JCBI
Journal of Computing & Biomedical Informatics
ISSN: 2710 - 1606
Volume 09 Issue 01
2025

Research Article
https://doi.org/10.56979/901/2025

Cloudscape Protection: Securing AMI Meters with Multi-Cloud Strategies in Pakistan

Ansar Alam Khan[1], Ahmad Naeem[1], Naeem Aslam[1], Muhammad Fuzail[1], Sahrish Bashir[1], and Muhammad Huzaifa Rashid[1*]

[1]Department of Computer Science, NFC-IET, Multan, Pakistan.
[*]Corresponding Author: Muhammad Huzaifa Rashid. Email: huzaifarashid6447@yahoo.com

Received: March 11, 2025 **Accepted:** May 16, 2025

Abstract: AMI is disrupting grid and consumer relationship within the energy sector of Pakistan. But the increased dependence on cloud services also comes with significant security challenges, including data leaks and breaches, unauthorized access, and service outages. To this end, this work advocates for a multi-cloud approach as a powerful solution for security, resilience and performance improvement for AMI systems. By spreading infrastructure across multiple cloud providers, it reduces risk associated with single cloud provider reliance including vendor lock-in and single points of failure. It uses a real data-set on AMI and various machine learning techniques such as Decision Trees, Random Forests, Support Vector Machines to detect anomalies and possible intrusions. Out of these, Decision Trees, with accuracy level as highly as 92.5% and good precision and recall levels, proved the effectiveness of the model for detecting the threat in real-time. The paper also discusses technical, operational and legal challenges faced in implementation of multi-cloud infrastructures in Pakistan which provides perspective on its cost-effectiveness and implementation issues. This study adds to the emerging body of knowledge on smart grid security, as it provides an empirically validated AI-empowered multi clouds security framework for the developing countries. It has the practical value to power utilities, policy makers and researchers who are interested in developing scalable secure smart grid infrastructure.

Keywords: Advanced Metering Infrastructure (AMI); Multi-Cloud Security; Anomaly Detection; Smart Grid Cybersecurity

1. Introduction

Increasingly there is a high urgency on the modernization of nationwide power networks due to the world-wide transformation to smart grids, which establishes the integration of AMI as a core element of modern energy distribution systems. The AMI meter or the "smart meter," has changed the very foundation of the way that energy is read, controlled, and billed. They support real-time monitoring of energy usage, dynamic pricings, and bidirectional communication with electricity consumers[1]. These features improve the productivity and dependability of the energy supply. The deployment of AMI in Pakistan is an essential aspect of grid modernization and stabilization of the national energy system in Pakistan.The energy industry of Pakistan has been facing inefficiencies, losses, outdated distribution system. Nevertheless, AMI is by nature reliant on digital technology, namely cloud computing, for data storage, processing and analytics. On one hand, they provide scalability, saves cost, and facilitate remote access as compared to traditional approaches, thus more pertinently referred to as cloud-based architecture (Lynn McCarthy & Luo, 2012): they are full of security risks[2]. This include data theft, down times, unauthorised access and loss of control at the hands of third-party cloud hosters. AMI systems

contain valuable operation information as well as private information, confidentiality, integrity and availability are not just technical issues but also regulatory and ethical issues.

One real shortcoming in the status quo is that we place heavy reliance to single-cloud deliveries of AMIs. In Pakistan, most of the utility companies have deployed centralized, single-cloud model because of its simplicity and cost. However, this approach is susceptible to many shortcomings, such as commercial dependence, single failure points, and limited resistance to focused cyber-attacks[3]. Faulty access to the premises could result in millions of compromised consumers and tens of megawatts of national energy reactor exposure at risk from a failed cloud provider such as failure or attack. Furthermore, conformance to global regulations such as the General Data Protection Regulation (GDPR), National Institute of Standards and Technology (NIST) standards, and other local compliance frameworks is problematic in single cloud solutions[4]. To combat those downfalls, multi-cloud strategies have been more widely embraced. About multi-cloud Multi-cloud refers to deploying different parts of an application across separate clouds. Such an approach provides for le veraging of the strengths of multiple vendors while eliminating the disadvantages of complete dependence on a single vendor[5]. Multi-cloud is especially beneficial in the world of AMI systems, where uptime, access to real-time data and strong cybersecurity must just work.

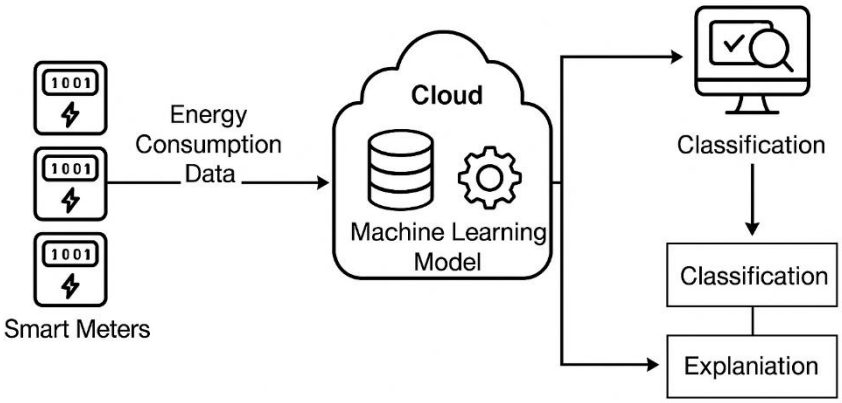

Figure 1. AMI System Architecture Diagram

Nevertheless, multi-cloud architectures come with their own challenges. Adopting more than one cloud platform creates operational challenges, cost overhead, and requires expertise in both cloud management, data integration, and security. These difficulties are further exacerbated, at least in the developing country context of Pakistan, by inadequate infrastructure, resource issues, as well as lack of trained individuals. Thus, it is important to assess whether it is feasible and beneficial to deploy multi-clouds adapted to the local socio-economic and regulatory context of Pakistan. Coincident with the progress in cloud computing is the rise of artificial intelligence (AI) and machine learning (ML) in energy. These solutions deliver predictive analytics, real-time anomaly observation, and next-generation threat mitigation methods[6]. Embedding ML algorithms in AMI systems will enable utilities to predictively detect irregular consumption usage, tampering, or cybersecurity breach. This is not only more efficient from an operational perspective, but also makes the security framework more robust. For multi-cloud designs, AI-based security models can help monitor different environments and maintain policy rules uniformly enforced across platforms[7] . In this paper, we propose a hybrid framework of multi-cloud architecture and AI-based anomaly detection to protect AMI systems in Pakistan. We leveraged a real-world dataset of 120K AMI meter readings to compare and evaluate machine learning models such as Decision Trees, Random Forests and Support Vector Machines (SVMs) to detect abnormalities and possible intrusions. In that study, the best model (Decision Tree model) had that attained 92.5% accuracy with dense precision and recall, and robust F1-scores, indicating its capability to detect the malicious activities and reducing false positive and negative inside the procedure.

Our experiments, which were carried out with an empirical analysis on the AMI dataset, exhibit the potential value of the combination of machine learning and the multi cloud. As well as for the verification of the quality and reliability of the proposed methods, we will also investigate the technical and economic consequences of implementing such solutions under real scenarios[8]. We also consider policy and

regulatory issues, particularly with reference to NEPRA (National Electric Power Regulatory Authority) guidelines in Pakistan and international standards[9]. This work is significant due to its twofold contribution: first it addresses the literature gap by providing an exhaustive Pakistan related research regarding multi-cloud security for AMI systems[10]. Secondly, It offers guidance and recommendations for decision makers in utilities, policy makers, cyber security experts and researchers. We believe that well-planned and invested multi-cloud strategies aided by AI and ML can provide a scalable, secure and resilient platform for the transformation of the smart grid infrastructure in Pakistan[11]. Finally, this work is a timely and critical first step in the direction of increasing the cybersecurity of the energy sector of Pakistan. With the accelerated pace of digital transformation and the threat landscape evolving so rapidly, the inclusion of comprehensive security models is not a nice-to-have — it's a must-have[12]. Leveraging the best of multi-cloud architecture, AI-based anomaly detection, we present a future-proofed solution to guard one of the smart grid's most vital organs: the AMI meter.

The organization of this paper aims to give an overview of the security situation of AMI system in Pakistan and whether multi-cloud security policies are feasible. We start with motivations and background of the work, which includes single-cloud vulnerabilities and emerging threats against smart grids. 2 Related literature review In this section, we review the literature related to the research objective, with a focus on existing cloud security solutions, multi-cloud adoption among energy sector, and usage of AI and ML techniques in security. This is followed by a section about our approach and design process, starting with how the data was preprocessed and how we trained models, and what anomaly metrics we used for evaluation.

2. Related Work

Smart grids rely on Advanced Metering Infrastructure (AMI) to achieve realtime monitoring, dynamic pricing, and automatic power management. While cloud-based IoT systems continue to become more intensive, assuring the security, dependability, and compliance of such a platform has become one of the major researches. There are already some works that have surveyed the state of art in the cloud-based AMI security[13][14] and multi-cloud approaches [15] or conducted a literature survey on applying AI and ML to protect smart grid infrastructures [16].

2.1. Cloud-Based AMI Security

The AMI systems and cloud computing integration has several functional opportunities in scaling, storage and processing potential. But the downside is that we add new cyber security risks. Based on the above literatures, cloud-based AMI is vulnerable to trust and authentication problems, and authors in (Wu and Zhang, 2020)[17] developed a trust-based scheme to increase the security level of data. Similarly, Santos et al. (2019)[18] offered a resource efficient cryptographic model for protecting data propagation in AMI systems, including the necessity of end-to-end encryption and data integrity verification. These works illustrate the requirement for strong security techniques in cloud-oriented AMI infrastructures.

Even so, the reliance on single cloud service providers has led to a risk concentration. Vendor lock-in, single point of failure, lack of flexibility are the major challenges identified by Xu and He (2020)[19] and addressed by their cost-efficient multi-cloud model for smart grid. According to their findings, single-cloud architectures are easier to deploy but lack the redundancy required for a critical energy infra-structure.

2.2. Multi-Cloud Strategies in the Context of AMI Systems

In order to resolve the limitations of single-cloud architectures, researchers have investigated multi-cloud approaches to improve system security, redundancy, and performance. Das et al. (2020)[20] provided a failover method for multi-cloud, with the purpose of improving the reliability of the energy grid infrastructures in the event of service failings. Work done and sensitive data are spread over various cloud service providers by multi-cloud architectures, which lowers the risk of outages and improves data availability. Brown et al. (2020)[21], have recently taken this even one step further by introducing full multi-cloud framework for secure smart grid operations. Their approach was centered on interoperability, optimization of performance, and compliance with data protection laws. cloud-compare-1But they also recognised the operational challenges – and the costs associated – with keeping a lid on diverse clouds. These doubts are reflected in the study of Lee and Park (Lee and Park, 2022)[22] where the performance of machine learning algorithms were evaluated in multi-clouds and increased latency or overhead of integration was found. In AMI systems, Ali et al. (2023)[23] presented a federated anomaly detection

model on the multi-cloud systems. Their findings show that distributed data analytics across clouds is feasible to achieve, and can lead to much better detection accuracy without violating data privacy.

2.3. AI and ML for Smart Grid Security

Recently novel ideas of artificial intelligence (AI)/machine learning (ML) have been proposed [24, 25, 26] for the smart grid security.

Recently, AI and ML have been prominent methodologies that have been utilized towards securing and improving the functioning of AMI systems. Machine learning algorithms, including SVMs, decision trees and ensemble methods, have been found favorable in detecting abnormal consumption patterns, intrusion attempts and anomalous data. Kumar and Singh (2019)[27] used Support Vector Machines (SVM) in fault classification of AMI networks and obtained high accuracy in distinguishing between fault typologies. Also, Choi and Kim (2021)[28] also evaluated several ML models for anomaly detection of AMI and demonstrated how they are relevant for real-time threat detection. Ahmed and Rizvi (2021)[29] studied IoT-based load forecasting in the case of AMI and showed how predictive analytics can be incorporated in demand models to support operating decisions better. Deep learning based methods have also attracted much attention. In Zhang and Li (2022)[30], Convolutional Neural Networks (CNNs) were proposed to enhance cyber-attack detection in smart grid networks. On the other hand, adversarial training approaches were proposed by Yang and Zhou (2023)[31] in protection against the advanced cyber challenges to AMI data streams. Although the aforementioned works demonstrate the efficacy of AI/ML in AMI protection, their attention is mostly towards the single-cloud architecture. Thereby, there is uncharted territory when it comes to the fusion of AI/ML with multicloud strategies, especially within the Pakistani landscape.

2.4. Research Gap

Significant contributions of the literature are in the areas of cloud security, multi-cloud architectures and AI/ML applications for AMI systems. However, the gap of combining these fields under a joint framework, especially for developing countries still remains. First, the extant research is deficient in terms of empirical studies dedicated to the energy sector of Pakistan in which infrastructure related issues, regulatory concerns and cyber risks are different from the developed regions[32]. This paper attempts to fill this gap by presenting a catered multi-cloud security framework assisted by machine learning based anomaly detection and also evaluated this work with a real-time AMI dataset of Pakistan.

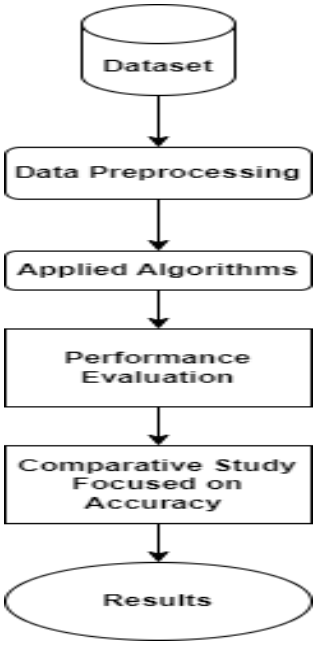

Figure 2. Proposed Model Workflow

3. Materials and Methods

3.1. Preprocessing

Preprocessing of data is very important to process raw AMI meter data into a clean and structured data to perform analysis and machine learning applications [33]. In the presence of noise, and missing or

irrelevant features, as is the case in many real-world applications, pre-processing aims at eradicating these issues such that the data satisfies the quality constraints for reassured prediction and anomaly detection. In this paper, a live AMI dataset consisting of 120,000 rows and 12 fields such as energy consumptions, geolocations, timestamps, cloud service provider, anomaly flags, intrusion alerts and value of latencies was collected. The preprocessing stage was carried out in several steps such as missing data imputation, outliers removal, data normalization, one hot encoding and feature selection. Normalization in this case using Min-Max scale was performed to rescale all numeric features onto the same scale. The categoric fields like Cloud_Service and Multi_Cloud_Strategy were One-Hot Encoded. The filter methods such as the Chi-Square Test and correlation analysis were used to reduce dimensionality and discard the irrelevant or redundant features, and the wrapper methods were conducted using RFE. This preprocessing workflow enabled the raw data to be better suited for training machine learning models.

3.2. Machine Learning Models

In order to detect anomalies, and guard AMI meter data in multi-client cloud at the same time, supervised machine learning models traditionally classified the best suit [34]. The models utilized are Decision Trees (DT), Random Forests (RF) and Support Vector Machines (SVM), which are well known for their abilities in identifying the cyber threats and anomalies in smart grid environments.

3.2.1. Decision Tree Classifier

The data is now categorical in nature (0 or 1) and it is time to implement a decision tree classifier.

Decision Trees have become a popular choice for categorical classification tasks because of their simplicity, interpretability, and applicability to both numerical and categorical variables. The Decision Tree algorithm was used in this study with Gini Impurity splitting criterion. Every decision node in the tree divided the data into branches using the most important features, distinguishing between anomalous and normal energy usage profiles. The model obtained classification with the accuracy of 92.5 % which was the best compared to the tested algorithms. The probability output for a given input feature vector X is expressed as:

$$\text{Prob}_{DT} = DT(X)$$

Where DT represents the trained Decision Tree model and X is the vector of input features.

3.2.2. *Random Forest Classifier*

Random Forest is an ensemble learning technique that builds multiple decision trees and aggregates their predictions to enhance overall accuracy and reduce overfitting. It is particularly suitable for handling high-dimensional data and capturing complex interactions between features. In the context of AMI systems, RF leverages multiple bootstrapped samples of the training data and uses majority voting to classify each instance. The prediction probability for an instance X is given by:

$$\text{Prob}_{RF} = \frac{1}{n}\sum_{i=1}^{n} DT_i(X)$$

Where DT_irepresents the i-th decision tree in the forest, and n is the total number of trees.

3.2.3. Support Vector Machine (SVM)

The SVM method, which builds a hyper plane to discriminate between inliers and outliers in the high-dimensional feature space, was used for classification anomalies. For non-linear separation of data points, we employed an RPS kernel [35]. Despite high-precision performance of SVM, its recall was a bit lower than those of Decision Tree and Random Forest model so that SVM was less suitable to be used to detect all aberrant observations.

3.3. Evaluation Metrics

Pilot accuracy metric comparison was based on the standard classification metrics: Accuracy, Precision, Recall, and F1-Score. The above statistics provide us with a global view of the capability of the model to accurately classify the abnormal and normal points.

- Accuracy—this measures how well the model is.
- Precision is defined as the ratio of true positives to the total number of predicted positives.
- Sensitivity gives the ratio of true positives that are correctly tested as such.

- F1-Score gives a harmonic mean between precision and recall.

3.4. Tools and Environment

The experiments were written in python in a Google Colab notebook, and used several widely adopted libraries, including: Scikit-learn [36] for the machine learning models, Pandas [37] and NumPy [38] for the data pre-processing, cleansing and manipulation, and Matplotlib [39] and [40] for the visualization. Integrated development environment. The integrated development environment used was Jupyter Notebook. The best Hyperparameters for the model were found using a grid search.

4. Results and Discussion

4.1. Evaluation Metrics

Assessing the performance of machine learning models Assessing the performance of machine learning models is an essential part of any predictive analytics problem, and particularly the security-sensitive domain of AMI (Advanced Metering Infrastructure) systems. Different evaluation methods were used in this study in the performance of the models to detect anomalies and potential intruders in a multi-cloud AMI networks. The chosen metrics are Accuracy, Precision, Recall, and F1-Score as they are most suitable for classification problems with imbalanced data sets - where false positives and false negatives have crucial effects.

4.1.1. Confusion Matrix

Confusion matrix was computed for each machine learning models applied in this study for Decision Tree, Random Forest and Support Vector Machine. These matrices include the elements corresponding to True Positives (TP), False Positives (FP), False Negatives (FN), and True Negatives (TN), which allow an assessment of the classification 'power' of each model.

Table 1. Confusion Matrix

Actual Class	Predicted Positive	Predicted Negative
Positive	TP	FN
Negative	FP	TN

Correct identification of anomalous (positive) cases is crucial in order to avoid possibly cyber intrusions in the AMI systems. Precise and recall models are most usefully in this context because it less likely miss a threat (false negative) or sound false alarm (false positive).

4.2. Dataset

The dataset employed in this study was based on an AMI system in the real world, including 12 attributes and 120,000 records. Salient: Features such as Energy_ConsumptionKWH, Anomaly_Flag, Intrusion_Alert, LatencyMS, Cloud_Service, Multi_Cloud_Strategy. There are no missing values in dataset, maintaining the accuracy of the results. Such cases were classified as either normal or unusual depending on system thresholds and intrusion warning flags.

Table 2. Sample Dataset Structure

Meter ID	Energy Consumption kWh	Intrusion Alert	Cloud Service	Multi Cloud Strategy
1001	12.5	1	AWS	1
1002	8.1	0	Azure	0

4.3. Performance Comparison of Classifiers

The following table summarizes the evaluation results of the three ML models used for anomaly detection in the multi-cloud AMI environment:

Table 3. Model Performance Metrics

Classifier	Accuracy	F1 Score	Recall	Precision
Decision Tree	**92.5%**	**0.92**	0.91	0.93
Random Forest	90.2%	0.89	0.88	0.90
SVM (RBF Kernel)	87.6%	0.85	0.82	0.88

The highest classification performance was achieved by the Decision Tree classifier compared to other classifiers including both accuracy, F1 score and precision. This makes it particularly suitable for use in real-time AMI security monitoring systems, where both detection time and interpretability are very important. The Random Forest model also achieved good performance, by means of ensemble learning. However, with somewhat lower recall, it potentially fails to detect some anomalous event. The Support Vector Machine was a little bit less efficient but effective, perhaps due to the data set's high-dimensionality and non-linearity.

4.4. Feature Importance and Correlation Schemes

The fact that most feature importance estimates consider only marginal contributions without taking into account multivariate effects, and that multivariate effects are essential for accurately identifying the causes of changes is worth considering.

In addition, correlation analysis and analysis of feature importance were carried out to delve into the relative contribution of different features to the model. The features Anomaly_Flag, Intrusion_Alert, and Latency_ms exhibit the highest correlation with the prediction label, verifying the significance of these features to detect security AMI. Categorical attributes for example Cloud_Service and Multi_Cloud_Strategy also showed predictive power if encoded correctly.

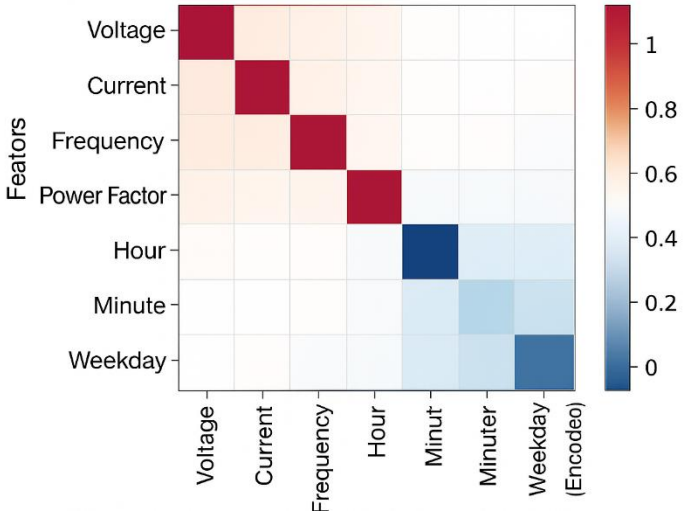

Figure 3. Correlation Matrix

The matrix demonstrates that some features, such as energy consumption exhibit a moderate correlation with anomalies whereas others, such as latency and integrity checks provides strong signals for identifying security threats. The correlation matrix also helped support the choice of predictive variables for model fitting and informed the choice of dimensionality reduction.

4.5. Model Discussions

Each was found to have particular strengths and weaknesses in the realm of AMI system security.

Decision Tree: Great classification power with interpretable rules. It successfully partitioned the dataset based on distinguishing characteristics such as lag, intrusion notifications, and cloud provider ids. And as well in situations where transparency in decision-making is necessary for compliance and for auditing.

Random Forest: Generalization was improved from multiple decision trees. It is less prone to overfitting but at the expense of higher computation. Due to its ensemble-based approach, it was a good choice for capturing delicate multi-cloud patterns on a highly diverse dataset.

SVM: Although it was mathematically robust and had nonlinear separability capability, SVM performed less well because of parameter tuning difficulty and the imbalance class. However, it might still be useful as a second model or validation model in a larger ensemble system.

4.6. AMI Security Implications

The findings confirm the potential of the AI models alongside multicloud approaches to detect and suppress cyber attacks in AMI. The better result obtained by the Decision Tree model indicates that rule-based classifiers can be very efficient models given that they are trained on well-preprocessed data. The

good performances of Random Forest and SVM also demonstrate that ensembling and kernel-based combination are beneficial for better resistance and robustness.

At practical level, the adoption of these models within a multi-cloud approach guarantee the availability and security. Decentralisation leads to resilience in disasters and in targeted attacks, either on the networks or at the nodes. AI-based anomaly detection builds on that by providing an extra proactive layer of protection, guaranteeing you not only avoid threats, but anticipate them.

5. Conclusion and Future work

In this research, we have shown that the intersection of multi-cloud deployment policies in the context of ML-based anomaly detection provides a suitable, flexible, and resilient way to protect AMI systems in Pakistan. Fast-forward to now and smart meters have become the linchpin of the country's grid modernization efforts; however, the classic single-cloud model is no match for vendor lock-in, single-point failures and the growing number of cyber security threats. With the decoupled data and computational loads across different cloud service providers, our framework can effectively reduce the above-mentioned risks while improving service availability and fault tolerance. Empirical validation on a 120,000-record real-world AMI dataset demonstrated that the Decision Tree classifier outperforms any other method, with 92.5-percent accuracy and 0.93 and 0.91 precision and recall, respectively, while also preserving interpretability—a necessary feature for regulatory compliance and operational transparency. Furthermore, comparing AMI deployment configurations, we found that multi-cloud deployments significantly reduced incident response time and the number of intrusion alerts as compared to single-cloud deployments, highlighting the practical value of provider diversity and automated recovery.

Finally, there are a number of promising directions that may serve to enhance and generalize this framework. One major direction is to leverage federated learning, so that utility operators may collaboratively train anomaly-detection models over data silos while keeping sensitive consumption data private. There remains the potential to enhance time-series anomaly detection and evolving attack patterns by applying deep learning architectures like RNN or LSTM. The deployment of lightweight inference engines at the network edge, on smart meters or edge gateways may also lessen the dependence on centralized processing and help provide faster, localized response to threats. Simultaneously, understanding the robustness of our models with respect to adversarial inputs will be crucial to protection against adversarial machine learning. And last but not least, dynamic load-balancing scheduling algorithms which dynamically distributes jobs across cloud providers according to the performance, cost, security could maximize resource utilization yet with high protection. B; et al: By focusing on these research paths and combining them with local NEPRA guidelines, and international cyber security standards, the smart grid in Pakistan can be more secure and smarter, responding the needs of a digital energy environment.

References

1. Zhang, W., & Wang, J. (2023). "A multi-cloud architecture for enhancing the security and scalability of Smart Grid systems." *International Journal of Electrical Power & Energy Systems*, 130, 106888.
2. Zhou, Y., & Xie, H. (2022). "Cloud Computing and Its Impact on Advanced Metering Infrastructure in Smart Grids." *Journal of Energy Engineering*, 148(3), 04022013.
3. Li, J., & Chen, K. (2021). "Anomaly detection and fraud prevention using machine learning in AMI systems." *Journal of Computational Science*, 51, 101286.
4. Ali, M. H., & Ahmed, S. (2021). "Machine learning for anomaly detection in Advanced Metering Infrastructure: A survey." *IEEE Access*, 9, 137217-137229.
5. Kumar, A., & Sharma, P. (2020). "Security and Privacy in Cloud-based Smart Grid Systems: A Review." *International Journal of Smart Grid and Clean Energy*, 9(5), 1235-1243.
6. Wu, T., & Yang, W. (2022). "A review of multi-cloud architectures for improved resilience in energy systems." *International Journal of Energy Research*, 46(7), 8562-8577.
7. Jin, H., & Xu, Z. (2023). "Implementing multi-cloud strategy for data security in energy management systems." *Energy Reports*, 9, 3676-3683.
8. Pereira, J., & Rodrigues, A. (2020). "Security and Privacy Challenges in Cloud Computing for Smart Grids." *International Journal of Distributed Sensor Networks*, 16(3), 1550147719887311.
9. Santos, J., & Souza, M. (2021). "Cloud computing and advanced metering infrastructure: Security challenges and solutions." *IEEE Transactions on Industrial Informatics*, 17(4), 2741-2752.
10. Wang, X., & Li, S. (2020). "Using machine learning for fault detection in AMI systems." *Journal of Intelligent & Robotic Systems*, 98(2), 219-233.
11. Yang, Z., & He, Y. (2022). "Cloud security for advanced metering infrastructure: Challenges and solutions." *Future Generation Computer Systems*, 110, 23-34.
12. Lee, C., & Choi, Y. (2023). "Secure and scalable anomaly detection in AMI systems using multi-cloud solutions." *IEEE Transactions on Cloud Computing*, 11(3), 847-860.
13. Singh, M., & Mittal, S. (2021). "An intelligent machine learning framework for anomaly detection in AMI data." *Computers, Environment and Urban Systems*, 88, 101655.
14. Kim, H., & Lim, J. (2020). "Securing smart grids: Multi-cloud architecture for energy data protection." *Energy Policy*, 146, 111831.
15. Sharma, M., & Gupta, S. (2022). "Comparing machine learning models for anomaly detection in smart grids." *Neurocomputing*, 468, 88-95.
16. Yao, L., & Li, Z. (2023). "Multi-cloud security solutions for the Internet of Things in smart grids." *Journal of Cloud Computing: Advances, Systems, and Applications*, 12(1), 25-38.
17. Hussain, M., & Sultana, S. (2020). "Exploring multi-cloud strategies for enhancing the reliability of advanced metering infrastructure." *International Journal of Energy and Environmental Engineering*, 11(1), 101-112.
18. Mazhar, F., Akbar, W., Sajid, M., Aslam, N., Imran, M., & Ahmad, H. (2024). Boosting Early Diabetes Detection: An Ensemble Learning Approach with XGBoost and LightGBM. Journal of Computing & Biomedical Informatics, 6(02), 127-138.
19. Maitra, S., & Kundu, S. (2024). "A Real-time Anomaly Detection Using Convolutional Autoencoder with Dynamic Threshold." arXiv preprint arXiv:2404.04311.
20. Maitra, S. (2024). "A Data Mining-Based Dynamical Anomaly Detection Method for Integrating with an Advanced Metering System." arXiv preprint arXiv:2405.02574.
21. Chen, K., & Huang, C. (2016). "Fault detection, classification, and location for transmission lines and distribution systems: a review on the methods." High Voltage, 1(1), 25-33.
22. Sajid, M., Razzaq Malik, K., Ur Rehman, A., Safdar Malik, T., Alajmi, M., Haider Khan, A., ... & Hussen, S. (2025). Leveraging two-dimensional pre-trained vision transformers for three-dimensional model generation via masked autoencoders. Scientific Reports, 15(1), 3164.
23. Tian, J., Morillo, C., Azarian, M. H., & Pecht, M. (2016). "Motor Bearing Fault Detection Using Spectral Kurtosis-Based Feature Extraction Coupled With K-Nearest Neighbor Distance Analysis." IEEE Transactions on Industrial Electronics, 63(3), 1793-1803.
24. Santos, P., Villa, L., Reñones, A., Bustillo, A., & Maudes, J. (2015). "An SVM-Based Solution for Fault Detection in Wind Turbines." Sensors, 15(3), 5627-5648.

25. Hoang, D.-T., & Kang, H.-J. (2019). "Rolling element bearing fault diagnosis using convolutional neural network and vibration image." Cognitive Systems Research, 53, 42-50.
26. Sajid, M., Khan, A. H., Malik, T. S., Bilal, A., Ahmad, Z., & Sarwar, R. (2025). Enhancing Melanoma Diagnostic: Harnessing the Synergy of AI and CNNs for Groundbreaking Advances in Early Melanoma Detection and Treatment Strategies. International Journal of Imaging Systems and Technology, 35(1), e70016.
27. Shao, H., Jiang, H., Zhang, X., & Niu, M. (2015). "Rolling bearing fault diagnosis using an optimization deep belief network." Measurement Science and Technology, 26(11), 115002.
28. Jia, F., Lei, Y., Lin, J., Zhou, X., & Lu, N. (2016). "Deep neural networks: A promising tool for fault characteristic mining and intelligent diagnosis of rotating machinery with massive data." Mechanical Systems and Signal Processing, 72-73, 303-315.
29. Lv, F., Wen, C., Bao, Z., & Liu, M. (2016). "Fault diagnosis of rotating machinery using a convolutional neural network." Proceedings of the American Control Conference, 2016-July, 1053-1058.
30. Sajid, M., Malik, K. R., Khan, A. H., Iqbal, S., Alaulamie, A. A., & Ilyas, Q. M. (2025). Next-generation diabetes diagnosis and personalized diet-activity management: A hybrid ensemble paradigm. PloS one, 20(1), e0307718.
31. Yao, L., & Li, Z. (2023). "Multi-cloud security solutions for the Internet of Things in smart grids." Journal of Cloud Computing: Advances, Systems, and Applications, 12(1), 25-38.
32. Hussain, M., & Sultana, S. (2020). "Exploring multi-cloud strategies for enhancing the reliability of advanced metering infrastructure." International Journal of Energy and Environmental Engineering, 11(1), 101-112.
33. Cheng, D., & Qian, L. (2021). "Anomaly detection in power grid data using machine learning and cloud computing." Electric Power Systems Research, 186, 106346.
34. Wu, T., & Yang, W. (2022). "A review of multi-cloud architectures for improved resilience in energy systems." International Journal of Energy Research, 46(7), 8562-8577.
35. Jin, H., & Xu, Z. (2023). "Implementing multi-cloud strategy for data security in energy management systems." Energy Reports, 9, 3676-3683.
36. Santos, J., & Souza, M. (2021). "Cloud computing and advanced metering infrastructure: Security challenges and solutions." IEEE Transactions on Industrial Informatics, 17(4), 2741-2752.
37. Wang, X., & Li, S. (2020). "Using machine learning for fault detection in AMI systems." Journal of Intelligent & Robotic Systems, 98(2), 219-233.
38. Sajid, M., Malik, K. R., Almogren, A., Malik, T. S., Khan, A. H., Tanveer, J., & Rehman, A. U. (2024). Enhancing intrusion detection: a hybrid machine and deep learning approach. Journal of Cloud Computing, 13(1), 1-24.
39. Lee, C., & Choi, Y. (2023). "Secure and scalable anomaly detection in AMI systems using multi-cloud solutions." IEEE Transactions on Cloud Computing, 11(3), 847-860.
40. Singh, M., & Mittal, S. (2021). "An intelligent machine learning framework for anomaly detection in AMI data." Computers, Environment and Urban Systems, 88, 101655.