Volume (1) No (9), 2025
Journal of Global Research in Multidisciplinary Studies (JGRMS)
Review Paper/Research Paper
Available online at https://saanvipublications.com/journals/index.php/jgrms/index

Anomaly Detection in Smart Grids Using Artificial Intelligence: A Survey of Techniques and Tools

Mr.Ram Pratap Singh
Department of Computer Science and Engineering,
Lakshmi Narain College of Technology
Bhopal
rampratap@lnct.ac.in

***Abstract*—The rapid advancement of smart grids has revolutionized modern energy distribution by integrating renewable energy resources, distributed generation, and advanced communication technologies. However, the growing complexity, interconnectivity, and cyber-physical integration have made smart grids increasingly vulnerable to various anomalies, including equipment failures, cyber-attacks, load forecasting errors, and sensor malfunctions. This paper presents a comprehensive survey of state-of-the-art techniques for anomaly detection in smart grids, with a focus on artificial intelligence (AI), hybrid frameworks, and semantic modeling approaches. A wide spectrum of AI-driven methodologies—such as cross-modal collaborative learning, hierarchical semantic representations, physics-informed hybrid algorithms, and deep learning architectures—are systematically reviewed to highlight their roles in improving cybersecurity, fault diagnosis, energy theft prevention, and real-time monitoring. The study also examines the inherent challenges posed by heterogeneous grid infrastructures, diverse data sources, and evolving threat landscapes. Furthermore, the survey identifies emerging directions for designing scalable, explainable, and adaptive anomaly detection frameworks integrated with real-time analytics, privacy-preserving mechanisms, and standardized benchmarking datasets. By synthesizing current advancements and open challenges, this work provides a structured foundation to guide future innovations in secure, resilient, and intelligent smart grid ecosystems.**

***Keywords*—Smart Grids, Anomaly Detection, Artificial Intelligence, Machine Learning, Cybersecurity, Real-Time Monitoring, Fault Diagnosis.**

I. INTRODUCTION

Smart Grid technologies and their integration with improved communication infrastructure, distributed energy resources (DER), renewable energy production and systems, and demand-side management have contributed greatly to power system management transformations in the contemporary world [1][2]. In contrast to traditional grids, Smart Grids facilitate two-way power flows and real-time information exchange, enabling decentralized generation and dynamic load management. These new developments maximize efficiency, economics and consumer involvement in the energy markets. Moreover, the popularity of electric vehicles and devices and appliances enabled by the Internet of Things, become the true bearers of the unprecedented automation and smarts in the operation of the grid, and that is to make the latter exceedingly complex [3][4].

The additional complexity though comes with major vulnerabilities. Smart Grids are increasingly at risk of cyber-attacks, failure of equipment, data modification and other uncoordinated grid characteristics [5], a factor that has the potential to jeopardize stability, reliability and security of power systems. To maintain a stable operation, it has become important to create a means through which anomaly detection can occur, suitable enough to identify and rectify them in real-time [6].

Artificial intelligence (AI) has emerged recently and is widely recognized in Smart Grid anomaly detection [7][8] to address these challenges. The AI-based techniques can easily extract hidden patterns and abnormal behaviours in a complex stream of data using large-scale, heterogeneous, and high-dimensional data captured by sensors, smart meters, and monitoring devices [9]. Yet, as much as data-based methods are effective in the detection of patterns, physics-based models provide the necessary mechanics required to fully describe the dynamics of operations present in a cyber-physical system (CPS). Hence, an AI-hybrid approach that combines physics-based knowledge with physics-deficient algorithms can provide a stronger, nonlinear, and scalable framework for anomaly detection in Smart Grids [10].

Machine learning, deep learning, reinforcement learning, and hybrid models are the AI methods most often used in this area. They are used for fault detection, load forecasting, intrusion detection, energy theft protection, and real-time monitoring [11]. Additionally, the prospect of implementing AI-based practices on edge-to-cloud platforms enables near real-time detection and response, thereby facilitating faster mitigation of anomalies and enhancing the cyber-resilience of grid infrastructures.

These advancements notwithstanding, there are still unaddressed challenges. Some of the most significant challenges are the absence of unified datasets, the inability to distinguish between the natural variations and the real anomalies, the challenge of designing big systems that connect, and the limited interpretability of the AI models [12]. Moreover, Smart Grids are highly dynamic, distributed systems that are vulnerable to advanced malicious attacks, and establishing adaptive, interpretable, and robust detection frameworks is therefore paramount [13]. To overcome these issues, need the latest algorithms, standardized testing environments, explainable AI approaches and field-deployment strategies. Moreover, interdisciplinary research, with the help of policy and industry-academia engagement, is also essential to close the growing divide between academic

improvement and actual application of anomaly detection solutions in Smart Grids.

A. *Structure of the Paper*

The structure of this study is organized as follows: Section II highlights the significance of smart grids and predictive maintenance. Section III defines the types of anomalies in smart grids. Section IV discusses AI techniques and implementation challenges. In Section V, the current research on anomaly detection is examined. Finally, Section VI ends with some thoughts and suggestions for future study.

II. Smart Grids and Their Importance

Integrating state-of-the-art communication, automation, and information technology with conventional power grids, smart grids are the logical next step for electrical power systems [14]. Smart grids allow utilities and consumers to communicate with each other in two ways, unlike traditional grids. Increased dependability, efficient energy distribution, and real-time monitoring are all made possible by this [15]. Smart grids are gaining significance in addressing the worldwide demand for sustainable and reliable energy infrastructure as a means to optimize energy usage, incorporate renewable resources, and guarantee system stability.

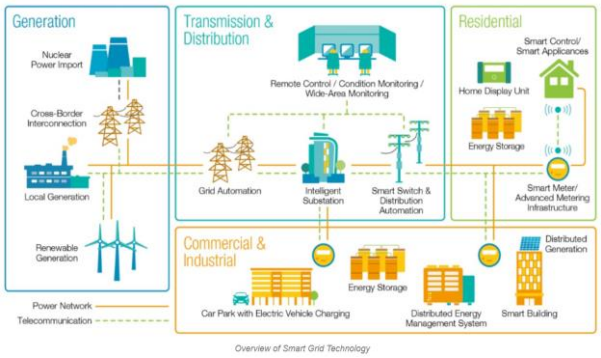

Fig. 1. Smart Grid Technology

Figure 1 illustrates the technological ecosystem of smart grids, highlighting the interconnectedness of generation, transmission, distribution, and consumption. It also shows the integration of renewable sources, intelligent substations, and consumer-side innovations like smart meters and EV charging, reinforcing the importance of smart grids in achieving efficiency and sustainability.

A. *Smart Grid Components*

Smart grids are built upon a wide range of interconnected components that collectively ensure reliable, secure, and efficient energy distribution [16]. The features enable real-time monitoring, Fault Management, and Renewable Energy integration, as well as consumer active participation in Energy Management. Some of the most important elements in building today's smart grid infrastructure are:

- **Transformers:** Transformers that increase or reduce voltage levels to transmit and distribute power and get power to customers safely and economically.
- **Circuit Breakers:** Protective devices that shut off electricity in the event of faults, or overloads thus preventing damage and ensuring safety.
- **Sensors:** The grid is embedded with sensors to continuously monitor the parameters of voltage, current, temperature and the environment.
- **Smart Meters:** Consumer premise devices that measure electricity use at a high resolution (enabling dynamic pricing, demand response and enhanced consumption analytics).
- **Communication Networks:** Support two-way data exchange between grid parts and control centers, necessary for real-time monitoring and control.
- **Energy Storage Systems and Distributed Energy Resources (DERs):** The integration that can be presented includes batteries, solar, and wind turbines to enable the grid to be more flexible and use renewable energy sources.

These elements allow conventional power grids and new forms of distributed energy resources to work together seamlessly; they are the backbone of smart grid architecture [17]. With the ability to connect intelligent sensing and storage technologies, as well as communication, the grid becomes an adaptable, two-way system that is user-centric. Figure 4 provides the best representation of this transformation, which has evolved into a decentralized, participatory, and flexible smart grid.

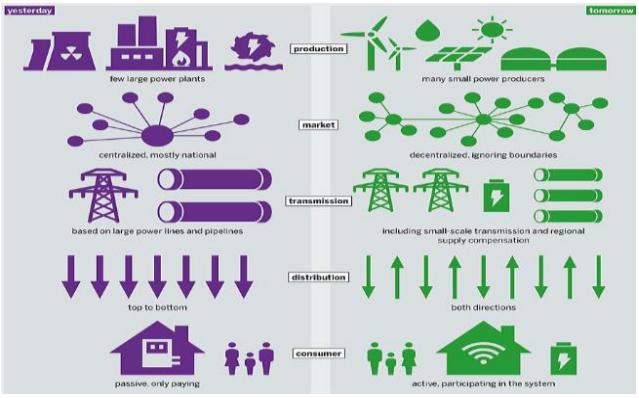

Fig. 2. Decentralized Smart Grid Future

Figure 2 illustrates a shift in the smart grid towards decentralized, consumer-controlled power systems, replacing more conventional power systems. There is a distinct shift in the modern energy system paradigm as opposed to the previous model of a few large power plants and command-and-control structure, and the future grid is that of a utility grid with distributed energy resources, local power generation and consumer involvement, also known as a proactive participation by the consumer in their utility grid.

B. *Common Failure Modes and Maintenance Challenges*

The infrastructure that comprises the smart grid is highly susceptible to operational malfunctions and maintenance-specific concerns, despite being advanced and data-driven. These failures may arise from equipment aging, environmental stress, cyber intrusions, or system complexity [18]. Addressing these challenges is crucial for ensuring reliable electricity delivery, maintaining grid reliability, and facilitating the sustainable integration of renewable energy sources. The key failure modes and challenges are:

- **Transformers:** Insulation degradation, overheat and mechanical wear down can cause the failure.

- **Circuit Breakers:** Contact wear, coil failures, and mechanical failure may be the cause of operational problems.
- **Sensors and Smart Meters:** Calibration drift, communication fault, and sensor dust contamination decrease data reliability.
- **Communication Systems:** Grid control can be compromised by Network latency, hack attacks, and hardware failures.

Maintenance issues are compounded by distributed assets, restricted access, voluminous heterogeneous data, and the requirement to ensure that downtime is absolutely minimal without affecting safety and reliability. Ensuring reliability and efficiency of smart grid components helps ward off outages and minimize costs, and consumer safety also enhances consistency, enhancing renewable integration and asset life. These issues highlight the importance of sophisticated strategies, such as predictive maintenance, to ensure the grid remains sustainable in its performance.

C. Predictive Maintenance in Smart Grids

Predictive maintenance in smart grids emphasizes anticipating equipment failures before they occur by analyzing condition-monitoring data, usage patterns, and performance indicators [19]. It is also an aggressive program, which not only reduces unplanned outages but also maximizes the use of resources and vital grid assets. Predictive strategies are not a new concept within the energy sector, and they are making utilities face reliability issues in the steady system developed with the help of more traditional methods.

Conventional maintenance strategies have always been at the center of the grid operations, but it is limited in comparison to the predictive strategies. On the one hand, reactive strategies do not implement measures until an issue arises, resulting in disruptions of services and associated downtime. Preventive strategies, on the other hand, compel regular checkups irrespective of the health of the equipment, which results in the waste of resources. To better clarify the distinction of predictive maintenance, one can discuss with the help of these two common practices that have defined maintenance in smart grids, as presented below:

- **Reactive Maintenance:** This maintenance method is to do repair or replacement of equipment after a failure has occurred. It is easy to install, but it can cause unplanned downtime, costly repairs, and pose safety issues.
- **Preventive Maintenance:** The plan involves the set maintenance at fixed intervals irrespective of the usefulness of the equipment. The purpose of preventive maintenance is to mitigate failures by actively maintaining the assets but it can cause an overload by unnecessary maintenance actions, labor costs, and inefficiencies in resources.

Predictive maintenance is smarter than reactive and preventive maintenance, as it focuses on predicting failures before they occur. That makes utilities shift toward expensive and unplanned interventions to timely and effective measures. The most important predictive maintenance benefits are as follows:

- Early Fault Detection: Catching problems at the early point of development to avoid the disastrous outcomes.
- Optimized Maintenance Scheduling: Conducting maintenance, however, only when the need arises thereby minimizing downtime and the associated operating costs.
- Extended Asset Lifespan: Keeping equipment in an optimal state of operation extends its lifetime.
- Improved Reliability and Safety: Reduction of the sudden outages reinforces the grid stability and safeguards the people and infrastructure.
- Data-driven decision-making: Using sensor data and the application of AI models to aid in proactive maintenance strategies.
- In general, predictive maintenance is a very important improvement non-traditional methods and the process of maintenance is harmonized with the needs of smart grids.

III. Anomaly Detection in Smart Grids and Its Types

Anomaly Detection in Smart Grids refers to the identification of unusual patterns or behavior in the grid data suggesting fault, cyber-attacks or failure of equipment. It relies on high-performance analytics and machine-learning computation to perceive real-time input from sensors, smart meters, and control frameworks. Effective anomaly detection aids in improving the grid power reliability, efficient energy distribution, for the improvements on fault diagnosis in the grid power system inspection and on the efforts of grid power system security.

A. Types of Anomalies in Smart Grids

Smart grids comprise digital communications, sensing, and control technologies that power and enhance the management of electricity. They, however, are complex and interconnected and open themselves to several anomalies. These anomalies when not detected can compromise performance--or disturb services or even cause major failures. The following is what may be described as constituent categories of anomalies that are likely to be found in smart grids:

1) Equipment Failures

Equipment failures are one of the most common and serious problems in smart grids [20]. They may occur due to the aging of equipment, manufacturing flaws, failure to service it, or due to some other kind of damage during severe weather. Examples include transformers failing due to overheating or blown insulation, circuit breakers not properly isolating faults, and power line faults or outages caused by physical damage or wear. There is a risk of causing blackouts, instability in voltage, and poor power quality, which can impact both customers and utility companies. Condition monitoring and AI-based predictive maintenance can enhance the ability to detect problems early, preventing downtime and significantly reducing maintenance costs.

2) Cyber-Attacks and Intrusions

Cyber-attacks and intrusions pose substantial threats to smart grids, as they target the digital and communication systems of these grids. Hackers can gain unauthorized access to control systems, disrupt operations, steal sensitive data, or manipulate grid functions [21]. Common attacks include malware infections, DoS attacks, and phishing schemes. These may trigger power outages, lead to damage to equipment, or trigger the liability and security of the grid. Preventing cyber-attacks on smart grids is crucial to deploying

effective cybersecurity practices, such as encryption and real-time monitoring and response, to intercept an intrusion in time before it develops into significant damage.

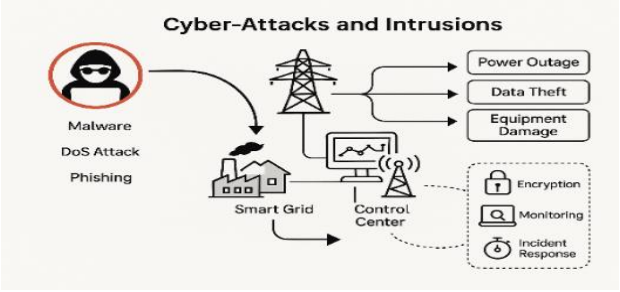

Fig. 3. Cyber Attacks and Intrusions

As shown in Figure 3, smart grids/control centers are subject to cyber-attacks like malware, DoS attacks, and phishing, causing such problems as power failure, data loss, and destruction or damage of equipment. It also indicates main defense techniques, such as encryption, monitoring and incident response.

3) Load Forecasting Errors

Forecasting Errors: The error between the actual electrical load consumed and the forecasted load values generated by a forecasting model is called an error in forecasting. These errors arise because load demand is influenced by numerous dynamic factors such as weather conditions, consumer behaviour, economic activity, and system disruptions, which are often difficult to predict precisely [22]. Since reliability issues, poor resource use, and hefty fines can result from inaccurate load forecasts, accurate load forecasting is crucial for power system operation and planning. The performance of the forecasting model can be assessed and enhanced using common metrics, such as RMSE and MAPE, which measure load forecasting errors. An assortment of statistical models, ML techniques, DL algorithms, and other load forecasting tools has been standardised in an effort to cut down on these kinds of mistakes.

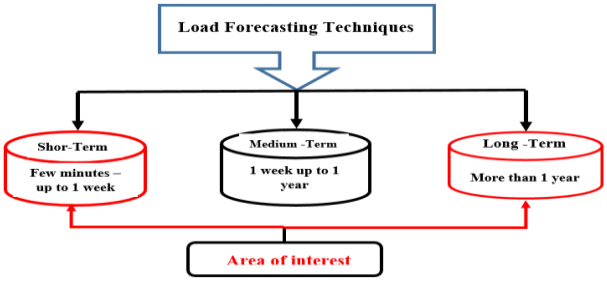

Fig. 4. Load Forecasting Techniques

Figure 4 illustrates a hierarchy of load forecasting methods based on prediction horizon, with short-term, medium-term, and long-term approaches depicted. Smart grid planners and managers are primarily interested in medium-term forecasting.

4) Sensor Malfunctions and Data Inconsistencies

It refers to errors or irregularities in the data collected from sensors due to hardware faults, communication issues, or environmental interference. Sensor malfunctions can cause incorrect, missing, or noisy measurements.[23] , while data inconsistencies arise when the recorded data does not align logically over time or between related sensors. These issues can severely impact the accuracy and reliability of systems that depend on sensor data, such as monitoring, control, and forecasting applications. Validating, filtering, and correcting techniques are essential for identifying and correcting sensor malfunctions and data inconsistencies, ensuring data integrity and maintaining system performance.

IV. Anomaly Detection Techniques And Supporting Tools In Smart Grids

The dynamic nature of modern smart grids makes them highly susceptible to a wide range of anomalies, including cyber intrusions, equipment malfunctions, and irregular consumption patterns [24]. Traditional monitoring systems often fail to capture these irregularities in real time due to the scale and complexity of smart grid infrastructures [25]. Thus, anomaly detection has become a vital function for providing reliability, efficiency, and resilience. AI, machine learning, and statistical analysis enable the detection of anomalies proactively, preventing potential large-scale impacts on other activities that may affect grid stability, data protection, or service disruption.

The tools and platforms supporting these techniques can also be considered vital. The errors detected by anomaly detection models are ideally tested in practical environments, simulated environments, big data frameworks, and cloud platforms. These tools both enable large-scale experimentation, as well as provide support for integrating heterogeneous data sources, including smart meters, sensors and communication networks. Combined, technology and tools are the synergy of smart grid intelligent anomaly detection systems.

A. Anomaly Detection Techniques in Smart Grids

Anomaly detection in smart grids plays a vital role in ensuring reliability, safeguarding infrastructure, and preventing disruptions caused by faults or malicious activities [26]. By identifying irregularities at an early stage, operators can take proactive measures to maintain stability and security [27]. The most recent developments employ statistical and AI-based models, as well as hybrid architectures, to enable increased scalability and accuracy across a wider range of operating conditions. The detection methods of anomaly are presented below:

- **Machine Learning (ML) Techniques:** Anomaly classification and pattern recognition using supervised and unsupervised learning techniques.
- **Deep Learning Models:** Neural networks such as CNNs and RNNs for capturing spatial-temporal patterns in grid data.
- **Federated Learning:** Distributed model training that protects user privacy without transferring data files across devices.
- **Graph-Based Models:** Utilize graph structure learning to detect complex interactions and anomalies in multi-source energy data.
- **Statistical Analysis:** Traditional methods like mean, variance, MAE, MAPE, RMSE to detect deviations from expected patterns.
- **Hybrid AI + Physics-Based Modeling:** Combine artificial intelligence with physical models for accurate and explainable detection.
- **Fuzzy Logic-Based Algorithms:** Rule-based systems (e.g., Artificial Bee Colony + Fuzzy Logic) for handling uncertainty in smart grid environments.

- **Transformer-Based Models:** Used in video or sequence-based anomaly detection leveraging attention mechanisms.
- **Quantum AI and Neural Networks:** Emerging technique integrating quantum computing for high-accuracy forecasting and anomaly detection.

B. Tools and Platforms

The deployment of AI-driven anomaly detection in smart grids requires a strong technological foundation, encompassing both computational and simulation resources [28]. The tools can serve not only to efficiently manage tremendous amounts of grid data but also to design, train and validate intelligent models reliably and at scale. There are three groups of tools and platforms, which can be divided to meet the wide range of needs in utilizing anomaly detection instruments, as shown in Figure.5, are given below:

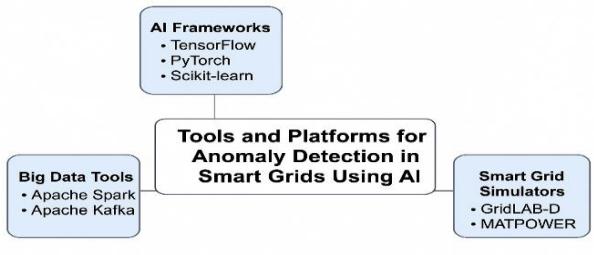

Fig. 5. Tools and Platforms for Anomaly Detection

1) AI Framework

ML model construction, training, and deployment are all made possible by AI frameworks [29]. They reduce the complexity of complicated calculations, speed up experimentation, and enhance scalability, which is essential to the problem of anomaly detection in smart grids. The most usual frameworks are presented below:

- **TensorFlow**: Deep Learning, an open-source framework created by Google, is extensively utilised for the construction and training of intricate neural network models.
- **PyTorch**: A widely used and adaptable Facebook deep learning library [30] that is perfect for AI model development and testing in the wild.
- **Scikit-learn**: A compact and powerful set of classical machine learning algorithms, ideal for use in prototypes and smaller to medium-sized projects.

2) Big Data Tools

Big data tools are essential in the management and processing of such vast amount of data in a smart grid. They provide flexibility in terms of being able to run anomaly detection systems in real time and have fault detection and the opportunity to scale. The tools used briskly include the following:

- **Apache Spark**: ML model training on smart grid data is a common use case for this general-purpose, rapid cluster computing system [31].
- **Apache Kafka**: The ability to detect abnormalities in live smart grid systems relies on a distributed streaming platform that can install and monitor data in real-time.

*3) **Smart Grid Simulators***

Smart grid simulators enable real-time, large-scale, open-architecture simulations to accelerate smart grid development [32]. They minimize inefficiencies in group work, offer safe experimental tests of systems and processes, and offer a cost-effective pre-deployment feedback, enhancing reliability and effectiveness and the implementation strategy.

a) GridLAB-D

The US Department of Energy developed this robust smart grid simulator so that anybody can model distribution networks, load patterns, market dynamics, and even the effects of weather. It can let researchers evaluate anomaly detection methods and system reaction in a risk-free environment and is important for creating synthetic data to train AI models.

b) Matpower

Power system optimisation and simulation can be achieved with this open-source MATLAB tool [33]. Power flow and optimal power flow problems are solved using it, and it provides a reliable baseline for verifying anomaly detection models driven by AI. Its flexibility allows seamless integration with custom scripts and external machine learning frameworks, enabling advanced analytics and real-world grid behaviour validation.

V. LITERATURE REVIEW

The literature review section explores recent advancements in anomaly detection for smart grids, emphasizing artificial intelligence, hybrid techniques, and semantic modeling. It highlights methodologies, applications, and challenges, showcasing diverse AI-driven approaches enhancing detection accuracy, robustness, and cybersecurity in evolving energy distribution systems.

Dong (2025) works deeply executes cross-modal collaborative learning and multi-level semantics representation for the data feature of multiple energy sources: Firstly, utilize the multi-channel attention mechanism to mine the correlation between energy consumption data in different models to realize the implementation of the weight attention of key features. Then, the hierarchical embedding network was used to map the multi-modal features to the high-dimensional unified semantic space, the temporal information and spatial relations were captured through different levels. [34].

Gaggero, Girdinio and Marchese (2025) Machine learning techniques are being used more and more in anomaly detection methods. These techniques are a revolutionary tool for data analysis. This survey aims to examine Smart Grid anomaly detection strategies, with a focus on methods that integrate AI with physics-based modelling. This work provides a comprehensive review of the existing literature by analysing the algorithms, use cases, performances, and validation of published papers, as well as by pointing out important gaps in the literature and suggesting ways forward for this area of study [35].

Anaraki et al. (2024) explore the peculiarity of low-voltage (LV) grids, which are growing increasingly intricate as a result of the extensive use of decentralized power plants, electric heat pumps, and solar panels. A variety of data-driven approaches, including methodologies like process grid data and statistical analysis as well as AI. In order to uncover any substantial anomalies in their activities, the investigation attempts to identify unexpected variations in energy use, unauthorized photovoltaic systems, and rapid fluctuations in grid demand. The findings suggest that, taking into account the goals of grid operators and their ability to differentiate

between short-term and long-term abnormalities, one approach may be better suited than another [36]

Guato Burgos, Morato and Vizcaino Imacaña (2024) Artificial intelligence is used to detect irregularities in smart grids. Searched digital archives for articles published between 2011 and 2023. Studies with diverse techniques were considered, experiments were proposed, and the most applied methodologies were identified through iterative searches. Data integrity assaults, anomalous consumption and measurements, intrusions, electrical data, network infrastructure, cyber-attack detection, and detecting devices are the seven SG anomaly-related objects of investigation. Cybersecurity challenges have been the subject of much research, particularly in the fight against intrusions, fraud, data fabrication, and unchecked network model alterations [37].

Banik et al. (2023) Cybersecurity, fault detection, electricity theft, and many more areas can benefit from analyzing smart grid data for anomaly detection. Several factors could have contributed to the unusual and suspicious actions, such as customers' unusual usage habits, problems with the grid infrastructure, power outages, cyberattacks from outside sources, or energy fraud. Academics have recently focused on smart grid anomaly detection, and it has found extensive use in a number of important sectors. An enormous challenge inside the smart grid is the implementation of reliable anomaly detection for all kinds of unusual behaviors. Aiming to cover both historical and current research on smart grid anomaly detection, this study compiles a literature catalogue [38].

Baker et al. (2022). This article discusses the problematic nature of PEDG's real-time anomaly detection and classification. The proposed approach to reaching ADS and ACS in real-time is based on integrating model predictive control (MPC) with long short-term memory (LSTM). Both the MPC and the LSTM detection network can make use of time-series input data for classification and anomaly correction. Future PEDG must have the capability to identify and repair power electronics' internal problems; here is where the proposed LSTM-MPC solution is useful; this will allow inverters' internal failures to be distinguished from anomalies. To enable PEDG to operate resiliently in the face of cyberattacks, it is necessary to identify and categorize internal faults such as an open circuit fault [39].

Table I provides a synopsis of current research on smart grid anomaly detection using artificial intelligence (AI), comparing various studies and highlighting their methods, results, limitations, and potential future research areas.

TABLE I. SUMMARIZES THE STUDY ON ANOMALY DETECTION IN SMART GRIDS USING ARTIFICIAL INTELLIGENCE

Reference	Study On	Approach	Key Findings	Limitations / Challenges	Future Research
Dong (2025)	Multi-modal energy source data analysis	Cross-modal collaborative learning & multi-channel attention	Improved feature extraction and anomaly detection accuracy using unified semantic representation	High computational complexity and scalability issues	Optimize multi-modal feature learning for large-scale smart grids
Gaggero et al. (2025)	AI & physics-based modeling in smart grids	Survey on AI-integrated anomaly detection methods	Highlights hybrid approaches combining AI and physical modeling for enhanced detection	Lack of real-time deployment insights; limited benchmarks	Develop real-time frameworks integrating AI and physics-based models
Anaraki et al. (2024)	Low-voltage grid anomaly detection	Statistical & AI-driven techniques	Effectively detects unauthorized installations and sudden load changes	Dependence on grid-specific objectives; low generalization	Build adaptable AI models applicable across diverse LV grid topologies
Guato Burgos et al. (2024)	Anomaly detection in infrastructure and cybersecurity using AI	Comprehensive literature survey	Identifies major anomaly types (cyber-attacks, intrusions, energy fraud) and detection devices	Limited experimental validations; lacks cross-domain insights	Incorporate hybrid AI models addressing cybersecurity and energy anomalies jointly
Banik et al. (2023)	Broad smart grid anomaly detection	Scoping review of AI-based approaches	Identifies cybersecurity anomalies, outages, fraud, and infrastructure failures	Absence of unified frameworks across multiple anomaly types	Develop integrated AI-driven anomaly detection architectures
Baker et al. (2022)	Real-time detection of anomalies in PEDG	LSTM + Model Predictive Control (MPC)	Achieves real-time anomaly classification and corrective actions in PEDG	High dependency on time-series quality; less tested on large datasets	Extend integrated LSTM-MPC methods for scalable, real-time smart grid environments

VI. CONCLUSION AND FUTURE WORK

The growing number of smart grids, spurred by distributed generation and the incorporation of renewable energy sources, has greatly increased the complexity of energy distribution systems. This complexity has made anomaly detection a critical component in ensuring reliability, security, and operational efficiency. Through an extensive review of existing literature, it is evident that AI-driven techniques and hybrid approaches have emerged as powerful tools for enhancing anomaly detection. Studies demonstrate that methods such as cross-modal collaborative learning, hierarchical semantic modelling, physics-based hybrid algorithms, and deep learning architectures have successfully addressed challenges related to cybersecurity, fault detection, energy theft prevention, and real-time monitoring. More flexible and robust detection frameworks are required due to the increasing complexity of cyber threats, the heterogeneity of grid infrastructures, and the variety of datasets.

Future research should concentrate on creating AI-based anomaly detection models that can scale, be explained, and adapt to different grid contexts. These models should be able to work well in these types of settings. Evolving smart grid ecosystems must incorporate privacy-preserving techniques, standardised benchmarking datasets, and real-time analytics to guarantee robustness, improve detection accuracy, and increase overall security and dependability.

REFERENCES

[1] H. S. Chandu, “Efficient Machine Learning Approaches for Energy Optimization in Smart Grid Systems,” *IJSART*, vol. 10, no.

9, pp. 67–75, 2024.

[2] S. Banik, S. K. Saha, T. Banik, and S. M. M. Hossain, "Anomaly Detection Techniques in Smart Grid Systems: A Review," in *2023 IEEE World AI IoT Congress (AIIoT)*, IEEE, Jun. 2023, pp. 0331–0337. doi: 10.1109/AIIoT58121.2023.10174485.

[3] S. Pandya, "Integrating Smart IoT and AI-Enhanced Systems for Predictive Diagnostics Disease in Healthcare," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 10, no. 6, pp. 2093–2105, Dec. 2024, doi: 10.32628/CSEIT2410612406.

[4] O. A. Omitaomu and H. Niu, "Artificial Intelligence Techniques in Smart Grid: A Survey," *Smart Cities*, vol. 4, no. 2, pp. 548–568, 2021, doi: 10.3390/smartcities4020029.

[5] S. B. Shah, "Machine Learning for Cyber Threat Detection and Prevention in Critical Infrastructure," *Dep. Oper. Bus. Anal. Inf. Syst. (OBAIS*, vol. 2, no. 2, 2025, doi: 10.5281/zenodo . 14955016.

[6] A. Cooper, A. Bretas, and S. Meyn, "Anomaly Detection in Power System State Estimation: Review and New Directions," *Energies*, vol. 16, no. 18, 2023, doi: 10.3390/en16186678.

[7] V. Thangaraju, "Enhancing Web Application Performance and Security Using AI-Driven Anomaly Detection and Optimization Techniques," *Int. Res. J. Innov. Eng. Technol.*, vol. 9, no. 3, 2025, doi: 47001/IRJIET/2025.903027.

[8] A. R. Bilipelli, "AI-Driven Intrusion Detection Systems for Large-Scale Cybersecurity Networks Data Analysis : A Comparative Study," *TIJER – Int. Res. J.*, vol. 11, no. 12, pp. 922–928, 2024.

[9] S. S. Ali and B. J. Choi, "State-of-the-Art Artificial Intelligence Techniques for Distributed Smart Grids: A Review," *Electronics*, vol. 9, no. 6, 2020, doi: 10.3390/electronics9061030.

[10] S. Sun, Y. Tang, T. Tai, X. Wei, and W. Fang, "A Review on the Application of Artificial Intelligence in Anomaly Analysis Detection and Fault Location in Grid Indicator Calculation Data," *Energies*, vol. 17, no. 15, 2024, doi: 10.3390/en17153747.

[11] J. Jithish, B. Alangot, N. Mahalingam, and K. S. Yeo, "Distributed Anomaly Detection in Smart Grids: A Federated Learning-Based Approach," *IEEE Access*, vol. 11, pp. 7157–7179, 2023, doi: 10.1109/ACCESS.2023.3237554.

[12] A. Fathollahi, "Machine Learning and Artificial Intelligence Techniques in Smart Grids Stability Analysis: A Review," *Energies*, vol. 18, no. 13, 2025, doi: 10.3390/en18133431.

[13] V. Prajapati, "Enhancing Threat Intelligence and Cyber Defense through Big Data Analytics: A Review Study," *J. Glob. Res. Math. Arch.*, vol. 12, no. 4, 2025.

[14] J. J. M. Escobar, O. M. Matamoros, R. T. Padilla, I. L. Reyes, and H. Q. Espinosa, "A Comprehensive Review on Smart Grids: Challenges and Opportunities," *Sensors*, vol. 21, no. 21, p. 6978, Oct. 2021, doi: 10.3390/s21216978.

[15] S. Pandya, "Predictive Analytics in Smart Grids : Leveraging Machine Learning for Renewable Energy Sources," *Int. J. Curr. Eng. Technol.*, vol. 11, no. 6, pp. 677–683, 2021.

[16] F. E. Abrahamsen, Y. Ai, and M. Cheffena, "Communication Technologies for Smart Grid: A Comprehensive Survey," *Sensors*, vol. 21, no. 23, p. 8087, Dec. 2021, doi: 10.3390/s21238087.

[17] V. Ethirajan and S. P. Mangaiyarkarasi, "An in-depth survey of latest progress in smart grids: paving the way for a sustainable future through renewable energy resources," *J. Electr. Syst. Inf. Technol.*, vol. 12, no. 1, p. 9, 2025, doi: 10.1186/s43067-025-00195-z.

[18] S. Avdaković, M. M. Dedović, E. Hasković, and Z. Jašarević, "Communication Technologies for the Smart Grid - A Short Review and a Case-Study Analysis," *Elektroteh. Vestnik/Electrotechnical Rev.*, vol. 92, no. 3, pp. 86–96, 2025.

[19] M. Cate, "Anomaly Detection Techniques in Smart Grid Networks Using AI," no. May, 2025.

[20] S. Tufail, I. Parvez, S. Batool, and A. Sarwat, "A Survey on Cybersecurity Challenges, Detection, and Mitigation Techniques for the Smart Grid," *Energies*, vol. 14, no. 18, 2021, doi: 10.3390/en14185894.

[21] T. T. Khoei, H. O. Slimane, and N. Kaabouch, "A Comprehensive Survey on the Cyber-Security of Smart Grids: Cyber-Attacks, Detection, Countermeasure Techniques, and Future Directions," *arXiv*, p. arXiv:2207.07738, 2022.

[22] T. Hong and S. Fan, "Probabilistic electric load forecasting: A tutorial review," *Int. J. Forecast.*, vol. 32, no. 3, pp. 914–938, 2016, doi: https://doi.org/10.1016/j.ijforecast.2015.11.011.

[23] D. D. Rao, V. Roy, K. Bhopte, K. Mukilan, P. K. Shukla, and R. V Patil, "Fuzzy-Based Cluster Head Management with Artificial Flora Optimization for Energy-Efficient and Secure Routing in Fog-Enabled Wireless Sensor Networks," in *2024 IEEE 2nd International Conference on Innovations in High Speed Communication and Signal Processing (IHCSP)*, IEEE, Dec. 2024, pp. 1–6. doi: 10.1109/IHCSP63227.2024.10960064.

[24] R. Q. Majumder, "A Review of Anomaly Identification in Finance Frauds Using Machine Learning Systems," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 5, no. 10, pp. 101–110, Apr. 2025, doi: 10.48175/IJARSCT-25619.

[25] M. Balamurugan, K. Narayanan, N. Raghu, G. B. Arjun Kumar, and V. N. Trupti, "Role of artificial intelligence in smart grid – a mini review," *Front. Artif. Intell.*, vol. 8, pp. 1–7, 2025, doi: 10.3389/frai.2025.1551661.

[26] M. A. Husnoo, A. Anwar, M. E. Haque, and A. N. Mahmood, "Decentralized Federated Anomaly Detection in Smart Grids: A P2P Gossip Approach," vol. 8807, pp. 0–1, 2025.

[27] H. Kali, "The Future Of Hr Cybersecurity: Ai-Enabled Anomaly Detection In Workday Security.," *Int. J. Recent Technol. Sci. Manag.*, vol. 8, no. 6, 2023, doi: 10.10206/IJRTSM.2025803096.

[28] A. Alshehri, M. M. Badr, M. Baza, and H. Alshahrani, "Deep Anomaly Detection Framework Utilizing Federated Learning for Electricity Theft Zero-Day Cyberattacks," *Sensors*, vol. 24, no. 10, 2024, doi: 10.3390/s24103236.

[29] Y. Li, X. Wei, Y. Li, Z. Dong, and M. Shahidehpour, "Detection of False Data Injection Attacks in Smart Grid: A Secure Federated Deep Learning Approach," *IEEE Trans. Smart Grid*, vol. 13, no. 6, pp. 4862–4872, 2022, doi: 10.1109/TSG.2022.3204796.

[30] A. Paszke *et al.*, "PyTorch: An Imperative Style, High-Performance Deep Learning Library," in *Advances in Neural Information Processing Systems*, 2019.

[31] M. Zaharia *et al.*, "Apache Spark: A unified engine for big data processing," *Commun. ACM*, vol. 59, no. 11, pp. 56–65, 2016, doi: 10.1145/2934664.

[32] R. Podmore and M. R. Robinson, "The Role of Simulators for Smart Grid Development," *IEEE Trans. Smart Grid*, vol. 1, no. 2, pp. 205–212, Sep. 2010, doi: 10.1109/TSG.2010.2055905.

[33] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-State Operations, Planning, and Analysis Tools for Power Systems Research and Education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, 2011, doi: 10.1109/TPWRS.2010.2051168.

[34] Y. Dong, "Correlation-Driven Multi-Level Multimodal Learning for Anomaly Detection on Smart Electric Grid," in *2025 2nd International Conference on Smart Grid and Artificial Intelligence (SGAI)*, 2025, pp. 254–257. doi: 10.1109/SGAI64825.2025.11009488.

[35] G. Gaggero, P. Girdinio, and M. Marchese, "Artificial Intelligence and Physics-Based Anomaly Detection in the Smart Grid: A Survey," *IEEE Access*, vol. 13, pp. 23597–23606, 2025, doi: 10.1109/ACCESS.2025.3537410.

[36] R. B. Anaraki, R. Palaniappan, U. Häger, and C. Rehtanz, "Data-driven Approaches for Anomaly Detection in Low-Voltage Grid Net Power," in *2024 IEEE PES Innovative Smart Grid Technologies Europe (ISGT EUROPE)*, 2024, pp. 1–5. doi: 10.1109/ISGTEUROPE62998.2024.10863001.

[37] M. F. G. Burgos and J. Morato, "A Review of Smart Grid Anomaly Detection Approaches Pertaining to Artificial Intelligence," *Appl. Sci.*, vol. 14, no. 3, p. 1194, Jan. 2024, doi: 10.3390/app14031194.

[38] S. Banik, S. K. Saha, T. Banik, and S. M. M. Hossain, "Anomaly Detection Techniques in Smart Grid Systems: A Review," in *IEEE World AI IoT Congress (AIIoT)*, 2023, pp. 1–7.

[39] M. Baker, A. Y. Fard, H. Althuwaini, and M. B. Shadmand, "Real-Time AI-Based Anomaly Detection and Classification in Power Electronics Dominated Grids," *IEEE J. Emerg. Sel. Top. Ind. Electron.*, vol. 4, no. 2, pp. 549–559, Apr. 2023, doi: 10.1109/JESTIE.2022.3227005.

