International Journal of Communication Networks and Information Security
2026, 18(1)
ISSN: 2073-607X,2076-0930
https://https://ijcnis.org/ Research Article

AI-Powered Smart Grids: Security Challenges and Intelligent Energy Management Approaches

Abhilasha Singh[1], Navanendra Singh[1], Omkar Singh[1*], Vinoth R[1]

[1] Assistant Professor, National Institute of Fashion Technology, Patna, India

*Corresponding Author: omkar.singh@nift.ac.in

ARTICLE INFO

Received: 06-12-2025
Accepted: 26-12-2025

ABSTRACT

Electric power systems are being transformed into smart grids that can operate with flexibility, efficiency, and resilience thanks to the confluence of enhanced sensing, communication, distributed energy resources, and artificial intelligence. With an emphasis on security issues and clever energy management strategies, this study examines the current status of AI-powered smart grids. We present an architectural overview, pinpoint attack surfaces and threat models, and look at particular security risks such as supply-chain vulnerabilities, data integrity assaults, and privacy violations. Next, we examine AI-driven methods for distributed generation coordination, demand response, energy forecasting, and real-time optimization, and we talk about how these methods relate to privacy and security issues. We then assess defense methods such as blockchain-enabled coordination, privacy-preserving analytics, federated learning, anomaly detection, and secure communication protocols. We offer case examples and a thorough design pattern that strikes a compromise between privacy, robustness, and performance. A research agenda for safe, intelligent, and reliable smart grids, as well as suggestions for practitioners, is included in the paper's conclusion.

Keywords: AI-powered smart grids, Intelligent energy management, Cybersecurity, Demand response, Federated learning

1. INTRODUCTION

Large percentages of renewable energy, customer involvement, and distributed generation are supported by flexible, data-rich infrastructures that are replacing rigid, centrally managed networks in electric power systems [1]. Environmental pressure, growing demand, and the development of digital technologies that enable real-time monitoring and control are all contributing factors to this shift. The outcome is the smart grid, a cyber-physical energy system that combines sophisticated power electronics, fast communication networks, and clever software to control electricity more effectively and consistently than in the past [2].

The core of this change is artificial intelligence. The amount, velocity, and variety of data generated by millions of sensors, smart meters, electric vehicles, and distributed energy resources are too much for traditional rule-based techniques to handle as grids become more dynamic and sophisticated [3]. Utilities and grid operators can estimate demand and renewable output, identify abnormalities, and optimize grid operation by using AI approaches to extract valuable insights from massive databases. These skills are essential for coordinating storage systems, integrating solar and wind power, and enabling responsive loads that aid in supply and demand balancing [4].

However, compared to conventional electricity networks, smart grids are significantly more vulnerable to hazards. The attack surface increases dramatically when digital communication, cloud platforms, and online decision-making tools become essential to physical infrastructure [5]. Stability can be disrupted and safety risks created by a coordinated manipulation of IoT-enabled loads, a series of compromised smart meters, or a well-timed cyberattack on a control center. The same AI methods that enable grid intelligence may also be targeted. An attacker

may, for instance, tamper with model inputs, contaminate training datasets, or obtain private data from consumption profiles. Because of these dangers, security is becoming a basic necessity rather than a luxury [6].

The transition to AI-powered smart grids makes it more crucial to create reliable, transparent, and resilient systems. Models for energy forecasting must be resilient to manipulated data. When anomalies are discovered, automated controllers must revert to safe modes [7]. Channels of communication must guarantee authenticity, integrity, and secrecy. Another big worry is privacy protection, particularly with comprehensive smart meter readings that can show behavioral patterns within homes and companies. Techniques that aggregate and analyze data without disclosing private information are essential for operators [8].

At the same time, AI offers a plethora of potential. Intelligent control techniques can lower peak loads, postpone expensive infrastructure improvements, and balance local supply and demand in microgrids. Both consumers and grid operators can gain from the optimization of storage and electric vehicle charging through the use of reinforcement learning techniques [9]. Utilities can detect equipment breakdowns before they happen with the aid of predictive maintenance. Each of these methods helps to increase the grid's overall resilience, lower operating costs, and improve energy efficiency [10].

The main driving force behind this study is the interplay between these opportunities and the risks involved. A thorough understanding of the entire ecosystem—including the sensors, communication networks, control platforms, AI models, and end-user behavior—is necessary to design an intelligent and secure smart grid [11]. It also necessitates being mindful of enemies who could take advantage of weaknesses in any system component. The advantages of advanced analytics and automation may be compromised if security is not taken into account during the design phase. On the other hand, by fostering trust among customers, authorities, and utilities, a well-thought-out security and privacy plan can facilitate the wider deployment of AI approaches [12].

The architecture of AI-powered smart grids, the security risks that emerge in such interconnected systems, and the intelligent energy management strategies that AI makes possible are all examined in this study [13]. Key attack surfaces are covered, such as adversarial attacks on machine learning models, data manipulation, communication manipulation, and IoT exploitation. Additionally, it examines grid security measures like encryption, intrusion detection systems, strong machine learning approaches, and privacy-preserving analytics. It also examines how AI aids in fault detection, distributed resource coordination, demand response, forecasting, and market decision-making [14].

The connection between energy management and security is another crucial area of focus. Rapid feedback loops in contemporary smart grids rely on fast and reliable data. Even highly developed AI systems will make dangerous or inaccurate conclusions if this material is tainted [15]. Thus, security measures that prevent manipulation of both data and models are necessary for efficient energy management. AI's capacity to identify anomalous patterns and identify assaults early is also advantageous to security solutions. The two dimensions must be developed jointly because they support one another [16].

The integration of AI will only get deeper as energy systems continue to change. There will be more autonomous decision-making and real-time communication amongst devices. Because of this, it is crucial to create systems that are not just clever and effective but also robust against disruptions and considerate of user privacy. This study seeks to contribute to a safer, effective, and intelligent energy future by reviewing technology, identifying problems, and describing possible remedies [17].

1.1 Motivation of the Research

Modern power systems are becoming more complicated, necessitating the use of intelligent technologies that can react swiftly and precisely to sudden shifts in supply and demand. The unpredictability of renewable energy sources poses additional difficulties for preserving grid stability as they continue to grow. The grid is now more vulnerable to a variety of cyberthreats due to the proliferation of smart meters, sensors, and Internet of Things devices. These dangers have demonstrated that conventional security techniques are insufficient to safeguard vital infrastructure [18]. AI has a lot of promise for forecasting, optimization, and automated decision-making, but these models need to be robust, transparent, and safe. As detailed consumer data gets increasingly sensitive, so does the demand for privacy-preserving analytics [16]. The fact that cybersecurity and AI-based energy management are frequently examined independently represents a significant research gap. Building reliable and effective smart grids can be achieved by addressing both issues at the same time. The necessity to combine different viewpoints and create solutions that improve stability without sacrificing security is what drives this study [19].

1.2 Key research contributions

The key contributions of the article are as follows:

- This work presents a structured analysis of AI-driven architectures for smart grids, highlighting how intelligence is embedded across sensing, communication, and control layers.
- It identifies major security vulnerabilities created by AI-enabled components and maps them to specific cyber and physical attack vectors.
- The study proposes a unified framework that links intelligent energy management functions with corresponding security requirements for safe operation.
- It evaluates advanced approaches such as federated learning, anomaly detection, and robust forecasting to show how AI can improve both efficiency and resilience.
- The paper outlines practical design guidelines for building secure, privacy-aware, and scalable AI-powered smart grids suitable for future large-scale deployment.

2. RELATED WORK

Over the past 20 years, there has been a steady increase in research on smart grids due to the growing digitization of power systems, large-scale integration of renewable energy sources, and rising energy consumption. Early research concentrated on enhancing utility-customer communication and automating meter reading [20]. Researchers moved toward sophisticated monitoring, distributed resource coordination, and real-time control as networking and sensor capabilities progressed. This change has been expedited by the advent of AI, which makes it possible for systems to optimize energy flows among dispersed and diverse components, learn from past patterns, and respond swiftly to disruptions. Alongside these advantages, increased reliance on cyber infrastructure led to the emergence of new hazards [21]. Concurrently, the literature on smart grid security has grown, highlighting the necessity of safeguarding equipment, data, communication protocols, and intelligent control algorithms. Key contributions from these three fields are reviewed in this section: Intelligent energy management techniques, cybersecurity issues in contemporary power networks, and AI-enabled smart grid intelligence [22].

Early research on smart grid intelligence looked at how sophisticated analytics may be supported by data from distributed energy sources, smart meters, phasor measurement units, and supervisory control systems. Researchers showed how useful machine learning is for defect detection, renewable energy projection, and short-term demand forecasting [23]. Before deep learning gained popularity, regression models, support vector machines, and ensemble approaches were frequently employed. Deep neural networks, LSTM-based time series models, and hybrid architectures became popular for capturing long-range temporal patterns and nonlinear dependencies as grid datasets expanded. Forecasting accuracy was clearly improved by these methods, which is essential for balancing variable renewable energy sources like solar and wind [24]. Other research concentrated on anomaly detection, identifying anomalous equipment behavior, voltage deviations, and atypical consumption patterns using clustering, probabilistic models, and autoencoders. AI was shown to be a promising method for enhancing situational awareness and visibility throughout the grid by this body of work [25].

Another important area of study has been intelligent energy management. As utilities sought alternatives to costly infrastructure investments, demand response programs gained popularity. Static pricing mechanisms and consumer incentives were the mainstays of early methods. Dynamic pricing, automated load control, and optimization techniques that reacted instantly to system conditions were introduced in later work [26]. Demand response techniques based on AI have had a significant impact. Deep reinforcement learning and Q-learning are two reinforcement learning algorithms that have demonstrated great promise for controlling battery storage, electric car charging, and thermostats [27]. Without human involvement, these systems are able to adjust or lower loads during periods of high demand. Energy use and storage techniques have been negotiated by homes, microgrids, and distributed energy resources through the use of multi-agent systems. In order to develop predictive control systems that anticipate shifts in supply and demand, studies have also looked into hybrid approaches that combine forecasting and optimization [28].

Another important field of study is microgrids. These localized, tiny grids have the ability to function both independently and in tandem with the main grid. AI has been used in microgrid energy management to manage demand-side coordination, storage dispatch, and generator scheduling. Neural networks and evolutionary algorithms have been studied for their ability to optimize power flows in grid-connected and islanded modes [29]. The challenge of preserving voltage and frequency stability during abrupt variations in solar or wind output is highlighted by research on microgrids that rely heavily on renewable energy. It has been demonstrated that under

such circumstances, AI-driven controllers—such as fuzzy logic systems and reinforcement learning—perform better than conventional proportional-integral controllers. This body of research shows how intelligent control may boost the uptake of clean energy, lower operating costs, and increase stability [30].

Concerns over cyber dangers grew as smart grids became increasingly linked. At first, security research concentrated on conventional IT problems like communication protocol protection, access control, and encryption. Studies explored how attackers can alter meter readings, intercept data, or initiate denial-of-service attacks in light of the development of sophisticated metering infrastructure [31]. According to research, compromised meters have the potential to interfere with billing systems, skew load predictions, or possibly cause grid instability. Subsequent research focused on weaknesses in distribution automation equipment, substations, and SCADA systems. Numerous studies pointed out that older devices lacked robust authentication and encryption because they were initially made for isolated contexts. They became targets for replay attacks, malware, and illegal control orders as a result [32].

Security issues brought about by AI itself have been investigated in more recent studies. AI models become excellent targets for enemies as they assume more responsibilities in forecasting, scheduling, and control. Small changes to input data can result in significant mistakes in model predictions, according to research on adversarial machine learning [33]. Researchers showed how an attacker may cause false alarms in anomaly detection systems, skew load projections, or interfere with demand response algorithms. Data poisoning, in which tainted training data gradually lowers model reliability, was the subject of other research. These results emphasize the necessity of strong, comprehensible AI models that are impervious to manipulation and uncertainty [34]. Concerns about privacy have also drawn attention. Privacy-preserving analytics is a top research topic since smart meter data might provide in-depth insights into household activity. To analyze without disclosing sensitive data, methods like homomorphic encryption, federated learning, and differential privacy have been suggested [35].

There is increasing interest in the nexus between AI and smart grid security. In order to detect cyberattacks, researchers have developed AI-based intrusion detection systems that examine network traffic, device activity, and power quality indications [36]. One of the most extensively researched risks in smart grids, fraudulent data injection, has been identified using machine learning. While some methods rely on deep learning to identify minute irregularities in measurement data, others employ statistical models. AI has also been used to address physical security issues, like detecting equipment malfunctions brought on by sabotage or natural disasters. These findings are consistent with a larger trend of employing clever strategies to improve resilience and situational awareness [37].

Decentralized and privacy-preserving learning initiatives are also gaining traction. Building forecasting or anomaly detection models without centralizing sensitive data has been investigated using federated learning. Federated techniques can reduce privacy threats while maintaining competitive accuracy, according to research [38]. But they also bring with them new difficulties, such as safeguarding model updates and thwarting gradient-based attacks. The literature often discusses blockchain and distributed ledger technologies as complementary methods for safe data sharing, tamper-resistant logging, and decentralized authentication. In order to guarantee integrity and trust in distributed energy systems, a number of studies suggest blockchain-AI designs [39].

Although predicting, control, security, and privacy have all shown promising results in the literature, most studies focus on these areas independently. While cybersecurity studies seldom take into account the operational limitations of real-time energy systems, AI-based energy management research frequently assumes that data and communication channels are reliable [40]. Researchers have started looking into integrated frameworks that see security, resilience, and efficiency as interdependent objectives. These studies highlight how crucial it is to protect the decision-making processes that depend on AI models as well as the data pipelines that supply them. This integrated approach is still developing, despite its potential, and there are still a lot of unanswered practical concerns [41].

3. ARCHITECTURAL OVERVIEW OF AI-POWERED SMART GRIDS

Sensing devices, communication networks, intelligence analytics, and automated control systems are all part of the layered and interconnected infrastructure that powers AI-powered smart grids. Coordinated energy flows across dispersed energy resources, adaptive decision-making, and real-time monitoring are all supported by this architecture. It is easier to grasp how intelligence is integrated into grid operations and how various parts work together to preserve security, efficiency, and stability when each layer is clearly understood [42].

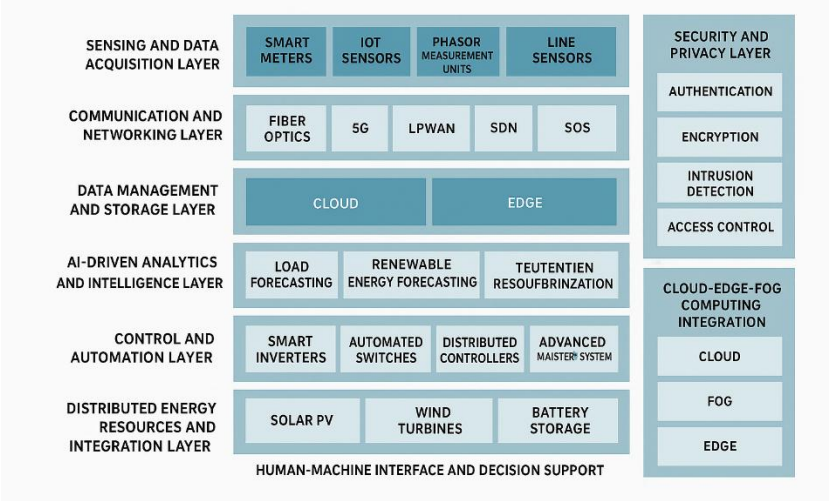

Fig 1.: AI-Powered Smart Grid Architecture

3.1 Sensing and Data Acquisition Layer

The smart grid architecture is built on the sensor layer. It consists of distributed monitors installed in commercial, industrial, and residential contexts, as well as smart meters, IoT sensors, phasor measurement units, and line sensors. Real-time data on voltage levels, current flows, frequency variations, load consumption, and equipment health are all captured by these instruments. This constant flow of data is crucial to the training, prediction, and decision support of AI models. Forecasting for renewable energy, anomaly detection, and demand response systems are all made more responsive by precise and high-resolution data. The number of access points susceptible to cyber threats has significantly increased due to the growth of edge devices in this layer, which also presents new difficulties [43].

3.2 Communication and Networking Layer

Secure, low-latency data transfer throughout the grid is guaranteed via the communication layer. It uses a combination of wired and wireless technologies, including fiber optics, 5G, low-power wide-area networks, and software-defined networking, to connect sensing equipment to substations, control centers, and cloud platforms. Network performance is a crucial component of the design since AI systems rely on timely and dependable data flows to operate properly. Real-time analytics are being supported by the increased integration of latency-sensitive protocols, intelligent routing, and traffic prioritization. To prevent infiltration attempts, this layer also includes network segmentation, authentication, and encryption. The precision of distributed machine learning models and the efficacy of automated control operations are directly impacted by good communication architecture [44].

3.3 Data Management and Storage Layer

Massive amounts of grid data are collected, cleaned, preprocessed, and stored by the data management layer. Platforms for cloud and edge computing collaborate to strike a balance between processing performance and storage needs. While cloud servers hold long-term historical datasets required for model training and predictive analytics, edge nodes frequently handle time-sensitive activities like local anomaly detection or frequency regulation. AI-powered systems need to integrate both structured and unstructured data from various sources, including market signals, weather stations, generation units, and customer devices. Data pipelines are built with scalability, low latency, and consistency in mind. This layer additionally uses regulated access control and anonymization techniques to address privacy issues [45].

3.4 AI-driven Analytics and Intelligence Layer

An AI-powered smart grid's intelligence layer is its essential component. It houses a range of machine learning, deep learning, and optimization models that carry out operations like demand response optimization, fault detection, load forecasting, renewable energy prediction, and voltage stability evaluation. Decentralized energy systems are being supported by distributed AI frameworks, such as multi-agent reinforcement learning and federated learning. These models assist operators in scheduling distributed energy resources, anticipating variations, and identifying security abnormalities before they become more serious. By converting unprocessed data into useful insights, the intelligence layer increases dependability and facilitates proactive decision-making [46].

3.5 Control and Automation Layer

This layer acts on the outputs of AI analytics by carrying out automated adjustments within the grid. It includes smart inverters, automated switches, distributed controllers, and advanced distribution management systems. Adjustments may involve rerouting power during congestion, balancing supply and demand, regulating voltage, or

isolating faulty components. AI-driven control techniques allow the grid to respond to disturbances rapidly without waiting for manual intervention. This layer also coordinates energy storage systems and electric vehicle charging stations to smooth load variations. By combining automation with predictive modeling, the grid becomes more resilient to fluctuations and equipment failures [47].

3.6 Distributed Energy Resources and Integration Layer

Distributed energy resources, including solar panels, wind turbines, battery systems, and microgrids, are integrated into contemporary smart grids. The smooth integration and coordinated functioning of these decentralized assets are the main goals of this layer. AI aids in balancing local demand with distributed sources, forecasting renewable generation, and optimizing storage cycles. AI algorithms are used by coordination mechanisms, including virtual power plants, decentralized optimization, and peer-to-peer energy trading, to match resources effectively. Instead of increasing unpredictability, the architecture makes sure that distributed resources enhance grid stability [48].

3.7 Security and Privacy Layer

Every layer of the architecture incorporates security. This layer specifies data protection guidelines, access control techniques, intrusion detection systems, and authentication mechanisms. AI-based security technologies classify risks, find abnormalities, identify malware, and forecast possible attack routes. Consumer data is safeguarded by privacy safeguards, which also prevent unwanted access to sensitive energy data. While preserving analytical efficiency, strategies like federated learning, safe multi-party computation, and differential privacy minimize data exposure. Attacks on a single component will not spread throughout the grid thanks to a tiered security strategy [49].

3.8 Cloud–Edge–Fog Computing Integration

A hybrid computing approach is being used more and more in smart grid architecture to enable scalability and real-time responsiveness. Long-term forecasting, data archiving, and extensive model training are all handled by cloud systems. By carrying out load filtering and intermediary analytics close to the substation level, fog nodes serve as a link between the cloud and sensors. Edge nodes perform localized intelligence and instantaneous control actions. By processing data closer to its source, this tiered computing system increases privacy, lowers communication traffic, and improves failure tolerance. Depending on criticality, bandwidth, and timing, AI workloads are dynamically split among cloud, fog, and edge [50].

3.9 Human–Machine Interface and Decision Support Layer

The last layer offers interactive control interfaces, dashboards, and visualizations to utilities, operators, and legislators. Decision-makers may assess risks, design energy distribution methods, and comprehend grid conditions with the use of AI-generated insights. Performance monitoring, emergency response, and scenario analysis are all supported via this interface. Human supervision is still crucial, particularly when handling safety-critical incidents or unclear model behavior. Supervisors can verify automated activities and uphold system accountability with the aid of decision support technologies [51].

Table 1: Architectural Layers in AI-Powered Smart Grids

Architectural Layer	Primary Components	Key Functions	AI Techniques Used	Advantages	Security & Privacy Concerns
Sensing and Data Acquisition Layer [52]	Smart meters, IoT sensors, PMUs, line sensors	Real-time measurement of voltage, current, frequency, and consumption data	Basic anomaly detection, signal preprocessing	Fine-grained monitoring, real-time visibility	Device tampering, false data injection, physical attacks
Communication and Networking Layer [53]	Fiber optics, 5G, LPWAN, SDN	Reliable data transmission between grid entities	Traffic optimization, congestion prediction	Low latency, high bandwidth, scalability	Eavesdropping, man-in-the-middle, denial-of-service attacks
Data Management and Storage Layer [54]	Cloud platforms, edge servers, databases	Data aggregation, storage, preprocessing	Data clustering, feature extraction	Efficient data handling, scalability	Data breaches, unauthorized access, privacy leakage
AI-Driven Analytics and Intelligence Layer [55]	ML models, deep learning engines, forecasting tools	Load forecasting, fault detection, demand response	Deep learning, reinforcement learning, federated learning	Improved prediction accuracy, adaptive control	Model poisoning, adversarial attacks, model inversion
Control and Automation Layer [56]	Smart inverters, automated switches, controllers	Real-time control, grid stabilization, self-healing	Reinforcement learning, optimization algorithms	Fast response, reduced human intervention	Command injection, unauthorized control actions
Distributed Energy	Solar PV, wind	Integration of	Predictive control,	Improved	Inverter attacks,

Resources Integration Layer [57]	turbines, battery storage, EVs	renewables and storage	optimization models	sustainability, flexibility	synchronization failures
Human–Machine Interface and Decision Support Layer [58]	Dashboards, control rooms, and visualization tools	Monitoring, decision-making, operator interaction	Decision-support systems, explainable AI	Enhanced situational awareness	Insider threats, data misuse
Security and Privacy Layer (Cross-cutting) [59]	Authentication systems, encryption, IDS, blockchain	Protection across all layers	AI-based intrusion detection, anomaly detection	Resilient and trustworthy operations	

4. THREAT LANDSCAPE AND ATTACK SURFACES

Because of its linked architecture, reliance on data, and integration of dispersed resources, AI-powered smart grids are vulnerable to a wide range of cyber and physical attacks. Attackers have several points of access thanks to the integration of IoT devices, communication networks, cloud platforms, and automated control systems. Designing secure and resilient energy systems requires an understanding of the threat landscape. The main types of threats are described in this section along with an explanation of how they affect various grid components [60].

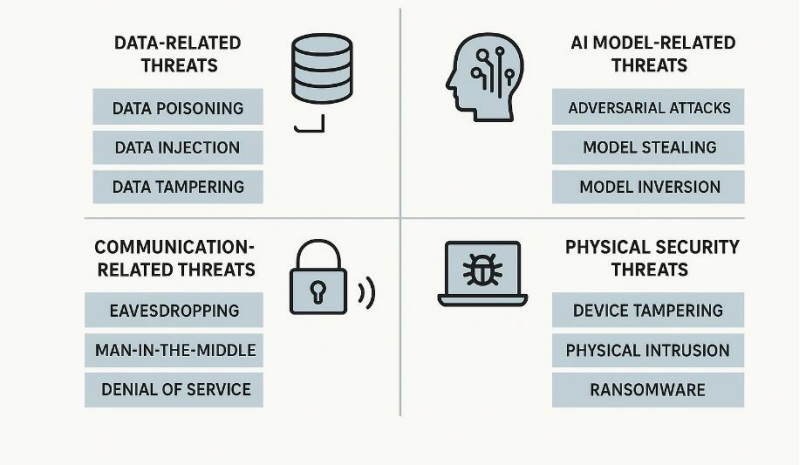

Fig. 2: AI Smart Grid Threats Infographic

4.1 Cyber Threats Targeting Sensing and IoT Devices

Sensing devices such as smart meters, PMUs, and IoT sensors are often deployed in large numbers and installed in unprotected environments. Their limited hardware resources make it difficult to implement strong security controls, making them vulnerable to several attacks [61]:

- Device spoofing: Attackers imitate legitimate sensors to inject false data or disrupt system visibility.
- Meter manipulation: By tampering with smart meters, attackers can alter billing data or manipulate load reports, affecting forecasting accuracy.
- Botnet recruitment: Compromised IoT devices can be used as part of a botnet to launch large-scale attacks on grid infrastructure.

Weak authentication and outdated firmware significantly increase the risk of device compromise.

4.2 Communication Network Attacks

Smart grids rely heavily on communication networks to transmit real-time data. Any disruption or manipulation of these networks can affect operations at multiple levels [62].

- Man-in-the-middle attacks: Attackers intercept and modify data in transit, injecting malicious commands or altering measurements.
- Denial-of-service (DoS): Flooding communication channels with excessive traffic can delay or block essential control messages.

- Traffic analysis: Adversaries monitor communication patterns to infer operational behavior or planning strategies.

These attacks undermine the reliability and timeliness of data that AI models depend on for accurate predictions.

4.3 Data Integrity and Poisoning Attacks

AI systems require large volumes of high-quality data. When adversaries compromise the integrity of this data, the results can be severe [63].

- Training data poisoning: Attackers manipulate the datasets used to train AI models, causing them to learn incorrect patterns.
- Real-time data injection: Small but consistent changes in sensor data can mislead load forecasting or fault detection systems.
- Label flipping: Incorrect labels assigned to training samples degrade classification performance.

These attacks can cause subtle degradation over time, making them difficult to detect without specialized monitoring tools.

4.4 Attacks on AI Models and Algorithms

AI introduces new vulnerabilities that traditional grid systems did not face. Threats targeting models and algorithms include [64]:

- Adversarial examples: Carefully crafted inputs force AI models to misclassify normal operating states as faults or vice versa.
- Model inversion: Attackers recover sensitive information from trained models, exposing user consumption data.
- Model extraction: By querying AI models repeatedly, adversaries approximate model behavior to craft targeted attacks.
- Drift exploitation: Attackers exploit model drift over time by gradually injecting biased data.

Securing model lifecycle processes—training, deployment, and monitoring—is essential for long-term reliability.

4.5 Cloud, Edge, and Fog Platform Vulnerabilities

Hybrid computing environments introduce multiple points of failure and exposure [65].

- Cloud misconfigurations: Incorrect access controls lead to unauthorized access to stored data or ML artifacts.
- Edge node compromise: Since edge nodes manage localized decisions, attackers who take control can directly influence grid operations.
- Insider threats: Employees or contractors with privileged access may misuse data or disrupt services.

Containerized environments and shared infrastructure amplify risks when resources are not properly isolated.

4.6 Attacks on Control and Automation Systems

Control systems convert analytics and algorithms into operational actions. When compromised, the physical consequences can be significant [66].

- Command injection: Attackers issue unauthorized control commands to alter voltage regulation, switch states, or power flows.
- Replay attacks: Previously captured valid commands are replayed to trigger unwanted actions.
- Substation automation compromise: Gaining access to intelligent electronic devices (IEDs) allows attackers to manipulate grid protection schemes.

These attacks can lead to power outages, equipment damage, and unstable operating conditions.

4.7 Physical Threats and Sabotage

While digital threats receive significant attention, physical attacks remain a critical concern [67].

- Tampering with field devices: Physically accessing meters, sensors, or control boxes can disrupt measurements or equipment behavior.
- Damage to infrastructure: Substations, transformers, or communication towers may be targeted to cause service disruption.
- Insider sabotage: Individuals with physical access can damage systems or bypass safety protocols.

Physical security measures such as surveillance, access control, and tamper-proof casing are essential.

4.8 Privacy Threats and Consumer Data Exposure

Smart grids collect detailed consumption profiles, which can reveal personal habits, occupancy patterns, and appliance usage [68].

- Unauthorized data access: Weak encryption or poorly secured databases expose sensitive customer information.
- Inference attacks: Even anonymized datasets can be linked with external information to identify individuals.
- Behavioral profiling: Attackers may track daily routines, creating privacy risks for households.

As data-driven applications grow, protecting consumer privacy becomes more challenging and more important.

Table 2: Threat Landscape and Attack Surfaces in AI-Powered Smart Grids

Threat Category	Attack Surface / Target	Attack Techniques	Potential Impact on Smart Grid	Detection Difficult	Typical Mitigation Approaches
IoT and Sensor-Level Attacks [69]	Smart meters, PMUs, IoT sensors	Device spoofing, meter tampering, firmware manipulation	False measurements, billing fraud, inaccurate forecasting	High	Device authentication, secure boot, tamper-resistant hardware
Communication Network Attacks [70]	Wired and wireless networks	Man-in-the-middle, packet injection, DoS/DDoS	Data loss, delayed control signals, service disruption	Medium	Encryption, network segmentation, traffic monitoring
Data Integrity and Poisoning Attacks [71]	Training and real-time datasets	False data injection, label flipping, data drift exploitation	Degraded AI performance, wrong operational decisions	Very High	Data validation, anomaly detection, secure data pipelines
AI Model and Algorithm Attacks [72]	Machine learning models	Adversarial inputs, model inversion, model extraction	Misclassification, privacy leakage, system instability	Very High	Robust training, adversarial defense, model access control
Cloud and Edge Infrastructure Attacks [73]	Cloud servers, edge nodes	Misconfiguration abuse, privilege escalation, malware	System-wide compromise, service outages	Medium	Secure configuration, runtime monitoring, access control
Control System Attack [74]	SCADA, IEDs, automation controllers	Command injection, replay attacks	Physical damage, grid instability, blackouts	Medium–High	Command authentication, state validation, redundancy
Physical Attacks and Sabotage [75]	Substations, field devices	Physical tampering, cable cutting, equipment damage	Local or regional outages, equipment loss	Low	Physical security, surveillance, access control
Privacy Attacks [76]	Consumer energy data	Inference attacks, unauthorized access	Loss of user privacy, regulatory violations	High	Differential privacy, encryption, access governance
Supply Chain Attacks [77]	Hardware and software components	Malicious implants, compromised updates	Hidden backdoors, long-term compromise	Very High	Vendor vetting, component verification, secure updates
Insider Threats [78]	Operators, maintenance staff	Credential misuse, intentional sabotage	Data leaks, operational disruption	High	Role-based access, activity logging, audits
AI-Enabled and Autonomous Attacks [79]	Multi-agent systems, digital twins	Self-learning malware, coordination manipulation	Adaptive attacks, cascading failures	Very High	AI-driven defense, behavioral analytics, resilience design

5. INTELLIGENT ENERGY MANAGEMENT APPROACHES

Energy management systems driven by AI enable smart grids to function effectively, adapt to changes, and remain stable in the face of fluctuating generation and load situations. These methods balance supply and demand while maximizing cost, dependability, and sustainability using real-time data, predictive analytics, and automated control techniques. The main AI-driven strategies that enhance the functionality and flexibility of contemporary smart grids are covered in this section [80].

5.1 Load Forecasting and Consumption Prediction

Accurate load forecasting is central to efficient grid planning. AI techniques such as deep learning, gradient boosting, and hybrid statistical–machine learning methods outperform traditional forecasting tools by capturing complex consumption patterns [81].

- Short-term forecasting: Helps with operational decision-making, dispatch scheduling, and demand response activation.
- Medium- and long-term forecasting: Supports infrastructure planning, investment decisions, and resource allocation.
- Context-aware forecasting: Integrates weather data, consumer behavior trends, seasonal effects, and socio-economic indicators.

AI models identify subtle variations in load profiles, reducing forecasting errors and allowing utilities to plan energy generation more effectively.

5.2 Renewable Energy Forecasting and Variability Management

The increasing integration of renewable sources like solar and wind introduces uncertainty into grid operations. AI helps manage this variability through accurate forecasting and adaptive control [82].

- Solar PV prediction: Uses satellite imagery, local irradiance data, and cloud movement analysis.
- Wind energy forecasting: Combines meteorological data, turbine-level measurements, and atmospheric models.
- Hybrid forecasting: Integrates multiple sources to improve prediction accuracy.

Better forecasting reduces reserve requirements and lowers operational costs while improving the stability of renewable-rich grids.

5.3 Demand Response Optimization

Demand response programs help shift, reduce, or reschedule consumption during peak periods. AI enhances these programs by learning consumption behavior and predicting user willingness to participate [83].

- Consumer segmentation: Clusters users based on response patterns and load flexibility.
- Dynamic pricing optimization: AI models suggest optimal tariff structures to encourage shifting of loads.
- Automated load control: Smart home systems and IoT devices use AI to adjust appliances without compromising user comfort.

These techniques decrease peak demand, reduce strain on infrastructure, and support sustainable grid operation.

5.4 Energy Storage Management

Energy storage systems are crucial for balancing intermittent renewable sources. AI-driven storage management ensures optimal charging and discharging cycles [84].

- Battery health prediction: Models estimate degradation rates to maximize lifespan.
- Multi-objective optimization: Balances cost, efficiency, and grid support requirements.
- Coordinated storage control: Manages distributed batteries across neighborhoods or microgrids.

Smart control of storage helps stabilize grid frequency, smooth load variations, and enhance resilience during outages.

5.5 Multi-Agent Systems for Distributed Energy Control

Smart grids increasingly rely on multi-agent systems that represent different grid entities such as substations, microgrids, storage units, and consumer devices. Each agent uses local intelligence to make decisions while coordinating with others [85].

- Autonomous decision-making: Agents regulate voltage, load balance, and resource allocation.
- Negotiation and cooperation: Agents communicate to resolve conflicts during resource shortages or congestion.
- Decentralized optimization: Reduces reliance on a single central controller.

This approach improves scalability and flexibility, especially in grids with large distributed energy resources.

5.6 Reinforcement Learning for Real-Time Control

Reinforcement learning (RL) provides adaptive control strategies that learn optimal actions through continuous interaction with the environment. RL is applied in several grid management tasks [86]:

- Voltage and frequency regulation: RL agents adjust control settings based on real-time feedback.
- Energy trading and market participation: Agents learn profitable bidding strategies while considering grid constraints.
- Storage and EV charging coordination: RL balances user needs with grid stability requirements.

RL-based controllers adapt quickly to new patterns, making them valuable in dynamic grid settings.

6. SECURITY AND PRIVACY MECHANISM

For AI-powered smart grids, security and privacy are crucial because they preserve customer data, guarantee dependable operations, and protect vital infrastructure. New dangers appear across gadgets, networks, and intelligent systems as the grid gets more digital and connected. Preventive, investigative, and response-oriented strategies must be combined for effective protection. The primary methods for securing contemporary smart grids and preserving the availability, confidentiality, and integrity of data and services are described in this section [87].

6.1 Identity Management and Strong Authentication

Identity management systems ensure that only trusted users and devices can access grid operations and data. Smart grids rely heavily on authentication schemes for sensors, smart meters, control systems, and cloud platforms [88].

- Multi-factor authentication: Adds layers such as passwords, certificates, and hardware tokens.
- Certificate-based authentication: Uses digital certificates to verify device identity.
- Lightweight credentialing: Designed for IoT devices with limited computing power.

Strong authentication prevents impersonation attacks and protects access to control interfaces.

6.2 Encryption and Secure Data Communication

Grid data travels across public and private networks, making secure communication necessary. Encryption helps protect data from interception or manipulation [89].

- End-to-end encryption: Protects data from source to destination.
- Transport layer security: Secures communication between field devices, substations, and cloud platforms.
- Key management systems: Rotate and distribute cryptographic keys securely.

Properly implemented encryption reduces risks related to eavesdropping, replay attacks, and unauthorized access.

6.3 Intrusion Detection and Anomaly Monitoring

Intrusion detection systems (IDS) monitor network traffic and device behavior to identify suspicious activity. AI-based IDS techniques are increasingly used because they detect subtle, evolving threats [90].

- Signature-based detection: Identifies known attack patterns.
- Anomaly detection: Uses machine learning to flag unusual network behavior.
- Hybrid systems: Combine both methods for broader coverage.

Anomaly-based IDS is especially useful in smart grids where attackers may attempt stealthy data manipulation.

6.4 AI-driven Threat Detection and Response

As cyberattacks become more complex, AI plays a stronger role in detecting abnormal events and coordinating responses [91].

- Deep learning classifiers: Identify malicious traffic or abnormal operating states.
- Behavioral analytics: Capture patterns in device behavior to detect infections or compromise.
- Automated response: Enables rapid isolation of compromised nodes or segments.

These systems improve detection accuracy and help limit the spread of attacks.

6.5 Network Segmentation and Zero Trust Architectures

Zero-trust models operate on the principle that no user or device is trusted by default. This approach reduces the impact of breaches [92].

- Micro-segmentation: Divides networks into small zones with restricted access.
- Continuous verification: Every request is authenticated and validated.
- Least-privilege policies: Devices and applications receive only the access they need.

Segmentation helps isolate compromised parts of the grid and prevents attackers from moving laterally.

6.6 Secure Firmware and Software Updates

Failure to update devices exposes the grid to known vulnerabilities. Secure update mechanisms ensure the integrity of upgrades [93].

- Digitally signed updates: Prevent unauthorized firmware installation.
- Secure boot: Ensures devices run only verified software.
- Over-the-air update protocols: Safely refresh firmware on remote devices.

These mechanisms keep devices protected against new threats

Table 3: Security and Privacy Mechanisms in AI-Powered Smart Grids

Security / Privacy Mechanism	Primary Techniques	Protected Assets	Key Benefits	Limitations / Challenges
Identity and Access Management [94]	Multi-factor authentication, digital certificates, and role-based access control	Devices, users, control systems	Prevents unauthorized access, enforces accountability	Credential management overhead, scalability issues
Encryption and Secure Communication [95]	End-to-end encryption, TLS, secure key management	Data in transit and at rest	Protects the confidentiality and integrity of grid data	Key distribution complexity, performance overhead
Intrusion Detection Systems (IDS) [96]	Signature-based, anomaly-based, hybrid IDS	Networks, devices, data flows	Early detection of cyber intrusions	False positives, training data dependency
AI-driven Threat Detection [97]	Deep learning, behavioral analytics, adaptive models	Control networks, AI pipelines	Detects advanced and unknown attacks	Vulnerability to adversarial inputs
Network Segmentation and Zero Trust [98]	Micro-segmentation, least-privilege access, continuous verification	Network infrastructure	Limits the lateral movement of attackers	Increased configuration complexity
Secure Firmware and Software Updates [99]	Secure boot, signed updates, OTA patching	IoT devices, control systems	Protects against malware and exploits	Legacy device compatibility issues
Blockchain-based Security [100]	Distributed ledger, smart contracts, immutability	Transactions, audit logs, energy trading data	Tamper resistance, decentralized trust	Scalability and latency concerns
Privacy-Preserving Data Analytics [85]	Differential privacy, homomorphic encryption, secure multi-party computation	Consumer data, usage patterns	Maintains privacy while enabling analytics	Computational overhead, reduced accuracy
Federated Learning [93]	Local model training, secure aggregation	Distributed datasets, AI models	Minimizes data exposure, improves privacy	Communication cost, model convergence issues
Resilience and Self-Healing Mechanisms [98]	Redundancy, fault isolation, adaptive reconfiguration	Grid operations, control systems	Fast recovery from attacks or failures	Higher deployment and maintenance cost
Secure Control and Command Validation [54]	Command authentication, state-aware validation	SCADA, automation systems	Prevents malicious or false control actions	Latency in critical decision paths

7. OPEN CHALLENGES AND RESEARCH DIRECTIONS

7.1 Scalable, low-latency secure coordination

Secure consensus and ledger systems often suffer from latency. Research is needed into lightweight, verifiable coordination mechanisms that operate within tight operational time windows [39].

7.2 Robustness beyond small perturbations

Most adversarial defenses focus on small input perturbations. Attackers in grid settings can craft large, stealthy manipulations that mimic legitimate anomalies. Techniques that model adversary intent and contextual plausibility are needed [12].

7.3 Data scarcity for rare events

Extreme weather and cascades are rare yet critical. Generative models and physics-informed simulations can help create training data for these scenarios, but ensuring realism remains a challenge [25].

7.4 Federated learning in highly heterogeneous environments

Device heterogeneity, intermittent connectivity, and non-iid data limit FL convergence. New aggregation and personalization methods that respect privacy while converging robustly are required [9].

7.5 Explainability and operator interaction

Operators need clear explanations and uncertainty bounds from AI systems. Bridging the gap between black-box models and certified, understandable policies is an open area [11].

7.6 Regulatory and economic incentives

Technical solutions must align with markets and regulations. Mechanisms to incentivize secure design—through liability rules, standards, or market products—are essential [13].

7.7 Human factors and usability

Security procedures and AI recommendations must be integrated into operator workflows; otherwise, they will be bypassed. Research into human-in-the-loop designs and alert fatigue mitigation is important [19].

Table 4: Open Challenges and Research Directions in AI-Powered Smart Grids

Challenge Area	Description of the Challenge	Impact on Smart Grid Operations	Current Limitations	Future Research Directions
Scalability of AI Models [21]	Managing AI models across millions of devices and data streams	Reduced performance and delayed decisions	Centralized training, high computational cost	Distributed and hierarchical learning, scalable federated AI
Data Quality and Availability [23]	Incomplete, noisy, or biased energy data	Inaccurate forecasting and control actions	Limited data validation, heterogeneous sources	Robust data cleansing, self-adaptive data validation
Security of AI Models [29]	Vulnerability to adversarial and poisoning attacks	Misleading predictions and unsafe actions	Lack of AI-specific security defenses	Adversarial training, explainable and verifiable AI
Privacy Preservation [35]	Protection of consumer behavior and usage patterns	Regulatory and trust issues	Trade-off between data utility and privacy	Advanced differential privacy, secure multi-party analytics
Real-Time Decision-Making [33]	Need for fast responses under dynamic conditions	Latency affects grid stability	Cloud dependence, slow inference	Edge intelligence, real-time reinforcement learning
Interoperability and Standardization [37]	Integration of heterogeneous devices and vendor	Deployment complexity and compatibility issues	Fragmented standards	Unified protocols, AI-aware grid standard
Explainability of AI Decisions [39]	Lack of transparency in AI-driven control actions	Reduced operator trust and accountability	Black-box model behavior	Explainable AI for grid operations and control
Resilience to Cyber-Physical Attacks [41]	Combined cyber and physical threat scenarios	Cascading failures and outages	Static defense mechanisms	Self-healing and adaptive defense frameworks
Integration of Distributed Energy Resources [52]	Coordinating renewables, storage, and EVs	Instability due to variability	Centralized coordination limitations	Multi-agent systems, decentralized optimization
Energy-Efficient AI Deployment [67]	High energy cost of AI computation	Increased operational overhead	Resource-intensive models	Lightweight models, green AI techniques
Regulatory and Ethical Concerns [91]	Compliance, fairness, and accountability	Barriers to adoption	Lack of AI-specific grid policies	Policy-aware AI design, ethical governance models
Human–AI Collaboration [100]	Balancing automation with human oversight	Operational errors and resistance to automation	Limited decision-support tools	Human-centered AI interfaces and decision aids

8. CONCLUSION

By adding intelligence, automation, and adaptability to each layer of the infrastructure, AI-powered smart grids are transforming the way energy systems function. This study demonstrated how AI creates new security and privacy issues while simultaneously enhancing forecasting, demand response, distributed energy coordination, and real-time

control. Strong security measures are becoming more and more necessary as grids become more data-driven and decentralized. Layered defenses, privacy-preserving analytics, and resilient architectures are crucial since threats ranging from data poisoning to device tampering can interrupt operations. A path forward is provided by the combination of methods like federated learning, anomaly detection, and secure communication protocols, which enable smart grids to gain from sophisticated analytics without revealing serious weaknesses. To ensure these systems are safe, transparent, and dependable, utilities, regulators, and tech developers must work together to build trustworthy AI-powered grids. AI can assist energy systems that are reliable, effective, and ready for the needs of a future powered by renewable energy sources with careful design and ongoing innovation.

REFERENCES

[1] **Ahmad, T., Zhang, D., Huang, C., & Chen, H. (2021). Artificial intelligence in sustainable energy systems: A review. Renewable and Sustainable Energy Reviews, 149, 111361.**

[2] **Aitzhan, N. Z., & Svetinovic, D. (2018). Security and privacy in decentralized energy trading through blockchain. IEEE Transactions on Dependable and Secure Computing, 15(5), 840–852.**

[3] **O. Singh, V. R, N. Singh et al., "Cost-Effective Machine Learning-based Localization Algorithm for WSNs", International Journal of Early Childhood Special Education, vol. 14, issue 2, ISSN: 1308-5581, pp. 7093-7105, 2022.**

[4] **Alimi, O. A., Ouahada, K., & Abu-Mahfouz, A. M. (2020). A review of machine learning approaches to power system security. Energies, 13(20), 5322.**

[5] **N. Singh, A. Singh, O. Singh, et al., "Automatically Positioning the Garment in a Warehouse at the Desired Place using Artificial Intelligence", International Journal of Early Childhood Special Education, vol. 14, issue 4, ISSN: 1308-5581, pp. 1249-1256, 2022.**

[6] **Anand, A., Gupta, R., & Tripathi, A. (2022). Privacy-preserving energy analytics using federated learning. IEEE Internet of Things Journal, 9(14), 12145–12156.**

[7] **Antonakakis, M., April, T., Bailey, M., et al. (2017). Understanding the Mirai botnet. USENIX Security Symposium, 1093–1110.**

[8]

[9] **O. Singh, A. Kushwaha et al. "Improving energy efficiency in scalable WSNs through IoT-driven approach", International Journal of Information Technology, vol. 17, ISSN:0973-5658, pp. 2659–2669, 2025.**

[10] **Bellavista, P., Giannelli, C., & Montanari, R. (2021). Federated learning in edge computing: A survey. IEEE Communications Surveys & Tutorials, 23(2), 1122–1154.**

[11] **O. Singh, N. Singh, A. Singh et al. "AI, IoT, and Blockchain in Fashion: Confronting Industry Applications, Challenges with Technological Solutions", International Journal of Communication Networks and Information Security, vol. 16, No. 4, ISSN: 2076-0930, pp. 393-410, 2024.**

[12] **Bissey, S., & Roy, S. (2023). AI-enabled intrusion detection for smart grids. Electric Power Systems Research, 219, 109234.**

[13] **Bou-Harb, E., Fachkha, C., & Debbabi, M. (2014). Cyber scanning: A comprehensive survey. IEEE Communications Surveys & Tutorials, 16(3), 1496–1519.**

[14] **O. Singh, V. R, A. Singh et al. "Navigating Security Threats and Solutions using AI in Wireless Sensor Networks", International Journal of Communication Networks and Information Security, vol. 16, No. 4, ISSN: 2076-0930, pp. 411-427, 2024.**

[15] **O. Singh and L. Kumar "MLCEL: Machine Learning and Cost-Effective Localization Algorithms for WSNs", International Journal of Sensors, Wireless Communications and Control- Bentham Science, vol. 13, No. 2, ISSN: 2210-3287, pp. 82-88, 2023.**

[16] **Choi, D. H., Kim, J., & Won, D. (2020). Cyber–physical security of power grids. Energies, 13(3), 638.**

[17] **Cleveland, F. (2008). IEC 62351 security standards. IEEE Power and Energy Society General Meeting, 1–6.**

[18] **L. Kumar, S. Kumar, O. Singh et al. "A Secure Communication with One Time Pad Encryption and Steganography Method in Cloud", Turkish Journal of Computer and Mathematics Education, vol. 12, No. 10, ISSN:1309-4653, pp. 2567-2576, 2021**

[19] **Deng, R., Yang, Z., Chen, J., & Chow, M. Y. (2015). Residential energy management. IEEE Transactions on Smart Grid, 6(3), 1378–1387.**

[20] **Diro, A. A., & Chilamkurti, N. (2018). Distributed attack detection in IoT. Future Generation Computer Systems, 82, 761–768.**

[21] **Dong, Z. Y., Zhao, J., Wen, F., & Xue, Y. (2014). From smart grid to energy internet. Proceedings of the IEEE, 102(6), 947–955.**

[22] O. Singh, V. R, A. Singh et al. "Artificial Intelligence for IoT-based Healthcare 5.0: Challenges and Solutions", International Journal of Information and Electronics Engineering, vol. 15, Issue. 06, ISSN:2010-3719, pp. 222-236, 2025.
[23] Fan, M., & Zhang, J. (2022). Privacy-aware demand response in smart grids. IEEE Transactions on Smart Grid, 13(4), 3091–3103.
[24] Fang, X., Misra, S., Xue, G., & Yang, D. (2012). Smart grid communication. IEEE Communications Surveys & Tutorials, 14(4), 944–980.
[25] Fawaz, A., Kim, K., & Kim, J. (2020). Data poisoning attacks on power systems. IEEE Transactions on Smart Grid, 11(4), 3365–3375.
[26] Gellings, C. W. (2009). The smart grid. IEEE Power & Energy Magazine, 7(2), 18–25.
[27] O. Singh, N. Singh, V. R et al. "Blockchain-driven Transformation in Healthcare 5.0: Opportunities and Challenges", International Journal of Information and Electronics Engineering, vol. 15, Issue. 06, ISSN:2010-3719, pp. 210-221, 2025.
[28] Gungor, V. C., et al. (2013). Smart grid technologies. IEEE Transactions on Industrial Informatics, 7(4), 529–539.
[29] He, Y., Mendis, G. J., & Wei, J. (2017). Real-time intrusion detection. IEEE Transactions on Smart Grid, 8(5), 2064–2075.
[30] Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I., & Tygar, J. (2011). Adversarial machine learning. Proceedings of the 4th ACM Workshop on Security and AI, 43–58.
[31] Huh, J. H., & Seo, K. (2018). Blockchain-based energy trading. Energy Procedia, 141, 374–379.
[32] Islam, S. R., et al. (2020). The internet of things for healthcare. IEEE Access, 8, 1722–1758.
[33] Kabalci, Y. (2020). A survey on smart grid architectures. Renewable and Sustainable Energy Reviews, 130, 109958.
[34] Kang, J., Yu, R., Huang, X., et al. (2017). Enabling local energy trading. IEEE Transactions on Industrial Informatics, 13(6), 3154–3164.
[35] Kshetri, N., & Voas, J. (2017). Blockchain-enabled e-voting. Computer, 50(11), 95–99.
[36] Liang, G., Zhao, J., Luo, F., Weller, S. R., & Dong, Z. Y. (2017). Cyber attacks and defenses. IEEE Transactions on Smart Grid, 8(3), 1373–1386.
[37] Liu, X., Shahidehpour, M., & Li, Z. (2019). Cybersecurity in microgrids. IEEE Transactions on Smart Grid, 10(3), 3169–3178.
[38] Lu, X., Wang, W., Ma, J., & Wang, J. (2021). Edge intelligence for smart grids. IEEE Network, 35(3), 112–118.
[39] McDaniel, P., & McLaughlin, S. (2009). Security and privacy challenges. IEEE Security & Privacy, 7(3), 75–77.
[40] Mnih, V., et al. (2015). Human-level control through deep reinforcement learning. Nature, 518(7540), 529–533.
[41] Mohsenian-Rad, A. H., et al. (2010). Autonomous demand-side management. IEEE Transactions on Smart Grid, 1(3), 320–331.
[42] Molina-Markham, A., et al. (2010). Revealing energy consumption. Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems, 1–6.
[43] Nguyen, T. T., & Le, L. B. (2014). Peer-to-peer energy trading. IEEE Transactions on Smart Grid, 5(2), 881–890.
[44] Niyato, D., et al. (2020). Edge intelligence. IEEE Communications Magazine, 58(1), 37–43.
[45] Papernot, N., et al. (2016). Distillation as a defense. IEEE Symposium on Security and Privacy, 582–597.
[46] Parag, Y., & Sovacool, B. K. (2016). Electricity market design. Nature Energy, 1(7), 1–6.
[47] Pillitteri, V. Y., & Brewer, T. L. (2014). Guidelines for smart grid cybersecurity. NISTIR 7628.
[48] Qi, J., Hahn, A., Lu, X., Wang, J., & Liu, C. C. (2015). Cybersecurity for distributed energy resources. IEEE Power and Energy Society General Meeting, 1–5.
[49] Rahman, M. A., & Mohsenian-Rad, H. (2017). False data injection attacks. IEEE Transactions on Smart Grid, 8(5), 2495–2505.
[50] Reka, S. S., & Dragicevic, T. (2018). Future of microgrids. Renewable and Sustainable Energy Reviews, 82, 2073–2084.
[51] Ren, Z., & Liang, G. (2022). AI-based cyber defense. IEEE Transactions on Industrial Informatics, 18(9), 6123–6134.
[52] Ryu, S., et al. (2019). Machine learning-based intrusion detection. Energies, 12(13), 2518.
[53] Siano, P. (2014). Demand response and smart grids. Renewable and Sustainable Energy Reviews, 30, 461–478.
[54] Singh, O., & Sharma, R. (2023). Security-centric AI–blockchain integration. Journal of Information Security and Applications, 70, 103293.

[55] Sneha, M., & Singh, S. (2021). Privacy in smart meters. Computer Communications, 176, 38–52.
[56] Srivastava, A., et al. (2012). Smart grid reliability. IEEE Power & Energy Magazine, 10(1), 24–37.
[57] Stankovic, J. A. (2014). Research directions for IoT. IEEE Internet of Things Journal, 1(1), 3–9.
[58] Sun, Q., et al. (2020). Edge computing in smart grid. IEEE Transactions on Industrial Informatics, 16(3), 1986–1996.
[59] Tan, S., De, D., Song, W. Z., Yang, J., & Das, S. K. (2016). Survey on smart grid cyber security. IEEE Communications Surveys & Tutorials, 19(1), 138–168.
[60] Tian, F. (2016). Blockchain and smart grid. IEEE International Conference on Smart Grid Communications, 1–6.
[61] Tong, L., Zhao, Q., & Zheng, S. (2013). Demand response with renewable integration. IEEE Journal on Selected Areas in Communications, 31(7), 1220–1234.
[62] Wang, J., et al. (2020). Deep learning-based fault detection. IEEE Transactions on Power Delivery, 35(2), 676–685.
[63] Wang, K., et al. (2018). A survey on energy internet. IEEE Communications Surveys & Tutorials, 20(3), 1826–1857.
[64] Wang, P., et al. (2021). Digital twins for power systems. IEEE Transactions on Smart Grid, 12(6), 4761–4772.
[65] Wei, L., et al. (2018). Machine learning-based cyber attack detection. IEEE Transactions on Smart Grid, 9(5), 4612–4624.
[66] Xie, L., et al. (2011). Detection of false data injection. IEEE Transactions on Smart Grid, 2(4), 638–646.
[67] Xu, Y., et al. (2020). Reinforcement learning for energy management. Applied Energy, 276, 115437.
[68] Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2012). A survey on smart grid communication. IEEE Communications Surveys & Tutorials, 15(1), 5–20.
[69] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning. ACM Transactions on Intelligent Systems and Technology, 10(2), 1–19.
[70] Yu, R., et al. (2018). Blockchain for distributed energy resources. IEEE Communications Magazine, 56(9), 192–197.
[71] Zeng, B., & Zhang, J. (2013). Multi-stage stochastic optimization. IEEE Transactions on Power Systems, 28(3), 2905–2913.
[72] Zhang, D., Shah, N., & Papageorgiou, L. G. (2015). Energy management systems. Applied Energy, 143, 252–264.
[73] Zhang, Y., et al. (2019). Data-driven anomaly detection. IEEE Transactions on Smart Grid, 10(6), 6573–6584.
[74] Zhang, Z., et al. (2021). Privacy-preserving energy trading. IEEE Transactions on Industrial Informatics, 17(7), 4908–4917.
[75] Zhao, J., et al. (2018). Cyber-physical security of power systems. IEEE Transactions on Power Systems, 33(1), 977–987.
[76] Zhou, L., et al. (2020). Deep learning for power systems. CSEE Journal of Power and Energy Systems, 6(1), 1–14.
[77] Zhou, Y., et al. (2022). Trust management in smart grids. IEEE Access, 10, 13456–13470.
[78] Zhu, B., Joseph, A., & Sastry, S. (2011). Taxonomy of cyber attacks. IEEE SmartGridComm, 380–388.
[79] Zhu, Q., & Basar, T. (2015). Game-theoretic cyber security. IEEE Control Systems Magazine, 35(1), 46–65.
[80] Zhuang, W., et al. (2021). AI-enabled V2G systems. IEEE Transactions on Vehicular Technology, 70(5), 4306–4318.
[81] Zhou, H., et al. (2023). Explainable AI for smart grids. IEEE Transactions on Smart Grid, 14(2), 1389–1401.
[82] Li, X., et al. (2023). Secure federated learning in smart grids. IEEE Internet of Things Journal, 10(11), 9876–9889.
[83] Kumar, R., & Singh, M. (2023). AI-based cyber resilience in power systems. Electric Power Systems Research, 223, 109475.
[84] Patel, S., et al. (2022). Edge-based energy analytics. IEEE Transactions on Industrial Informatics, 18(10), 7102–7113.
[85] Hassan, N., et al. (2023). Adversarial robustness in energy AI models. Applied Energy, 341, 120912.
[86] Roy, S., et al. (2022). Digital twin security for smart grids. IEEE Access, 10, 86455–86468.
[87] Banerjee, A., et al. (2023). Blockchain-enabled secure energy trading. Future Generation

Computer Systems, 139, 311–322.
[88] **Mishra, D., et al. (2022). Privacy leakage in smart metering. Information Sciences, 589, 101–116.**
[89] **Chen, X., et al. (2023). Trust-aware multi-agent control. IEEE Transactions on Smart Grid, 14(3), 2441–2453.**
[90] **Das, S., et al. (2021). AI-based fault diagnosis. IEEE Transactions on Power Delivery, 36(6), 3549–3559.**
[91] **Ghosh, A., et al. (2022). Cyber-physical attack modeling. IEEE Systems Journal, 16(4), 6345–6356.**
[92] **Li, Y., et al. (2021). Secure edge computing. IEEE Network, 35(2), 22–28.**
[93] **Ahmad, R., et al. (2023). Energy-efficient AI models. Sustainable Energy Technologies and Assessments, 56, 103017.**
[94] **Wang, S., et al. (2022). Zero trust for smart grids. IEEE Security & Privacy, 20(4), 56–64.**
[95] **Zhou, X., et al. (2023). AI-driven demand response security. IEEE Transactions on Smart Grid, 14(4), 3201–3213.**
[96] **Luo, F., et al. (2021). Resilient operation of power grids. IEEE Transactions on Power Systems, 36(2), 1606–1617.**
[97] **Zhang, H., et al. (2022). Lightweight authentication for IoT grids. IEEE Internet of Things Journal, 9(18), 16823–16835.**
[98] **Ali, S., et al. (2023). Privacy-preserving digital twins. Future Energy Systems, 2(1), 45–59.**
[99] **Singh, P., & Yadav, R. (2022). AI governance in energy systems. Energy Policy, 165, 112963.**
[100] **Chen, Y., et al. (2023). Secure multi-agent reinforcement learning. IEEE Transactions on Neural Networks and Learning Systems, 34(9), 6201–6214.**
[101] **Verma, A., et al. (2023). Cybersecurity benchmarking for smart grids. IEEE Transactions on Smart Grid, 14(5), 4022–4034.**