Integrating Machine Learning for Anomaly Detection and Pattern Recognition in Smart Grid Power Data

Chang Xu[1,*], Pengcheng Zhang[2], Ning Luo[2], Fei Zheng[2] and Wenzhong He[3]

[1]*Guizhou Power Grid Co., Ltd Guiyang 550002, Guizhou, China*
[2]*Guizhou Power Grid Co., Ltd. Power Grid Planning Research Center, Guiyang 550003, Guizhou, China*
[3]*Guizhou Qianchi Information Corp., Ltd. Guiyang 550007, Guizhou, China*
E-mail: yasio4@163.com
[*]*Corresponding Author*

Received 16 April 2025; Accepted 03 June 2025

Abstract

The integration of machine learning (ML) for anomaly detection and pattern recognition in smart grid power data represents a significant advancement in the management and optimization of modern electrical power systems. This research explores how ML algorithms can process and analyze the enormous volumes of data generated by smart grids, focusing specifically on identifying anomalies and recognizing patterns that traditional methods might miss. By implementing ML techniques, this study aims to enhance the predictive capabilities, operational efficiency, and overall security of smart grid systems while addressing critical challenges such as data quality, cybersecurity threats, and scalability issues.

The transformative potential of ML in smart grid management is demonstrated through various applications, including load forecasting, fault detection, and intrusion prevention. The research examines both supervised and

Distributed Generation & Alternative Energy Journal, Vol. 40_3, 595–614.
doi: 10.13052/dgaej2156-3306.4037

unsupervised learning approaches, evaluating their effectiveness in different scenarios. Additionally, the study highlights the importance of deep learning models in handling the complex, high-dimensional data characteristic of smart grid environments.

The findings indicate that ML integration significantly improves anomaly detection rates and pattern recognition accuracy, contributing to more stable and reliable power distribution systems. Furthermore, the research identifies key areas for future development, including the need for more sophisticated models capable of handling increasingly complex data landscapes and enhanced cybersecurity measures to protect against emerging threats.

Keywords: Smart grids, machine learning, anomaly detection, pattern recognition, power systems.

1 Introduction

Electrical energy is a manufactured commodity like clothing, furniture or tools and when that energy is used in the passage of time we call it power. Energy is essential for any economical development of a country if its supply stops, numerous routine functions come to halt. Contemporary energy availability has led to shorter work days, higher production, better diets and improved production [1].

Energy is generated from different means and to transfer it to people in the form of electrical power we need grid stations. These stations then transfer the generated power to the respective substation and finally to the consumer. Grid station comprises expensive instruments such as transformers, relays, batteries and current transformers which are in constant use to transmit power due to which it faces severe challenges like failure of these equipment, power outages and inefficiencies in power distribution. Such issues can lead to significant disruption and economic losses [2].

To mitigate such problems conventional grid systems are poised toward smart grid systems. Smart grids integrate information and digital communication technologies with power grid systems, enabling two-way communication and power flow. Thus enhances the security, reliability, and efficiency of the power system. Which can further be enhanced by the machine learning algorithm since the SG system keeps track of the power data that can be fed to any relevant machine learning algorithm to improve the system which will be discussed in this research work. However the difference between conventional grid and smart grid is depicted by Figure 1. As can be seen

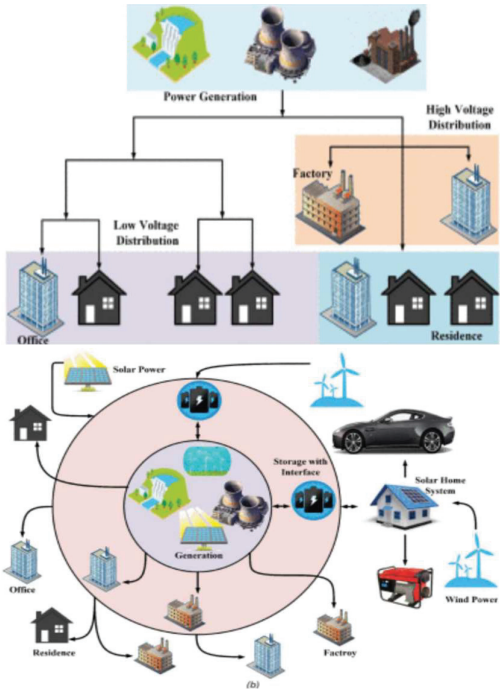

Figure 1 Comparison of conventional and smart grid power flow structures.

in conventional grid systems, power flows uni-directional whereas in a smart grid it is bi-directional between the generation and distribution sides.

Smart grids necessitate continuous connectivity and communication, which is facilitated by devices equipped with these features. These devices, interconnected with other network nodes via the internet, constitute the Internet of Things (IoT). Each object within this network possesses a distinct digital identity. The IoT integrates everything into a sophisticated network of intelligent objects that are self-aware, capable of interacting with their surroundings, and able to process data. These smart devices possess the ability to interact seamlessly across the network architecture [3]. A prime example is smart meters, which deliver comprehensive insights through detailed data collection – information crucial for precise analytics and autonomous operational choices. Such functionality elevates the smart grid's performance beyond traditional power distribution systems. Nevertheless, the voluminous data produced requires immediate computation and secure archiving for subsequent examination. Studies have analyzed information gathered from

intelligent monitoring points located in substations, along distribution lines, and within centralized databases. The datasets encompass market dynamics, illumination levels, electrical performance parameters, topographical details, and meteorological conditions.

Precise and efficient prediction models for energy consumption are essential for optimizing the entire energy lifecycle, from generation to distribution. For instance, the vast amounts of energy data collected every 15 minutes from hundreds of thousands of smart meters (measuring in kWh) introduce challenges to prediction models, demanding high data quality to ensure their effectiveness in smart grids (SG). These models need to account for various predictive factors like renewable energy generation, power market purchases, and daily load distribution, all of which are integral to ensuring the security and sustainability of SG systems.

Studies have shown that electricity consumption predictability improves with a dynamic response to demand. The volume of data generated by smart grids is enormous, making analysis much more complex and requiring dynamic energy management (DEM) to handle the flow of power, observing system, real-time functionality, and production scheduling. This kind of extensive, high-frequency data, known as "big data," cannot be analyzed with traditional methods, and researching its use in power generation, optimization, and forecasting has become central, particularly for renewable systems like wind power.

Furthermore, the data collected by SGs often contains personal information that is protected by law. Additionally, this data may include sensitive information at both organizational and national levels, which, if manipulated, could pose threats to the stability and safety of the grid itself, making data security essential. With smart grids now functioning as IoT-based cyber-physical systems, they are increasingly susceptible to cyberattacks, emphasizing the need for strong security measures to protect both grid operations and data integrity. In this context, machine learning offers promising solutions for big data processing, enabling robust prediction and security capabilities within SGs.

Section 4 of the article delves into the application of the Internet of Things (IoT) in distributed power systems. It underscores the importance of IoT devices [4], which can exchange information and receive commands, within the context of smart grids. These devices, connected via the internet, enable extensive communication and data transfer autonomously, eliminating the need for human intervention.

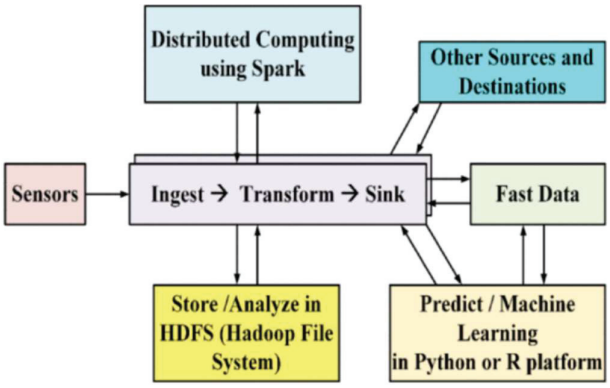

Figure 2 IoT framework block diagram.

In their work, Khan et al. characterize the Internet of Things (IoT) as an interconnected ecosystem of sensory and actuating mechanisms that exchange data across diverse platforms via a unified architecture. This integration is accomplished through pervasive, seamless monitoring capabilities, advanced analytical processing, and sophisticated data visualization techniques, with cloud infrastructure serving as the core operational backbone. Every entity within this network incorporates a dedicated processing unit, facilitating its recognition and communication with adjacent components. As illustrated in Figure 2, this framework demonstrates how sensor-collected information can be relayed to multiple destination systems through various software environments to execute designated functions.

Subsequently, Figure 3 illustrates the projected growth in IoT devices with the passage of time, highlighting the significant increase in their deployment. The figure shows that the number of IoT devices has grown from approximately 13 billion in 2015 to a projected 30 billion and beyond by 2020.

Furthermore Figure 4 discusses the introduction of IoT in the smart grid. It highlights the framework for IoT-implemented layers for smart grids, showing how every IoT layer points to a specific layer of smart grid infrastructure [5]. from which the power sector can greatly be benefited such as improvement in transmission and distribution efficiency, better utilization of renewable energy sources, and enhanced energy management in smart homes and cities. For example, smart meters, which provide two-way communication while measuring power, are a fundamental concept in IoT. These meters

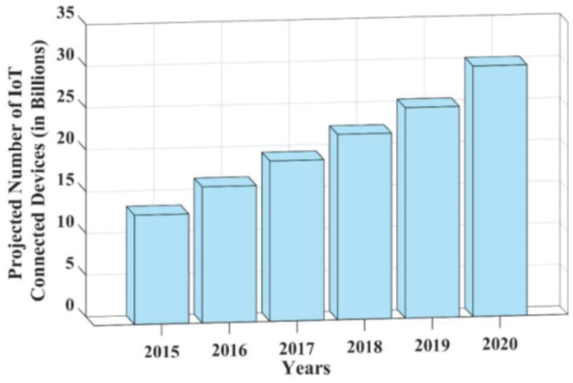

Figure 3 Projected growth of IoT devices over time.

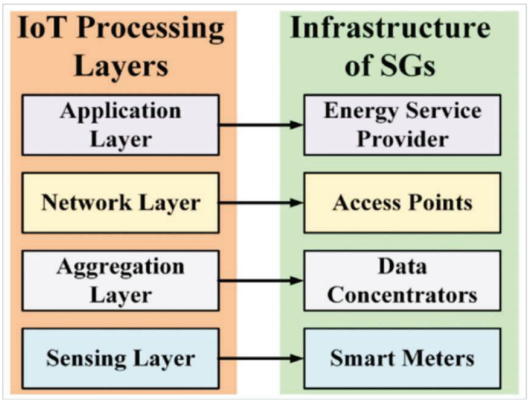

Figure 4 Structural implementation of IoT layers in smart grids.

transmit measurement data to utility suppliers through a mesh network, allowing better tracking of consumption and generation.

1.1 Big Data

The incorporation of Big Data analytics into the smart grid infrastructure underscores the challenges that the substantial volume of data produced by IoT devices presents to traditional data transfer, storage, and analysis techniques. Given that Big Data consists of enormous datasets, it necessitates more advanced methods for data capture, curation, management, and analysis, which exceed the capabilities of conventional tools. In other words, Big Data is distinguished by its large volume, high velocity, and significant

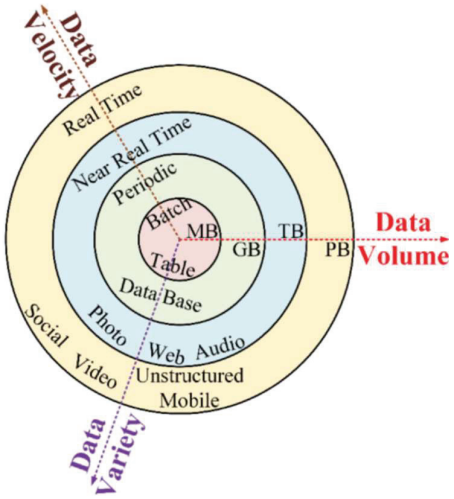

Figure 5 Characteristics defining big data.

variety, as shown in Figure 5. These characteristics make Big Data particularly suitable for handling the data generated by IoT devices in the smart grid [6].

1.2 Advantages of Big Data

Big Data analytics in the smart grid offers several benefits, including enhanced load forecasting, advanced data acquisition techniques, and cost-effectiveness. It also underscores the importance of cloud-based systems for storing and analyzing the data generated by the smart grid. These cloud-based systems utilize machine learning algorithms to detect anomalies within the system [7].

1.3 Application of Machine learning algorithm on Big Data

Now that we have large data coming from various sensors in smart grids it's better to utilize it further to enhance smart grid functionalities and protect the system from anomalies using machine learning algorithms. It emerges as a crucial solution, handling the immense data volumes produced by IoT-enabled grid systems [8]. As the concluding component in the intelligent grid framework, it enables a continuous loop of information gathering, evaluation, and strategic choices. Through the application of machine learning methodologies, we attain the capacity to process and interpret data effectively,

Table 1 Comparison of data mining methodologies

Steps Involved	Fayyad	Cios	SEMMA	CRISP-DM
Determining objective	■	■		■
Collection of data	■	■	■	■
Cleaning of data	■	■	■	■
Reducing data	■		■	■
Problem Reformulation	■			
Exploration of the data	■		■	
Tools selection	■		■	
Model Construction	■	■	■	■
Model Validation	■	■	■	■
Interpreting result	■	■	■	■
Deployment	■	■		■

Note. ■ denotes that the step is part of the corresponding methodology.

thereby allowing the smart grid to operate as designed. Machine learning (ML) refers to the process of equipping systems with the ability to derive patterns from data and generate forecasts based on these learned patterns [9]. This involves a variety of algorithms that process data through specific instructions to deliver predictions and decisions that are data-driven [10]. The process of building and refining these algorithms to achieve the desired performance is outlined in Table 1.

Machine learning implementations in intelligent grid operations address numerous essential functions, including demand forecasting, tariff optimization, energy production estimation, ideal resource allocation, fault identification, adaptive regulation, capacity assessment, and security breach detection – each representing vital dimensions in contemporary electrical infrastructure [11]. For example, Xu et al. [12] constructed a framework employing extreme learning machines (ELMs) to assess transient stability conditions, demonstrating exceptional precision and computational efficiency when implemented on the New England 39-bus network. ELMs distinguish themselves through rapid training phases and proficiency in processing intricate datasets.

In related research, Wang et al. [13] proposed a core vector machine (CVM) methodology tailored for analysis of extensive datasets acquired from phasor measurement units (PMUs), with validation similarly conducted on the New England bus system configuration. The CVM approach specializes in managing voluminous data collections while delivering reliable categorization and predictive modeling capacities.

Within transmission infrastructure, machine learning techniques can interpret information derived from PMUs and micro-PMUs (μPMUs) for purposes such as network visualization and oscillation monitoring. Computational resources like the power plant model validation toolkit (PPMV) and the free flight risk evaluation system (FRAT) frequently synergize with these machine learning applications to enhance overall functionality. These tools enhance the ability to monitor and control power systems effectively, leveraging the power of machine learning to process and analyze vast amounts of data. As machine learning is integrated into various stages of renewable energy-based smart grids, it presents significant research opportunities. For instance, support vector machines (SVM) are extensively used to address numerous renewable energy challenges, offering solutions for optimization and prediction within smart grids.

Li et al. [14] utilized machine learning methodologies to analyze customer preferences and utilization trends. Concurrently, Remani et al. [15] applied reinforcement learning algorithms to enhance residential load management, taking into account renewable energy integration and diverse pricing models. Robust big data analytics play a critical role in identifying and addressing islanding phenomena prior to grid stabilization. Jurado et al. introduced a composite demand-side management framework incorporating entropy-based feature extraction, machine learning techniques, and soft computing approaches. P. Siano et al. investigated multiple computational methods – including extreme learning machines, support vector regression, advanced radial basis function neural networks with second-order decay, and error correction training techniques – to enhance the precision of electrical load predictions.

Machine learning is also being applied in various security-related functions in smart grids, as illustrated in Figure 6. Both unsupervised and supervised methods can handle diverse tasks such as threat detection and data categorization [16]. However, one of the most impactful and promising areas for ML in the future energy landscape is the renewable energy sector. Therefore, subsequent sections delve into the integration of ML in SGs, particularly in the context of renewable energy.

However Deka et al. addresses significant vulnerabilities in machine learning (ML) applications within power systems, particularly emphasizing the susceptibility of these systems to adversarial attacks. In critical tasks such as load forecasting, outage detection, and disturbance classification, ML models are highly reliant on input data, making them prone to manipulation by adversarial examples, where slight, targeted perturbations in data lead

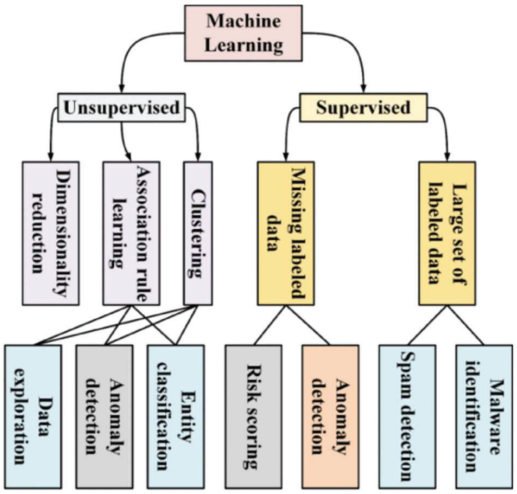

Figure 6 Machine learning applications in smart grids.

to erroneous outputs [17]. For instance, adversarial modifications to input data in a neural network-based classifier for power quality disturbances led to a 70% misclassification rate, potentially allowing harmful disturbances to go undetected and jeopardizing grid stability. Similarly, an RNN-based load forecasting model experienced severe drops in accuracy – up to 55% error increases – due to minor input alterations in occupancy and temperature data, which could mislead operators in demand management and destabilize the grid. These attacks reveal a critical security gap in ML applications for power systems, where adversaries do not require direct access to ML models; they only need to perturb inputs subtly to impact model performance drastically. Such vulnerabilities highlight the urgent need for resilient ML models tailored to power systems that can withstand adversarial manipulations, as these disruptions could lead to significant operational and security risks in increasingly automated and data-dependent power infrastructures [18].

1.4 Integrating ML for Anomaly Detection and Pattern Recognition in Smart Grids: A Review

The integration of machine learning (ML) and deep learning (DL) into Industry 4.0 has proven transformative, particularly in the smart grid domain. Kotsiopoulos et al. [19] explore the deployment of ML and DL as core enablers within smart grids, which generate vast data volumes from connected and automated systems. This literature review provides a detailed

analysis of how ML and DL algorithms have been adapted to meet the smart grid's complex demands. For instance, Bayesian networks, SVM, ANN, and ensemble methods are widely applied for tasks such as demand forecasting, load profiling, anomaly detection, and fault identification [20]. Deep learning models, especially convolutional neural networks (CNNs), autoencoders, and RNNs, provide robust tools for handling high-dimensional data, performing predictive maintenance, and bolstering cybersecurity via anomaly detection mechanisms.

The review identifies several essential challenges that arise in implementing ML/DL in the smart grid. Scalability is a significant issue, as the data influx grows exponentially, demanding architectures that can scale effectively. Model selection is also critical; different algorithms perform variably depending on data type and task requirements, making it crucial to tailor models specifically for applications within smart grids [18]. Cybersecurity risks represent another major concern, as cyberattacks on smart grids could disrupt operations and compromise user data [21]. Thus, the paper emphasizes the need for robust, secure architectures capable of both protecting data flows and accommodating the unique conditions of smart grid environments. This review by Kotsiopoulos et al. underscores the necessity of ongoing advancements in ML and DL to support the evolving requirements of Industry 4.0 and the reliable operation of smart grids.

Subsequently Cui et al. (2018) propose a machine learning-based anomaly detection (MLAD) methodology to enhance load forecasting accuracy under potential cyberattacks. The authors enlighten the essential role of load forecasting for both economic and operational stability in power systems, which, despite its criticality, faces growing exposure to cyber threats that can mislead grid operators and compromise grid security [22]. The proposed MLAD approach operates through a multi-step process beginning with load forecasts generated by neural networks. These forecasts are then processed via k-means clustering, reconstructing the data to serve as a baseline against which deviations, indicative of cyber intrusions, can be detected. A naive Bayes classifier is employed to classify cyberattack templates, including pulse, scaling, and ramping attacks, while dynamic programming determines precise attack timing and parameters [23].

The MLAD method presents a robust alternative to traditional detection techniques such as Symbolic Aggregation Approximation (SAX), which has limitations in identifying complete attack patterns. Through simulations, MLAD demonstrated higher detection accuracy and resilience, effectively identifying cyber intrusions in various attack scenarios and outperforming

SAX in both sensitivity and specificity. This research emphasizes the growing need for resilient, data-driven detection methods within the power grid's cybersecurity landscape, as well-crafted cyber defenses are essential to maintaining both stability and reliable operation in the face of increasingly sophisticated cyber threats.

Whereas Akhtar et al. (2023) covers the transformative role of deep learning in addressing challenges within electric power systems, particularly in managing the increased complexity brought about by renewable energy integration, rising electricity demand, and the need for grid stability [24]. The authors provide an in-depth review of how deep learning models, such as CNNs, RNNs, and deep reinforcement learning, are applied across various domains within power systems, including load forecasting, fault detection, security assessment, and renewable energy management. The study highlights how these models enhance predictive accuracy and operational reliability by processing high-dimensional data from sources like smart meters and SCADA.

Their finding also identifies critical challenges that constrain deep learning's effectiveness in power systems. Issues such as data quality and availability, computational complexity, and the need for interpretability are discussed as significant obstacles to implementation. The authors also emphasize that, despite its potential, deep learning requires scalable computational platforms, standardization, and interdisciplinary collaboration to meet the power grid's operational and reliability demands. This study underscores the need for advanced algorithm development, robust hardware support, and adaptive models that can ensure deep learning's successful integration into the evolving landscape of power systems [25].

2 Methodology

For the detection of abnormality in the power system, since the system is data driven consisting of images and data coming from various instruments, a suitable model should be a deep learning model to detect various anomalies in the energy grid.

2.1 Anomaly Detection Using Deep Learning Model

Deep learning (DL) has become incredibly popular recently because it stands out at understanding raw data and uncovering hidden patterns through multiple layers of abstraction. It's been applied in many fields, Encompassing

NLP, image categorization, object identification, and behavior recognition. Real-time anomaly detection, which pinpoints potential issues and assists in recovery from failures quickly, also benefits greatly from DL [26]. Subsequently, conventional machine learning methods struggle with data at large scale as well as sequential data and usually can't differentiate between the events if it's normal or abnormal, but in a deep learning model, it can easily distinguish between the normal data and abnormal one [27].

Mathematically, deep learning models for abnormality detection depend upon the following equation:

$$\begin{cases} \text{H0: I x} = \delta \\ \text{H1: other} \end{cases} \tag{1}$$

We can define H_0 and H_1 as hypotheses representing normality and abnormality, respectively. The indicator function I, learned by a neural network, processes image data x and compares it against a threshold δ. whereas such technique can also be called as binary classification problem [28].

Deep learning frameworks for identifying anomalies can be categorized into three main types based on data labeling availability: supervised, semi-supervised, and unsupervised approaches. Supervised learning represents the traditional method for detecting anomalies, utilizing datasets where both typical and atypical instances are clearly labeled to train the model effectively. However, this method necessitates a substantial amount of labeled data, which can be time-consuming to gather, especially since anomalies are rare and harder to capture. Despite its superior performance, supervised learning faces challenges due to the scarcity of labeled data and class imbalance [29].

Conversely, semi-supervised learning operates with limited labeled data, whereas unsupervised learning identifies underlying patterns in completely unlabeled datasets, effectively tackling issues related to limited training examples and uneven class distribution. This has driven substantial investigation into semi-supervised and unsupervised techniques. Figure 7 offers a comprehensive overview of these three methodologies [30].

Unsupervised learning is crucial for detecting abnormalities because of the unavailability of labeled data. It helps to identify the natural boundary between normal and abnormal data. The basic architecture used in the unsupervised deep learning model is Autoencoders (AEs). For instance, a relational autoencoder (AE) efficiently extracts features from Models that handle high-dimensional data and achieve low error rates with well-known datasets have been developed. Abati et al. created a technique using deep

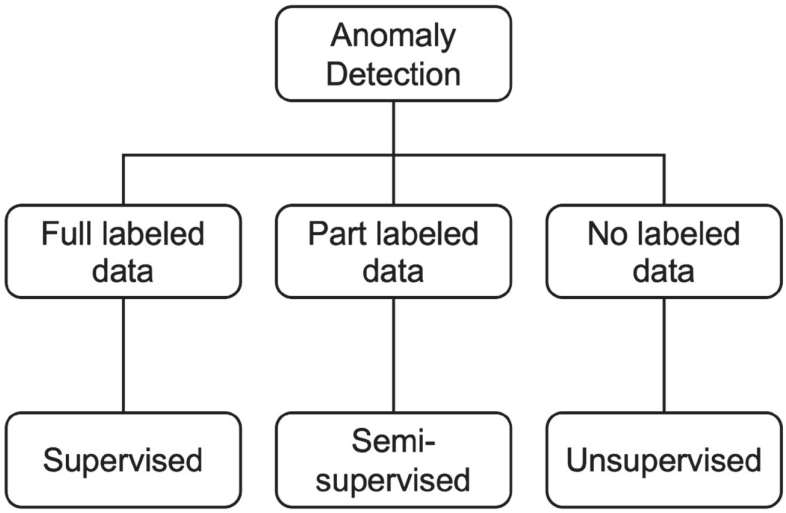

Figure 7 Anomaly detection system for power grids using deep learning models.

autoencoders (AEs) and a parametric density estimator to model the probability distribution. Their research, applied to images, videos, and cognitive data, showed that the method can be adapted to different contexts. Another approach used a hybrid technique where a deep AE reduces dimensions and passes the extracted features to a Gaussian mixture model (GMM). The parameters for the AE and GMM are shared and optimized together, addressing the issue of inconsistent optimization in decoupled models, which is a significant departure from the cascade architecture [31].

On the other hand, Recurrent Neural Networks (RNNs) are frequently employed in an unsupervised manner to handle time-series data. For instance, a recurrent neural network (RNN) was utilized for early cyber attack detection, surpassing dynamic principal component analysis (PCA) in performance. Singh proposed a method leveraging long short-term memory (LSTM) networks for anomaly detection, highlighting the balance between prediction accuracy and anomaly detection capability. It was noted that settings optimal for prediction may not be best for anomaly detection. This methodology was evaluated across three authentic datasets, demonstrating its effectiveness for time series analysis and anomaly identification. Lawson et al. presented a GAN-based approach for detecting abnormalities in patrol robots. Within each surveillance context, a distinct GAN architecture is developed to recognize typical patterns without supervision. For real-time implementation, a compact moving window technique is utilized.

Table 2 various techniques used for anomaly detection using deep learning model

Methodology	References	Features
Convolutional neural network	Supervised Semi-supervised	Capacity for dealing with large data
RNN Long short-term memory	Supervised Semi-supervised Unsupervised	Processing time series data
AutoEncoder	Semi-supervised Unsupervised	Simple, capable of learning from unlabeled data
GANs	Semi-supervised: Unsupervised	Generate realistic data to enhance the classifier's performance

The technique was assessed using a mobile robot that generates circular visual data, resulting in minimal false alarms.

Furthermore, Table 2 provides a summary of the techniques used in related studies. Different methods have shown effectiveness in various detection scenarios. However, our aim was to select a specific DL model that fits specifically for power grids to detect various abnormalities that arise often in the system.

3 Discussion

As illustrated in the table, both traditional machine learning (ML) and deep learning (DL) approaches are data-dependent and incorporate both deterministic and stochastic optimization methods. but, DL models with specialized features, such as denoising modules, tend to be more resilient to noisy data compared to conventional ML models [30]. While DL can benefit significantly from large datasets, its performance declines sharply under scarce-data conditions. This limitation could be partially mitigated through techniques like data augmentation or multimodal data integration (e.g., combining time-series and image data). Nevertheless, these strategies introduce additional complexity and computational costs, and their effectiveness depends heavily on the quality and compatibility of the fused data sources [32].

Despite these advancements, our approach shares the broader limitation of data dependency in AI-driven anomaly detection. Current methodologies, including ours, struggle to achieve ultra-reliable performance when limited to single-modality data (e.g., time-series or images alone). Multimodal data fusion offers a promising direction but remains challenging due to unresolved issues such as feature alignment, interpretability, and scalability [33]. Future

work should focus on optimizing data-efficient learning paradigms and robust multimodal integration to address these gaps.

4 Conclusion

In essence, the integration of deep learning model into smart grid systems offers significant improvements in anomaly detection and pattern recognition, enhancing the overall efficiency and security of power grids. The study highlights the effectiveness of DL algorithms in processing large datasets, identifying anomalies, and predicting patterns, which are imperative for supporting the stability and reliability of smart grids. The research underscores the importance of continuous advancements in DL techniques to address emerging challenges in smart grid management. However, future work should focus on developing more sophisticated ML models that can handle the increasing complexity and volume of smart grid data. Additionally, exploring the integration of advanced cybersecurity measures within ML frameworks will be essential to protect smart grid systems from potential cyber threats. Further research is also needed to enhance the scalability and adaptability of ML technique to ensure their effective implementation in diverse smart grid environments.

Funding

Research and Application of Distribution Network Pattern Recognition and Intelligent Planning Technology (GZKJXM20220093) from Guizhou Power Grid Co., Ltd.

References

[1] Camarinha-Matos, L. M. (2016). “Collaborative smart grids – A survey on trends”. Renew. Sustain. Energy Rev., vol. 65, pp. 283–294.
[2] Hossain, E. et al. (2014). “A comprehensive study on microgrid technology”. Int. J. Renew. Energy Res., vol. 4, pp. 1094–1107.
[3] Yu, W. et al. (2014). “Bridging the gap between complex networks and smart grids”. J. Control Decision, vol. 1, no. 1, pp. 102–114.
[4] Gubbi, J. et al. (2013). “Internet of Things (IoT): A vision, architectural elements, and future directions”. Future Generat. Comput. Syst., vol. 29, no. 7, pp. 1645–1660.

[5] Cecati, C. et al. (2015). "A novel RBF training algorithm for short-term electric load forecasting and comparative studies". IEEE Trans. Ind. Electron., vol. 62, no. 10, pp. 6519–6529.
[6] Jurado, S. et al. (2015). "Hybrid methodologies for electricity load forecasting: Entropy-based feature selection with machine learning and soft computing techniques". Energy, vol. 86, pp. 276–291.
[7] Tannahill, B. K. et al. (2014). "System of systems and big data analytics – Bridging the gap". Comput. Elect. Eng., vol. 40, no. 1, pp. 2–15.
[8] Zhang, N. et al. (2014). "A distributed data storage and processing framework for next-generation residential distribution systems". Electr. Power Syst. Res., vol. 116, pp. 174–181.
[9] Chang, X. et al. (2025). "Advanced Machine Learning Solutions for Power Load Forecasting and Power Grid Planning Optimization". Distributed Generation & Alternative Energy Journal, vol. 40, no. 2, pp. 259–278.
[10] Paul, A. et al. (2016). "SmartBuddy: Defining human behaviors using big data analytics in social Internet of Things". IEEE Wireless Commun., vol. 23, no. 5, pp. 68–74.
[11] Kotsiopoulos, A. et al. (2021). "A review of machine learning and deep learning applications in smart grids". Applied Sciences, vol. 12, no. 11, pp. 5336.
[12] Xu, Y. et al. (2011). "Real-time transient stability assessment model using extreme learning machine". IET Gener. Transmiss. Distrib., vol. 5, pp. 314–322.
[13] Wang, B. et al. (2016). "Power system transient stability assessment based on big data and the core vector machine". IEEE Trans. Smart Grid, vol. 7, no. 5, pp. 2561–2570.
[14] Li, B. et al. (2011). "Predicting user comfort level using machine learning for smart grid environments". Proc. IEEE PES Innov. Smart Grid Technol. (ISGT), pp. 1–6.
[15] Remani, T. et al. (2018). "Residential Load Scheduling With Renewable Generation in the Smart Grid: A Reinforcement Learning Approach". IEEE Systems Journal. pp. 1–12. 10.1109/JSYST.2018.2855689.
[16] Frincu, M. et al. (2014). "Accurate and efficient selection of the best consumption prediction method in smart grids". Proc. IEEE Int. Conf. Big Data (Big Data), pp. 721–729.

[17] Esmalifalak, M. et al. (2017). "Detecting stealthy false data injection using machine learning in smart grid". IEEE Syst. J., vol. 11, no. 3, pp. 1644–1652.
[18] Chen, J.-L. et al. (2011). "Estimation of monthly solar radiation from measured temperatures using support vector machines – A case study". Renew. Energy, vol. 36, no. 1, pp. 413–420.
[19] Kusiak, A. et al. (2011). "Adaptive control of a wind turbine with data mining and swarm intelligence". IEEE Trans. Sustain. Energy, vol. 2, no. 1, pp. 28–36.
[20] Liu, W. Y. et al. (2015). "The structure healthy condition monitoring and fault diagnosis methods in wind turbines: A review". Renew. Sustain. Energy Rev., vol. 44, pp. 466–472.
[21] B. Dickson, Exploiting Machine Learning in Cybersecurity, Mar. 2016, [online] Available: https://techcrunch.com/2016/07/01/exploiting-machine-learning-in-cybersecurity/.
[22] Mellit, A. et al. (2009). "Artificial intelligence techniques for sizing photovoltaic systems: A review". Renew. Sustain. Energy Rev., vol. 13, no. 2, pp. 406–419.
[23] Negnevitsky, M. et al. (2009). "Machine learning applications for load price and wind power prediction in power systems". Proc. 15th Int. Conf. Intell. Syst. Appl. Power Syst. (ISAP), pp. 1–6.
[24] Chia, Y. Y. et al. (2015). "A load predictive energy management system for supercapacitor-battery hybrid energy storage system in solar application using the support vector machine". Appl. Energy, vol. 137, pp. 588–602.
[25] Zhou, F. et al. (2022). "A Comprehensive Survey for Deep-Learning-Based Abnormality Detection in Smart Grids with Multimodal Image Data". Applied Sciences, vol. 12, no. 11, pp. 5336.
[26] Huang, D. et al. (2025). "AI Prediction of Power Grid Faults Based on Deep Learning and Improvement of Emergency Response Efficiency in Automated Repair". Distributed Generation &Alternative Energy Journal, 40(01), 63–84.
[27] Liberati, F. et al. (2017). "Economic model predictive and feedback control of a smart grid prosumer node". Energies, vol. 11, no. 1, pp. 48.
[28] Ucar, F. et al. (2018). "Power quality event detection using a fast extreme learning machine". Energies, vol. 11, no. 1, pp. 145.
[29] Morales-Velazquez, L. et al. (2017). "Smart sensor network for power quality monitoring in electrical installations". Measurement, vol. 103, pp. 133–142.

[30] Alshareef, S. et al. (2014). "A new approach based on wavelet design and machine learning for islanding detection of distributed generation". IEEE Trans. Smart Grid, vol. 5, no. 4, pp. 1575–1583.
[31] Jiang, H. et al. (2017). "Big data-based approach to detect locate and enhance the stability of an unplanned microgrid islanding". J. Energy Eng., vol. 143, no. 5, pp. 04017045.
[32] Guo, C. et al. (2024). "Research on Optimization of Distribution Network Connection Mode Based on Graph Neural Network and Genetic Algorithm". Distributed Generation & Alternative Energy Journal, vol. 39, no. 6, pp. 1179–1208.
[33] Chen, Yize et al. (2018). "Is Machine Learning in Power Systems Vulnerable?". arXiv preprint arXiv:1808.08197.

Biographies

Chang Xu (1988.12–), female, graduated from the School of Urban Science and Technology, Chongqing University with a bachelor's degree. After graduation, I worked as an economist at the Power Grid Planning and Research Center of Guizhou Power Grid Co., Ltd. My current research direction is engaged in primary planning work for distribution networks.

Pengcheng Zhang (May 1996), male, graduated from Tongji University with a master's degree in Electronic and Information Engineering. After graduation, I worked as an engineer at the Power Grid Planning and Research Center of Guizhou Power Grid Co., Ltd. My current research direction is engaged in primary planning work for distribution networks.

Ning Luo (1986.02–), female, graduated from Guizhou University with a master's degree in Electrical Engineering. After graduation, I worked as a senior engineer at the Power Grid Planning and Research Center of the Power Grid Co., Ltd. My current research direction is engaged in primary planning work for distribution networks.

Fei Zheng (1995.12–), male, graduated from Guizhou University with a Bachelor's degree in Electrical Engineering. After graduation, I worked as a senior engineer at the Power Grid Planning and Research Center of Power Grid Co., Ltd. My current research direction is engaged in primary planning work for distribution networks.

Wenzhong He (1981.08–), male, graduated from Sichuan Agricultural University with a Bachelor's degree in Computer Science and Technology. After graduation, I worked as a senior engineer at Guizhou Qianchi Information Co., Ltd. My current research direction is working in information technology.