 8(5), 2213-2221.

Liu, Y., Tian, J., Yuan, X., Ye, B., Sang, Z., Yao, X., Li, L., Liu, T. (2022), Real-time pricing response attack in smart grid. Iet Generation Transmission and Distribution, 16(12), 2441-2454.

Mittra, S., Aprameya, A., Mohanta, B.K. (2021), Smart Grid Power Theft and Fault Detection using IoT and Blockchain. In: 2021 International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA). IEEE. p1-5.

Mohanty, S., Panda, S., Panda, S., Rout, P.K., Sahu, B.K., Bajaj, M., Zawbaa, H.M., Kumar, N.M., Kamel, S. (2022), Demand side management of electric vehicles in smart grids: A survey on strategies, challenges, modeling, and optimization. Energy Reports, 8, 12466-12490.

Mohassel, R.R., Fung, A.S., Mohammadi, F., Raahemifar, K. (2014), A survey on advanced metering infrastructure. International Journal of Electrical Power and Energy Systems, 63, 473-484.

Naiho, H.N.N., Layode, O., Adeleke, G.S., Udeh, E.O., Labake, T.T. (2024), Addressing cybersecurity challenges in smart grid technologies: Implications for sustainable energy infrastructure. Engineering Science and Technology Journal, 5(6), 1995-2015.

Okedu, K., Al Salmani, W. (2019), Smart grid technologies in Gulf Cooperation Council countries: Challenges and opportunities. International Journal of Smart Grid, 3(2), 93-102.

Qatar General Electricity and Water Corporation (KAHRAMAA). (2022), Annual Statistics Report 2022 (Prepared by Planning and Quality Department, in collaboration with KAHRAMAA Departments; Production: Public Relations and Communication Department). Doha: KAHRAMAA Publications.

Raza, M.A., Aman, M., Abro, A.G., Tunio, M.A., Khatri, K.L., Shahid, M. (2022), Challenges and potentials of implementing a smart grid for Pakistan's electric network. Energy Strategy Reviews, 43, 100941.

SaberiKamarposhti, M., Kamyab, H., Krishnan, S., Yusuf, M., Rezania, S., Chelliapan, S., Khorami, M. (2024), A comprehensive review of AI-enhanced smart grid integration for hydrogen energy: Advances, challenges, and future prospects. International Journal of Hydrogen Energy, 67, 1009-10252.

Simmhan, Y., Kumbhare, A., Cao, B., Prasanna, V.K. (2011), An Analysis of Security and Privacy Issues in Smart Grid Software Architectures on Clouds. New York: IEEE.

Sun, Q., Ge, X., Liu, L., Xu, X., Zhang, Y., Niu, R., Zeng, Y. (2011), Review of smart grid comprehensive assessment systems. Energy Procedia, 12, 219-229.

Tang, D., Fang, Y., Zio, E. (2023), Vulnerability analysis of demand-response with renewable energy integration in smart grids to cyber attacks and online detection methods. Reliability Engineering and System Safety, 235, 109212.

Tchao, E.T., Quansah, D.A., Klogo, G.S., Boafo-Effah, F., Kotei, S., Nartey, C., Ofosu, W. K. (2021), On cloud-based systems and distributed platforms for smart grid integration: Challenges and prospects for Ghana's Grid Network. Scientific African, 12, e00796.

Wei, L., Rondon, L.P., Moghadasi, A., Sarwat, A.I. (2018), Review of Cyber-Physical Attacks and Counter Defense Mechanisms for Advanced Metering Infrastructure in Smart Grid. In: Transmission and Distribution Conference and Exposition.

Wu, J., Wu, Y., Wang, L., Ye, H., Lu, J., Li, Y. (2024), Challenges and advances in rechargeable batteries for extreme-condition applications. Advanced Materials, 36(4), 2308193.