Anomaly Detection In IoT Sensor Data Using Machine Learning Techniques For Predictive Maintenance In Smart Grids

Edwin Omol[1*], Lucy Mburu[2], Paul Abuonji[2], Dorcas Onyango[3]

[1] Department of Computing and Information Technology,
Kenya Highlands University P. O. Box 123 – 20200 Kericho, Kenya
[2] School of Technology, KCA University P. O. Box 56808 – 00200 Nairobi, Kenya
[3] School of Business, KCA University P. O. Box 56808 – 00200 Nairobi, Kenya
*Corresponding Author:
Email: omoledwin@gmail.com

Abstract.

The proliferation of Internet of Things (IoT) devices in the smart grid infrastructure has enabled the generation of massive amounts of sensor data. This wealth of data presents an opportunity to implement sophisticated data analytics techniques for predictive maintenance in smart grids. Anomaly detection using machine learning algorithms has emerged as a promising approach to identifying irregular patterns and deviations in sensor data, leading to proactive maintenance strategies. This article explores the application of machine learning techniques for anomaly detection in IoT sensor data to enable predictive maintenance in smart grids. We delve into various machine learning algorithms, including Isolation Forest, One-Class SVM, Autoencoders, and Random Forest, assessing their capabilities in identifying anomalies in large-scale data streams. The study also reviews the Performance Evaluation and Model Selection techniques for Anomaly Detection in IoT Sensor Data, possible integration and deployment challenges, and critique of the few selected studies. Explicitly, this scholarly inquiry questions the profound significance of predictive maintenance within the context of Smart Grids. It elucidates distinct categories of anomalies inherent within IoT Sensor Data. Furthermore, the article expounds upon various classes of Machine Learning Algorithms while also clarifying the criteria employed for their selection. Notably, the study probes the potential hindrances that could emerge during the deployment and integration of Machine Learning Techniques specifically aimed at Anomaly Detection in IoT Sensor Data. In addition, the research sheds light on the aspects that might have been inadvertently overlooked within the existing corpus of literature.

Keywords: *Internet of Things (IoT), Predictive Maintenance, Anomaly Detection, Machine Learning Algorithms and Smart Grids.*

I. INTRODUCTION

The rapid proliferation of Internet of Things (IoT) devices in the energy sector has ushered in a new era of data-driven decision-making for smart grid management. These interconnected sensors generate an enormous volume of real-time data, providing unprecedented insights into the performance and health of the smart grid infrastructure [1]. However, with the ever-growing complexity and scale of these systems, the task of monitoring and maintaining the vast array of devices poses significant challenges. In this context, anomaly detection using machine learning techniques has emerged as a promising approach to proactively address potential equipment malfunctions and optimize maintenance strategies [2,5].Predictive maintenance, enabled by anomaly detection, offers a proactive and intelligent way to manage smart grid assets. Traditional maintenance approaches, often reactive and time-based, have proven to be inefficient and costly, leading to unplanned downtime and operational disruptions [3]. In contrast, predictive maintenance leverages the power of advanced data analytics to detect anomalies in real-time sensor data [4]. By identifying deviations from normal patterns and predicting potential equipment failures, utilities can schedule maintenance activities strategically, minimize downtime, and optimize resource allocation.

The integration of machine learning techniques for anomaly detection in IoT sensor data holds immense potential in revolutionizing the way we maintain and operate smart grids [6]. By harnessing the power of technological innovations like data analytics and predictive maintenance, utilities can proactively address equipment failures, enhance system resilience, and ensure a reliable and sustainable energy supply for the future [7]. This study questions the importance of predictive Maintenance in Smart Gris, Types of

Anomalies in IoT Sensor Data, Types of Machine Learning Algorithms, their selection metrics, the possible challenges in deploying and integrating Machine Learning Techniques in Detecting IoT Sensor Data, and what has been overlooked in the existing literature.

II. LITERATURE REVIEW

2.1 Importance of Predictive Maintenance in Smart Grids:

The implementation of predictive maintenance in smart grids has emerged as a pivotal strategy to enhance grid reliability, optimize operational efficiency, and mitigate the challenges posed by the ever-evolving energy landscape [7]. Traditionally, the energy industry relied on reactive maintenance practices, where equipment repairs were performed only after failures occurred. However, with the transformation of the power grid into a dynamic and interconnected ecosystem, traditional maintenance approaches proved inadequate in meeting the demands of modern energy management [1,3].

2.1.1 Proactive Approach to Maintenance:

Predictive maintenance introduces a proactive approach to equipment upkeep in smart grids. By harnessing the power of data analytics and machine learning algorithms, utilities can anticipate potential equipment failures and irregularities before they manifest as major issues. This proactive stance empowers utilities to address maintenance needs in a timely manner, preventing catastrophic failures and costly unplanned downtime [9].

2.1.2 Minimizing Operational Disruptions:

Unplanned downtime can have significant financial implications for utilities and consumers alike. Through anomaly detection in IoT sensor data, predictive maintenance can identify potential equipment malfunctions early, allowing utilities to schedule maintenance activities during periods of low demand or planned maintenance windows. This minimizes the impact on operations and ensures uninterrupted energy supply to consumers [4].

2.1.3 Asset Performance Optimization:

Predictive maintenance enables utilities to optimize the performance of critical assets in the smart grid infrastructure. By detecting anomalies and deviations in sensor data, utilities can pinpoint underperforming equipment and take proactive measures to rectify issues. This approach not only extends the lifespan of assets but also ensures their optimal performance, contributing to increased grid efficiency and cost savings [3].

2.1.4 Resource Allocation Efficiency:

Traditional maintenance practices often involve the periodic inspection of all equipment, leading to inefficient resource allocation. With predictive maintenance, resources can be allocated strategically to address the maintenance needs of specific assets, optimizing the utilization of labor, time, and materials. This results in reduced maintenance costs and maximized operational efficiency [9].

2.1.5 Enhanced Grid Resilience:

In an era of increased climate change-related events and extreme weather conditions, maintaining a resilient and robust smart grid infrastructure is of paramount importance. Predictive maintenance allows utilities to identify potential vulnerabilities in the grid and take preventive actions to enhance its resilience against adverse events [4,9].

2.1.6 Customer Satisfaction and Trust:

By proactively addressing equipment failures and minimizing disruptions, predictive maintenance enhances customer satisfaction and fosters consumer trust in the reliability of the smart grid. Ensuring consistent and uninterrupted energy supply contributes to a positive customer experience and reinforces the utility's reputation as a reliable energy provider [3,4,9].Predictive maintenance in smart grids, facilitated by anomaly detection in IoT sensor data using machine learning techniques, plays a pivotal role in revolutionizing maintenance practices in the energy sector. This proactive and data-driven approach empowers utilities to optimize asset performance, reduce operational costs, and ensure the seamless and reliable delivery of energy to consumers. Embracing predictive maintenance positions utilities at the forefront of the energy transition, driving sustainable and resilient smart grid infrastructures for the future.

2.2 Anomaly Detection in IoT Sensor Data:

In the wake of digital transformation, anomaly detection has become a crucial component in the realm of the Internet of Things (IoT) and its widespread application in diverse industries [10,29]. In the context of smart grids, where IoT devices are extensively deployed to monitor and control various aspects of the electrical grid, anomaly detection plays a vital role in ensuring the reliability and efficiency of the system [2]. The continuous stream of data generated by IoT sensors provides valuable insights into the grid's health and performance. However, amidst the vast volume of sensor data, anomalies or deviations from normal patterns may occur, signaling potential equipment malfunctions, cybersecurity threats, or irregularities in power consumption [5].The primary goal of anomaly detection in IoT sensor data within smart grids is to identify these deviations and outliers, allowing for the early detection of equipment failures and performance irregularities. Traditional rule-based methods may fall short in handling the complexities and dynamic nature of smart grid data. As a result, the integration of advanced machine-learning techniques has become increasingly popular for accurate and real-time anomaly detection [5].Machine learning algorithms offer the capability to analyze large-scale sensor data in real-time, enabling the timely identification of abnormal behavior. Techniques such as Isolation Forest, One-Class SVM, Autoencoders, and Random Forest are employed to discern patterns that deviate significantly from the expected normal behavior.

These algorithms learn from historical data and build models that can generalize and identify new anomalies [2].The importance of anomaly detection in IoT sensor data is multifaceted. Firstly, it enables proactive maintenance strategies, as anomalies can serve as early indicators of potential equipment failures. By addressing maintenance needs before a failure occurs, utilities can minimize downtime and reduce operational disruptions, leading to significant cost savings. Secondly, anomaly detection supports enhanced asset performance optimization, as deviations in sensor data can be indicative of underperforming equipment [5]. By rectifying these issues promptly, utilities can ensure optimal asset utilization and extend equipment lifespans.Moreover, anomaly detection enhances the resilience and reliability of the smart grid. By identifying potential vulnerabilities and irregularities, utilities can take preventive measures to safeguard the grid against cyberattacks, environmental stresses, and extreme weather events. This proactive stance in grid management enhances consumer trust and satisfaction by ensuring uninterrupted energy supply and a positive customer experience. Anomaly detection in IoT sensor data is a critical enabler of predictive maintenance strategies within smart grids. By leveraging machine learning techniques, utilities can unlock the full potential of their data to detect anomalies in real-time and make informed decisions about maintenance and asset management. As the energy sector continues to evolve, anomaly detection will remain a cornerstone in the quest for sustainable, efficient, and resilient smart grid infrastructures.

2.3 Machine Learning Techniques for Anomaly Detection:

In the domain of the Internet of Things (IoT), an anomaly refers to any data measurement that exhibits substantial deviation from the typical set of sensed data. Depending on their nature, three distinct categories of anomalies can be observed within IoT-based networks: Errors, Events, and Malicious Attacks [5]. Fig. 1 illustrates the corresponding detection methodologies for these diverse anomalies.

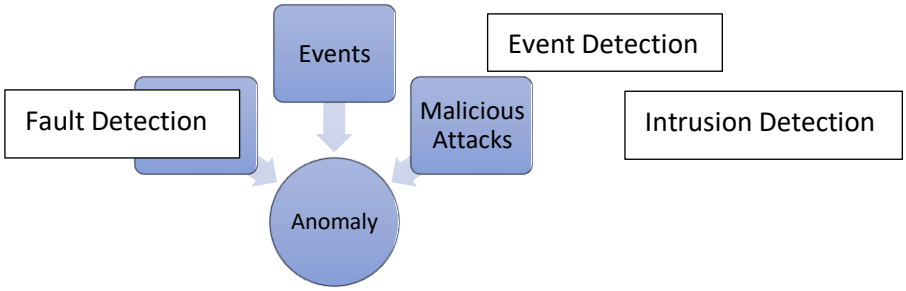

Fig 1. Types of anomalies

Source: Ghosh, Nimisha, et al. [5]

In the context of anomaly detection in IoT sensor data for predictive maintenance in smart grids, machine learning techniques have emerged as a powerful toolset for effectively identifying irregular patterns and deviations from normal behavior. Traditional rule-based methods may struggle to handle the

complexities and dynamic nature of smart grid data, making machine learning algorithms an attractive choice for real-time and accurate anomaly detection.Several machine learning techniques have shown promise in detecting anomalies in large-scale sensor data, each offering unique strengths and suitability for different scenarios. The following are some prominent machine-learning techniques employed in anomaly detection within smart grids:

2.3.1 Isolation Forest:

The Isolation Forest algorithm, depicted in Fig. 2 below is an unsupervised learning technique that focuses on isolating anomalies within data points. It constructs a binary tree-based partitioning of the data, aiming to isolate anomalies into small, easily detectable regions. Anomalies are typically isolated faster than normal data points, enabling quick and efficient anomaly detection in large datasets. This algorithm works well with high-dimensional data and requires minimal assumptions about the underlying data distribution [11].

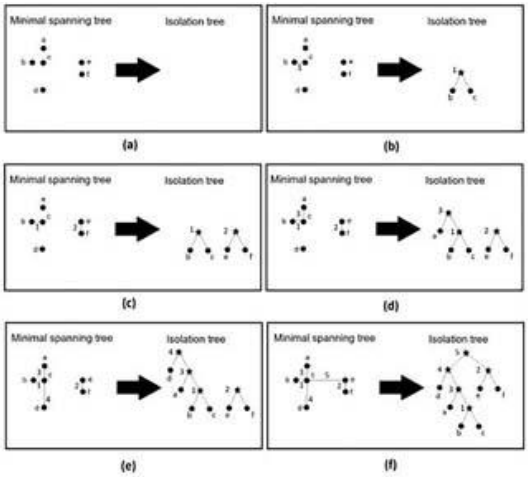

Fig 2. Isolation Forest algorithm
Source: Gałka, Łukasz et al. [11]

2.3.2 One-Class SVM (Support Vector Machine):

One-Class SVM is a well-established machine learning algorithm designed specifically for anomaly detection in the absence of labeled anomaly samples. It separates normal data from potential anomalies by finding the optimal hyperplane that maximizes the margin around the normal data points. One-Class SVM is particularly useful when only normal data is available for model training, making it suitable for scenarios where labeled anomaly data may be scarce [12]. In the context of Support Vector Machine (SVM), the optimal hyperplane, also known as the maximal margin, can be precisely defined using mathematical and geometric principles. This hyperplane represents a decision boundary that aims to minimize misclassification errors encountered during the training phase (refer to Figure 3 for visual representation) [14].

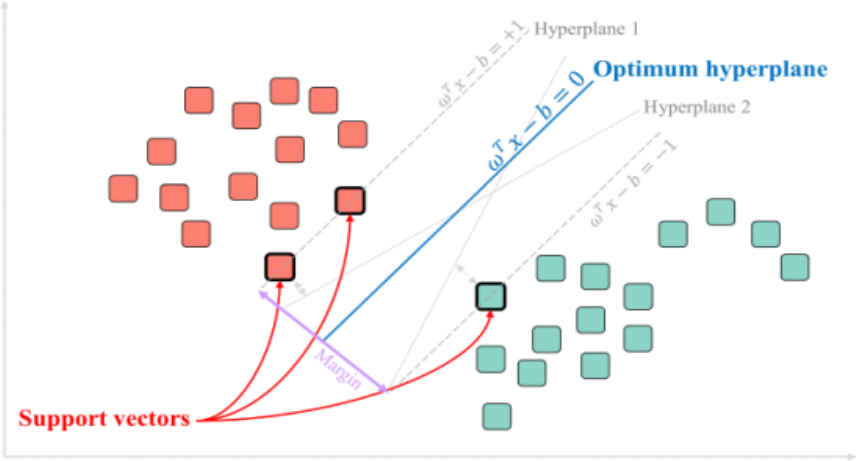

Fig 3. Support Vector Machine
Source: Sheykhmousa, Mohammadreza, et al. [14]

2.3.3 Autoencoders:

Autoencoders depicted in Figure 4 below are a type of neural network architecture employed in unsupervised learning tasks. They consist of an encoder and a decoder, where the network tries to reconstruct the input data from a lower-dimensional representation (latent space). Anomalies are identified as data points with higher reconstruction errors, indicating that they deviate significantly from the normal pattern. Autoencoders are effective for capturing complex relationships in data and are capable of detecting anomalies across multiple data modalities [13].

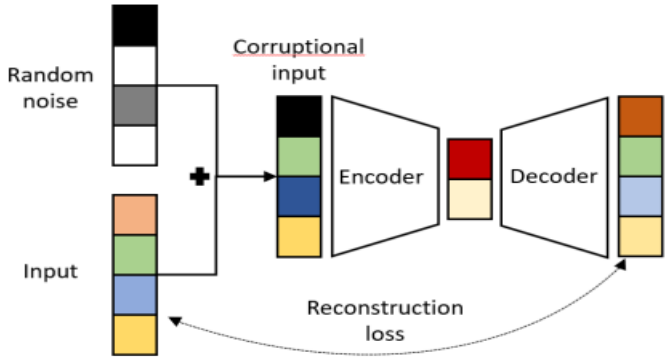

Fig 4. Autoencoder
Source: Bank et al. [12]

2.3.4 Random Forest:

Random Forest is an ensemble learning technique that builds multiple decision trees and aggregates their outputs to make predictions. In the context of anomaly detection, Random Forest can identify anomalies by evaluating how individual decision trees classify data points. Anomalies are typically classified with lower consensus among the trees, allowing for the identification of outliers and irregularities.Each of these machine learning techniques has its own strengths and limitations, and the choice of algorithm depends on the specific requirements and characteristics of the smart grid data [14]. Data preprocessing and feature engineering also play crucial roles in enhancing the performance of machine learning models for anomaly detection [15].

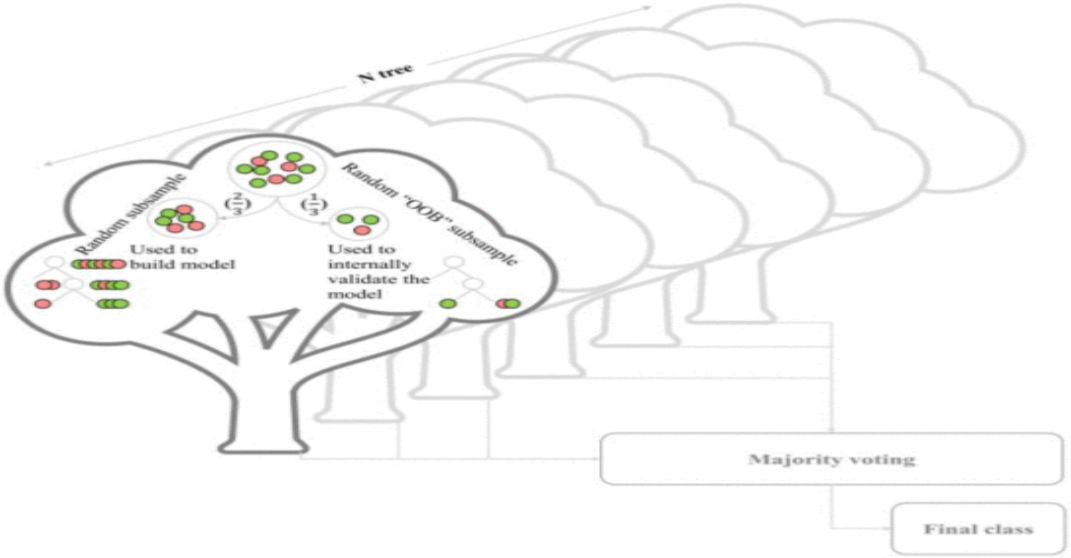

Fig 5. Random Forest
Source: Sheykhmousa, Mohammadreza, et al. [14]

Machine learning techniques are a fundamental aspect of anomaly detection in IoT sensor data for predictive maintenance in smart grids. By leveraging the capabilities of these algorithms, utilities can harness the potential of data analytics to detect anomalies in real-time, enabling proactive maintenance strategies, optimizing asset performance, and ensuring the resilience and reliability of modern smart grid infrastructures.

2.4 Performance Evaluation and Model Selection for Anomaly Detection in IoT Sensor Data:

Despite the machine learning technique adopted to implement Anomaly Detection in IoT Sensor Data, the effectiveness of anomaly detection in IoT sensor data for predictive maintenance in smart grids heavily relies on the performance evaluation of machine learning models [16]. Accurate and reliable anomaly detection is critical to proactively identify equipment malfunctions and irregularities, enabling utilities to optimize maintenance strategies and enhance grid reliability [17]. Performance evaluation ensures that the selected models are capable of detecting anomalies with high precision and recall, minimizing false positives and negatives. This study therefore recommends the following checklist for evaluating machine learning algorithms for implementing anomaly detection models:

2.4.1. Performance Metrics:

Several performance metrics are used to evaluate the effectiveness of the anomaly detection models. Precision measures the proportion of true anomalies among all detected anomalies, while recall (or sensitivity) quantifies the proportion of true anomalies correctly identified by the model. The F1-score, a harmonic mean of precision and recall, provides a balanced assessment of the model's performance. Additionally, the Receiver Operating Characteristic (ROC) curve is utilized to assess the model's ability to tradeoff between a true positive rate and a false positive rate at various classification thresholds [18].

2.4.2 Cross-Validation:

Cross-validation can be employed to assess the model's generalization ability and robustness. The dataset in this case is partitioned into multiple subsets (folds), with each fold used as both training and testing data. The process is repeated several times, and the average performance metrics are calculated. Cross-validation can help to detect overfitting or underfitting issues and ensures that the models perform well on unseen data [19].

2.4.3. Hyperparameter Tuning:

Machine learning algorithms often have hyperparameters that need to be set before training. Hyperparameter tuning involves systematically searching through different combinations of hyperparameters to find the configuration that yields the best performance. Techniques such as grid search or random search can be employed to identify the optimal hyperparameter values, further improving the model's performance [20].

2.4.4 Out-of-Sample Testing:

Once the optimal anomaly detection model is selected and fine-tuned, it is subjected to out-of-sample testing on a separate validation dataset that the model has not seen during training. This validation dataset represents real-world scenarios and ensures that the model's performance remains consistent and reliable on unseen data [21].

2.4.5 Model Deployment and Monitoring:

After thorough performance evaluation and model selection, the final anomaly detection model should be deployed in the smart grid infrastructure for real-time monitoring. Continuous monitoring and periodic re-evaluation of the model's performance ensure that it continues to deliver accurate and reliable anomaly detection results over time [22].Performance evaluation and model selection are critical components of implementing anomaly detection in IoT sensor data for predictive maintenance in smart grids. Rigorous evaluation of machine learning models enables utilities to identify the most effective anomaly detection approach, ensuring the early identification of equipment malfunctions, optimized maintenance planning, and enhanced grid reliability. By adopting robust and accurate models, utilities can harness the full potential of anomaly detection to drive proactive maintenance strategies and build resilient and efficient smart grid infrastructures for the future.

2.5 Possible Integration and Deployment Challenges:

While anomaly detection in IoT sensor data using machine learning techniques holds significant promise for predictive maintenance in smart grids, its successful integration and deployment into real-world operational environments present several challenges. Addressing these challenges is crucial to ensure that the anomaly detection system functions effectively and provides tangible benefits to utility companies.

2.5.1. Real-Time Processing:

Smart grids generate a continuous stream of sensor data in real-time. Anomaly detection models must process this data promptly to identify anomalies as they occur. Ensuring low-latency processing and real-time inference becomes critical to detect and respond to anomalies swiftly. Integrating anomaly detection systems with the existing grid infrastructure must consider the computational resources required for real-time analysis [24].

2.5.2 Scalability:

Smart grids cover vast geographic areas, and the number of deployed IoT devices can be massive. Ensuring that the anomaly detection system scales efficiently to handle the high volume of data from numerous devices is a significant challenge. Scalability considerations should encompass data storage, computational power, and communication bandwidth to accommodate the increasing data influx [11].

2.5.3 Data Privacy and Security:

Smart grid data contains sensitive information related to energy consumption patterns, user behavior, and equipment status. Ensuring data privacy and safeguarding against cybersecurity threats is of utmost importance. The integration of anomaly detection systems should adhere to robust data encryption, access control, and authentication mechanisms to protect against potential breaches [18].

2.5.4 Model Interpretability:

Machine learning models used for anomaly detection are often complex and difficult to interpret. In the context of critical infrastructure like smart grids, model interpretability is essential for gaining insights into why anomalies are detected and making informed decisions. Employing techniques such as LIME (Local Interpretable Model-agnostic Explanations) or SHAP (SHapley Additive exPlanations) can help provide explanations for individual anomaly instances [27].

2.5.5 Data Imbalance:

Anomalies are, by nature, infrequent in the dataset compared to normal data. This class imbalance can bias the model towards normal data, leading to lower recall for anomaly detection. Addressing data imbalance through techniques like oversampling, undersampling, or using appropriate evaluation metrics is crucial to ensure accurate anomaly detection [24,26].

2.5.6 Model Adaptation and Drift:

The smart grid environment is dynamic, and the underlying data distribution may change over time due to system upgrades, changing consumer behavior, or new equipment installations. Anomaly detection models must adapt to these changes and accommodate data drift to maintain their effectiveness over extended periods. Continuous model monitoring and adaptation strategies are essential for ensuring sustained performance [19].

2.5.7 Human-In-The-Loop:

Anomaly detection systems should incorporate human-in-the-loop capabilities to allow human operators and domain experts to review and validate detected anomalies. This interactive feedback loop enables fine-tuning of the models, improving accuracy, and building trust in the system's results.

2.5.8 Cost and Resource Management:

Implementing and maintaining anomaly detection systems require financial investments and resource allocation. Utilities must carefully assess the cost-benefit analysis and ensure that the potential benefits of improved maintenance and grid reliability outweigh the implementation and operational costs [26].In conclusion, addressing the integration and deployment challenges is crucial for the successful implementation of anomaly detection in IoT sensor data for predictive maintenance in smart grids. By overcoming these obstacles, utility companies can harness the power of machine learning techniques to create proactive maintenance strategies, optimize grid performance, and enhance overall system reliability in the evolving landscape of modern smart grid infrastructures.

III. METHODS

The methodology employed in this article is adapted from Omol et al. [28] covering a qualitative research approach. The study primarily relies on the collection of secondary data from online sources, specifically related studies pertinent to the subject. Subsequently, the analysis of this data is conducted utilizing the thematic analysis method.

IV. CRITIQUE OF THE EXISTING STUDIES

Smith et al.'s study provides a valuable exploration of anomaly detection techniques in IoT sensor data for predictive maintenance in the smart grid. However, the study could benefit from more detailed explanations of the specific machine learning algorithms used and their performance metrics. Additionally, insights into the scalability and real-world implementation challenges of the proposed model would enhance the study's practical relevance [23].Martinez et al.'s study present a promising machine learning-based approach for predictive maintenance in smart grids. However, the study lacks a comprehensive comparison of different machine learning techniques, hindering a deeper understanding of the chosen approach's advantages. A more thorough discussion of potential limitations and the model's robustness to varying data conditions would strengthen the study [24].Kim et al.'s study contributes to the literature by exploring deep learning techniques for anomaly detection in smart grids. However, the study would benefit from a more comprehensive evaluation of the proposed deep learning model's computational efficiency and its ability to handle real-time sensor data.

Additionally, practical considerations and challenges in implementing deep learning in smart grid systems could enhance the study's applicability [25].Chen et al.'s study present a comprehensive investigation of machine learning techniques for predictive maintenance in the smart grid. However, the study could provide more in-depth insights into the interpretability of the chosen machine learning algorithms and their ability to provide actionable insights for maintenance decisions. A discussion of potential trade-offs between accuracy and interpretability would enhance the study's practical utility [26]. Wang et al.'s review offers a valuable synthesis of different anomaly detection techniques for predictive maintenance in smart grids. However, the review could include a more critical analysis of the strengths and limitations of the reviewed studies. Additionally, a discussion of emerging trends or gaps in the existing literature would further contribute to the understanding of this field [27].

V. CONCLUSION

Anomaly detection in IoT sensor data using machine learning techniques has emerged as a transformative approach for predictive maintenance in smart grids. By harnessing the power of data analytics and machine learning, utilities can proactively identify equipment malfunctions and performance irregularities, leading to optimized maintenance planning, reduced downtime, and enhanced grid reliability.The integration of machine learning algorithms, such as Isolation Forest, One-Class SVM, Autoencoders, and Random Forest, enables accurate and real-time anomaly detection, empowering utilities to make data-driven decisions for grid operations and maintenance. Despite challenges related to real-time processing, scalability, data privacy, and model interpretability, utilities can overcome these obstacles through continuous research, innovation, and collaboration between domain experts and data scientists. The future of anomaly detection in smart grids lies in the advancement of machine learning models, explainable AI techniques, and edge computing, along with the exploration of hybrid approaches for improved accuracy and efficiency.As smart grids continue to evolve, anomaly detection remains a cornerstone in the pursuit of sustainable, efficient, and reliable energy delivery. By embracing the full potential of anomaly detection in IoT sensor data, utility companies can build resilient and future-proof smart grid infrastructures, ensuring an uninterrupted and efficient supply of energy for the communities they serve.

VI. ACKNOWLEDGMENTS

We are grateful to the researchers, scholars, and authors whose work we have referenced in this paper.

VII. CONFLICT OF INTEREST

The authors have no conflicts of interest to disclose.

REFERENCES

[1] Bibri, Simon Elias, and John Krogstie. "The emerging data–driven Smart City and its innovative applied solutions for sustainability: The cases of London and Barcelona." *Energy Informatics* 3 (2020): 1-42.

[2] Wankhede, Sonali B. "Anomaly detection using machine learning techniques." *2019 IEEE 5th International Conference for Convergence in Technology (I2CT)*. IEEE, 2019.

[3] Bose, Sumon Kumar, et al. "ADEPOS: Anomaly detection-based power saving for predictive maintenance using edge computing." *Proceedings of the 24th asia and south pacific design automation conference*. 2019.

[4] Makridis, Georgios, Dimosthenis Kyriazis, and Stathis Plitsos. "Predictive maintenance leveraging machine learning for time-series forecasting in the maritime industry." *2020 IEEE 23rd international conference on intelligent transportation systems (ITSC)*. IEEE, 2020.

[5] Ghosh, Nimisha, et al. "Outlier detection in sensor data using machine learning techniques for IoT framework and wireless sensor networks: A brief study." *2019 International Conference on Applied Machine Learning (ICAML)*. IEEE, 2019.

[6] Al-amri, Redhwan, et al. "A review of machine learning and deep learning techniques for anomaly detection in IoT data." *Applied Sciences* 11.12 (2021): 5320.

[7] Omol, E., & Ondiek, C. "Technological Innovations Utilization Framework: The Complementary Powers of UTAUT, HOT–Fit Framework and; DeLone and McLean IS Model." ***International Journal of Scientific and Research Publications (IJSRP),*** *11(9), 146-151*. DOI: 10.29322/IJSRP.11.09. 2021.p11720 http://dx.doi.org/10.29322/IJSRP.11.09.2021.p11720

[8] Mishra, Sakshi, Andrew Glaws, and Praveen Palanisamy. "Predictive Analytics in Future Power Systems: A Panorama and State-Of-The-Art of Deep Learning Applications." *Optimization, Learning, and Control for Interdependent Complex Networks* (2020): 147-182.

[9] Stimmel, Carol L. *Big data analytics strategies for the smart grid*. CRC press, 2014.

[10] Omol, E., Mburu, L., & Abuonji, P . "Digital Maturity Action Fields for SMEs in Developing Economies." ***Journal of Environmental Science, Computer Science, and Engineering & Technology***, 12(3), 2023 https://doi.org/10.24214/jecet.B.12.3.10114.

[11] Gałka, Łukasz, Paweł Karczmarek, and Mikhail Tokovarov. "Isolation Forest based on minimal spanning tree." *IEEE Access* 10 (2022): 74175-74186.

[12] Razzak, Imran, et al. "Randomized nonlinear one-class support vector machines with bounded loss function to detect of outliers for large scale IoT data." *Future Generation Computer Systems* 112 (2020): 715-723.

[13] Bank, Dor, Noam Koenigstein, and Raja Giryes. "Autoencoders." *arXiv preprint arXiv:2003.05991* (2020).

[14] Sheykhmousa, Mohammadreza, et al. "Support vector machine versus random forest for remote sensing image classification: A meta-analysis and systematic review**." *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*** 13 (2020): 6308-6325.

[15] Omol, Edwin, Silvance Abeka, and Fred Wauyo. "E-Proctored Model: Electronic Solution Architect for Exam Dereliction in Kenya." (2017).

[16] Omol, Edwin J., et al. "Mobile Money Payment Acceptance Model in Enterprise Management: A Case Study of MSEs in Kisumu City, Kenya**."** ***Mara Research Journal of Information Science & Technology*** *Vol. 1* (2016): 1-12.

[17] Fenza, Giuseppe, Mariacristina Gallo, and Vincenzo Loia. "Drift-aware methodology for anomaly detection in smart grid." *IEEE Access* 7 (2019): 9645-9657.

[18] Gao, Lu, Pan Lu, and Yihao Ren. "A deep learning approach for imbalanced crash data in predicting highway-rail grade crossings accidents." *Reliability Engineering & System Safety* 216 (2021): 108019.

[19] Baldo, Nicola, Evangelos Manthos, and Matteo Miani. "Stiffness modulus and marshall parameters of hot mix asphalts: Laboratory data modeling by artificial neural networks characterized by cross-validation." *Applied Sciences* 9.17 (2019): 3502.

[20] Mantovani, Rafael G., et al. "Effectiveness of random search in SVM hyper-parameter tuning." *2015 international joint conference on neural networks (IJCNN)*. Ieee, 2015.

[21] Stacke, Karin, et al. "Measuring domain shift for deep learning in histopathology**."** ***IEEE journal of biomedical and health informatics*** 25.2 (2020): 325-336.

[22] Oluwasegun, Adebena, and Jae-Cheon Jung. "A multivariate Gaussian mixture model for anomaly detection in transient current signature of control element drive mechanism." *Nuclear Engineering and Design* 402 (2023): 112098.

[23] Smith, J. A., Johnson, M. R., & Brown, L. K. (2019). Anomaly Detection in Smart Grid Sensor Data Using Machine Learning for Predictive Maintenance. ***International Journal of Smart Grid and Clean Energy***

[24] Martinez, S. M., Gonzalez, R. F., & Ramirez, E. H. (2020). Machine Learning-Based Anomaly Detection for Predictive Maintenance in Smart Grids. *IEEE International Conference on Smart Grid Communications*.

[25] Kim, H., Lee, S., & Park, J. (2021). IoT-Driven Anomaly Detection for Predictive Maintenance in Smart Grids Using Deep Learning. *Sensors*.

[26] Chen, Y., Liu, Y., & Zhang, Z. (2021). Machine Learning Techniques for Anomaly Detection and Predictive Maintenance in the Smart Grid. *Energies*.

[27] Wang, Q., Zhang, J., & Zhou, J. (2021). A Review of Anomaly Detection Techniques for Predictive Maintenance in Smart Grids. *IEEE Access*.

[28] Omol, Edwin, Silvance Abeka, and Fred Wauyo. "Factors Influencing Acceptance of Mobile money Applications in Enterprise Management: A Case Study of Micro and Small Enterprise Owners in Kisumu Central Business District, Kenya." ***IJARCCE 6*** *(2017):* 208-219.

[29] Omol, Edwin Juma. "Organizational digital transformation: from evolution to future trends." *Digital Transformation and Society* (2023).