Heliyon 10 (2024) e35683

Contents lists available at ScienceDirect

Heliyon

journal homepage: www.cell.com/heliyon

Review article

Big data analytics and artificial intelligence aspects for privacy and security concerns for demand response modelling in smart grid: A futuristic approach

S. Sofana Reka [a], Tomislav Dragicevic [b], Prakash Venugopal [c], V. Ravi [c], Manoj Kumar Rajagopal [c,*]

[a] Centre for Smart Grid Technologies, School of Electronics Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India
[b] Centre of Electric Power and Energy, Technical University of Denmark, Denmark
[c] School of Electronics Engineering, Vellore Institute of Technology, Chennai, Tamilnadu, India

ARTICLE INFO

Keywords:
Machine learning
Artificial intelligence
Smart grid
Security threats
Demand response modelling.1.Introduction

ABSTRACT

Next generation electrical grid considered as Smart Grid has completely embarked a journey in the present electricity era. This creates a dominant need of machine learning approaches for security aspects at the larger scale for the electrical grid. The need of connectivity and complete communication in the system uses a large amount of data where the involvement of machine learning models with proper frameworks are required. This massive amount of data can be handled by various process of machine learning models by selecting appropriate set of consumers to respond in accordance with demand response modelling, learning the different attributes of the consumers, dynamic pricing schemes, various load forecasting and also data acquisition process with more cost effectiveness. In connected to this process, considering complex smart grid security and privacy based methods becomes a major aspect and there can be potential cyber threats for the consumers and also utility data. The security concerns related to machine learning model exhibits a key factor based on different machine learning algorithms used and needed for the energy application at a future perspective. This work exhibits as a detailed analysis with machine learning models which are considered as cyber physical system model with smart grid. This work also gives a clear understanding towards the potential advantages, limitations of the algorithms in a security aspect and outlines future direction in this very important area and fast-growing approach.

1. Introduction

The completely new framework of electric grid [1–3] globally brings in great efficiency and new features to the consumers and the utility through two-way communication. Modernizing the electric grid [1–5] with more communication features, creates various security aspects at a larger scale. Smart grid creates optimal solution for generation and transmission pattern [4] in storing energy data. In the growing aspect of smart grid [5] dynamic needs of distributed energy resources are very much needed. Thereby smart grid creates constant connectivity and bidirectional communication with the required devices with great capabilities. The connected

* Corresponding author.
E-mail address: manojkumar.r@vit.ac.in (M.K. Rajagopal).

https://doi.org/10.1016/j.heliyon.2024.e35683
Received 26 April 2024; Received in revised form 15 July 2024; Accepted 1 August 2024
Available online 5 August 2024

devices are interlinked in a bigger complex network which are employed with smart devices like smart meters [5,6] which creates communication between the utility and the consumers. These devices create a dataset of the energy consumption to the utility which demonstrates as one of the best communicated frameworks. Numerous research works has been established in the recent years which exhibits the importance of the intelligent devices and storage of large amount of data which are connected to the databases [5–7]. This massive amount of data which are generated from the Internet of things (IoT), wireless devices are automated at a great level to analyses the data. The shift towards the data and security aspects of data should be analyzed at the larger level inorder to understand the privacy parameters in smart grid demand response modelling systems [7,8]. Machine learning approaches are identified as the important tool for the challenges which put forth by the new generation electricity grid. Artificial intelligence [8–11] at a larger level analyses the decision making and also schedules the control which are monitored towards various devices. There is a rising increase in machine learning model solutions starting from load forecasting, scheduling, demand response modelling [12,13] and also security aspects in smart grid. Optimization are required at a larger aspect from generation side to distribution side and for efficient model prediction based on electricity energy consumption. There are numerous analyses for the quality of data collected including demand response modelling for consumer's needs. These involves the dynamic need of security purposes for a cyber-physical system models [12,13]. Adequate level of protection system is needed for the proper enhancement of the grid with the data analysis. Machine learning model creates an appealing remedy for processing of data and utilizing efficient security solutions.

There are various works in literature which gives detailed study on smart grid. Initial works exhibits on the demand response modelling in smart grid with the usage of effective machine learning models are done for the process of load forecasting models. Load scheduling analysis were done based on long term and less impact of these approaches with communication technologies. AI based analysis with these demand response modelling in smart grid [1–8] creates an important development for a cyber physical aspect with security which brings in required modelling for self-organized algorithms. As the entire analysis are based on the two important terms big data and Internet of things hand in hand which projects as an automated analysis. This modelling with machine learning aspects creates a learning process which forms a core subarea of artificial intelligence. This creates an interdisciplinary domain drawing ideas to identify patterns in the data and the used patterns which are used to predict loads in a decision-making environment [14,15]. This work gives a clear picture of the evolution of the power system towards the smart grid with IoT data analysis growth that are followed. Of course, managing the massive volume of data in this connected system, properly analyzing it, and ensuring its safety, as well as safeguarding this new power grid from attacks [16,17] produced in both the physical and digital realms founds to be an important task. This work can serve as a foundation for upcoming academic and industrial researchers by highlighting current constraints and outlining potential remedies along with their efficacy. In last few decades, security is evolved as one of the major concern as the conventional power grids are advanced into smart grids. Due to complex network infrastructure and handling large volume of data, smart grid encounters many security challenges. Fig. 4 shows an overall idea of security threats involved for integrated smart grid system such as data management threats, network threats and physical threads [1].

Data management threats includes data breaches, unauthorized access and integrity of data [2]. Smart grid generally collects vital information of the customer which includes their personal details, energy consumption pattern and operational data. A data breach may lead to disclosing of important information about the smart grid and customers which can be understand by the attackers and used to harm the smart grid system. Unauthorized access to smart grid system allow attackers to modify readings, alter operational data, block communications and even it may cause temporary or permanent service disruptions. Guaranteeing data integrity is highly pivotal in smart grid since tampered data may produce improper energy/load distribution, incorrect analysis of the grid's status which further affect the safe and reliable operation of the smart grid system. Various network threads involved in smart grid are Network Communication Protocol Vulnerabilities, Denial of Service (DoS) attacks, malware attacks. Vulnerabilities in network communication protocol enable the unauthorized access to smart grid [20] system to manipulate its data. Especially, wireless communication protocol used in smart meters can be easily accessed by attackers if proper security protocol is not implemented on it. DoS attack on smart grid is aimed to degrade its performance or making it completely inaccessible causing service disruptions or outages. By installing malicious software on the smart grid system, the malware can easily penetrate into grid's control system and disturb the grid operations significantly [3]. Some of the security concerns involved in physical threats are Infrastructure Sabotage, Theft and Vandalism, Component Tampering and Legacy Systems [4]. By making Infrastructure Sabotage i.e physical attack on the smart grid infrastructures such as substations, transformers, and power lines, the attackers can make major impact on the overall grid's functionality. Data breaches and service interruptions may result from physical theft or vandalism of grid components, such as smart metre and control systems. Vulnerabilities may be introduced into the grid by component tampering via suppliers' compromised hardware or software components. This includes the potential for viruses or backdoors to be installed on equipment that has been acquired. Since many smart grid systems are using obsolete technologies without latest security features, they are easily prone to cyberattacks today because these system upgrades can be expensive and complicated.

The rest of the work is organized as follows. Section 2 exhibits the smart grid as cyber physical system model considering various important features of demand response modelling. Section 3 gives the glimpse of two aspects it exhibits the overall analysis of machine learning perspective in smart grid and later shows the in-depth machine learning approaches to demand response modelling for consumer and utility perspective. Section 4 exhibits security aspects in smart grid which portrays an overall impact of the challenges involved in building machine learning models in these modernize grid globally. Section 5 excerpt from this comprehensive study includes recommendations for future research topics with conclusion.

2. Demand response modelling in smart grid – a cyber physical system perspective

Smart grid creates a holistic infrastructure of integrating IoT [18] devices with the ability to communication to many devices and

control center more effectively. Fig. 1 gives a general smart grid infrastructure where the communication interface between the consumers and the control center carrying large amount of data places founds to be a crucial role. In this analysis of smart grid, demand response modelling is an important model involved by the electrical resources [1–7] for the energy reduction by the consumption made by the users in the peak hours. At a cyber physical perspective demand response modelling results in reduction of several parameters including operation and installation costs and also reduces larger amount which involves various potential failures. Fig. 2 represents the various demand response modelling in smart grid. The utility-based companies in this aspect encourages demand response modelling for the consumers [19] by offering lesser prices during the required non peak hours depending whether the users are in residential, commercial and industrial sectors.

The dynamic pricing involved for demand response modelling involves an important analysis in all the end use consumers like industrial, commercial and the domestic needs. The users tend to change their scheduling pattern based on the consumption of electricity usage from various periods in a day and based on the information as a dual aspect from the aggregator.

Demand response in smart grid [20] is on a major concern and a broader vision on electrical power systems. As the important section in smart grid demand response modelling [21] portrays an important aspect of cyber-physical modelling in smart grid with computing analysis. There are price-based demand response programmes which are based on electricity prices where there are changes in period and users can make productive scheduling for proper patterns which can be based on the time of use, real time pricing scheme and also the critical peaks. In connection to the incentive-based demand response schemes where the consumers reduce the electricity prices which are based on the incentives from the utility providers. As electricity markets exhibits a director relationship with demand response. There are different stakeholders involving with the electricity markets and related to the demand response modelling. The electricity market stakeholders can hold from the grid operators, suppliers including the retailers, the end users and the suppliers involved for the service with aggregators [22]. There are various challenges involved in a smart grid starting from the load forecasting in the peak time, demand response-based balancing which involves both peak and non-peak period. Demand response products globally can participate in the different electricity markets in their zone and artificial intelligence tools are very much important for this purpose. In smart grid, each of the different demand response strategies require different machine learning based solutions for the successful attributes towards in demand response solutions. Demand response management for interruptible load usage creates an importance towards the response of the users with reliability of the models. The important analysis in the other features of the smart grid concern different monitoring networks which can be accomplished by the models. The usage of the models involving real time monitoring, early warning considering transmission side. Other important components also involves the in case of conductor galloping as such as monitoring tower collapse and also there can be checks for possible discharge in the conductor.

3. Role of machine learning applications in smart grid

Artificial intelligence (AI) paves an important role with its multidisciplinary feature at larger aspects in the energy domain with the smart grid. The intelligent agents involved in AI provides an environment in smart grid which analyses larger amount of data with data driven paradigm. AI approaches involved can be considered both for single and multi-agent requirements in smart grid portfolio. As we

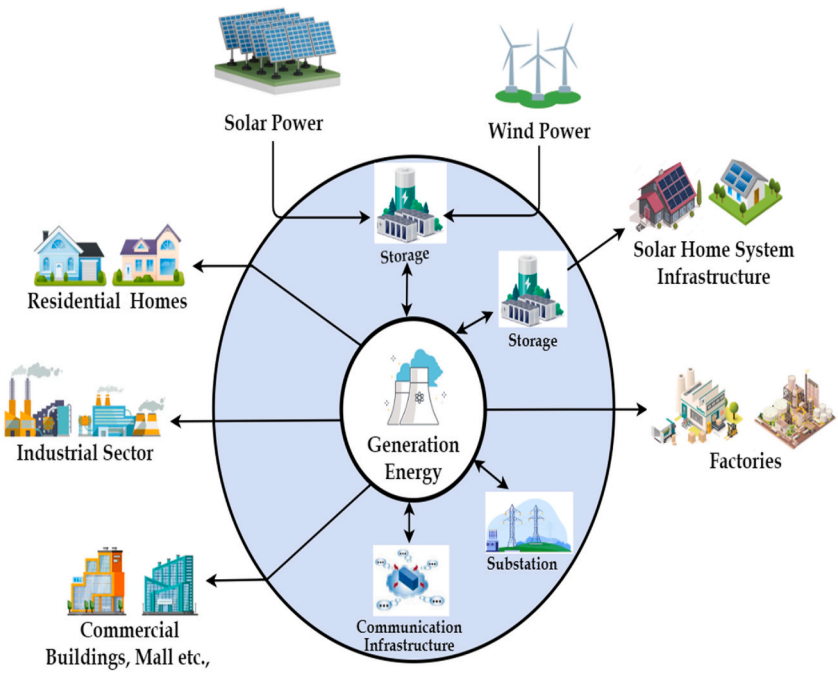

Fig. 1. Smart grid infrastructure.

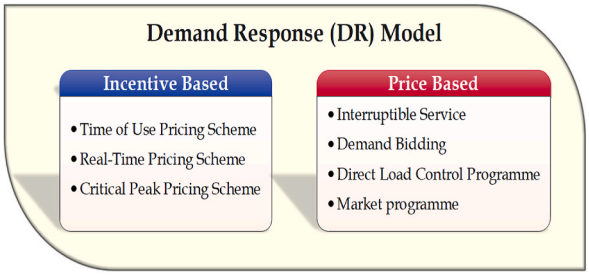

Fig. 2. Various Categories involved in Demand Response modelling for Smart Grid analysis.

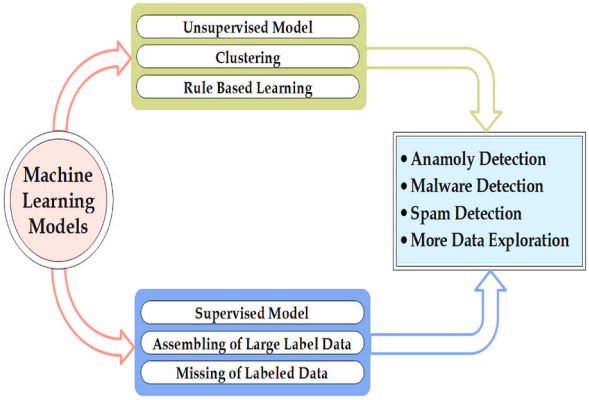

Fig. 3. Machine Learning Models involved in Demand response for Smart Grid objectives.

are in the era of wireless devices and huge data there is greater need for AI approaches and machine learning models at the subset of AI. This larger approach of AI is involved to identify patterns in automatic fashion and thereby using this automated data to predict, analyze and also understand the decision making process in a very uncertain environments also. Machine learning models in general brings in concepts from various domains of statistics, computing, mathematics and engineering aspects. In terms of models there are different models which includes supervised, unsupervised and the reinforcement learning process. The need of these models is mainly focused in demand response modelling in smart grid in literature. Considering in demand response model, supervised learning techniques are involved to focus on the forecasting strategy in demand and electricity prices. Fig. 3 represents various machine learning aspects in smart grid. By transforming the inputs into a comparatively higher dimension of features, it unravels the relationships between demand, pricing and other attributes. Their main application is involved in non-aggregated load modelling where they provide a good understanding of DR dynamics. These can be analyzed by models of kernel based, tree based and also the linear regression models. In kernel-based methods the input data are considered in feature space and they are involved by different process for non-aggregated load modelling. In work [23] the attributes are considered based on the flexibility of data with power prices models. In work [24] the kernel based model are done based on the aggregated power received from the time and the type of price involved considering daily peak load estimation process. There is slight drawback where the resulting performance can be very computationally intensive for large datasets due to the input parameter. As in this work the DR space is the kernel structure which gives the load balancing of the data. There are few works in literature [21,22] which illustrates the prediction of electric vehicle charging based on demand response day ahead estimation. Table 1 and 2 depicts the importance of machine learning models in smart grid.

Demand response [1–10] modelling are also considered in tree based methods where extensive works has been done on the price forecasting [23] and load forecasting process. In work [25,26] the DR models are analyzed based on tree based methods where the usage of multiple regression trees [24] are involved to predict the consumption of power from different parameters and also use classification and regression trees for the process of load forecasting [25]. Regression trees [26] are used when the process of handling missing data which promotes the process of overfitting and founds to be unstable in DR process. Thereby regression trees are involved to provide prediction tasks at complex level and also prediction in hourly basis [22–25], but over usage and training of regression trees and classification models can leads to overfitting of the models and newer data and nodes will be affected in prediction with respect to the training set of the models. The Linear Regression Models, as mentioned in Ref. [21], are useful in scenarios like predicting electric vehicle charging patterns where the inputs and outputs are linear. They are very efficient and interoperable but they are not useful with non-linear data. To deal with this, the Tree-based methods, as discussed in Ref. [24], come into play, which are very viable in situations that require aggregation of power data for predicting daily power loads. They can understand complex decision rules, find hidden patterns, can handle non-linear data but there is always a problem of overfitting causing inaccurate predictions [22]. which is based on predicting EV charging patterns with the context of DR. For effective load management, a fusion of strengths of the above prediction

Table 1
Analysis of Machine Learning Modelling in Demand response with security analysis and big data perspective.

Research Objective	DSM method/Technique	Results/outcome	Ref.
Analysis of different data driven methodologies of AI in Demand Response (DR) applications	various machine learning, ANN, multi agent systems	specific AI methods required for DR applications	[1]
Detailed comparison study on various techniques used in DSM optimization problem is performed	Genetic Algorithm, The particle swarm optimization (PSO), ant colony optimization (ACO), game theory algorithm (GTA), linear programming (LP), non-LP (NLP), and dynamic programming	There are many drawbacks in the single algorithm approach hence it is recommended to use hybrid algorithms-based optimization models	[4]
To ensure secure and efficient energy utilization in IoT-enabled smart grid environments by addressing potential security threats	Resilient Agent Model to detect and control intrusions, Advanced Energy Management Agent (AEMA) for optimizing energy utilization, interface Control Agent (ICA) component manages the communication interfaces	The simulation results validated under various scenario showcasing reduced vulnerability to intrusions and optimal energy utilization	[6]
To enhance the theoretical framework for quantifying network flexibility potential in smart grids.	k-means clustering to identify energy consumption patterns, CNN architectures to assess their effectiveness in classifying the substations	The proposed CNN model with multiple convolutional layers (CNN2) showed mean accuracy exceeding 88.8 % across different clusters and scenarios.	[7]
To evaluate the performance of control algorithms for implementing DR strategies in residential area.	Rule-Based Algorithm to minimize energy expenditure, Machine learning for predictive modelling and an optimization algorithm.	Predictive controls for residential buildings reduced heating system costs by up to 40 % and resulted in a lower carbon footprint by up to 39 %.	[8]
A dynamic pricing DR algorithm proposed for energy management in smart grids	The dynamic pricing problem was formulated as a discrete finite Markov decision process (MDP) and Q-learning, a type of reinforcement learning (RL), was adopted to solve the decision-making problem.	The proposed DR algorithm effective in managing the energy supply-demand balance in the electricity market and enhancing the reliability of electric power systems.	[9]
To develop a privacy-centric DR model to address the need for efficient energy management while ensuring user privacy in the smart grid system.	demand response model developed which combines machine learning with cloud–fog computing. To address privacy concerns, a Generative Adversarial Network (GAN) combined with Q-learning model is proposed.	The model demonstrated effective scheduling of appliances, leading to efficient energy management in residential settings and addressed the privacy concerns.	[12]
Development of a comprehensive consumer behavior learning model for real-time DR in smart grids to enhance the accuracy and effectiveness of appliance-level power forecasting	An ensemble approach employs a hybrid Convolutional Neural Network-Long Short-Term Memory (CNN-LSTM) and eXtreme Gradient Boosting (XG-Boost) model to capture the stochastic nature of appliance power usage at fine-grained intervals, dynamic itemset counting (DIC) algorithm utilized to identifies patterns in appliance usage	The ensemble model outperformed reference models in terms of RMSE and MAE, demonstrating superior predictive accuracy for appliance-level power usage.	[13]

Table 2
Comparison analysis ML approaches with smart grid security.

Type of security threats	Traditional Security Measures	Machine Learning Approaches	Comparison Analysis	Ref.
Data breaches	• Firewalls and Intrusion Detection Systems (IDS) • Encryption • Access Control	Anomaly Detection Behavioral Analysis Predictive Analytics	Adaptability: ML models adapt to new and evolving threats more effectively than static rules in traditional systems. Real-time Detection: ML provides more effective real-time detection compared to signature-based IDS, which may miss zero-day attacks. Complexity Handling: ML can handle and analyze large volumes of complex data more efficiently than traditional methods.	[95–100]
Unauthorized Access	Password Protection and Multi-Factor Authentication (MFA) Access Control Lists Role-Based Access Control (RBAC)	User Behavior Analytics (UBA) Adaptive Authentication Risk-Based Access Control	Dynamic Security: ML provides adaptive and dynamic security measures that traditional static controls cannot match. Insider Threat Detection: ML is more effective at detecting insider threats by analyzing subtle behavioral changes that traditional methods may overlook. Automation: ML automates the detection and response to unauthorized access, reducing reliance on manual intervention.	[102], [103], [104], [105]
Integrity of Data	Checksums and Hashing Digital Signatures	Real-time Data Validation False Data Injection Detection	F0B7 **Proactive Detection**: ML can detect integrity issues proactively, often before they cause significant harm. F0B7 **Scalability**: ML scales more effectively with the growing amount of data in smart grids, providing continuous and real-time validation.	[110–115]

techniques could be the most beneficial in capturing all the interactions between EV charging, electricity demand and pricing dynamics.

Ensemble learning also are considered at larger aspects presently [27] for load forecasting. In Ref. [28] temporal ensemble learning process are involved for forecasting data based on the demand on a specific time period. Ensemble learning is a process of developing a model based on the weak learning nodes. In work [29,30] gradient models are involved for the forecasting accuracy comparing with the based models for a short term. The concept of Temporal Ensemble Learning, featured in Ref. [27], introduces a paradigm where models are created from interconnected weak learning nodes. They give accurate data forecasting within specific time-frames improving robustness. In contrast, their efficacy for short-term predictions is spotlighted in Refs. [29,30] which outperform their traditional counterparts in terms of accuracy. Other than the load forecasting, supervised learning is involved for other requirements in demand response. In approach of unsupervised learning models [30], the attempts to analyses pattern in the data are found to be not a well-structured problem. In this process the data to be analyzed are not well know prior, this creates the approach with error matric. In this process environment which requires unlabeled data can be considered. This aspect can be very well suited for demand response modelling in smart grid. As in DR model unlabeled data is an advantage where unsupervised [30] learning can be used such as clustering, as the data can be done by the format of latent factors, graph structure and also the completion of matrix [28]. However, unsupervised learning models [30], which, while attempting to decipher patterns in data, grapple with the challenge of structuring uncharted data patterns. This approach leads to error matrices and uncertainties, primarily due to the unpredictable nature of the analyzed data. Nonetheless, its utilization is apt for scenarios necessitating the analysis of unlabeled data, thus offering a fitting approach for demand response modelling within the intricate landscape of the smart grid. Main analysis where the usage of unsupervised algorithms can be used in demand response modelling in smart grid should be on clustering methods. In clustering methods in this context, the load profiles with scheduling can form groups such that the clusters are made dissimilar with the profiles. Grouping can be made to positively identify the households for scheduling patterns based on the demand response events and the incentive-based programmes can be given to the consumers for their participation. The main area of focus comes under the clustering of load profiles coupled with scheduling information to identify each household. Many clustering algorithms are in practice [29] considering the K means algorithm [31,32] can be used where the prediction of K cluster are based on the data point in each cluster [32]. This data point in the k cluster is based on the centroid distance and the k-based centroid has to be the smallest considering all other centroids in this algorithm. So, K means clustering methods can be used mainly to group in residential environment based on the requirement based on the load data considered in a period of several weeks. This features are mainly done based on self-organizing map [33] in this case the load shapes are made based on the 24 h monitoring in a day profile and also based on the peak with average consumption of load.

In work [34] this has been analyzed based on the dataset which helps to group the entire process based on the cluster households. In this process real time pricing schemes are considered and it requires to exhibit the load profile clustering process based on the dynamic pricing schemes. However, some critical concerns [61] with K-means algorithm are (1) defining number of clusters in advance, which is not practical when a smart grid is a dynamic entity; (2) doesn't provide a global optimum solution but focuses on local optimum, which is not ideal in most scenarios. Other involvement in unsupervised learning for demand response modelling in smart grid are the challenges involved in the user profile segmentation considering different load patterns. This helps gives a great advantage for the aggregators for the flexibility of the asset involved and for the interaction between consumers and the utility. Considering the process of reinforcement learning [31] where learning is done based on the interaction. This learning process are based on the agent approach where it completely focusses on goal-oriented learning process which are considered in an uncertain environment. The main aspect of reinforcement learning is based on the exploration done with the reward process from the agent at a delayed aspect and also considering the process of trial-and-error strategy. The concept of this learning process is based on the Markov decision process [35] which data considered to be sequential and the information receives based on the reward from the agent.

In this regard for the approach of demand response modelling in smart grid using reinforcement learning [36] can be analyzed based on scheduling patterns and taking in control of various account from the interaction with the users which are completely data driven. In work [37,38] the approach of demand response pricing analysis can be made for the utility and also analysis of elasticity model can be created at a larger extent by dynamically adjusting price schemes in response to grid conditions and consumer behavior, fostering effective energy management and incentivizing DR participation. In perspective of DR, the most important of reinforcement learning used are the Q learning [39,40] process. This process is found to be independent of policy and helps to create an optimal action plan and the learning is profited by discounted reward by the execution of the action and the agent sets the policy with a learning factor. The agent learns through a cycle of action execution, reward feedback, and policy adjustment. There are methods used for DR purposes for the purpose of multi agent mechanisms in the literature [41] where the workload distribution for data privacy is efficiently managed through collaborative agents. This learning methods are mainly used in the purpose of distributing the workload parameter for the data privacy considered for the users. Multi agent approaches are used. For the process of handling complex and better computational algorithms for DR approaches are made which results them in better DR scenario in smart grid environment. Previous approaches to reinforcement learning lacked scalability due to complexity issues of the algorithms. However, using deep learning in reinforcement learning has enabled RL algorithms to scale to decision-making problems, introducing the field of Deep Reinforcement Learning (DRL) [47]. The work [48] proposes an approach for demand response modelling using reinforcement learning methods by exploring Q-learning with eligibility traces and importance-weighting.

Let us look at an example about Reinforcement Learning for DR in a Smart Grid. In the context of a smart grid, let us consider a residential area where multiple households are connected to the grid. The utility company aims to optimize energy consumption [49] during peak hours by implementing a demand response strategy. The goal is to encourage residents to reduce their electricity consumption during high-demand periods, thereby ensuring grid stability and minimizing the need for additional power generation.

Starting with the environment setup, each household's state comprises its current energy consumption, time of day, weather conditions, and historical consumption pat-terns. The available actions include reducing energy usage, maintaining the current consumption, or increasing energy usage. The utility provides rewards based on the energy reduction achieved by each household during peak hours. Higher rewards are given for substantial reductions. The utility deploys a reinforcement learning agent to each household. The agent's goal is to learn an optimal policy that maximizes the cumulative rewards over time. The policy guides the agent's actions in response to different states. Initially, the agents explore different actions to learn the rewards associated with each action in various states. Over time, the agents shift towards exploiting the learned knowledge to make decisions that lead to higher rewards. The Q-learning algorithm is employed by each agent to determine the best actions in different states. The Q-values represent the expected cumulative rewards from taking a specific action in a particular state. The agents update these Q-values based on the rewards received and the potential rewards of future actions. Through iterative episodes of interactions with the environment, the agents refine their policies. They gradually learn to reduce energy consumption during peak hours to maximize rewards while considering factors like weather conditions and time of day. During peak hours, the agents dynamically adjust household appliances, such as thermostats, water heaters, and lighting systems, based on the optimal policy learned through reinforcement learning. The actions could involve setting thermostats to lower temperatures, turning off non-essential lights, and delaying energy-intensive tasks like laundry or dishwashing. Over time, as agents continue to interact with the environment and receive feedback, they fine-tune their actions. The utility monitors the grid's stability and the collective reduction in energy consumption achieved during peak hours. If successful, this demand response strategy helps prevent overloading the grid and potentially reduces the need for additional power generation, resulting in cost savings and environmental benefits. Considering another branch of machine learning methods which involves the learning process of different levels of representation and considering the raw data, which are the deep learning models [42] which are discovered for the best representation models.

Deep learning models are well versed in considering for more hidden layers of complexity. There are different architectures considering the feed forward neural network [43], convolutional neural [43] autoencoders [43] and also nowadays the architecture of deep reinforcement learning process [44] are also involved. The analysis made for deep learning models in demand response modelling can be done in different attributes of the user's behavior, controlling of events, consumers analysis can be made on a personalized approach for the utility services at every multilevel hidden layers. There are different models like long term short term memory architecture [45], convolutional neural network [45] which are involved for processing data with feed forward architecture. Deep learning models have the capacity for learning nonlinear data analysis, complex based correlations in such the prediction accuracy model are made in the process. These models, characterized by multiple layers of representation, excel in extracting intricate patterns from raw data. Deep learning architectures involves huge data which have computational analysis to train and found to be more complex based systems. In general, for smart grid and the requirement in residential buildings there is a great requirement of implementing prediction model. Considering this work [46] a deep recurrent neural network is considered in residential buildings which frameworks demand-supply for a small duration of time. In this process there forms a five layered model which considers the first layer moved on to the daily consumption pattern. The subsequent second layer involves the output at a particular instance of time. The state of art of deep learning approaches are made can be involved for many aspects in demand response for modelling starting from electric load forecasting to the prediction model, state estimation factor, involvement of energy sharing followed by energy theft detection. Machine learning models are highly data driven and the models work on complex algorithms, which are also vulnerabilities that can be exploited either via incorporating calculated falsified data or altering the behavior of the model [53,54]. There are multiple security concerns for machine learning models in recent times, some of which are: Poisoning of data [50,51], which is injected into training data to manipulate and control the models. This displays the vulnerabilities in all types of models and affect the accuracy and working. Feature collision attacks [50] are further built on poisoned data sets to misclassify a specific target. As detailed in work [57], defense strategies against data poisoning such as reject on negative impact to remove malicious samples and method using bagging ensemble construction have been proposed over the last decade to improve the validity of the model affected.

Backdoor attacks, dynamic [52] and/or static, which is typically exploited by inputting a certain trigger, and that attacks a particular behavior of the model, thus altering the output [50]. Defense methods for backdoor attacks proposed such as spectral signatures [62], NEO, which is an agnostic model framework to identify and mitigate backdoor [63]. Adversarial attacks [55], are smaller and imperceptible attacks that feed calculated erroneous inputs to the model, which fools the model into making incorrect classifications and/or predictions. This affects the learning of the model and is difficult to resolve as the inputs can camouflage as anomalies within the dataset. A most common occurrence of adversarial attacks is in image processing and identification models [56]. Evasion attacks, work similar to data poisoning but these attacks are carried out on test data. The main goal is to alter the model via the test data, so that classifier makes a wrong classification for the input given. In work [57], strategies to work for the protection of the model against evasion attacks such as distillation [58] and adversarial training and ensemble adversarial training [59] and Multi-strength adversarial training (MAT) [60] to mitigate evasion attacks have been detailed towards their effectiveness and usage concerns to fight evasion attacks.

Comparison with Traditional Methods: It would be beneficial to include a comparison of ML approaches [90–94] with traditional security measures used in smart grids. This comparison could highlight the advancements ML provides over conventional methods.The efficacy of these advanced methodologies underscores their pivotal role in reshaping demand response modelling in the smart grid era. As technology evolves, their implementation opens doors to dynamic energy management, accurate load forecasting, and the efficient utilization of resources within the intricate fabric of the modern energy landscape. Integrating various modelling approaches is a multidimensional approach for exact demand response in the context of smart grid architecture. A complete toolkit for efficient decision-making in dynamic energy domains is created by the combination of tree-based methods, ensemble learning, and supervised procedures. Unsupervised learning discovers latent patterns in data using clustering techniques like K-means and self-organizing maps,

boosting understanding of energy usage. Energy use is optimized through demand response reinforcement learning, demonstrating AI's transformational impact in changing energy management techniques.

4. Security aspects and big data analytics in smart grid – cyber physical system approach

Security concerns with the application of machine learning models creates a path of overall structure of cyber-physical system modelling. Fig. 4 shows an overall idea of security threats involved for integrated smart grid system. Handling large amount of data based on machine learning model, proper depiction of cyber-attacks to the smart grid should be carried out with much concern. The system targeted can be affected with large amount of data leakage which disrupts the entire model considering the interaction between the users and the utility. At the aspect the available information in a smart grid system starting from the name of the user, account details, meter requirement, billing history and also the home network [105–110]. Considering the component of billing and debt collection, there can be loss to the customers and expose of personal information. At the consumer level the security and privacy involved with the communication infrastructure creates a possibility of attacks. Home gateway at this situation creates a communication structure for deployment of smart grid infrastructure. The configuration is controlled by the suppliers. Network attack also can be more important concern for home energy management. Every component involves the cryptography key measures the different involvement of protocols starting for key exchange and generation. There should be different protection levels made at every aspect of the protocol concerned.

In general, for suitable security concerned with smart proper communication infrastructure in smart grid is an important aspect which involves the characteristics of communication in smart homes or offices considering home area network [106] and involves smart meter readings for effective local energy management [115]. In this aspect relatively lower transmission rate, furthermore neighborhood area networks and wide area networks [108] are involved in accordance with the communication deployed in the aspect within certain kilometers which requires transmission up to some Gbps [114,115]. With respect to increased researchers on big data analytics in smart grid there are found to be lot of open issues. The data usage in most of information and database structures are still with respect to the ideal data founds to be increasing the barrier for data sharing among different applications. Moreover, the complete lack of vision in this analysis, where the majority of the utility companies are still looking for investments on from the data side of the utility. The analysis of big data prospects in smart grid.

Because of their great efficacy, accuracy, and precision, machine learning (ML) techniques have been widely applied in a variety of SG applications, including power system control and monitoring, abnormal diagnosis, and attack detection [5]. In order to mitigates various security challenges of the smart grid system as discussed above, various ML methods can be used. For data management related threats, system is required to continuously analyze the data pattern and user behavior to identify any unusual access patterns or user behavior and indicating potential breaches [6]. A machine learning algorithm which support anomaly detection and user behavior analysis can be used for detecting data management related threats. Similarly, for network threats, ML model can be used to analyze network traffic in real-time to detect anomalies, suspicious patterns, and potential attacks, enhancing overall network security. To predict potential physical security threats, a ML model can be used by analysing data from sensors and other monitoring devices, enabling proactive measures. Therefore, by employing an appropriate machine learning algorithm related to anomaly detection and

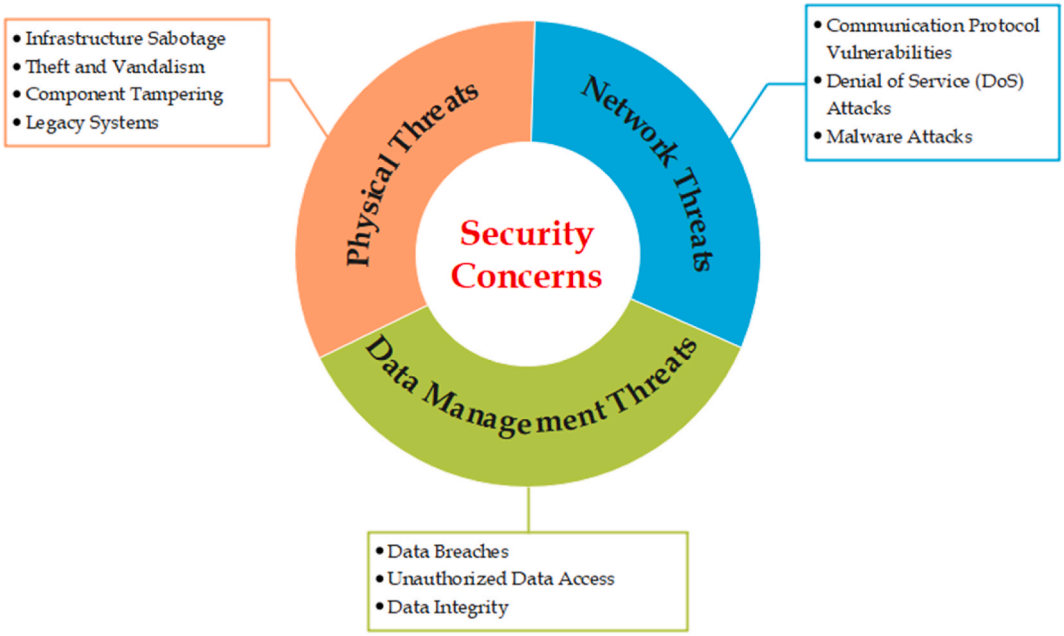

Fig. 4. Security aspects for integrated smart grid system for effective cyber physical system model.

behavioral analysis major of the security concerns in smart grid system can be addressed.

Cyber security strategies can be done at two levels of protection and also the detection. The protection aspects involve different strategy both at the hardware and also at the administrative aspects. The detection processes can be done effectively by many machine learning models. The models are applicable for exhibiting a suitable solution for the protection and detection. Cyber vulnerabilities [75–81] in a high form at the prospect of handling huge data and the preserving the data forms to be a preliminary task for machine learning models. On a general aspect, security aspect to be considered for the smart meter where the end point of handling data between the consumer and the utility. The framework had to be made with the concept of assessing different types of risks and top security measures had to be concerned for the same. As for this approach layered security framework can be done for securing the smart grid. Involvement with layered security structure creates the data and the security requirements to be made where each layer can be considered starting from strategy, requirements, application security, privacy consideration, tamper management which involves at the physical layer aspect.With the rise of machine learning and AI's presence in almost every domain across the world, many recent developments have been seen and proposed with respect to the incorporation of machine learning into the future of smart grids. In current scenarios, the huge influx of data in large expansive smart grids are not handled well. Issues with the volume, velocity and complexity of the data obtained is not being handled smoothly, thus self-sustaining and operating smart grids will be the next step to move forward towards. The work [64] has proposed a novel belief propagation-based algorithm to identify False Data Injection Attacks (FDIAs) in smart grids to enhance the security and reliability of the smart grids. Defense mechanisms against white-box and black-box attacks like these are highly required as machine learning models are very vulnerable to data-based attacks and behavioral attacks. Further areas of scope in academic interest include power flow optimization [65], energy management [66], integration of microgrid [67,68], cybersecurity with focus on the machine learning models, demand response optimization [69] and more.

Sanju Kumari et al. [70], explores demand response management within smart grids through big data analytics. The study specifically evaluates the utility of the Prophet model, a forecasting tool, against the traditional ARIMA model for predicting electricity demand. The approach involves a process of filtering and processing vast datasets to remove outside values and noise, thereby extracting relevant data for analysis. The processed data is then modeled using the Prophet model to generate forecasts that are instrumental in demand response management. The methodology addresses time-series forecasting challenges, such as data with irregular intervals, missing data points, and complex seasonality patterns without the need for manual parameter tuning. The comparative analysis of the ARIMA and Prophet models for forecasting electricity consumption yielded quantifiable results. The research forecast 2016's energy consumption based on data from 2014 to 2015 which consists of 10,00,000 records. The mean square error (MSE) for the Prophet model was significantly lower at 0.67546 compared to the ARIMA model's 1.06877. Similarly, the mean absolute error (MAE) for the Prophet model was 0.5308, less than the ARIMA model's 0.6239, indicating a closer match to the actual data points. The thesis by James Timilehin Oyedokun [71] focuses on enhancing demand response (DR) in smart grids using big data analytics techniques on smart meter data.It addresses the challenges of identifying customers with DR potential and estimating customer demand baselines for more efficient DR programs. The author prepares the data by normalizing the smart meter data from customers. This method introduces a clustering technique based on k-medoids, combined with dynamic time warping (DTW) as the distance metric, to organize the analyzed smart meter data [82–89]. This methodology is based on long short-term memory (LSTM) recurrent neural networks for estimating customer baselines, utilizing data from similar previous days during demand response (DR) event periods for training the model. A novel aspect of this methodology is its consideration of the demand rebound effect, which refers to the increase in energy consumption following a DR event as customers return to their usual consumption patterns. This method is tested on the publicly available Irish smart meter data. This work contributes to the smart grid field by offering data-driven strategies to improve DR program targeting and effectiveness, leveraging the increasing availability of smart meter data.

The study conducted by Ioannis Antonopoulos et al. [72], aims to analyze residential demand response (DR) behavior using data from the Smart Grid Smart City (SGSC) trial. The methodology is the identification of important features that influence demand response behavior. This involves analyzing the data to understand which household characteristics significantly affect energy usage patterns during demand response events. The research employs a variety of machine learning models, including linear models, gradient boosting regression, random forest regression, and dense neural networks, to predict the impact of household characteristics on demand response behavior. The study trains the selected models on the SGSC dataset, followed by a validation process. The result gives minimum RMSE values range from 18.711 ± 0.714 for Gradient Boosting regression to maximum of 19.721 ± 1.611 for Random Forest regression. The MAE ranges from 15.246 ± 0.631 for Gradient Boosting regression to 16.107 ± 1.389 for Random Forest regression, showing similar performance levels across models. The R^2 values range from -0.108 ± 0.240 for Random Forest regression to 0.015 ± 0.018 for Gradient Boosting regression, indicating varying degrees of model fit to the data. This ensures the models' accuracy and their ability to predict demand response behavior effectively. Broeer et al. [73] proposes a smart grid modelling framework that integrates wind power, emphasizing demand response's role in managing wind's variability. The paper employs an agent-based modelling approach using the GridLAB-D simulation platform, enabling the detailed representation of smart grid components.

The model includes a detailed representation of generators, transmission and distribution systems, loads (both thermostatic and non-thermostatic), and market dynamics. A key aspect of the modelling is the simulation of a real-time pricing (RTP) electricity market, where suppliers and demanders can bid into the market. The model is extended to include wind power generation, assessing the impact of its variability on the smart grid and exploring the mitigating role of demand response. The model's validation against the Olympic Peninsula demonstration project provides empirical support for its effectiveness in capturing the dynamics of a smart grid system.The study demonstrates that DR can effectively reduce peak loads and manage distribution congestion by allowing loads to interact within a market clearing process. The simulation results reveal that introducing 35 MW of wind power into a system with 10,000 residential houses can significantly impact the electricity market dynamics, highlighting the necessity for diverse load participation to maintain system reliability and efficiency. This work reveals that the high wind power scenarios led to lower market

prices, prompting loads to become unresponsive when prices fell below a certain threshold and vice versa. These dynamics were captured through detailed simulations, providing insights into the potential for smart grids [105] to enhance the integration of renewable energy sources.

In this work [100] the main focus on exhibit two way-based communication which shows the process of implementing real time portable based load forecasting device which shows better degree of accuracy and the process develops the basic understanding machine learning models. Furthermore, this exhibits execution analysis based on better performance with this analysis. Considering the work [101] which shows two main issues where the work involves offloading based on IoT cloud infrastructure [116–120] with data transmission [121–123]. The other section of the work involves the process of enhancing the noise and faulty models using deep learning architecture. This shows the need of the proposed model using edge-based computing platforms. In work [103] the main objective aims on creating a hardware testbed which is done in accordance with the enhancement of MQTT which uses edge computing perspective.

Simmhan Y et al. [74],developed advanced data analytics and scalable machine learning models to address the complexities and dynamic requirements of smart grid systems. The research introduces a sophisticated information integration pipeline to streamline the collection, processing, and analysis of diverse smart grid data. It employs scalable machine learning models to predict demand, optimize grid performance, and enhance decision-making processes. The real-world smart grid data from the Los Angeles Smart Grid Project, encompassing various data points related to energy consumption, generation, and distribution are used for testing purposes. The proposed platform significantly improves the capability to forecast energy demand with high accuracy, employing scalable machine learning models. From the findings it is evident that cloud-based platforms can effectively support the complex analytics required for modern smart grids, paving the way for more sustainable and efficient energy systems. Fog Computing (FC) [75] is integrated into Smart Grids (SG) to enhance Big Data Analytics capabilities. The authors propose PPFG mathematical framework aiming at optimizing the location, capacity, and number of Fog Computing Nodes (FCNs) to minimize average response delay and energy consumption in network elements.

5. Conclusion

This work projects the growing interest of AI solutions in smart grid at a larger perspective. The study gives an understanding about machine learning model visibility at smart grid perspective with security concerns as a holistic cyber physical model. This work enables more understanding towards the most important section of demand response modelling in smart grid with machine learning aspects. This work details on the different security attacks that cause concern in usage of machine learning models and details on the supporting and weakening points regarding their use. This study shows the growing interest of research community of machine learning in demand response which identifies suitable solutions. This work gives a path for AI/ML modelling to establish as a mainstream as aspect looking forward as model for energy-based demand response modelling in smart grid. At the future perspective security aspects in smart grid at the different aspects of modelling in deep learning aspects in end point and network security. The research analysis can also be done on the basis of advanced smart metering process with 5G and 6G aspects at the communication layer. Many advancements in related to cryptography, differential privacy is involved with the practical concerns of false data injection, data theft and also insider cyber-attacks with the integration of cloud fog can be analyzed with future directons. environment.

Data availability statement

No data was used for the research described in this work.

Funding

This work was supported and funded by Vellore Institute of Technology, Chennai. We acknowledge VIT chennai for the great support.

CRediT authorship contribution statement

S. Sofana Reka: Writing – review & editing, Writing – original draft, Validation, Software, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Tomislav Dragicevic:** Formal analysis, Data curation. **Prakash Venugopal:** Writing – original draft, Software, Project administration, Methodology, Investigation. **V. Ravi:** Validation, Supervision. **Manoj Kumar Rajagopal:** Funding acquisition, Conceptualization.

Declaration of competing interest

The authors have no conflict of interest.

References

[1] M.L. Tuballa, M.L. Abundo, A review of the development of Smart Grid technologies, Renew. Sustain. Energy Rev. 59 (2016) 710–725.

[2] R. Zafar, A. Mahmood, S. Razzaq, W. Ali, U. Naeem, K. Shehzad, Prosumer based energy management and sharing in smart grid, Renew. Sustain. Energy Rev. 82 (2018) 1675–1684.
[3] E. Espe, V. Potdar, E. Chang, Prosumer communities and relationships in smart grids: a literature review, evolution and future directions, Energies 11 (10) (2018) 2528.
[4] S.K. Kim, J.H. Huh, A study on the improvement of smart grid security performance and blockchain smart grid perspective, Energies 11 (8) (2018) 1973.
[5] J. Abdella, K. Shuaib, Peer to peer distributed energy trading in smart grids: a survey, Energies 11 (6) (2018) 1560.
[6] M.I. Khalil, N.Z. Jhanjhi, M. Humayun, S. Sivanesan, M. Masud, M.S. Hossain, Hybrid smart grid with sustainable energy efficient resources for smart cities, Sustain. Energy Technol. Assessments 46 (2021) 101211.
[7] N.M. Kumar, A.A. Chand, M. Malvoni, K.A. Prasad, K.A. Mamun, F.R. Islam, S.S. Chopra, Distributed energy resources and the application of AI, IoT, and blockchain in smart grids, Energies 13 (21) (2020) 5739.
[8] H. Manoharan, Y. Teekaraman, I. Kirpichnikova, R. Kuppusamy, S. Nikolovski, H.R. Baghaee, Smart grid monitoring by wireless sensors using binary logistic regression, Energies 13 (15) (2020) 3974.
[9] I. Alotaibi, M.A. Abido, M. Khalid, A.V. Savkin, A comprehensive review of recent advances in smart grids: a sustainable future with renewable energy resources, Energies 13 (23) (2020) 6269.
[10] E. Hossain, I. Khan, F. Un-Noor, S.S. Sikander, M.S.H. Sunny, Application of big data and machine learning in smart grid, and associated security concerns: a review, IEEE Access 7 (2019) 13960–13988.
[11] T. Kotsiopoulos, P. Sarigiannidis, D. Ioannidis, D. Tzovaras, Machine learning and deep learning in smart manufacturing: the smart grid paradigm, Computer Science Review 40 (2021) 100341.
[12] A.K. Bashir, S. Khan, B. Prabadevi, N. Deepa, W.S. Alnumay, T.R. Gadekallu, P.K.R. Maddikunta, Comparative analysis of machine learning algorithms for prediction of smart grid stability, International Transactions on Electrical Energy Systems 31 (9) (2021) e12706.
[13] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, Z. Han, Detecting stealthy false data injection using machine learning in smart grid, IEEE Syst. J. 11 (3) (2014) 1644–1652.
[14] T. Ahmad, R. Madonski, D. Zhang, C. Huang, A. Mujeeb, Data-driven probabilistic machine learning in sustainable smart energy/smart energy systems: key developments, challenges, and future research opportunities in the context of smart grid paradigm, Renew. Sustain. Energy Rev. 160 (2022) 112128.
[15] L. Cui, Y. Qu, L. Gao, G. Xie, S. Yu, Detecting false data attacks using machine learning techniques in smart grid: a survey, J. Netw. Comput. Appl. 170 (2020) 102808.
[16] S.S. Reka, T. Dragicevic, Future effectual role of energy delivery: a comprehensive review of Internet of Things and smart grid, Renew. Sustain. Energy Rev. 91 (2018) 90–108.
[17] S.S. Reka, P. Venugopal, H.H. Alhelou, P. Siano, M.E.H. Golshan, Real time demand response modeling for residential consumers in smart grid considering renewable energy with deep learning approach, IEEE Access 9 (2021) 56551–56562.
[18] T. Mazhar, R.N. Asif, M.A. Malik, M.A. Nadeem, I. Haq, M. Iqbal, S. Ashraf, Electric vehicle charging system in the smart grid using different machine learning methods, Sustainability 15 (3) (2023) 2603.
[19] I. Ortega-Fernandez, F. Liberati, A review of denial of service attack and mitigation in the smart grid using reinforcement learning, Energies 16 (2) (2023) 635.
[20] S. Zidi, A. Mihoub, S.M. Qaisar, M. Krichen, Q.A. Al-Haija, Theft detection dataset for benchmarking and machine learning based classification in a smart grid environment, Journal of King Saud University-Computer and Information Sciences 35 (1) (2023) 13–25.
[21] V.K. Mololoth, S. Saguna, C. Åhlund, Blockchain and machine° learning for future smart grids: a review, Energies 16 (1) (2023) 528.
[22] T. Mazhar, H.M. Irfan, I. Haq, I. Ullah, M. Ashraf, T.A. Shloul, D.H. Elkamchouchi, Analysis of challenges and solutions of IoT in smart grids using AI and machine learning techniques: a review, Electronics 12 (1) (2023) 242.
[23] S.Y. Diaba, M. Elmusrati, Proposed algorithm for smart grid DDoS detection based on deep learning, Neural Network. 159 (2023) 175–184.
[24] Y. Li, X. Wei, Y. Li, Z. Dong, M. Shahidehpour, Detection of false data injection attacks in smart grid: a secure federated deep learning approach, IEEE Trans. Smart Grid 13 (6) (2022) 4862–4872.
[25] T. Berghout, M. Benbouzid, S.M. Muyeen, Machine learning for cybersecurity in smart grids: a comprehensive review-based study on methods, solutions, and prospects, International Journal of Critical Infrastructure Protection (2022) 100547.
[26] N. Mostafa, H.S.M. Ramadan, O. Elfarouk, Renewable energy management in smart grids by using big data analytics and machine learning, Machine Learning with Applications 9 (2022) 100363.
[27] W. Tang, H. Wang, X.L. Lee, H.T. Yang, Machine learning approach to uncovering residential energy consumption patterns based on socioeconomic and smart meter data, Energy 240 (2022) 122500.
[28] S.H. Majidi, S. Hadayeghparast, H. Karimipour, FDI attack detection using extra trees algorithm and deep learning algorithm-autoencoder in smart grid, International Journal of Critical Infrastructure Protection 37 (2022) 100508.
[29] G. Fragkos, J. Johnson, E.E. Tsiropoulou, Dynamic role-based access control policy for smart grid applications: an offline deep reinforcement learning approach, IEEE Transactions on Human-Machine Systems 52 (4) (2022) 761–773.
[30] T. Alquthami, M. Zulfiqar, M. Kamran, A.H. Milyani, M.B. Rasheed, A performance comparison of machine learning algorithms for load forecasting in smart grid, IEEE Access 10 (2022) 48419–48433.
[31] S. Tiwari, A. Jain, N.M.O.S. Ahmed, Charu, L.M. Alkwai, A.K.Y. Dafhalla, S.A.S. Hamad, Machine learning-based model for prediction of power consumption in smart grid-smart way towards smart city, Expet Syst. 39 (5) (2022) e12832.
[32] L. Zhang, Y. Gao, H. Zhu, L. Tao, A distributed real-time pricing strategy based on reinforcement learning approach for smart grid, Expert Syst. Appl. 191 (2022) 116285.
[33] A. Alzoubi, Machine learning for intelligent energy consumption in smart homes, Int. J. Comput. Integrated Manuf. 2 (1) (2022).
[34] K.M. Alhamed, C. Iwendi, A.K. Dutta, B. Almutairi, H. Alsaghier, S. Almotairi, Building construction based on video surveillance and deep reinforcement learning using smart grid power system, Comput. Electr. Eng. 103 (2022) 108273.
[35] K. Park, I. Moon, Multi-agent deep reinforcement learning approach for EV charging scheduling in a smart grid, Appl. Energy 328 (2022) 120111.
[36] A. Mosavi, S. Ardabili, A.R. Varkonyi-Koczy, List of deep learning models, in: International Conference on Global Research and Education, Springer International Publishing, Cham, 2019, September, pp. 202–214.
[37] C. Janiesch, P. Zschech, K. Heinrich, Machine learning and deep learning, Electron. Mark. 31 (3) (2021) 685–695.
[38] A. Mathew, P. Amudha, S. Sivakumari, Deep learning techniques: an overview, in: Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2020, 2021, pp. 599–608.
[39] G. Menghani, Efficient deep learning: a survey on making deep learning models smaller, faster, and better, ACM Comput. Surv. 55 (12) (2023) 1–37.
[40] T. Kotsiopoulos, P. Sarigiannidis, D. Ioannidis, D. Tzovaras, Machine learning and deep learning in smart manufacturing: the smart grid paradigm, Computer Science Review 40 (2021) 100341.
[41] M. Massaoudi, H. Abu-Rub, S.S. Refaat, I. Chihi, F.S. Oueslati, Deep learning in smart grid technology: a review of recent advancements and future prospects, IEEE Access 9 (2021) 54558–54578.
[42] F. Pallonetto, M. De Rosa, F. Milano, D.P. Finn, Demand response algorithms for smart-grid ready residential buildings using machine learning models, Appl. Energy 239 (2019) 1265–1282.
[43] C. Xu, Z. Liao, C. Li, X. Zhou, R. Xie, Review on interpretable machine learning in smart grid, Energies 15 (12) (2022) 4427.
[44] D. Zhang, X. Han, C. Deng, Review on the research and practice of deep learning and reinforcement learning in smart grids, CSEE Journal of Power and Energy Systems 4 (3) (2018) 362–370.
[45] D. Zhang, X. Han, C. Deng, Review on the research and practice of deep learning and reinforcement learning in smart grids, CSEE Journal of Power and Energy Systems 4 (3) (2018) 362–370.

[46] Y. Wang, Q. Chen, D. Gan, J. Yang, D.S. Kirschen, C. Kang, Deep learning-based socio-demographic information identification from smart meter data, IEEE Trans. Smart Grid 10 (3) (2018) 2593–2602.
[47] K. Arulkumaran, M.P. Deisenroth, M. Brundage, A.A. Bharath, Deep reinforcement learning: a brief survey, IEEE Signal Process. Mag. 34 (6) (2017) 26–38.
[48] Z. Wen, D. O'Neill, H. Maei, Optimal demand response using device-based reinforcement learning, IEEE Trans. Smart Grid 6 (5) (2015) 2312–2324.
[49] M. Xue, C. Yuan, H. Wu, Y. Zhang, W. Liu, Machine learning security: threats, countermeasures, and evaluations, IEEE Access 8 (2020) 74720–74742.
[50] M. Goldblum, D. Tsipras, C. Xie, X. Chen, A. Schwarzschild, D. Song, T. Goldstein, Dataset security for machine learning: data poisoning, backdoor attacks, and defenses, IEEE Trans. Pattern Anal. Mach. Intell. 45 (2) (2022) 1563–1580.
[51] G. Sun, Y. Cong, J. Dong, Q. Wang, L. Lyu, J. Liu, Data poisoning attacks on federated machine learning, IEEE Internet Things J. 9 (13) (2021) 11365–11375.
[52] A. Salem, R. Wen, M. Backes, S. Ma, Y. Zhang, Dynamic backdoor attacks against machine learning models, in: 2022 IEEE 7th European Symposium on Security and Privacy (EuroS&P), IEEE, 2022, June, pp. 703–718.
[53] Z. Guan, L. Bian, T. Shang, J. Liu, When machine learning meets security issues: a survey, in: 2018 IEEE International Conference on Intelligence and Safety for Robotics (ISR), 2018, pp. 158–165, https://doi.org/10.1109/IISR.2018.8535799. Shenyang, China.
[54] M. Xue, C. Yuan, H. Wu, Y. Zhang, W. Liu, Machine learning security: threats, countermeasures, and evaluations, IEEE Access 8 (2020) 74720–74742, https://doi.org/10.1109/ACCESS.2020.2987435.
[55] O. Ibitoye, R. Abou-Khamis, A. Matrawy, M.O. Shafiq, The Threat of Adversarial Attacks on Machine Learning in Network Security–A Survey, 2019 *arXiv preprint arXiv:1911.02621*.
[56] X. Ma, Y. Niu, L. Gu, Y. Wang, Y. Zhao, J. Bailey, F. Lu, Understanding adversarial attacks on deep learning based medical image analysis systems, Pattern Recogn. 110 (2021) 107332.
[57] W. Jiang, H. Li, S. Liu, X. Luo, R. Lu, Poisoning and evasion attacks against deep learning algorithms in autonomous vehicles, IEEE Trans. Veh. Technol. 69 (4) (2020) 4439–4449.
[58] N. Papernot, P. McDaniel, X. Wu, S. Jha, A. Swami, Distillation as a defense to adversarial perturbations against deep neural networks, in: Proc. IEEE Symp. Secur. Privacy, 2016, pp. 582–597.
[59] F. Tramèr, A. Kurakin, N. Papernot, I. Goodfellow, D. Boneh, P. McDaniel, Ensemble adversarial training: attacks and defenses, in: Int. Conf. Learn. Representations (ICLR), 2018.
[60] C. Song, et al., MAT: a multi-strength adversarial training method to mitigate adversarial attacks, in: Proc. IEEE Comput. Soc. Annu. Symp. VLSI, 2018, pp. 476–481.
[61] A. Al-Wakeel, J. Wu, N. Jenkins, K-means based load estimation of domestic smart meter measurements, Appl. Energy 194 (2017) 333–342.
[62] B. Tran, J. Li, A. Madry, Spectral signatures in backdoor attacks, Adv. Neural Inf. Process. Syst. 31 (2018).
[63] S. Udeshi, S. Peng, G. Woo, L. Loh, L. Rawshan, S. Chattopadhyay, Model agnostic defence against backdoor attacks in machine learning, IEEE Trans. Reliab. 71 (2) (2022) 880–895.
[64] B.R. Amin, S. Taghizadeh, S. Maric, M.J. Hossain, R. Abbas, Smart grid security enhancement by using belief propagation, IEEE Syst. J. 15 (2) (2020) 2046–2057.
[65] H. Abdi, S.D. Beigvand, M. La Scala, A review of optimal power flow studies applied to smart grids and microgrids, Renew. Sustain. Energy Rev. 71 (2017) 742–766.
[66] S.K. Rathor, D. Saxena, Energy management system for smart grid: an overview and key issues, Int. J. Energy Res. 44 (6) (2020) 4067–4109.
[67] K.A. Nigim, W.J. Lee, Micro grid integration opportunities and challenges, in: 2007 IEEE Power Engineering Society General Meeting, IEEE, 2007, June, pp. 1–6.
[68] X. Zhou, T. Guo, Y. Ma, An overview on microgrid technology, in: 2015 IEEE International Conference on Mechatronics and Automation (ICMA), IEEE, 2015, August, pp. 76–81.
[69] D. Neves, A. Pina, C.A. Silva, Comparison of different demand response optimization goals on an isolated microgrid, Sustain. Energy Technol. Assessments 30 (2018) 209–215.
[70] A. Jindal, N. Kumar, M. Singh, A unified framework for big data acquisition, storage, and analytics for demand response management in smart cities, Future Generat. Comput. Syst. 108 (2020) 921–934.
[71] C. Tu, X. He, Z. Shuai, F. Jiang, Big data issues in smart grid–A review, Renew. Sustain. Energy Rev. 79 (2017) 1099–1107.
[72] C. Ibrahim, I. Mougharbel, H.Y. Kanaan, N. Abou Daher, S. Georges, M. Saad, A review on the deployment of demand response programs with multiple aspects coexistence over smart grid platform, Renew. Sustain. Energy Rev. 162 (2022) 112446.
[73] K. Zhou, C. Fu, S. Yang, Big data driven smart energy management: from big data to big insights, Renew. Sustain. Energy Rev. 56 (2016) 215–225.
[74] S. Kumari, N. Kumar, P.S. Rana, A big data approach for demand response management in smart grid using the prophet model, Electronics 11 (14) (2022) 2179.
[75] M.A. Khan, A.M. Saleh, M. Waseem, I.A. Sajjad, Artificial intelligence enabled demand response: prospects and challenges in smart grid environment, IEEE Access 11 (2022) 1477–1505.
[76] I. Antonopoulos, V. Robu, B. Couraud, D. Kirli, S. Norbu, A. Kiprakis, S. Wattam, Artificial intelligence and machine learning approaches to energy demand-side response: a systematic review, Renew. Sustain. Energy Rev. 130 (2020) 109899.
[77] S. Ahmadzadeh, G. Parr, W. Zhao, A review on communication aspects of demand response management for future 5G IoT-based smart grids, IEEE Access 9 (2021) 77555–77571.
[78] E. Sarker, P. Halder, M. Seyedmahmoudian, E. Jamei, B. Horan, S. Mekhilef, A. Stojcevski, Progress on the demand side management in smart grid and optimization approaches, Int. J. Energy Res. 45 (1) (2021) 36–64.
[79] H. Hui, Y. Ding, Q. Shi, F. Li, Y. Song, J. Yan, 5G network-based Internet of Things for demand response in smart grid: a survey on application potential, Appl. Energy 257 (2020) 113972.
[80] M. Babar, M.U. Tariq, M.A. Jan, Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid, Sustain. Cities Soc. 62 (2020) 102370.
[81] R. Krč, M. Kratochvílová, J. Podroužek, T. Apeltauer, V. Stupka, T. Pitner, Machine learning-based node characterization for smart grid demand response flexibility assessment, Sustainability 13 (5) (2021) 2954.
[82] F. Pallonetto, M. De Rosa, F. Milano, D.P. Finn, Demand response algorithms for smart-grid ready residential buildings using machine learning models, Appl. Energy 239 (2019) 1265–1282.
[83] R. Lu, S.H. Hong, X. Zhang, A dynamic pricing demand response algorithm for smart grid: reinforcement learning approach, Appl. Energy 220 (2018) 220–230.
[84] Q.V. Pham, M. Liyanage, N. Deepa, M. Vvss, S. Reddy, P.K.R. Maddikunta, W.J. Hwang, Deep Learning for Intelligent Demand Response and Smart Grids: A Comprehensive Survey, 2021 arXiv preprint arXiv:2101.08013.
[85] M. Babar, M.U. Tariq, M.A. Jan, Secure and resilient demand side management engine using machine learning for IoT-enabled smart grid, Sustain. Cities Soc. 62 (2020) 102370.
[86] S.S. Reka, P. Venugopal, V. Ravi, T. Dragicevic, Privacy-based demand response modeling for residential consumers using machine learning with a cloud–fog-based smart grid environment, Energies 16 (4) (2023) 1655.
[87] S. Sharda, M. Singh, K. Sharma, A complete consumer behaviour learning model for real-time demand response implementation in smart grid, Appl. Intell. 52 (1) (2022) 835–845.
[88] S. Ali, A.U. Rehman, Z. Wadud, I. Khan, S. Murawwat, G. Hafeez, O. Samuel, Demand response program for efficient demand-side management in smart grid considering renewable energy sources, IEEE Access 10 (2022) 53832–53853.
[89] R. Krc, M. Kratochvílová, J. Podroužek, T. Apeltauer, V. Stupka, T. Pitner, Machine learning-based node characterization for smart grid demand response flexibility assessment, Sustainability 13 (2021) 2954, 2021.

[90] W. Ahmed, H. Ansari, B. Khan, Z. Ullah, S.M. Ali, C.A.A. Mehmood, R. Nawaz, Machine learning based energy management model for smart grid and renewable energy districts, IEEE Access 8 (2020) 185059–185078.
[91] M. Elsisi, C.L. Su, M.N. Ali, Design of reliable IoT systems with deep learning to support resilient demand side management in smart grids against adversarial attacks, IEEE Trans. Ind. Appl. (2023).
[92] I. Antonopoulos, V. Robu, B. Couraud, D. Flynn, Data-driven modelling of energy demand response behaviour based on a large-scale residential trial, Energy and AI 4 (2021) 100071.
[93] C. Ibrahim, I. Mougharbel, H.Y. Kanaan, N. Abou Daher, S. Georges, M. Saad, A review on the deployment of demand response programs with multiple aspects coexistence over smart grid platform, Renew. Sustain. Energy Rev. 162 (2022) 112446.
[94] E.J. Salazar, M. Jurado, M.E. Samper, Reinforcement learning-based pricing and incentive strategy for demand response in smart grids, Energies 16 (3) (2023) 1466.
[95] R. Kakkar, A. Kumari, S. Agrawal, S. Tanwar, GTS-CS: a game theoretic strategy for distributed EV charging station using multiple photovoltaic, in: 2023 IEEE International Conference on Power Electronics, Smart Grid, and Renewable Energy (PESGRE), IEEE, 2023, December, pp. 1–6.
[96] O.I. Obaid, S.A.B. Salman, Security and privacy in IoT-based healthcare systems: a review, Mesopotamian Journal of Computer Science 2022 (2022) 29–39.
[97] O.M. Alyasiri, A.H. Ali, Exploring GPT-4's characteristics through the 5Vs of big data: a brief perspective, Babylonian Journal of Artificial Intelligence 2023 (2023) 5–9.
[98] A. Kumari, S. Tanwar, RAKSHAK: resilient and scalable demand response management scheme for smart grid systems, in: 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), IEEE, 2021, January, pp. 309–314.
[99] A. Kumari, R.K. Patel, U.C. Sukharamwala, S. Tanwar, M.S. Raboaca, A. Saad, A. Tolba, AI-empowered attack detection and prevention scheme for smart grid system, Mathematics 10 (16) (2022) 2852.
[100] A. Mukherjee, P. Mukherjee, N. Dey, D. De, B.K. Panigrahi, Lightweight sustainable intelligent load forecasting platform for smart grid applications, Sustainable Computing: Informatics and Systems 25 (2020) 100356.
[101] A. Mukherjee, P. Mukherjee, D. De, N. Dey, iGridEdgeDrone: hybrid mobility aware intelligent load forecasting by edge enabled Internet of Drone Things for smart grid networks, Int. J. Parallel Program. 49 (3) (2021) 285–325.
[102] A. Kumari, S. Tanwar, A data analytics scheme for security-aware demand response management in smart grid system, in: 2020 IEEE 7th Uttar Pradesh Section International Conference on Electrical, Electronics and Computer Engineering (UPCON), IEEE, 2020, November, pp. 1–6.
[103] A. Mukherjee, N. Dey, D. De, EdgeDrone: QoS aware MQTT middleware for mobile edge computing in opportunistic Internet of Drone Things, Comput. Commun. 152 (2020) 93–108.
[104] C.X. Wang, X. You, X. Gao, X. Zhu, Z. Li, C. Zhang, L. Hanzo, On the road to 6G: visions, requirements, key technologies, and testbeds, IEEE Communications Surveys & Tutorials 25 (2) (2023) 905–974.
[105] D.K. Kumar, K.K. Reddy, G.J.W. Kathrine, Smart Grid Protection with AI and Cryptographic Security, in: 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), IEEE, 2024, June, pp. 246–251.
[106] X. Zhang, C. Huang, D. Gu, J. Zhang, J. Xue, H. Wang, Privacy-preserving statistical analysis over multi-dimensional aggregated data in edge computing-based smart grid systems, J. Syst. Architect. 127 (2022) 102508.
[107] C. Feng, Y. Wang, Q. Chen, Y. Ding, G. Strbac, C. Kang, Smart grid encounters edge computing: opportunities and applications, Advances in Applied Energy 1 (2021) 100006.
[108] J.A.S. Aranda, R. dos Santos Costa, V.W. de Vargas, P.R. da Silva Pereira, J.L.V. Barbosa, M.P. Vianna, Context-aware edge computing and Internet of things in smart grids: a systematic mapping study, Comput. Electr. Eng. 99 (2022) 107826.
[109] S. Rani, M. Shabaz, A.K. Dutta, E.A. Ahmed, Enhancing privacy and security in IoT-based smart grid system using encryption-based fog computing, Alex. Eng. J. 102 (2024) 66–74.
[110] A. Shukla, P.K. Sadhu, S. Dutta, S.K. Sahu, B. Dey, An island detection approach in 6G paradigm for an active distribution network–A future perspective for next generation smart grids, Comput. Electr. Eng. 111 (2023) 108932.
[111] M. Adil, H. Song, M.K. Khan, A. Farouk, Z. Jin, 5G/6G-enabled metaverse technologies: taxonomy, applications, and open security challenges with future research directions, J. Netw. Comput. Appl. (2024) 103828.
[112] L.P. Rachakonda, M. Siddula, V. Sathya, A comprehensive study on IoT privacy and security challenges with focus on spectrum sharing in Next-Generation networks (5G/6G/beyond), High-Confidence Computing (2024) 100220.
[113] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future, Elec. Power Syst. Res. 215 (2023) 108975.
[114] M.Z. Gunduz, R. Das, Cyber-security on smart grid: threats and potential solutions, Comput. Network. 169 (2020) 107094.
[115] J. Mendel, Smart grid cyber security challenges: overview and classification, e-mentor 68 (1) (2017) 55–66.
[116] A.O. Otuoze, M.W. Mustafa, R.M. Larik, Smart grids security challenges: classification by sources of threats, Journal of Electrical Systems and Information Technology 5 (3) (2018) 468–483.
[117] M. Ozay, I. Esnaola, F.T.Y. Vural, S.R. Kulkarni, H.V. Poor, Machine learning methods for attack detection in the smart Grid, IEEE Transact. Neural Networks Learn. Syst. 27 (8) (2016) 1773–1786.
[118] S. Tufail, I. Parvez, S. Batool, A. Sarwat, A survey on cybersecurity challenges, detection, and mitigation techniques for the smart grid, Energies 14 (18) (2021) 5894.
[119] M. Ghiasi, T. Niknam, Z. Wang, M. Mehrandezh, M. Dehghani, N. Ghadimi, A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: past, present and future, Elec. Power Syst. Res. 215 (2023) 108975.
[120] T.T. Khoei, H.O. Slimane, N. Kaabouch, A comprehensive survey on the cyber-security of smart grids: cyber-attacks, detection, countermeasure techniques, and future directions, arXiv preprint arXiv:2207.07738 (2022).
[121] M.Z. Gunduz, R. Das, Cyber-security on smart grid: threats and potential solutions, Comput. Network. 169 (2020) 107094.
[122] A.O. Otuoze, M.W. Mustafa, R.M. Larik, Smart grids security challenges: classification by sources of threats, Journal of Electrical Systems and Information Technology 5 (3) (2018) 468–483.
[123] Z. El Mrabet, N. Kaabouch, H. El Ghazi, H. El Ghazi, Cyber-security in smart grid: survey and challenges, Comput. Electr. Eng. 67 (2018) 469–482.