Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

Unlocking the Potential of Artificial Intelligence and Blockchain: A Pathway to Secure, Efficient, and Intelligent Smart Grids in Pakistan's Energy Sector

Engr. Shazia Feroz (Corresponding Author)
Department of Electronics Engineering Technology, Benazir Bhutto Shaheed University of Technology and Skill Development, Khairpur Mir's, -66020, Sindh, Pakistan. Email: shaziaferoz@bbsutsd.edu.pk

Abdul Qadeer Laghari
Department of Basic Sciences and Related Studies, Benazir Bhutto Shaheed University of Technology and Skill Development, Khairpur Mir's, -66020, Sindh, Pakistan. Email: leghariqadeer@bbsutsd.edu.pk

Basit Ahmad
Department of Electrical Engineering, NFC Institute of Engineering and Technology Multan, Punjab, Pakistan. Email: basitahmad3884@gmail.com

Muhammad Touseef Ul Hassan
Department of Computer Science, University of Gujrat, Punjab, Pakistan.
Email: iamtouseef2000@gmail.com

Mudassar Rafique
Department of Electrical Engineering, Superior University Lahore, Punjab, Pakistan. Email: mudassarrafique737@gmail.com

Muhammad Kamran
Department of Computer Science, University of Agriculture, Faisalabad, Punjab, Pakistan. Email: hafazkamran313@gmail.com

Abstract
The integration of Artificial Intelligence (AI) and Blockchain technologies in the energy sector has the potential to revolutionize the management and optimization of smart grids, especially in developing countries like Pakistan. The country's energy sector faces persistent challenges such as inefficiency, unreliable supply, and limited integration of renewable energy sources. This paper explores how AI and Blockchain can address these issues by enhancing grid efficiency, improving security, and enabling decentralized, transparent energy trading systems. AI can contribute to predictive maintenance, load forecasting, and optimization of renewable energy integration, while Blockchain offers secure, transparent, and immutable records for energy transactions, facilitating peer-to-peer energy trading and smart contract automation. By combining these technologies, Pakistan's energy sector can unlock significant improvements in operational efficiency, cost reduction, and sustainability. The paper also highlights the barriers to adoption, including technological infrastructure challenges, regulatory hurdles, and the need for skilled workforce development. Through an examination of global case studies and potential solutions tailored to

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

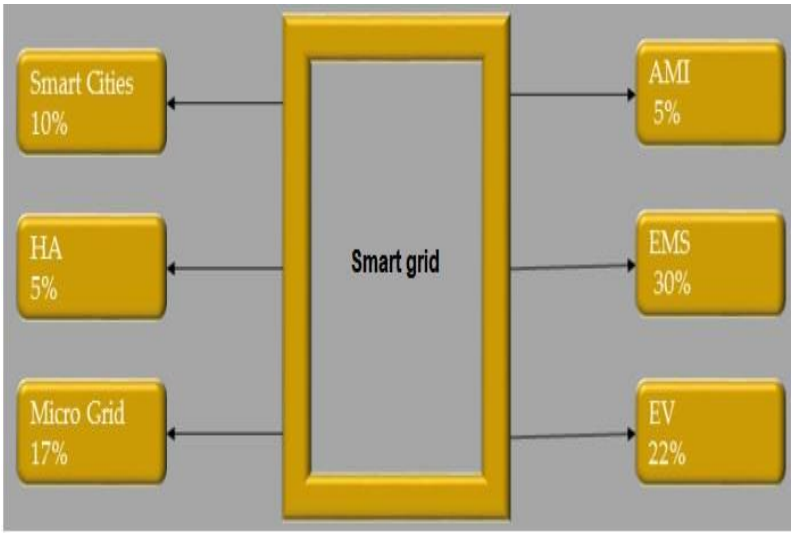
Vol. 3 No. 3 (March) (2025)

Pakistan's context, this paper outlines a pathway for the successful deployment of AI and Blockchain in smart grids, positioning Pakistan to lead in energy innovation and contribute to global sustainability goals.

Keywords: Artificial Intelligence (AI), Blockchain, Technological Infrastructure, Regulatory Hurdles, Grid Efficiency, Renewable Energy Integration

Introduction

Modern technologies have been integrated into traditional electrical infrastructure to create what is known as a "smart grid." A smart grid incorporates various methods for managing operations and controlling power distribution. Key components of a smart grid include smart meters, appliances installed at consumer sites, production meters, renewable energy generators, smart inverters, and other resources aimed at improving energy efficiency at grid locations [1]. Renewable energy generators help reduce energy costs because they harness free energy from natural sources. However, their availability is variable and depends on factors such as temperature, humidity, wind speed and direction, and geographical location. For instance, solar energy production is influenced by sunlight intensity, cloud cover, and temperature [2]. Similarly, the amount of power that can be generated from wind is heavily dependent on wind speed and direction. To optimize the use of renewable energy sources, accurate forecasting of wind, solar, and battery state of charge is essential. This is made possible by advanced technologies that provide real-time data on these variables. The smart grid's communication capabilities allow sensors to transmit and receive data, continuously providing data packets to the grid. These packets contain crucial information related to energy generation, consumption, voltage, and frequency [2]. However, the battery management system in smart grids is vulnerable to cybersecurity risks due to the communication channels used to transmit charge status data. If these channels are compromised, overcharging or undercharging of batteries can occur, potentially rendering them useless [3]. Figure 1 illustrates the components of a power grid, which includes the various electrical support systems that ensure efficient operation.



Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

Figure 1: Components of a power grid that houses electrical support systems [2,3].

The traditional grid is very different from the smart grid as it offers good power quality, is self healing, cost effective by exploiting the renewable energy potentials, adaptive generation of power and an environmentally friendly operation. It likewise quantify the production of distributed energy sources, real time watching over vitality utilization at the client level, coordinating AI models for assignments mechanization, remote vitality checking, speedy harm location, and quick activity to imperfections. These are benefits that make the smart grids far more attractive than conventional grids. Complexity is one of the two main challenges, along with cybersecurity. The task of addressing vulnerabilities becomes more difficult when smart grid data is stored on the cloud [4]. Beyond physical security, cybersecurity is essential for maintaining the smart grid's reliability and safety. A study [5] highlights that older, non-smart grids are also vulnerable to cyberattacks, demonstrating how criminal software can manipulate various components of a power grid, including the CPU, GPU, hard drives, screen brightness, and even laser printers. The study suggests that such attacks could lead to the disruption of 2.5 to 9.8 million devices, potentially destabilizing the system. Further research [6] found that when an attacker gains control over an IoT botnet of high-power smart appliances, it can cause frequency instability, line failures, and increased operational costs. These attacks can manipulate energy consumption, leading to widespread shortages. As the complexity of the grid increases, so does the potential for problems. Power networks, already complex in nature, are undergoing significant changes due to the development of renewable energy sources, advanced signal processors, and sophisticated sensors. These changes are disrupting the industry, making it more vulnerable to issues. Given the current situation, it is crucial for electricity producers and consumers to exchange information bidirectionally. The traditional power infrastructure is being replaced by smart grids, which dynamically monitor and regulate energy flow to provide consistent electricity to customers [7]. Data from studies on smart grids are illustrated in Figure 2.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

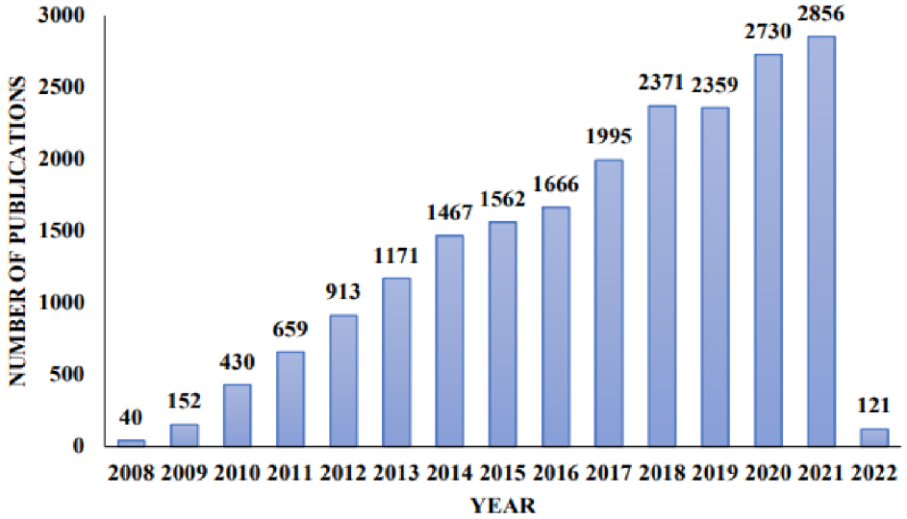


Figure 2. Publication statistics on SG [8].

Artificial intelligence encompasses various techniques, including machine learning, deep learning, data mining, evolutionary algorithms, fuzzy logic, and others. Among these, machine learning is gaining increasing attention from researchers for its role in detecting threats. In [9], the authors applied machine learning methods such as random forests, support vector machines, and neural networks to identify jamming attacks. Their experimental results demonstrated that the random forest approach performed exceptionally well. The authors also employed machine learning to detect social engineering attacks, utilizing unsupervised learning, which allows the system to recognize cyberattacks without prior knowledge of them. They examined accuracy, speed, and reliability of different machine learning models in their study. Their findings indicate that of other techniques, support vector machines have best performance as shown by computer simulations [10].

In [18], the authors use machine learning techniques to defend against brute force attacks imposed on the Secure Shell (SSH) protocol at the network layer. They made use of classifiers like K-Nearest Neighbors, Decision trees and Naive Bayes making use of which they were able to detect scalable detection models, which could be used for making predictions. Another study that the author of [11] contributes is also separated and inspired by the statistical and economic concept called 'First difference' which is an experiment. In order to create a classifier capable of identifying threats to network time synchronization, this approach was further used. It was found from the study that Artificial Neural Networks (ANNs) were more effective than traditional means in recognizing network security problems. The work also detects man in the middle (MITM) attacks using ANNs and achieved a high detection rate. [12] uses machine learning techniques so that hackers at smart grids are identified and removed, and simulations of it show that the method has a high detection rate. The same methods of deep learning have also been used to track cyberattacks on smart grids. As an example, [13] constructed two types of deep learning ensemble models of decision trees and a deep neural network respectively, through usage of ten fold crossover validation for testing purposes. The outcomes demonstrated that the suggested version surpassed acknowledged methods (random forests, AdaBoost, DNN) [14]. Another AI technique which has been explored for

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

detecting cyberattacks on smart grids is called Data mining. Previous research using data mining to detect false data injection (FDIA) attacks in smart grid was reviewed by the authors of [15]. Using data mining techniques, hidden patterns in large volume of data can be discovered and thus make crucial insights. In [16], the authors used the Common Path Mining technique to detect FDIA in their networks. This method classifies sequences as attacks if they match one of the predefined paths, each representing a unique series of vulnerabilities. Additionally, the authors of [17] applied a Casual Event Graph to detect FDIA in smart grids, training data mining algorithms on historical datasets. These techniques can be computationally efficient, even with large data volumes, aiding in the detection of FDIA. Fuzzy logic-based methods have also been developed for detecting network intrusions. For example, [18] introduced artificial immune systems using fuzzy logic to identify threats such as network flooding. Fuzzy logic is employed to distinguish between legitimate and illegal traffic, and it has been applied to identify jamming attacks. This method evaluates precise channel data, low packet ratios, and received signal intensity to determine if connection loss is caused by jamming. It is effective for both intermittent and persistent jamming scenarios. Fuzzy logic has also been integrated with other methods [19] for detecting various cyberattacks. Another AI-driven approach involves evolutionary algorithms, which are frequently used for optimization. Genetic algorithms, a prominent example of evolutionary algorithms, mimic natural selection processes. In [20], the authors proposed a genetic algorithm-based method for intrusion detection that uses two phases: training and detection. Their approach, which eliminates non-essential components from the detection process, proved effective for various network intrusions. The authors of [21] explored the potential of genetic algorithms in combination with other machine learning techniques to identify FDIA. Their simulation results indicated that genetic algorithms, along with three other machine learning methods, could effectively detect FDIA. Figure 3 illustrates various components of the smart grid.

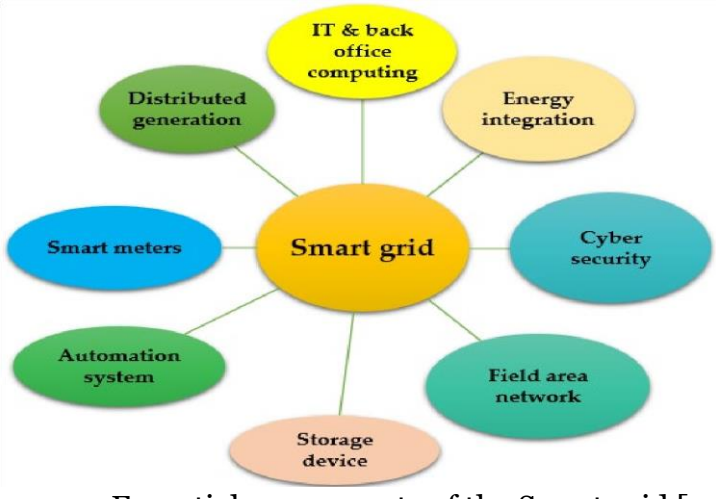


Figure 3. Essential components of the Smart grid [22].

Advanced Metering Infrastructure (AMI) plays a crucial role in the architecture of smart grids. The primary function of AMI is to measure the energy consumption of various integrated devices, such as solar panels, gas meters,

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

smart appliances, and water heaters. Within the AMI system, smart meters, data concentrators, and central systems continuously communicate with each other [23]. The Meter Data Management System (MDMS) receives information from electricity meters via the AMI host system and is responsible for organizing and analyzing the data sent by utility systems. By implementing AMI, utilities and service providers can reduce costs and enhance the quality of service [24]. Real time monitoring, measurement as well as analysis of data from power grid is an important need that was catered by the Supervisory Control and Data Acquisition (SCADA) system. SCADA provides reliable communication over a short as well as long distances leading to it to be fit for different installations [25]. This system includes three main components as the Human Machine Interface (HMI), the Master Terminal Unit (MTU), and the Remote Terminal Unit (RTU) [26]. Essentially, the RTU is made up of 3 elements: (1) the one which handles the data processing, (2) the one that carries out logic programs programmed by MTU, and (3) the one which configures the network [27]. The MTU plays an essential role in managing and monitoring the RTU, while the HMI provides the SCADA operator with a graphical user interface for system control. Demand-Side Management (DSM) is a key feature of the smart grid, focusing on regulating residential energy consumption. By balancing supply and demand, DSM helps improve the stability of power markets [28]. The benefits of DSM include enhanced short-term reliability, reduced peak-to-average demand ratios, lower consumer bills, and decreased production costs. Figure 4 illustrates the structure of the paper.

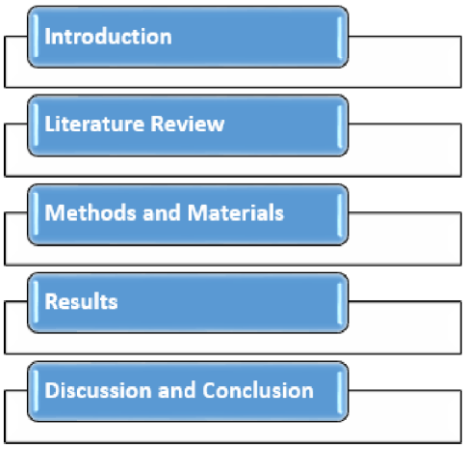


Figure 4. Structure of the paper.

Literature Review

In a multi-energy microgrid, there are many uncertainties regarding the interactions between renewable energy sources, power demand, and electricity transaction costs. To address this, a two-stage, mixed-integer, deterministic linear programming model has been developed. This model can be solved by linearizing the constraints and generating and reducing uncertain scenarios. The proposed method is tested on a microgrid using the IEEE 33-bus distribution network to manage energy from various sources [29]. As smart grids replace traditional electrical grids, ensuring system security has become a major challenge. However, if security is considered from the outset in both design and infrastructure, this issue can be addressed. Implementing robust cybersecurity

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

measures is therefore essential. The National Institute of Standards and Technology (NIST) initially identified confidentiality, integrity, and availability as the core principles of smart grid security [30]. However, the authors emphasize the importance of accountability in securing the smart grid, especially when unauthorized access to sensitive data occurs. Integrity ensures that data is transmitted without alteration or deletion, while availability guarantees that users can access the system's data when needed. Accountability ensures that actions within the system can be traced back to specific individuals, devices, or organizations. This is crucial for securing the grid, as it allows recorded data to be used as evidence in case of an attack, verifying the actions of each user, including administrators, and confirming the accuracy of data from each device. Therefore, applying the four principles—confidentiality, integrity, availability, and accountability—is the most effective way to protect smart grid systems. Smart grid networks are vulnerable to various attacks, primarily due to inadequate communication security. Artificial Intelligence (AI) plays a significant role in cybersecurity, particularly in areas such as machine learning, natural language processing, and robotic process automation, which are increasingly used in digital manufacturing. Cybersecurity has long leveraged similar techniques. For instance, machine learning has been used in filtering systems since the early 2000s. Over time, methods have evolved, and today's algorithms are capable of making more complex decisions. Recent advancements in AI have greatly enhanced the digital security of smart grids, improving defenses against various cyber threats. Machine learning is commonly applied in security (fraud and virus detection), privacy protection, business, and IT. Despite being largely unnoticed, AI helps organizations detect threats quickly, streamline response times, and ensure adherence to best security practices. While technologies like AI, 5G, and others hold promise for addressing these challenges, the energy sector must continue to invest in cybersecurity to stay ahead of cyberattacks. AI is also used for intrusion detection in computer networks and can track user identities if necessary. Figure 5 illustrates the relationship between AI and cybersecurity.

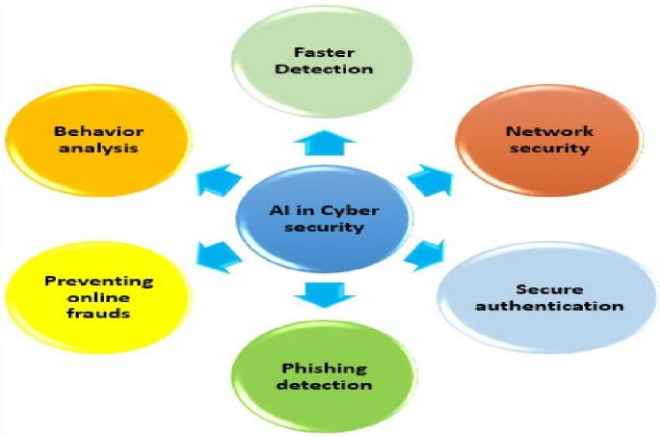


Figure 5. AI in Cybersecurity [31].

AI algorithms can detect irregularities such as infrequent database usage, frequent location changes, abnormal access times, and other anomalies. In contrast, machine learning simplifies the identification of data patterns that

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

facilitate automated learning. By leveraging knowledge of cyber threats, smart grid users can quickly and efficiently address issues. While current security systems are effective at detecting and preventing common threats, they struggle to keep pace with the increasing demand for cybersecurity. These methods are not equipped to handle zero-day vulnerabilities, which represent a slow, evolving type of cyberattack. Therefore, a more adaptive approach is needed to analyze datasets and uncover hidden security risks. Machine learning has proven to be highly effective in identifying previously unknown threats by utilizing adaptive baseline behavior models. The security landscape would be significantly transformed if predictive analytics and machine intelligence were integrated with both known and unknown datasets. Table 3 demonstrates how AI can be used to enhance security.

Jamming is one of the most common methods used to attack smart grids. An attacker can disrupt communication by emitting continuous or intermittent signals. Various types of jammers, including continuous, random, deceptive, and reactive jammers, can affect the operation of the smart grid network [32]. In "flow-jamming" attacks, multiple jammers are deployed across the network to slow down or block normal traffic flow, affecting the current network layer. Jamming can be a highly effective strategy, especially when used against a vulnerable system. In a centralized model, the jammer can be controlled to emit just enough power to disrupt a specific packet [33]. In contrast, in a decentralized jammer model, jammers collaborate with neighboring jammers to optimize their effectiveness. Spoofing attacks are another significant threat to smart grid networks. The list of attacks includes spoofing of MAC addresses, ARP addresses, GPS, identity, and data. A spoofing attack can compromise the security, reliability, stability, and operation of the network and thus have a threat to the integrity, confidentiality, and accountability of the smart grid. The attacks can happen from any of the following networks, data link and physical layers. In an injection attack, an attacker aims, for example, to control alteration, removal or new data injection in a network that in turn might influence the working of smart grid and lead to black out. This kind of cyber attack can lead to corrupted data, turn data integrity upside down and introduce malicious nodes in the network. In contrast to other attacks injection attacks can occur on any of these transport, network or data link layer. Flooding attacks are another form of cyberattack that can affect smart grid networks, limiting system access at the network or application layer. These attacks can overwhelm a system by forcing it to process fake messages, which consumes all its resources, and can prevent individual nodes from joining the network. Man-in-the-Middle (MITM) attacks also pose a significant threat to the smart grid. These attacks, which target the session and network layers, occur when an attacker positions themselves between two authorized devices and intercepts their communication. While the devices continue to communicate, the attacker secretly joins the conversation, altering the data or gaining unauthorized access to sensitive information [34]. These attacks can jeopardize the security and privacy of the network. Social engineering is another form of cyberattack that can target smart grid technology, typically affecting the application layer and posing risks to system privacy. The authors argue that social engineering represents one of the greatest threats to information security. Techniques such as robocalls, phone or window fraud, and reverse social engineering are used to deceive victims into revealing confidential

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

information. Such attacks expose individuals to the theft of personal data for impersonation or malicious purposes, undermining their sense of security. Listening attacks, a passive form of attack, also target communication routes in smart grids. These attacks, which affect the network layer, compromise the privacy of the smart grid by allowing a malicious user to eavesdrop on conversations between nodes in a local area network (LAN). The intercepted sensitive data can then be exploited to disrupt the network's security.

The physical and data link layers of a smart grid are common targets for timing-sensitive attacks (TSA). TSAs are capable of managing, monitoring, and safeguarding large regions as well as 3-phase measurement devices. Accurate synchronized measurements are essential for many smart grid applications, and most measuring instruments are now equipped with GPS for precise time synchronization. However, like other GPS-enabled devices, these instruments are vulnerable to spoofing attacks. Smart grids require rapid communication and control signals, which makes them more prone to cyberattacks such as GPS spoofing and time-sensitive access breaches. Using techniques like hybrid brute force, reverse brute force, and credential stuffing, attackers can compromise the presentation layer, session layer, or network layer. Figure 6 illustrates the classification of cyberattacks.

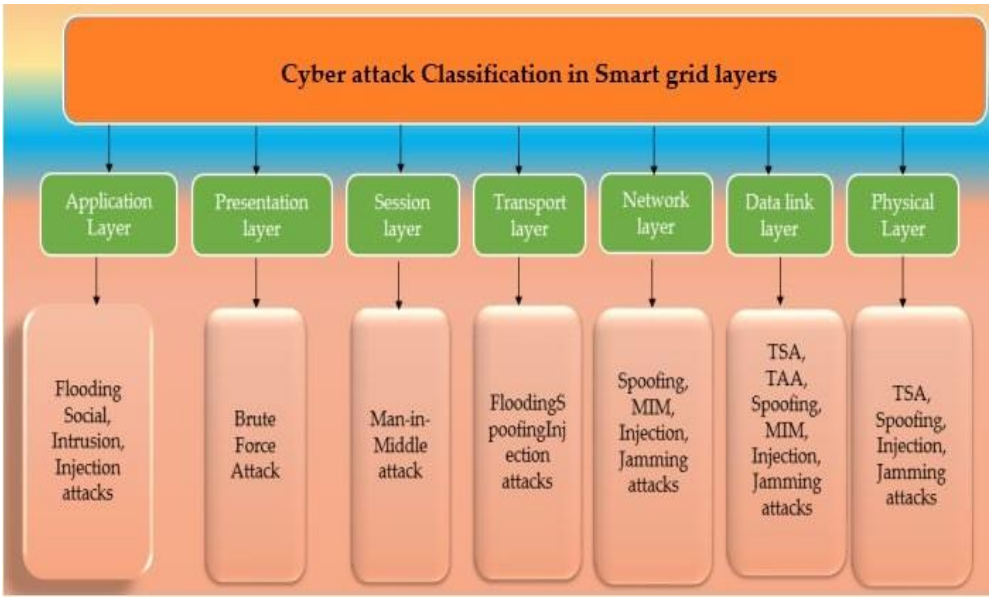


Figure 6. Cyber-Attack Classification Based on Communication Layers [35].

Methods and Materials

Research Method

In recent years, there has been a significant increase in research on IoT security, with many scholars showing growing interest in the topic. By utilizing AND/OR search operators, we were able to gather a large volume of relevant information on subjects such as "IoT," "Machine Learning," "Deep Learning," "threats," "cyberattacks," and "vulnerabilities." Additionally, we expanded our search to include terms like "blockchain," "healthcare," and "Data Mining" to explore potential solutions to the issue of IoT security breaches.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

Exclusion and Inclusion

Publications related to IoT and machine learning were identified using keyword strings and searched in databases such as IEEE, Springer, Scopus, Google Scholar, A.C.M., Science Direct, and Wiley. These studies cover topics like machine learning classification, IoT security, and the integration of health systems. Initially, only peer-reviewed papers, published after review, were selected for inclusion. This research focuses on exploring studies that highlight machine learning approaches to enhance IoT security. After the initial search, irrelevant papers were excluded, and only a select few articles were reviewed. The purpose of this review was to establish standards for machine learning research criteria and methodologies, and additional recommendations were not considered by the committee.

Objective of the Study

Our main objectives of the study are.
To know about the smart grid and its security issues.
To know about the different types of attacks on smart grid.
To know about the different methods to overcome these issues.
To know about the Open Issues, Challenges, and Future Research Directions.

Smart Grid Communication Challenges

Interference

For the smart grid to function properly, smart meters need to be installed in both homes and businesses. In modern households, the use of technology is becoming increasingly common, and Home Area Networks (H.A.N.s) are now nearly universal. In densely distributed environments, Network Area Controllers and smart meters may interact, potentially leading to inaccurate readings from the meters and jeopardizing the stability of the system. Additionally, power line harmonics could cause communication equipment on the smart grid to fail.

Transmission of Data Rate

The communication infrastructure of the smart grid is crucial for several reasons, including data collection and analysis, as well as sending instructions to the system's various nodes. However, the smart grid also depends on a large number of real-time sensors and smart meters, which together produce a significant amount of data that needs to be transmitted quickly while ensuring its accuracy. Moreover, a solid foundation for mutual understanding must be established. Therefore, the smart grid demands a network connection that is both reliable and secure.

Regulation

The electrical grid consists of various components that must work together efficiently. Specifically, the smart grid relies on the interaction of multiple factors, each fulfilling a unique role. A well-organized communication network is crucial for the successful operation of such a system. Consequently, there has been a global push to standardize and create universally accepted guidelines. This movement is backed by several organizations, including IEEE, the European Committee for Standardization, the American National Standards Institute, and the International Telecommunication Union.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

Results

Cyber-Attacks and Security Risks

It is common to observe various cyberattacks, including details about the attackers, the vulnerabilities they exploit, the security weaknesses they target, and the potential risks or consequences of these attacks. These are critical factors that must be taken into account. A security flaw occurs whenever there is a threat to the confidentiality, integrity, or availability of data, systems, or other resources. Each cybersecurity incident presents a unique risk to the systems and networks of individuals or organizations. Often referred to as "malware," this malicious software is specifically designed to damage a user's computer, server, or network. Malware can infiltrate a system by exploiting security vulnerabilities, such as when a user unknowingly installs spyware by opening a harmful attachment or visiting an infected website. In many cases, the user remains unaware that the malware is present. Malicious software can infiltrate systems in various ways. A user might be tricked into installing malware by downloading a fake file that appears legitimate, visiting a site known for spreading malware, or connecting to an infected device or system. Another example is when users visit malicious websites and are misled into installing harmful software. Any computing device is susceptible to being compromised by malicious software. Cyberattacks can target various systems, including process control systems like Supervisory Control and Data Acquisition (SCADA) systems, end-user devices, servers, and the hardware that connects them. Malicious software, much like the harm it causes, comes in different forms and types, such as bot programs, Trojan horses, spyware, viruses, ransomware, and worms. The harmful programs of these types continue to evolve and become more sophisticated. An area where the most cost effective strategy for long term security could be implemented is strong controls at system boundaries. An example of this technology is detection and prevention systems such as firewalls and antivirus software. They can use security barriers to build security barriers for restricting the user’s access to the protected internal resources. Nevertheless, with such protections in place, there exists some chance that the credentials may be misused by someone. The severity of such a misuse will dictate whether the organisation holds to its accountability policy by imposing consequences. Unfortunately, complete security measures, access controls and accountability systems under the genesys aren't always fool proof. The Internet of Things (IoT) is supposed to make things work together without humans in the loop to communicate with other things and other devices through the Internet. With the incorporation of IoT, it can detect and prevent issues like fires, break ins, overheating and allows doors to be automatically unlocked upon someone approaching. The Smart Workspace system is aimed to reinforce employees’ device utilization in the work place and is based on co usage of the on-hand AI chatbot and Telegram messengers. Also, it provides remote management for office technology. The chatbot can notify employees if a device can be turned on or off or remind them to activate the fan if the temperature rises too high. By enabling workers to control all office technology from a single internet-connected device, such as a smartphone or laptop, the Internet of Things (IoT) and artificial intelligence can help employees save time and reduce utility costs. Telegram Messenger, which is experiencing rapid growth, currently has 62 million active users, with 15 million daily active users and 1 million new

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

users joining each week. Since Telegram can be used with or without a smartphone and is accessible through a web browser, many people use it daily to communicate with family, friends, and colleagues.

The term "smart grid" refers to a power system that incorporates sensing technologies, communication, digital control, information technology, and other field equipment to optimize its operations, enhancing both the efficiency and responsiveness of the power grid. The Internet of Things (IoT), particularly Wireless Sensor Networks (WSN), can be used to monitor and measure the performance of Photovoltaic Generation Systems. In agriculture, IoT is applied to identify optimal farming locations, ensuring that the appropriate crops are planted. In healthcare, IoT is used to monitor heart rates. Additionally, IoT technology can be used to develop smart door locks through Mobile Backend as a Service and create home automation and security systems using Low-Cost Real-Time solutions, such as the ESP8266, an affordable and simple IoT device. Neuro-fuzzy systems have attracted significant interest from researchers across various fields due to their enhanced learning and reasoning abilities. These systems integrate the use of fuzzy inference systems to represent implicit information with the learning ability of artificial neural networks that learn from experience. Since computers are very complex, it is necessary to develop them at great speed and precision; thus, soft computing techniques have been proposed for modeling, predicting and controlling dynamic nonlinear systems. Examples of soft computing techniques are fuzzy logic systems and artificial neural networks. These two approaches are starting to be integrated between different research and engineering fields to deal with complex challenges. The use of fuzzy logic increases tremendously an intelligent machine's ability to reason and make conclusion based on that; it represents qualitative and usually imprecise data and permits expression in symbolic form in machine learning. They are used because they can learn, they are reliable and because they can process information in a parallel manner. Due to its ability to represent knowledge and to learn on its own, the neuro fuzzy system constitutes an excellent starting point for solution of machine learning problems.

Among all the approaches to model nonlinear dynamic systems, the Takagi-Sugeno-Kang (TSK) fuzzy inference is the most effective one. The concept of learning the model of TSK system as a "multimodal" technique is that linear submodels were utilized to describe the behavior of the overall complex nonlinear dynamic system. ANFIS is one of the most popular neurofuzzy techniques that has been used in many applications such as regression, model, forecasting and control. ANFIS employs a TSK-type fuzzy inference system within a 5-layer network structure. Its two types of parameters are premise and consequence. The relationships between these two sets of variables are described as fuzzy if-then rules. The biggest disadvantage of ANFIS is that it is a computationally intensive model, and even it has been found to generate highly complex models for relatively simple problems. Recently, due to the advancement in learning algorithms, as well as the network architecture, the accuracy and training time of standard neurofuzzy network have been significantly improved. For a neuro-fuzzy system to perform effectively, it should possess certain characteristics: it must be capable of rapid learning, adapt in real-time, continuously optimize itself to minimize global error, and require minimal computational resources. However, due to the use of hybrid techniques for

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

continuous improvement, many neuro-fuzzy inference systems tend to have longer learning times. In some cases, manual adjustment of certain parameters may be necessary. On the other hand, diffusion learning methods are prone to causing overfitting and local minima. In these methods, input weights and hidden layer biases are randomly selected and can be considered part of a linear system, while the output weights of Extreme Learning Machines (ELM) are determined through a simple generalized inverse operation, as opposed to using conventional methods. Since most Cyber-Physical Systems (CPSGs) rely on wireless communication, these channels are vulnerable to attacks. Information technology attacks refer to those that restrict access to data. Classical complex attacks typically target communication networks, such as cognitive radio networks and mobile ad hoc networks. These attacks disrupt the network by blocking trusted routing and exploiting infected insider nodes, leading to slower performance. A compromised sensing node may provide false channel sensing data following an attack, benefiting the attacker while harming more reliable nodes. Complex attacks are typically used by adversaries for two main purposes. The first goal is to cause disruption, where dishonest individuals falsely claim a channel is idle when it is actually in use. The second goal is exploitation, where attackers make it appear that a channel is unoccupied in order to monopolize it. Attackers can enhance the effectiveness of their attacks by prioritizing these objectives. The flaw in the Aurora generator was discovered by the Idaho National Laboratory, where an attacker uses a series of improper control commands to attempt to open and close the circuit breaker on a generator in this type of attack. Interruptions refer to the disconnection of a generator from the utility grid. When the system and generator become unsynchronized, the safety mechanism can activate. The goal of the Aurora Attack is to cause the circuit breaker to reclose. This attack manipulates the generator's electrical output and rotational speed, leading to physical damage. This occurs because the safety features of the generator are deliberately delayed to prevent accidental tripping. Closing the circuit breakers in this scenario can damage the generator due to the frequency and phase angle mismatch between the generator and the main grid. The vulnerability of specific circuit breakers to Aurora attacks can be assessed using a scoring method based on vulnerability rating variables. Further modeling and research on the impact of an Aurora attack on the PCC and synchronous generator breakers of the microgrid are discussed in [36]. Sync-check relays, once used to protect against Aurora attacks, are no longer allowed under the IEEE 1547 Standard due to their potential to unintentionally isolate a microgrid. The authors demonstrated that tripping a microgrid's main circuit breaker could damage the synchronous generator. Recently, the retail sector has placed greater focus on demand-response technology, which can improve the performance of the electrical grid. At its core, demand-response is an incentive-based control system where incentives are delivered through command signals. In [37], a simulation was conducted to demonstrate an attacker aiming to widen the gap between production and consumption by compromising the transmission channel and altering market prices through an attack time series, making the attack much more powerful. This type of attack differs from one-time assaults, where malicious code is inserted only once. In [38], the authors examined attacks that could inject false pricing information at any point over an extended period. Repeated attacks can create power imbalances, leading to overproduction,

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

financial losses, and poor power quality. The authors quantified the damage caused by these repeated attacks using a technique called "sensitivity analysis." To analyze the system's behavior over time, they employed a sensitivity function based on the z-transform. [39] explored challenges related to energy-exchange systems, where controllers in the end-user network quickly receive price signals from the active market and rapidly transmit bid information back to the controllers. Hackers can access the data exchanged between a prosumer and a market agent. The pricing attack was exacerbated by the insertion of false prices and quantities from prosumers through malware, causing fluctuations in the market clearing price, varying energy usage by each prosumer, and a decrease in overall demand on distribution feeders. Figure 7 shows the different types of attacks on the smart grid.

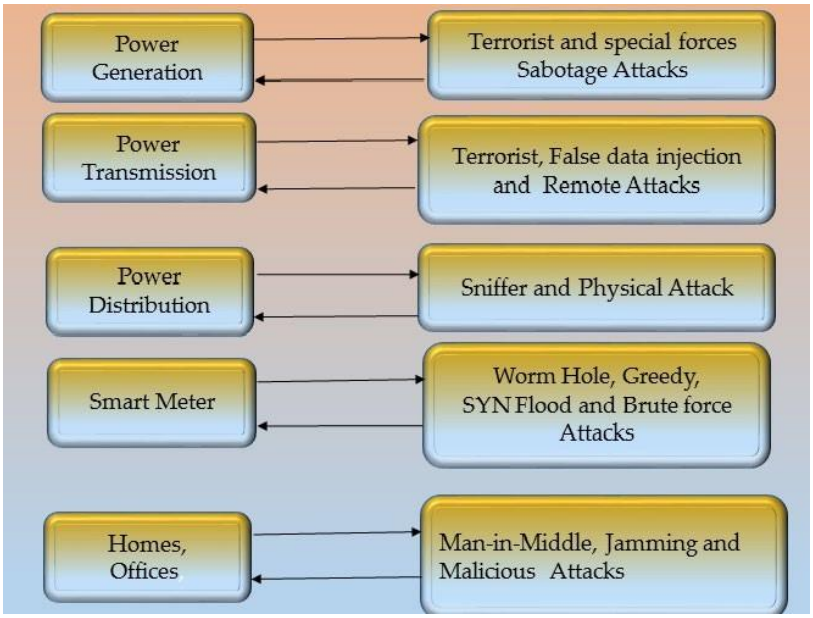


Figure 7: The possible attacks on the smart grid [40].

ML and DL Algorithms for Cybersecurity

One of the most effective ways to address the limitations of traditional cybersecurity methods is through the use of machine learning and deep learning algorithms. These approaches are capable of detecting intrusions targeting the network in question. Machine learning is increasingly viewed as a crucial component of cybersecurity, as it can be applied for both offensive and defensive purposes. One such study [41] explored various machine learning techniques for identifying security vulnerabilities in IT systems. These methods included random forests, support vector machines, naive Bayes, decision trees, artificial neural networks, and deep belief networks. The study primarily focused on three key security challenges: intrusions, spam, and malware.

Support Vector Machine Support Vector Machine

The use of Support Vector Machines (SVM) enhances machine learning capabilities. It has been demonstrated that SVM improves the performance of various cybersecurity applications. However, SVM is not commonly used in real-time applications due to its high resource requirements. By applying kernel

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

transformations to the data, SVM identifies the optimal separation between samples. The SVM method uses kernels to process data and find the best boundary between different sets. In [42], the authors developed a model that combines deep feature extraction with multi-layer support vector machines to detect abnormal behavior in large volumes of network traffic data, thereby ensuring the security of distributed networks.

K-Nearest Neighbor

The K-Nearest Neighbor (KNN) method evaluates the similarity or dissimilarity between two classes based on the distance between them in a dataset. This is mainly because KNN does not make any assumption, and it can adjust easily to the different types of data that currently exist compared to other machine learning algorithms. The supervised learning technique is a decision tree where it helps in predicting model output by using a labeled dataset correctly. It is a type of supervised learning, which is also known as decision trees, in which it uses labeled data to make accurate predictions. The flowchart structure of decision tree method is similar. In the processing of the large scale cybersecurity dataset (UGR'16) for improving anomaly detection preparation it used decision tree and multilayer perceptron.

Deep Belief Network

According to the description, a deep belief network can be thought of as comprised of multiple layers of which each can be a restricted Boltzmann machine. The advantage of this approach is that it can be used when large databases need to be processed in cybersecurity applications. The authors did a thorough review of back usage of deep belief networks and other deep learning techniques in cybersecurity. In [43], the authors also tested the performance of a deep belief network using the NSL KDD dataset for face recognition, pedestrian detection, intrusion detection tasks and compared it with a region extreme learning machine technique. In [44], the design of deep neural network based on traffic and payload parameters has been developed to facilitate network performance monitoring. This was made for specifically identifying the hacker behavior in the SCADA.

Recurrent Neural Networks

The recurrent neural network (RNN) is distinguished from other neural networks by its directed graph structure. RNNs generate bidirectional signals and extend the network through loops. While RNNs typically take longer to process than feed-forward neural networks, making them less suitable for real-time applications, they have been used to enhance the accuracy of intrusion detection systems that rely on datasets. In [45], a novel artificial intelligence-based method was developed to address the issue of improper data injection in DC microgrids. Researchers utilized renewable energy sources (RESs) and a nonlinear auto-regressive external model (NARX) to predict DC voltages and currents. NARX aims to improve network performance in terms of speed, accuracy, and ease of understanding, compared to traditional RNNs [46].

Convolutional Neural Networks

Convolutional Neural Networks (CNNs) stand out from other deep learning

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

algorithms because they can learn directly from raw data, eliminating the need for data extraction, which is typically performed before model training. CNNs often incorporate hidden networks, pooling networks, convolutional networks, and fully-connected networks. In the realm of cybersecurity, there is no single dominant CNN approach. However, the numerous security and privacy challenges faced by organizations have led to the development of various CNN-based methods. For example, CNNs have been used to create a multiclass classification model for IoT networks as part of an advanced technique for detecting abnormal intrusions, helping to identify potential threats. In this method was applied to detect cyber-attacks on industrial control systems, creating a scaled-down version of a broad range of industrial water treatment facilities. In CNNs were used to recognize DoS attacks on IoT networks, while a different deep CNN approach was proposed for malware detection [47]. CNNs also allow for efficient use on GPUs, and a multi-CNN fusion technique was introduced to detect intrusion attacks on industrial IoT networks [48]. Figure 8 shows the supervised learning process.

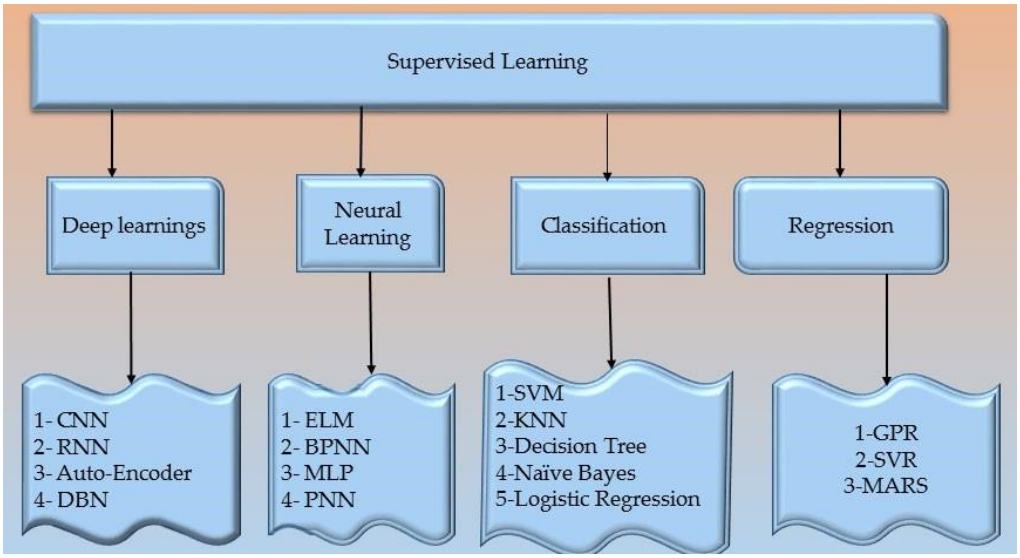


Figure 8. Supervised learning techniques in the smart grid.

Blockchain-Based Detection and Mitigation

The authors of [49] examined each publication released between 2016 and 2022 that specifically addresses protective measures for blockchain-based systems. Bitcoin, the first cryptocurrency built on a blockchain, was introduced in 2008, while Ethereum, the first blockchain-based cryptocurrency with smart contracts, debuted in 2015. Another application of blockchain technology is in public blockchain projects. Although blockchain technology was originally associated with the virtual currency Bitcoin, recent research suggests it has a wide range of potential uses. According to [50], further investigation was conducted to explore how blockchain technology could enhance cybersecurity. The authors explored various solutions to address security issues within blockchain systems. To mitigate the risk of cybercrime, a web-based cybersecurity awareness platform

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

was developed. The proposed method utilizes blockchain technology to ensure software security against hackers. It has been demonstrated that blockchain technology, with its security features, can be used to develop a data-transfer system with an object-categorization algorithm. Blockchain, a type of distributed ledger technology, has recently become one of the most valuable tools across various industries. Each block on the blockchain contains data, an index, a timestamp, a hash, and the hash of the previous block. Many experts believe that a block cipher is the foundation of blockchain's reliability. If the hash value of one block changes, all subsequent blocks in the chain must also be modified, which is typically time-consuming and costly to accomplish on a computer. According to the authors of [51], blockchain technology should be used to create a policy architecture for data flow between autonomous system operations and agents that are not performing their tasks. These measures were taken to address the FDIA (False Data Injection Attack). The model consists of three components: "data," "detection," and "blockchain." Figure 11 illustrates the applications of blockchain.

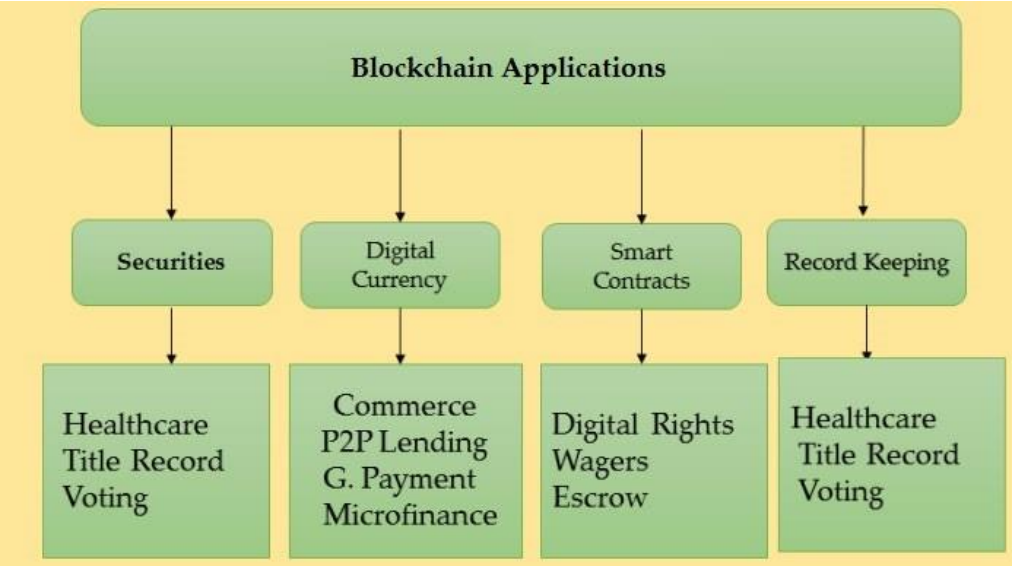


Figure 11. The blockchain Applications.

The data layer collects information and sends it to the detection layer for community detection. The blockchain layer ensures the security of both the community detection process and transaction records. In their study, the authors developed a blockchain-based system that enables encrypted communication between smart meters and service providers. This approach prevents FDIA from occurring on the smart meter side. In this research, smart meters act as controller nodes, initiating all interactions with the service provider. Data is shared and verified across the network by auditing and broadcasting transactions. Service providers communicate with each other using a peer-to-peer (P2P) network. A new transaction or block cannot be added until consensus is reached, and only after that can the new block be incorporated. Each transaction generates a unique key using the SHA-256 algorithm. In this research, the authors demonstrated that a blockchain-based framework could enhance data transmission and reception within a P2P service provider network.

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

The study [52] introduced a decentralized security model utilizing smart contracts and the lightning network within a blockchain environment. This method includes various processes such as registration, scheduling, verification, and payment. In [53], the authors developed a product power system device design that combines hardware security with a blockchain-based approach to maintain a distributed security mechanism that verifies the origin of incoming communications. Table 8 illustrates the blockchain-based detection and mitigation methods.

Hardware-Based Security

The smart grid system is ineffective without devices that connect to the internet. These devices, which collect, process, and transmit data over the network, must be resilient to cyberattacks. In [54], the authors highlighted some of the most significant hardware security challenges. Security vulnerabilities can emerge in various forms, including physical attacks, hardware Trojans, and side-channel attacks. During a physical attack, the attacker aims to avoid detection by the authentication process. System weaknesses are exploited through reverse engineering to plan the attack. Using side-channel analysis, an attacker can uncover cryptographic keys by examining various factors such as current, voltage, and frequency. Hardware Trojans refer to intentional modifications or additions to a circuit, which can steal sensitive information, alter the circuitry, or reduce the system's reliability. The authors suggest that path delay fingerprinting can be used to detect hardware Trojans. IoT devices such as smart meters, sensors, and communication devices face the challenge of balancing energy consumption with power efficiency. Physical Unclonable Functions (PUFs) are ideal for low-power IoT devices because they enable secure authentication without requiring cryptographic expertise. However, with advancements in machine learning, it is now possible to predict PUF behavior with 95% accuracy by analyzing historical data and events. To protect PUFs from machine learning-based attacks, the authors of the study [55] introduced the Configurable Tristate PUF (CTPUF), which uses an XOR-based approach to obscure the relationship between the challenge and the response. This makes it difficult for machine learning models to detect consistent patterns between challenges and responses in chaotic environments. The study's findings indicated that machine learning models, including support vector machines, artificial neural networks, and logistic regression, achieved around 60% accuracy when using CTPUF. Another study [56] employed machine learning models to highlight the vulnerabilities of voltage-over-scaling (VOS)-based authentication. The researchers proposed a VOS technique resistant to machine learning attacks by combining previous challenges with keys. The results showed that when the challenge self-obfuscation structure was applied, the machine learning model's accuracy dropped to approximately 51.2%.

Future Work

While this paper explores the potential of integrating Artificial Intelligence (AI) and Blockchain into Pakistan’s energy sector, several areas warrant further investigation and development:

Dialogue Social Science Review (DSSR)
www.thedssr.com

ISSN Online: 3007-3154
ISSN Print: 3007-3146

DIALOGUE SOCIAL SCIENCE REVIEW

Vol. 3 No. 3 (March) (2025)

Pilot Projects and Real-World Implementation
Future work should focus on designing and executing pilot projects to test the integration of AI and Blockchain in Pakistan's existing energy infrastructure. These pilot projects can provide valuable insights into the technical, economic, and social impacts of these technologies and help identify real-world challenges in the local context.

Scalability and Interoperability Studies
As AI and Blockchain technologies are implemented, research on the scalability of these solutions to larger, more complex grid systems will be essential. Additionally, ensuring interoperability between new smart grid technologies and Pakistan's current infrastructure will require in-depth studies and development.

AI-Driven Energy Forecasting Models
Future research can enhance AI-based predictive models for more accurate energy demand forecasting and optimization. Incorporating more granular data from various sources such as weather forecasts, energy consumption patterns, and renewable energy production could improve the efficiency and reliability of the grid.

Blockchain-based Regulatory Framework
Future work could focus on developing a Blockchain-based regulatory framework that automates compliance, reporting, and energy trading within Pakistan's energy market. This would streamline processes and enhance transparency, enabling seamless integration of decentralized energy trading systems.

Addressing Policy and Regulatory Challenges
Further research is needed to understand the specific policy and regulatory challenges associated with adopting AI and Blockchain technologies in Pakistan's energy sector. This could involve proposing new policies or regulations to facilitate the safe and effective integration of these technologies while ensuring they align with global standards.

Capacity Building and Skill Development
Future work could focus on developing training programs to enhance the technical capabilities of Pakistan's workforce. This includes building expertise in AI, Blockchain, and smart grid technologies to ensure the sustainable and long-term adoption of these innovations.

Integration with Distributed Energy Resources (DERs)
As distributed energy resources such as solar panels, wind turbines, and battery storage systems become more prevalent, future research could explore how AI and Blockchain can be used to integrate these systems into smart grids effectively. This would enable better management of renewable energy sources and reduce reliance on traditional energy sources.

Evaluation of Environmental Impact
An important area for future work is assessing the environmental impact of deploying AI and Blockchain-based smart grids in Pakistan. Research could

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 3 (March) (2025)

explore how these technologies can further reduce the carbon footprint of the energy sector and contribute to Pakistan's climate goals.

Global Collaboration and Knowledge Sharing

Lastly, fostering global collaboration and knowledge-sharing through partnerships with international organizations, energy experts, and academic institutions will be crucial. Future work could focus on creating a global network to share best practices, technologies, and lessons learned from the deployment of AI and Blockchain in other energy sectors.

Conclusion

The integration of Artificial Intelligence (AI) and Blockchain technologies holds immense potential for revolutionizing Pakistan's energy sector, particularly in the context of smart grid development. By leveraging AI for predictive maintenance, load forecasting, and renewable energy integration, and utilizing Blockchain for secure, transparent energy transactions, these technologies can address the critical challenges faced by the country's energy infrastructure. AI can enhance grid efficiency and reliability, while Blockchain can facilitate decentralized energy trading, improve transparency, and reduce inefficiencies. While the promise of these technologies is significant, successful deployment in Pakistan's energy sector will require overcoming several challenges. These include addressing technological infrastructure gaps, navigating regulatory hurdles, and building a skilled workforce capable of managing and implementing these advanced systems. However, the potential benefits—including operational cost reductions, improved sustainability, and increased energy security—make the integration of AI and Blockchain a compelling opportunity. Through an examination of global case studies and tailored solutions for Pakistan's unique context, this paper has outlined a pathway for the integration of these transformative technologies. With concerted efforts from the government, energy providers, and technological experts, Pakistan can lead the way in adopting innovative energy solutions, contributing not only to its own energy security but also to global sustainability goals. Ultimately, the successful deployment of AI and Blockchain in Pakistan's smart grids could serve as a model for other developing nations, demonstrating how cutting-edge technologies can create a more efficient, sustainable, and secure energy future.

References

Ding, J., Qammar, A., Zhang, Z., Karim, A., & Ning, H. (2022). Cyber threats to smart grids: Review, taxonomy, potential solutions, and future directions. *Energies*, *15*(18), 6799.

Mololoth, V. K., Saguna, S., & Åhlund, C. (2023). Blockchain and machine learning for future smart grids: A review. *Energies*, *16*(1), 528.

Moreno-Munoz, A., Bellido-Outeirino, F. J., Siano, P., & Gomez-Nieto, M. A. (2016). Mobile social media for smart grids customer engagement: Emerging trends and challenges. *Renewable and Sustainable Energy Reviews*, *53*, 1611-1616.

Abrahamsen, F. E., Ai, Y., & Cheffena, M. (2021). Communication technologies for smart grid: A comprehensive survey. *Sensors*, *21*(23), 8087.

Ugwu, J., Odo, K. C., Ohanu, C. P., García, J., & Georgious, R. (2022).

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Vol. 3 No. 3 (March) (2025)

Comprehensive review of renewable energy communication modeling for smart systems. *Energies*, *16*(1), 409.

Jaiswal, D. M., & Thakre, M. P. (2022). Modeling & designing of smart energy meter for smart grid applications. *Global Transitions Proceedings*, *3*(1), 311-316.

Kim, Y., Hakak, S., & Ghorbani, A. (2023). Smart grid security: Attacks and defence techniques. *IET Smart Grid*, *6*(2), 103-123.

Appasani, B., Mishra, S. K., Jha, A. V., Mishra, S. K., Enescu, F. M., Sorlei, I. S., ... & Bizon, N. (2022). Blockchain-enabled smart grid applications: Architecture, challenges, and solutions. *Sustainability*, *14*(14), 8801.

Mollah, M. B., Zhao, J., Niyato, D., Lam, K. Y., Zhang, X., Ghias, A. M., ... & Yang, L. (2020). Blockchain for future smart grid: A comprehensive survey. *IEEE Internet of Things journal*, *8*(1), 18-43.

Takiddin, A., Ismail, M., Zafar, U., & Serpedin, E. (2022). Deep autoencoder-based anomaly detection of electricity theft cyberattacks in smart grids. *IEEE Systems Journal*, *16*(3), 4106-4117.

Abed, A. K., & Anupam, A. (2023). Review of security issues in Internet of Things and artificial intelligence-driven solutions. *Security and Privacy*, *6*(3), e285.

Vatsyayan, V., Chakraborty, A., Rajarajan, G., & Fernandez, A. L. (2022). A detailed investigation of popular attacks on cyber physical systems. In *Cyber Security Applications for Industry 4.0* (pp. 1-42). Chapman and Hall/CRC.

Ghiasi, M., Niknam, T., Wang, Z., Mehrandezh, M., Dehghani, M., & Ghadimi, N. (2023). A comprehensive review of cyber-attacks and defense mechanisms for improving security in smart grid energy systems: Past, present and future. *Electric Power Systems Research*, *215*, 108975.

Khoei, T. T., Slimane, H. O., & Kaabouch, N. (2022). A comprehensive survey on the cyber-security of smart grids: Cyber-attacks, detection, countermeasure techniques, and future directions. *arXiv preprint arXiv:2207.07738*.

Zeng, H., Ng, Z. W., Zhou, P., Lou, X., Yau, D. K., & Winslett, M. (2022, October). Detecting cyber attacks in smart grids with massive unlabeled sensing data. In *2022 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)* (pp. 1-7). IEEE.

Berghout, T., Benbouzid, M., & Muyeen, S. M. (2022). Machine learning for cybersecurity in smart grids: A comprehensive review-based study on methods, solutions, and prospects. *International Journal of Critical Infrastructure Protection*, *38*, 100547.

Shah, S. F. A., Iqbal, M., Aziz, Z., Rana, T. A., Khalid, A., Cheah, Y. N., & Arif, M. (2022). The role of machine learning and the internet of things in smart buildings for energy efficiency. *Applied Sciences*, *12*(15), 7882.

Luo, J. (2022). A bibliometric review on artificial intelligence for smart buildings. *Sustainability*, *14*(16), 10230.

Mazhar, T., Irfan, H. M., Haq, I., Ullah, I., Ashraf, M., Shloul, T. A., ... & Elkamchouchi, D. H. (2023). Analysis of challenges and solutions of IoT in smart grids using AI and machine learning techniques: A review. *Electronics*, *12*(1), 242.

Zamponi, M. E., & Barbierato, E. (2022). The dual role of artificial intelligence in

ISSN Online: 3007-3154
ISSN Print: 3007-3146

developing smart cities. *Smart Cities*, *5*(2), 728-755.

Aguilar, J., Garces-Jimenez, A., R-moreno, M. D., & García, R. (2021). A systematic literature review on the use of artificial intelligence in energy self-management in smart buildings. *Renewable and Sustainable Energy Reviews*, *151*, 111530.

Yılmaz, Y., & Uludag, S. (2021). Timely detection and mitigation of IoT-based cyberattacks in the smart grid. *Journal of the Franklin Institute*, *358*(1), 172-192.

Farrukh, Y. A., Ahmad, Z., Khan, I., & Elavarasan, R. M. (2021, November). A sequential supervised machine learning approach for cyber attack detection in a smart grid system. In *2021 North American Power Symposium (NAPS)* (pp. 1-6). IEEE.

Haque, N. I., Shahriar, M. H., Dastgir, M. G., Debnath, A., Parvez, I., Sarwat, A., & Rahman, M. A. (2020). Machine learning in generation, detection, and mitigation of cyberattacks in smart grid: A survey. *arXiv preprint arXiv:2010.00661*.

Gumaei, A., Hassan, M. M., Huda, S., Hassan, M. R., Camacho, D., Del Ser, J., & Fortino, G. (2020). A robust cyberattack detection approach using optimal features of SCADA power systems in smart grids. *Applied Soft Computing*, *96*, 106658.

Khazaei, J., & Amini, M. H. (2021). Protection of large-scale smart grids against false data injection cyberattacks leading to blackouts. *International Journal of Critical Infrastructure Protection*, *35*, 100457.

Bertone, F., Lubrano, F., & Goga, K. (2020). Artificial intelligence techniques to prevent cyber attacks on smart grids. *Annals of Disaster Risk Sciences: ADRS*, *3*(1), 0-0.

Deepa, N., Pham, Q. V., Nguyen, D. C., Bhattacharya, S., Prabadevi, B., Gadekallu, T. R., ... & Pathirana, P. N. (2022). A survey on blockchain for big data: Approaches, opportunities, and future directions. *Future Generation Computer Systems*, *131*, 209-226.

Tufail, S., Batool, S., & Sarwat, A. I. (2021, March). False data injection impact analysis in ai-based smart grid. In *SoutheastCon 2021* (pp. 01-07). IEEE.

Acharya, S., Dvorkin, Y., & Karri, R. (2021). Causative cyberattacks on online learning-based automated demand response systems. *IEEE transactions on smart grid*, *12*(4), 3548-3559.

Kumari, A., Patel, R. K., Sukharamwala, U. C., Tanwar, S., Raboaca, M. S., Saad, A., & Tolba, A. (2022). AI-empowered attack detection and prevention scheme for smart grid system. *Mathematics*, *10*(16), 2852.

Yamin, M. M., Ullah, M., Ullah, H., & Katt, B. (2021). Weaponized AI for cyber attacks. *Journal of Information Security and Applications*, *57*, 102722.

Li, Y., & Yan, J. (2022). Cybersecurity of smart inverters in the smart grid: A survey. *IEEE Transactions on Power Electronics*, *38*(2), 2364-2383.

De Dutta, S., & Prasad, R. (2020, October). Cybersecurity for microgrid. In *2020 23rd International Symposium on Wireless Personal Multimedia Communications (WPMC)* (pp. 1-5). IEEE.

Makala, B., & Bakovic, T. (2020). Artificial intelligence in the power sector. *International Finance Corporation: Washington, DC, USA*.

Franki, V., Majnarić, D., & Višković, A. (2023). A comprehensive review of artificial intelligence (AI) companies in the power sector. *Energies*, *16*(3),

ISSN Online: 3007-3154
ISSN Print: 3007-3146

1077.

Mhlanga, D. (2023). Artificial intelligence and machine learning in the power sector. In *FinTech and artificial intelligence for sustainable development: The role of smart technologies in achieving development goals* (pp. 241-261). Cham: Springer Nature Switzerland.

Szczepaniuk, H., & Szczepaniuk, E. K. (2022). Applications of artificial intelligence algorithms in the energy sector. *Energies*, *16*(1), 347.

Szczepaniuk, H., & Szczepaniuk, E. K. (2022). Applications of artificial intelligence algorithms in the energy sector. *Energies*, *16*(1), 347.

Raihan, A. (2023). A comprehensive review of artificial intelligence and machine learning applications in energy sector. *Journal of Technology Innovations and Energy*, *2*(4), 1-26.

Cherepovitsyna, A. (2023). Artificial intelligence in the energy sector. In *Handbook of Research on Artificial Intelligence, Innovation and Entrepreneurship* (pp. 173-187). Edward Elgar Publishing.

Oum, K. R. (2022). Artificial intelligence and energy sector. *Impact of Artificial Intelligence on Organizational Transformation*, 123-129.

Ashraf, W. M., Uddin, G. M., Tariq, R., Ahmed, A., Farhan, M., Nazeer, M. A., ... & Dua, V. (2023). Artificial intelligence modeling-based optimization of an industrial-scale steam turbine for moving toward net-zero in the energy sector. *ACS omega*, *8*(24), 21709-21725.

Rizvi, S. M. A., & Jamal, T. A STUDY OF ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING (ML) IN POWER SECTOR: AN ANALYSIS.

Patel, S., Pandey, P., Gautam, A., Shukla, G., & Makwana, A. (2024). Use of Artificial Intelligence (AI) in Power Sector to enhance Safety and Performance. *International Journal of Research and Analytical Reviews, IJRAR*, *11*(2).

Cheng, L., & Yu, T. (2019). A new generation of AI: A review and perspective on machine learning technologies applied to smart energy and electric power systems. *International Journal of Energy Research*, *43*(6), 1928-1973.

Manoharan, G., Ashtikar, S. P., & Nivedha, M. (2024). Harnessing the power of artificial intelligence in reinventing the manufacturing sector. In *Using Real-Time Data and AI for Thrust Manufacturing* (pp. 113-137). IGI Global.

Franki, V., Majnarić, D., & Višković, A. (2023). *A Comprehensive Review of Artificial Intelligence (AI) Companies in the Power Sector*. *Energies 2023, 16, 1077*.

Ahmad, T., Zhang, D., Huang, C., Zhang, H., Dai, N., Song, Y., & Chen, H. (2021). Artificial intelligence in sustainable energy industry: Status Quo, challenges and opportunities. *Journal of Cleaner Production*, *289*, 125834.

Espina-Romero, L., Noroño Sánchez, J. G., Gutiérrez Hurtado, H., Dworaczek Conde, H., Solier Castro, Y., Cervera Cajo, L. E., & Rio Corredoira, J. (2023). Which industrial sectors are affected by artificial intelligence? A bibliometric analysis of trends and Perspectives. *Sustainability*, *15*(16), 12176.

Razak, A., Nayak, M. P., Manoharan, G., Durai, S., Rajesh, G. A., Rao, C. B., & Ashtikar, S. P. (2023). Reigniting the power of artificial intelligence in education sector for the educators and students competence. In *Artificial Intelligence and Machine Learning in Smart City Planning* (pp. 103-116).

ISSN Online: 3007-3154
ISSN Print: 3007-3146

Elsevier.

Anagnoste, S. (2018). The road to intelligent automation in the energy sector. *Management Dynamics in the Knowledge Economy*, *6*(3), 489-502.

Ashraf, W. M., Arafat, S. M., Niazi, S. G., Farooq, M., Riaz, F., Hayat, N., & Uddin, G. M. (2021, March). Artificial intelligence as an operation excellence tool for the power sector. In *book of abstracts* (p. 337).

Sharma, A., Tyagi, R., Verma, A., & Paul, A. (2022). Review on Digitalisation and Artificial Intelligence in human Resource function of Energy sector. *Water and Energy International*, *65*(2), 38-46.

Mobayo, J. O., Aribisala, A. F., Yusuf, S. O., & Belgore, U. (2021). The awareness and adoption of artificial intelligence for effective facilities management in the energy sector. *Journal of Digital Food, Energy & Water Systems*, *2*(2).

Barykina, Y. N., Zakharov, S. V., Yuan, J., Ibragimova, A. V., & Fan, X. (2023). Applications of artificial intelligence methods in the energy sector. In *BIO Web of Conferences* (Vol. 71, p. 02010). EDP Sciences.