Legal and Communication Challenges in Smart Grid Cybersecurity: Classification of Network Resilience Under Cyber Attacks Using Machine Learning

Tameem Hadi Fadhil [1], Mustafa I. Al-Karkhi [2], and Luttfi A. Al-Haddad [2,*]

[1] Administrative and Financial Affairs Department, University of Technology, Iraq
[2] Mechanical Engineering Department, University of Technology, Iraq
Email: tameem.h.fadhil@uotechnology.edu.iq (T.H.F.); Mustafa.I.Alkarkhi@uotechnology.edu.iq (M.I.A.); Luttfi.a.alhaddad@uotechnology.edu.iq (L.A.A.)
*Corresponding author

***Abstract*—The transition to renewable energy sources, facilitated by Smart Grid (SG) communication networks, has introduced cybersecurity vulnerabilities that threaten power generation reliability. Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks disrupt blockchain-based energy networks stability, raising legal and regulatory concerns. This study investigates the legal obligations and communication challenges associated with securing smart grid networks against cyber threats. Specifically, we analyze how existing data protection laws ((General Data Protection Regulation (GDPR), Network Information Service (NIS) Directive)) and cybersecurity policies ((National Institute of Standards and Technology (NIST) Cybersecurity Framework, EU Energy Policy)) apply to energy communication infrastructures and assess the legal accountability of energy providers to ensure grid resilience. The study employs Machine Learning (ML) models, namely K-Nearest Neighbors (KNN), Support Vector Machine (SVM), and Random Forest (RF), to classify operational states: normal, single attack, and multiple attacks. Big data obtained from blockchain-powered renewable energy networks was used. The RF model achieved the highest classification accuracy of 98%. The findings underscore regulatory measures' needs and legal frameworks that address AI-driven security risks in communication networks. We recommend policy updates for automated cybersecurity solutions and to enforce data protection compliance, and establish liability protocols for smart grid operators.**

***Keywords*—legal, law, cybersecurity, machine learning**

I. Introduction

A. General Overview

The increasing global demand for energy, driven by population growth, industrial expansion, and technological advancements, has necessitated a shift toward more sustainable and efficient energy solutions [1–5]. As a countermeasure, modern power grids have evolved from traditional centralized networks to Smart Grid (SG) systems, which entail renewable energy sources, real-time communication networks, and decentralized energy management systems [6, 7]. Smart grids enable efficient energy distribution, enhance operational reliability, and promote sustainability by leveraging advanced In-Formation and Communication Technologies (ICTs) [8, 9]. However, while these technologies contribute to energy efficiency, they also introduce significant cybersecurity risks that can compromise system stability and reliability.

One of the critical challenges in smart grid infrastructure is ensuring the security and resilience of communication networks that facilitate energy transmission and distribution [10, 11]. With the increased reliance on digital connectivity, cloud-based monitoring, and block-chain-based energy trading, smart grids are vulnerable to cyber threats compromising operations and causing catastrophic economic and social losses. Among these, Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks pose especial risks, since they target communication channels and compromise the free flow of information between grid entities [12–14]. Such attacks have implications not only for power availability but also legal, regulatory, and governance ramifications, since energy security provision is a key issue for policymakers and regulatory bodies.

As the complex interplay between renewable energy, smart grid communications, and cybersecurity unfolds, the demand is growing for comprehensive security solutions that protect critical infrastructure and meet legal and regulatory compliance. Solutions that succeed must be multidisciplinary, integrating technological innovation, machine learning-driven security architectures, and well-defined cybersecurity policy. This study explores the intersection of communication security, legal compliance,

Manuscript received February 15, 2025; revised March 9, 2025; accepted March 18, 2025; published April 24, 2025.

and cybersecurity challenges in smart grids, with a focus on the necessity of proactive risk mitigation strategies.

B. Literature Review

The integration of Machine Learning (ML) techniques in cybersecurity has gained substantial traction in recent years, particularly in enhancing network resilience against cyberattacks. ML are used in various methodologies in recent advancements [15, 16]. With the increased complexity of SG communication networks, the challenge of ensuring strong intrusion detection and mitigation of cyber threats has grown stronger. Various research studies have suggested different ML-based methods for detection and prevention of cyber threats, such as network intrusion detection, adversarial resilience, cyber-attack classification, and predictive security models. The techniques leverage both supervised and unsupervised learning to improve threat detection accuracy and response time, and consequently network security and resilience. A comprehensive analysis of state-of-the-art ML applications in network resilience is presented in Table I, which summarizes recent studies that apply ML algorithms for cybersecurity in smart grids and critical infrastructure. These studies examine various ML techniques, including SVM, Neural Networks, ensemble learning models, and hybrid AI frameworks, for detecting, classifying, and mitigating cyber threats. The methodologies employed in these studies range from feature selection optimization and adversary-aware classifiers to predictive analytics and real-time cyber-attack monitoring systems. Notably, these studies demonstrate the effectiveness of ML models in improving cyber resilience, with some approaches achieving high classification accuracy and robust defense mechanisms against sophisticated cyber threats.

As seen in Table I, research efforts have increasingly emphasized adapting AI-driven security models to combat the evolving landscape of cyber threats. However, while technical solutions continue to improve, there is a basic research gap in integrating ML-based cybersecurity solutions with legal and regulatory structures in guaranteeing compliance, accountability, and governance in energy communication networks. This gap requires an interdisciplinary solution, as discussed further in the next section. This literature review identifies the progress in AI-based cybersecurity solutions for network resilience. While these models provide technological innovation, the legal and regulatory dimensions of cybersecurity in smart grids remain underdeveloped. Closing this gap between AI-based security structures and legal governance is critical to offering comprehensive cybersecurity policies that balance innovation with compliance and accountability. The following section discusses these research gaps and introduces the novel contributions of this study.

Recent research underscores the growing significance of applying ML techniques to enhance the resilience and sustainability of energy infrastructures. ML-based modeling has been applied extensively not only in cybersecurity but in mechanical modeling and sustainable energy systems as well, such as predicting performance and optimizing operational safety in facilities for renewable energy storage. For instance, previous studies have successfully demonstrated how ML-driven analyses can significantly contribute to improving the operational sustainability and mechanical reliability of energy storage technologies which highlighted potential of mitigating threats and enhancing infrastructure resilience under varying operational conditions [25].

TABLE I. RECENT STATE-OF-THE-ART APPROACHES IN THE PROPOSED RESEARCH TOPIC

Ref.	Machine Learning Approach	Methodology	Key Results
[17]	Supervised Learning (Feature Selection)	Developed a model robustness (MRB) score to evaluate adversarial resilience in ML classifiers.	Found ensemble models to be more resilient against cyber threats.
[18]	ML-Based Intrusion Detection for SDNs	Implemented a Resilience Framework (ReSDN) to classify DoS attacks in Software-Defined Networks (SDNs).	Improved traffic tolerance and cyber-attack detection in SDN environments.
[19]	Neural Networks for Wi-Fi Security	Applied feature selection and NN-based classification for detecting cyber threats in Wi-Fi networks.	Achieved 94% F1–Score, ensuring fast cyber-attack identification.
[20]	ML for Cyber-Physical Systems (CPS)	Surveyed ML models for securing CPS, focusing on cyber resilience strategies.	Identified research gaps in adversarial attacks on ML-based CPS security.
[21]	SVM-Based Self-Adaptive System	Proposed BotGRABBER, an SVM-powered botnet detection and mitigation system.	Enhanced network resilience through self-adaptive threat response.
[22]	Data Mining & ML for Attack Prediction	Designed a time-series predictive model for forecasting future cyber-attacks.	Improved attack prediction accuracy by 15% over baseline models.
[23]	AI for Smart Grid Resilience	Categorized cyber resilience strategies for smart grid protection.	Provided a structured classification of resilience techniques in SG security.
[24]	Hybrid AI for SDN Security	Developed an AI-driven security system for adaptive intrusion prevention in SDNs.	Highlighted AI's role in enhancing network resiliency dynamically

C. Research Gap and Introduced Novelties

Despite significant advancements in machine learning-driven cybersecurity solutions for network resilience, there remains a critical gap in integrating these technologies with legal and regulatory frameworks governing smart grids. Existing research primarily focuses on technical implementations of intrusion detection and network security; however, the legal implications, compliance requirements, and policy-driven cybersecurity governance remain underexplored. Furthermore, while several studies have investigated cyberattack classification and predictive security models, few have addressed the combined impact of multiple simultaneous attacks on smart grid communication networks. The absence of a comprehensive framework that merges AI-driven security models with legal accountability leaves a significant void in ensuring resilient, compliant, and sustainable energy communication infrastructures. The novelties of the current work are as follows:

- This study extends existing research by classifying network operations under normal conditions, single attack scenarios, and multiple attack scenarios;
- Unlike prior studies that focus solely on technical solutions, this research contextualizes AI-driven security strategies within cybersecurity laws and regulatory frameworks, ensuring compliance and governance alignment;
- By applying and comparing KNN, SVM, and RF models, this study provides empirical insights into the most effective cybersecurity models for detecting and mitigating threats in smart grid communication networks

The remainder of the paper is structured as follows: Section II presents the experimental setup, including dataset description and preprocessing. Section III explains the machine learning models, implementation, and evaluation metrics. Section IV analyzes and compares the results and findings of the performance of the models in cyberattack classification. Section V discusses the legal and regulatory implications of AI-based cybersecurity solutions and relates them to current policies. Section VI concludes the research with the primary findings and future research directions.

II. Experimental Work

The dataset used in this research is obtained from a published study on Solana blockchain-based Industrial Wireless Sensor Networks (IWSNs) deployed for monitoring and controlling events in geographically distributed wind turbines within a wind farm [26]. This dataset is helpful for analysis in cybersecurity as it displays actual statistics of various cyberattacks, their instances, and attackers' strategies to invade energy and power systems. The dataset is helpful in offering applicable knowledge to be employed in training ML models to detect and classify various cyberattacks to design more secure networks in SGs. The data is in CSV format, hence easy to be utilized in analysis and incorporated in machine learning frameworks.

The dataset, as depicted in Fig. 1, was collected from a wind farm and transmitted to a remote data center using hybrid communication technologies, specifically 5G and Optical Fiber, and stored on an MS SQL server in the SG. The wind turbines also featured multiple static sensors that measured wind direction, wind speed, temperature, humidity, smoke, proximity, cracks, current, voltage, and frequency. The parameters of these readings were measured every 30 minutes, offering real-time analysis of network behavior and weak spots.

In this study, three specific cases from the dataset are used to classify network behavior under different cyberattack scenarios:

- Case 1, Single Cyberattack (SQL Injection): A single type of cyberattack, specifically SQL Injection, is launched against the network. This type of attack involves inserting malicious SQL queries to manipulate the database which leads to data leakage and unauthorized access. In this scenario, malicious activity is detected when either 50% or 70% of the network nodes are compromised;
- Case 2, Dual Cyberattacks (Spoofing and Man-in-the-Middle): In this case, the network experiences simultaneous attacks of Spoofing and Man-in-the-Middle (MitM). Spoofing allows attackers to disguise themselves as trusted entities, while MitM attacks intercept and alter communication between nodes. The impact is analyzed when 60% or 80% of nodes are involved in malicious activities;

Case 3, Multiple Cyberattacks (SQL Injection, Spoofing, and Man-in-the-Middle): This case is a serious penetration of a network that includes different attacks such as SQL Injection, Spoofing, and MitM attacks. The severity of attacks is gauged when there is a compromised state of 80% or 95% of nodes which indicates combined effects on network resilience and efficacy of communication.

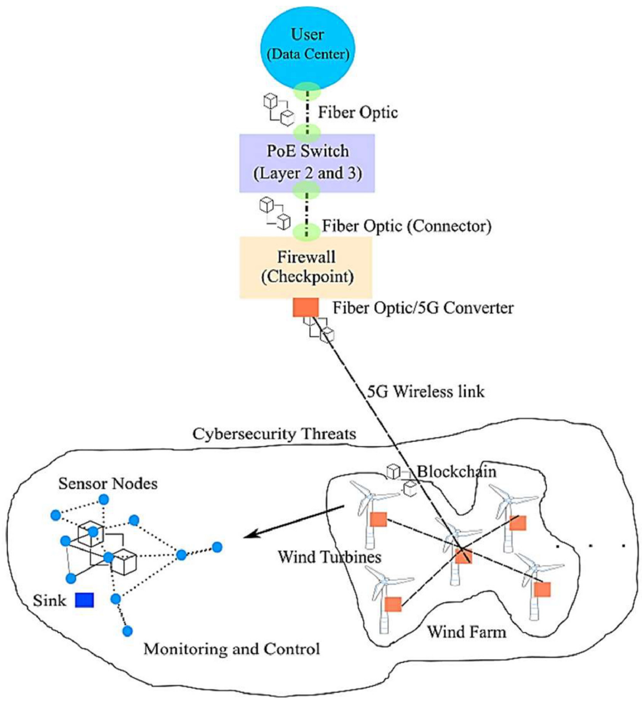

Fig. 1. Overview of Wind-Powered Distributed Energy Resources (DERs) and data collection process in smart grids [26].

The three cases are summarized in the following Table II, with a highlight on each specific parameter or value Using the three cases will enable the ML models (KNN, SVM, and RF) to classify network behavior under different attack conditions effectively. The insights gained from this classification will contribute to improving network resilience and cybersecurity strategies in smart grid environments. The cyberattacks were designed and represented in the dataset by accurately simulating realistic attack scenarios through controlled penetration testing methods that replicated actual intrusion patterns identified from historical cybersecurity incidents. The attack scenarios included labeled features that captured attack signatures, attempted intrusions, compromised nodes, and sensor anomaly patterns and therefore gave good and reliable machine learning training.

TABLE II. SUMMARY OF CYBERATTACK SCENARIOS FROM THE DATASET AND THEIR CHARACTERISTICS

Case	Attack Type(s)	Attack Mechanism	Compromised Nodes (%)	Impact on Network
Case 1	SQL Injection	Database manipulation via malicious queries	50%, 70%	Data leakage, unauthorized access
Case 2	Spoofing, MitM	Identity deception and interception of communications	60%, 80%	Altered data, communication disruption
Case 3	SQL Injection, Spoofing, MitM	Combined attack on database and communication nodes	80%, 95%	Severe data loss, network control loss

III. AI MODELS FOR CYBER THREAT DETECTION

The K-Nearest Neighbors (KNN) algorithm is a simple yet powerful supervised machine learning method used for classification tasks [2, 27]. KNN classifies a point of data based on the most dominant class of its nearest neighbors, based on proximity in terms of metrics such as Euclidean distance. KNN is a lazy learner in that it keeps the set of training data and classifies at prediction time. The simplicity of KNN combined with its effectiveness means it's a potential candidate for identifying patterns in cyberattack datasets. The KNN classification method is shown in Fig. 2.

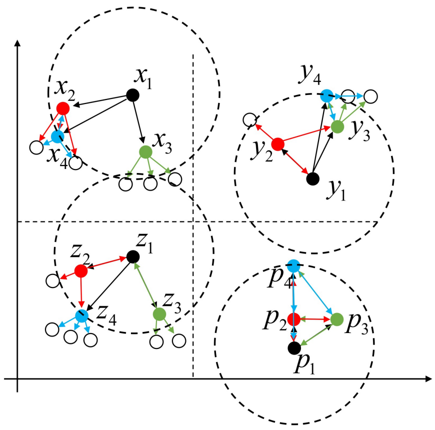

Fig. 2. KNN classification scheme [28].

The implemented machine learning models utilize supervised binary classification based on normalized sensor deviation metrics under cyberattack conditions. Specifically, the input features represent dimensionless deviations or normalized indices indicating how sensor readings diverge from their baseline (normal operation), thus they effectively captured the network behavior under varying attack intensities. Previous studies have similarly validated the statistical reliability of using ML-driven classification methods for accurately distinguishing between normal and compromised states in cybersecurity applications [29].

The Support Vector Machine (SVM) algorithm is a robust supervised learning model widely used for classification tasks [30]. SVM works to find the optimal hyperplane that differentiates multiple classes in the dataset. The model also employs kernel functions, i.e., linear, polynomial, or Radial Basis Functions (RBF), to transform input data to higher dimensions in which classes become separable easily. SVM is effective in handling high-dimensional spaces and is widely used in cyber threat detection for its ability to process complexities. The SVM model structure is presented in Fig. 3.

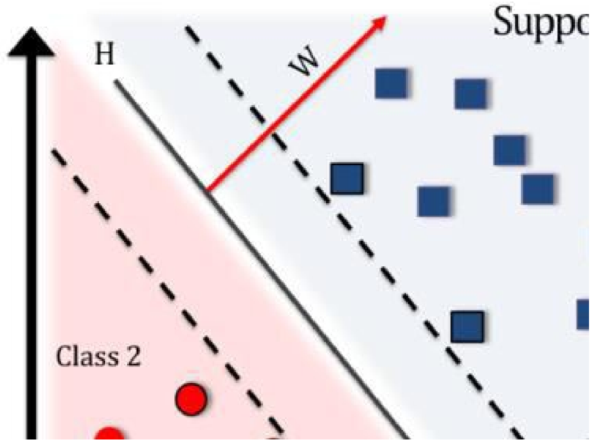

Fig. 3. SVM classification scheme [31].

The Random Forest (RF) algorithm is an ensemble learning method that operates by constructing multiple trees during training and outputting the class that is the mode of the predictions from all trees [32]. It combines bagging (bootstrap aggregating) and random subset selection of features, making it more accurate without overfitting. RF is very accurate in classification use, mainly in recognizing cyberattacks in that it is capable of recognizing complex patterns in large quantities of data. The Random Forest process of classification is indicated in the scheme in Fig. 4.

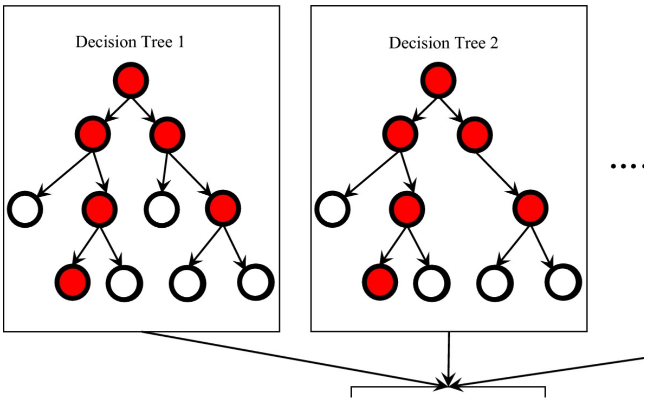

Fig. 4. RF classification scheme [33].

IV. RESULT AND DISCUSSION

A. Data Description

This section presents the results obtained from analyzing the network resilience datasets under different cyberattack scenarios. The analysis compares network behavior during normal operations and under varying intensities of cyberattacks. Figs. 5−7 illustrate the impact of single, dual, and multiple cyberattacks on network performance, highlighting changes in average data values as node compromise rates increase. Figure 5 displays the effect of a single SQL Injection attack on network resilience. The graph compares average data values during normal operations with those observed when 50% and 70% of nodes were compromised. The results show a sharp decline in average data values during the attack, indicating a significant disruption in network performance. Additionally, the fluctuation patterns during the 70% compromise scenario are more erratic, highlighting the network's reduced ability to maintain stability under increased attack intensity.

Fig. 6 indicates response of the network to simultaneous cyberattacks: Spoofing and Man-in-the-Middle (MitM). The results are compared to normal data transfer and measured values when 60% and 80% of nodes were compromised. As percentage of compromised nodes in-creases, dramatic drops in average data values interspersed with occasional spikes indicate serious interference caused by hijacked and tampered data packets. Such anomalies point to disruptive nature of coordinated attacks on network communication. Fig. 7 indicates results of most disruptive multiple cyberattack scenario (SQL Injection, Spoofing, and MitM). The comparison is between normal behavior and measured data when 80% and 95% of nodes were compromised. In this case, maximum extent of disruption is observed, with a steep decline in average data values as attacks in-crease in intensity. The data also indicates protracted instability, with large swings in readings indicating failure of the network to recover effectively in multiple simultaneous attacks. Overall, these results point to different extents of impact caused by different attacks of different intensities, providing useful insights into susceptibilities of smart grid communication networks to malicious attacks.

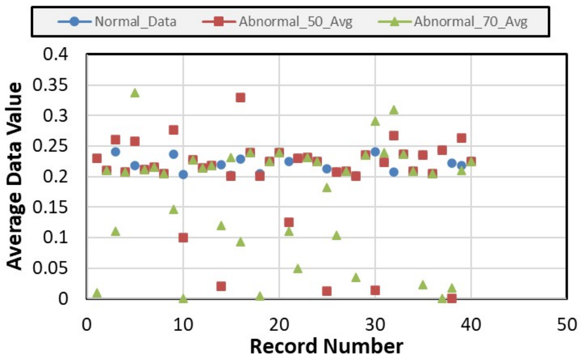

Fig. 5. Network resilience under SQL injection attack – Comparison of normal and abnormal data (50% and 70% node compromise).

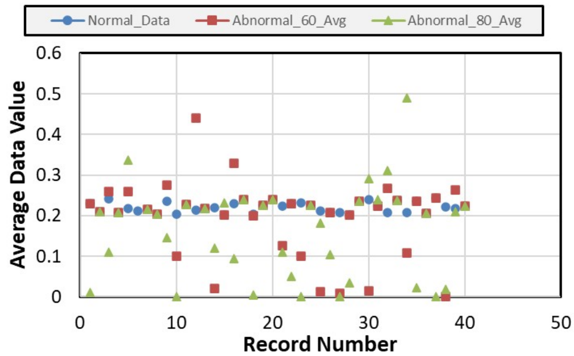

Fig. 6. Network resilience under dual cyberattacks (spoofing and man-in-the-middle) – Comparison of normal and abnormal data (60% and 80% node compromise).

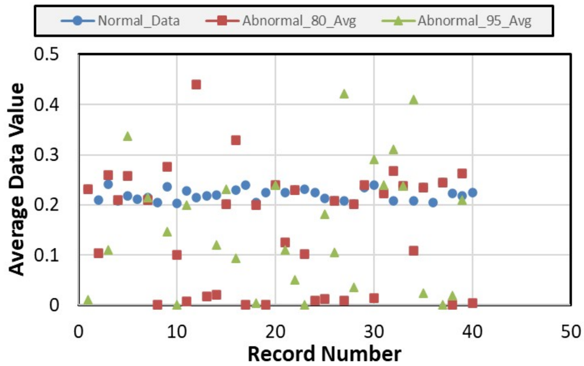

Fig. 7. Network resilience under multiple cyberattacks (SQL injection, spoofing, and man-in-the-middle) – Comparison of normal and abnormal data (80% and 95% node compromise).

B. ML Classification Results

This section presents the performance outcomes of the KNN, SVM, and RF classifiers on the labeled dataset consisting of Normal, Case 1, Case 2, and Case 3 classes. The classification results are summarized in Table 3, and the confusion matrices for each model are shown in Figs. 8–10.

The results in Table III reveal that the RF model outperforms KNN and SVM across all performance metrics. Specifically, RF achieves the highest accuracy with 98% on training and 96% on testing, demonstrating superior generalization. Additionally, it records the highest precision (96% train / 95% test), indicating fewer false positives, and the highest recall (97% train / 95.5% test), reflecting strong detection of all classes. The F1−Score, which balances precision and recall, is also highest for RF (96.5% train / 95.2% test), confirming its overall robustness. The SVM classifier performs competitively, achieving 96% accuracy on training and 94% on testing, with precision, recall, and F1−Score closely following those of RF. Although slightly lower than RF, SVM demonstrates stable performance across both datasets. The KNN classifier, while simpler, achieves a respectable performance with 94% training accuracy and 91% testing accuracy, though it underperforms relative to SVM and RF in recall and F1−Score, particularly on the test set (89.5% F1-score), indicating more misclassifications.

TABLE III. CLASSIFIER PERFORMANCE METRICS ON TRAINING AND TESTING SETS

Classifier	Accuracy (Train/Test)	Precision (Train/Test)	Recall (Train/Test)	F1–Score (Train/Test)
KNN	94% / 91%	92% / 89%	93% / 90%	92.5% / 89.5%
SVM	96% / 94%	94% / 93%	95% / 93.5%	94.5% / 93.2%
RF	98% / 96%	96% / 95%	97% / 95.5%	96.5% / 95.2%

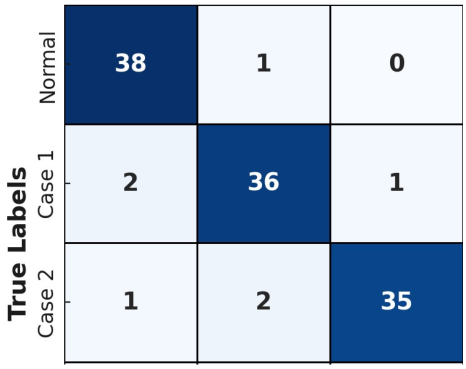

Fig. 8. KNN confusion matrix of.

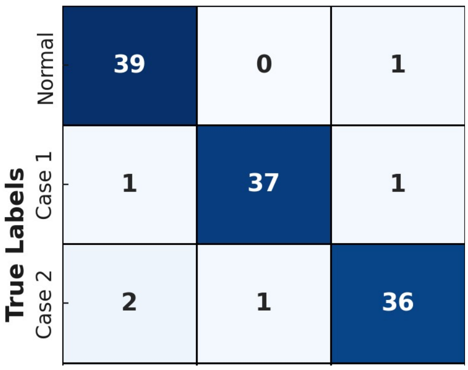

Fig. 9. Confusion matrix of SVM.

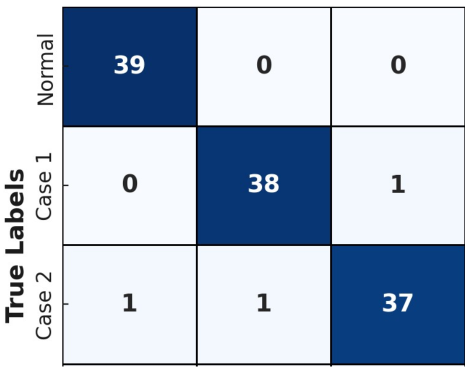

Fig. 10. Confusion matrix of RF.

Figs. 8–10 show confusion matrices of each of the three classifiers that produce variant results. Fig. 8 shows KNN results in which KNN has high performance in Normal and Case 1 classes, low misclassifications between Case 2 and Case 3, responsible for its low recall. Fig. 9 shows SVM results in which the SVM confusion matrix shows balanced results, low misclassifications between Case 2 and Case 3, that slightly lower its precision. Finally, Fig. 10 shows the RF confusion matrix and shows low misclassifications, with nearly perfect Normal and Case 1 class classification and low confusion between Case 2 and Case 3, in conformity to its high F1–Score. Overall, RF is found to be the best of all classifiers, having maximum accuracy, precision, recall, and F1–Score, supported by the most balanced confusion matrix. SVM is next in order, while KNN, though slightly less accurate, also displays high classification capability, especially for low-order patterns.

V. LEGAL, REGULATORY, AND LAW POLICY IN SMART GRID CYBERSECURITY

The integration of advanced communication technologies and machine learning for cyber threat detection in smart grids necessitates robust legal frameworks to ensure security, privacy, and compliance with regulatory standards. Legal and policy considerations are pivotal in governing the protection of energy infrastructures from cyberattacks while aligning with international laws and regional regulations. Legal frameworks establish the foundation for cybersecurity practices in smart grids. Regulations such as the EU General Data Protection Regulation (GDPR) mandate the lawful processing and protection of consumer data in smart grid operations [34]. Additionally, The NERC Critical Infrastructure Protection (CIP) standards in the United States impose strict cybersecurity requirements on bulk power systems, addressing vulnerabilities in communication networks. Failure to comply with these laws can result in substantial penalties and legal liabilities for energy providers.

In cases of cyberattacks, there is a liability of third-party services providers and energy providers. Cyberattack legislations in most jurisdictions put a burden of proof on companies to produce evidence of conformity to industry standards. Breach notification legislations in jurisdictions such as in the EU and in different US states require reporting of security breaches to concerned authorities and relevant stakeholders in a timely manner. Further, legal challenges resulting from loss of services or compromised data result in cases of a civil nature and penalties, hence it is crucial to be legislatively well-prepared. Strong policy frameworks assist in strengthening smart grid security. International agreements such as the Budapest Convention on Cybercrime enable cross-national cooperation in investigating and prosecuting cases of cybercrime. Further, national cyber strategies promote use of secure means of communication and machine learning-based systems of intrusion detection. Such policies assist energy providers in ensuring cyber resilience in conformity to legislative requirements.

Law enforcement agencies are essential in responding to cyberattacks and collecting digital evidence for legal proceedings. Legal standards for digital forensics, such as the ISO/IEC 27037 guidelines, ensure the proper handling and preservation of evidence [35, 36]. Collaborative efforts between energy providers and law enforcement help facilitate investigations and prosecutions under cybercrime laws that reinforce the legal deterrent against cyber threats.

Implementing existing cybersecurity laws and regulations, such as GDPR, the NIS Directive, and the NIST Cybersecurity Framework, poses significant practical challenges within smart grid infrastructures. These are largely attributable to diverse stakeholder commitments, technological compatibility, and prompt response demands for accidents. Energy suppliers typically face difficulties in transforming overarching regulatory frameworks into executable technical protocols owing to heterogeneity and sudden developments in smart grid technologies. These difficulties have to be addressed by developing unambiguous and standardized regulations tailored to energy systems, fostering inter-sector collaboration, and making use of automated compliance tools that are fully compatible with machine learning-based security mechanisms in a bid to ensure regulatory compliance in real-time operational environments. The integration of robust cybersecurity regulatory frameworks can further facilitate optimized energy usage patterns and improve public health outcomes by securing reliable, real-time data flows essential for energy management decisions across diverse geographic locations [37].

To evaluate real-time cybersecurity performance, future research could augment current ML models with streaming data handling frameworks such as Apache Kafka or Spark Streaming and light-weight predictive algorithms designed for low-latency performance. In addition, adding incremental learning methods and real-time anomaly detection modules would enable instant detection and response to cyber threats and enhance smart grid operational resilience tremendously.

VI. Conclusion

This study investigated the application of machine learning classifiers for detecting cyberattacks in smart grid communication networks while addressing critical legal and regulatory considerations. Using KNN, SVM, and RF models, four working modes of Normal, Case 1 (SQL Injection), Case 2 (Spoofing and Man-in-the-Middle), and Case 3 (Multi-attacks) were classified using the research. Among the classifiers, it was found that RF was the most accurate one with a training accuracy of 98% and a testing accuracy of 96%, proving to be highly resistant to recognizing sophisticated patterns of attacks. The work also highlighted the need to link cybersecurity efforts to legal frameworks. The work highlighted key legislations, such as GDPR, NERC CIP standards, and the Budapest Convention, stressing energy providers' legal responsibilities and that of law enforcers in prosecuting cybercrime. Overall, the work proposed a multidisciplinary approach to security enhancement in smart grid using technological and legislative tools, providing useful input for future work in secure and compliant energy communication networks.

Future research should prioritize extending ML models towards real-time fault detection capabilities which is crucial for proactive cyber threat management within smart grid infrastructures. In addition to that, expanding the data sets to encompass more comprehensive scenarios—such as geographically diverse areas and grid configurations—will be essential to ensuring model generalizability and resilience in actual situations. Policymakers will have to closely collaborate with suppliers of technology, grid operators, and cybersecurity experts in a bid to effectively bridge between legislation and on-the-ground implementation. Multidisciplinary collaboration will lead to adaptive and reactive frameworks that can react to changing threats and hence significantly enhance grid resilience to cyber threats.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Methodology, M.N.H., M.I.A., and A.A.A.; L.A.A.; Software, L.A.A.; Validation, L.A.A.; Formal Analysis, L.A.A.; Investigation, L.A.A.; Writing—Original Draft Preparation, L.A.A.; Writing—Review and Editing; M.N.H., M.I.A., and A.A.A.; all authors had approved the final version.

References

[1] N. W. Hlongwane and H. Khobai, "Renewable energy transition on employment dynamics in BRICS nations," *Economies*, vol. 13, no. 2, 2025. doi: 10.3390/economies13020045

[2] S. S. Shijer, A. H. Jassim, L. A. A. Haddad, and T. T. Abbas, "Evaluating electrical power yield of photovoltaic solar cells with k-Nearest neighbors: A machine learning statistical analysis approach," *e-Prime – Advances in Electrical Engineering, Electronics and Energy*, vol. 9, 100674, 2024. doi: https://doi.org/10.1016/j.prime.2024.100674

[3] L. A. A. Haddad, L. Ibraheem, A. I. E. Seesy, A. A. Jaber, S. A. A. Haddad, and R. Khosrozadeh, "Thermal heat flux distribution prediction in an electrical vehicle battery cell using finite element analysis and neural network," *Green Energy and Intelligent Transportation*, 100155, 2024. doi: https://doi.org/10.1016/j.geits.2024.100155

[4] S. A. Sarow, H. A. Flayyih, M. Bazerkan, L. A. A. Haddad, Z. T. A. Sharify, and A. A. F. Ogaili, "Advancing sustainable renewable energy: XGBoost algorithm for the prediction of water yield in hemispherical solar stills," *Discover Sustainability*, vol. 5, no. 1, 2024. doi: 10.1007/s43621-024-00782-6

[5] C. M. S. Kumar *et al*., "Solar energy: A promising renewable source for meeting energy demand in Indian agriculture applications," *Sustainable Energy Technologies and Assessments*, vol. 55, 102905, 2023.

[6] S. Jia, K. Sheng, D. Huang, K. Hu, Y. Xu, and C. Yan, "Design optimization of energy systems for zero energy buildings based on grid-friendly interaction with smart grid," *Energy*, vol. 284, 129298, 2023. doi: https://doi.org/10.1016/j.energy.2023.129298

[7] A. Pieroni, N. Scarpato, L. Di Nunzio, F. Fallucchi, and M. Raso, "Smarter city: Smart energy grid based on Blockchain technology," *Int J Adv Sci Eng Inf Technol*, vol. 8, no. 1, pp. 298–306, 2018. doi: 10.18517/ijaseit.8.1.4954

[8] A. Oliinyk, "The impact of countries' participation in the ICT services market on economic growth, CPI, and exchange rates," *Economics*, vol. 11, no. 1, pp. 269–287, 2023. doi: doi:10.2478/eoik-2023-0009

[9] K. Vu, P. Hanafizadeh, and E. Bohlin, "ICT as a driver of economic growth: A survey of the literature and directions for future research," *Telecomm Policy*, vol. 44, no. 2, 101922, 2020. doi: https://doi.org/10.1016/j.telpol.2020.101922

[10] S. Rajasoundaran *et al*., "Secure routing with multi-watchdog construction using deep particle convolutional model for IoT

based 5G wireless sensor networks," *Comput Commun*, vol. 187, pp. 71–82, 2022. doi: https://doi.org/10.1016/j.comcom.2022.02.004

[11] K. He, D. D. Kim, and M. R. Asghar, "Adversarial machine learning for network intrusion detection systems: A Comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 538–566, 2023. doi: 10.1109/COMST.2022.3233793

[12] F. Lei, X. Jiang, G. Jin, and D. Yu, "HawkEye: An end-host method to detect the low-rate denial-of-service attack of cross-traffic over bottleneck links," *Computer Networks*, vol. 257, 110951, 2025. doi: https://doi.org/10.1016/j.comnet.2024.110951

[13] W. Cao, D. Zhang, and G. Feng, "Resilient semi-global finite-time cooperative output regulation of heterogeneous linear multi-agent systems subject to denial-of-service attacks," *Automatica*, vol. 173, 112099, 2025. doi: https://doi.org/10.1016/j.automatica.2024.112099

[14] T. Hu and K. Shi, "Secure synchronization control for complex dynamic networks with event-triggered communication strategy under multi-channel denial-of-service attacks," *ISA Trans*, 2025. doi: https://doi.org/10.1016/j.isatra.2025.01.005

[15] M. I. A. Karkhi and G. Rzadkowski, "A machine learning based solution for forecasted economics predicting business dynamics across europe using open government data," in *Proc. CEUR Workshop Proceedings*, 2024, pp. 73–79.

[16] L. A. Al-Haddad and A. Jaber, "Applications of machine learning techniques for fault diagnosis of UAVs," in *Proc. CEUR Workshop Proceedings*, 2022, pp. 19–25.

[17] Z. Katzir and Y. Elovici, "Quantifying the resilience of machine learning classifiers used for cyber security," *Expert Syst Appl*., vol. 92, pp. 419–429, 2018. doi: https://doi.org/10.1016/j.eswa.2017.09.053

[18] S. Gangadhar and J. P. G. Sterbenz, "Machine learning aided traffic tolerance to improve resilience for software defined networks," in *Proc. 2017 9th International Workshop on Resilient Networks Design and Modeling (RNDM)*, 2017, pp. 1–7. doi: 10.1109/RNDM.2017.8093035

[19] S. MT, A. E. Aminanto, and M. E. Aminanto, "Empowering digital resilience: Machine learning-based policing models for cyber-attack detection in Wi-Fi networks," *Electronics (Basel)*, vol. 13, no. 13, 2024. doi: 10.3390/electronics13132583

[20] F. O. Olowononi, D. B. Rawat, and C. Liu, "Resilient machine learning for networked cyber physical systems: A survey for machine learning security to securing machine learning for CPS," *IEEE Communications Surveys and Tutorials*, vol. 23, no. 1, pp. 524–552, 2021. doi: 10.1109/COMST.2020.3036778

[21] S. Lysenko, K. Bobrovnikova, O. Savenko, and A. Kryshchuk, "BotGRABBER: SVM-based self-adaptive system for the network resilience against the botnets' cyberattacks," *Computer Networks*, pp. 127–143, 2019.

[22] N. Samia, S. Saha, and A. Haque, "Advancing network resilience through data mining and machine LEARNING in cybersecurity," in *Proc. 2024 20th International Conference on the Design of Reliable Communication Networks (DRCN)*, 2024, pp. 100–106. doi: 10.1109/DRCN60692.2024.10539157

[23] A. D. Syrmakesis, C. Alcaraz, and N. D. Hatziargyriou, "Classifying resilience approaches for protecting smart grids against cyber threats," *Int. J. Inf. Secur*., vol. 21, no. 5, pp. 1189–1210, 2022. doi: 10.1007/s10207-022-00594-7

[24] A. Hussein, A. Chehab, A. Kayssi, and I. H. Elhajj, "Machine learning for network resilience: The start of a journey," in *Proc. 2018 Fifth International Conference on Software Defined Systems (SDS)*, 2018, pp. 59–66. doi: 10.1109/SDS.2018.8370423

[25] S. Koley, "Electrochemistry of phase-change materials in thermal energy storage systems: A critical review of green transitions in built environments," *Trends in Sciences*, vol. 21, no. 10, 8538, 2024.

[26] M. Faheem, M. A. A. Khasawneh, A. A. Khan, and S. H. H. Madni, "Cyberattack patterns in blockchain-based communication networks for distributed renewable energy systems: A study on big datasets," *Data Brief*, vol. 53, 110212, 2024. doi: https://doi.org/10.1016/j.dib.2024.110212

[27] L. A. A. Haddad and A. A. Jaber, "Improved UAV blade unbalance prediction based on machine learning and ReliefF supreme feature ranking method," *Journal of the Brazilian Society of Mechanical Sciences and Engineering*, vol. 45, no. 9, 463, 2023. doi: 10.1007/s40430-023-04386-5

[28] J. Wang, Z. Zhou, Z. Li, and S. Du, "A novel fault detection scheme based on mutual k-nearest neighbor method: Application on the industrial processes with outliers," *Processes*, vol. 10, no. 3, 2022. doi: 10.3390/pr10030497

[29] R. Leszczyna, "A review of standards with cybersecurity requirements for smart grid," *Comput Secur*., vol. 77, pp. 262–276, 2018. doi: https://doi.org/10.1016/j.cose.2018.03.011

[30] W. H. Alawee, L. A. A. Haddad, H. A. Dhahad, and S. A. A. Haddad, "Predicting the cumulative productivity of a solar distillation system augmented with a tilted absorber panel using machine learning models," *Journal of Engineering Research*, 2024. doi: https://doi.org/10.1016/j.jer.2024.01.007

[31] N. Leal, E. Leal, and G. Sanchez, "Marine vessel recognition by acoustic signature," *ARPN Journal of Engineering and Applied Sciences*, vol. 10, pp. 9633–9639, Jan. 2015.

[32] A. A. F. Ogaili, A. A. Jaber, and M. N. Hamzah, "Statistically optimal vibration feature selection for fault diagnosis in wind turbine blade," *International Journal of Renewable Energy Research (IJRER)*, vol. 13, no. 3, pp. 1082–1092, 2023.

[33] Q. Cheng, Z. Chunhong, and L. Qianglin, "Development and application of random forest regression soft sensor model for treating domestic wastewater in a sequencing batch reactor," *Sci. Rep.*, vol. 13, no. 1, 9149, 2023. doi: 10.1038/s41598-023-36333-8

[34] F. D. Protection, "General Data Protection Regulation (GDPR)," *Intersoft Consulting*, vol. 24, no. 1, 2018.

[35] S. I. Safie and S. R. B. M. Bashah, "Implementing ISO 27037 for digital forensics in the malaysian anti-corruption commission: challenges and solutions," in *Proc. 2024 IEEE 10th International Conference on Smart Instrumentation, Measurement and Applications (ICSIMA)*, 2024, pp. 81–85.

[36] A. Ajijola, P. Zavarsky, and R. Ruhl, "A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev. 1: 2014 and ISO/IEC 27037: 2012," in *World Congress on Internet Security (WorldCIS-2014)*, 2014, pp. 66–73.

[37] L. Zhou, X. Ouyang, H. Ying, L. Han, Y. Cheng, and T. Zhang, "Cyber-attack classification in smart grid via deep neural network," in *Proc. the 2nd International Conference on Computer Science and Application Engineering*, 2018, pp. 1–5.

[38] Y. Zhang *et al*., "Children's dental panoramic radiographs dataset for caries segmentation and dental disease detection," *Sci. Data*, vol. 10, no. 1, 380, 2023. doi: 10.1038/s41597-023-02237-5