

Deep Learning and Blockchain for Smart Grids: Integration, Challenges, and Future Directions

*Ilham Husam Hasan Albakry¹, Haider TH. Salim ALRikabi*¹, Faisal T. Abed¹, and Hawraa Hussain Jabor¹*

¹Wasit University, College of Engineering, Electrical Engineering Department, Wasit, ALKut, Iraq

Abstract. The transition in the direction of sustainable power systems is limited by the rapid growth of global energy demand driven by population growth and urbanization. Recent market forecasts demonstrate high economic growth based on an increasing reliance on smart grid infrastructures. Despite the potential benefits, Smart Grids remain characterized by several consequential problems such as cyber vulnerabilities, complexities of big-data management issues, security considerations, and issues arising from centralized control architectures. The field of combining blockchain technology with AI and other emerging technologies is gaining high relevance. AI-empowered blockchain technologies offer blockchain-based solutions to data integrity, decentralization, and automation. This review paper surveys current developments in the integration of Smart Grids, Deep Learning, and Blockchain. The contributions of this paper are: Firstly, identifying and analysing recent literature from different perspectives. Then, examining the potential research areas along with their existing limitations. In addition, introduce a new systems-based architecture that provides a novel approach to the collaboration among key techniques smart grid, deep learning, and blockchain.

1 INTRODUCTION

Electric power can be considered a key resource for the modern world that suits the requirements of society and enables development towards sustainable life aspects. Some of the problems presented by the classical and traditional power system include increased energy demand, energy decline when transmitted from points of generation to points of consumption, power failures, and the integration of renewable power sources [1]. This demonstrates a continuous increase due to the rising global energy demand, which can be attributed to the growing population at a quite rapid rate, with increased urbanization [2]. In addition, the increasing contribution of renewables to power generation is contingent upon effective and smart power management systems, thereby contributing further to the market value of smart grid technology on a worldwide basis. Interconnection of power grids and

*Corresponding Author: hdhiyab@uowasit.edu.iq

production with better use for distributed infrastructure are other factors contributing to the growing implementation of smart grids [3], [4]. These grids combine state-of-the-art technology to deliver efficiency and the environment. These systems offer high flexibility, smooth integration with renewable energy sources, enhanced operational efficiency, and lower energy losses. Additionally, they provide real-time monitoring and smart decision-making to optimize energy management[4]. However, smart grids face challenges such as cybersecurity issues, big data system administration, privacy protection, and the challenges of distributed operation. These challenges move the eye to the importance of intelligent energy (using AI, ML, and DL) technology that can yield sustainable and efficient energy, as DL could be considered as a major part to guide the analysis of large energy data used by sensors in the context of identifying complex patterns previously unknown using traditional approaches[5]. Applications include load forecasting, fault detection, energy theft detection, and demand response optimization, all of which contribute to safer, more efficient, and sustainable energy systems [6].

The combination of AI, DL, and blockchain will lead the next generation, where there is intelligent and secure infrastructure for smart power. Special emphasis has been given to the incorporation of blockchain technology in addition to artificial intelligence in the design of smart power systems. These technologies are designed to keep the systems "running ideally and with greatest data integrity"[5].

This review discusses how the AI-based Smart grid is shifting towards using Blockchain can enhance security through the decentralized, immutable infrastructure of blockchain technology. Key applications include Peer-to-Peer (P2P) energy trading, smart contracts for automated transactions, thereby providing data robustness and integrity[7]. Accordingly, the contribution of this review can be listed below:

- Review and analyse the recent state-of-the-art works of Smart Grid, Blockchain, and Deep Learning integration from four specific perspectives.
- Discuss the limitations and challenges of the key technique integration and give insight into future works.
- Suggest new and novel system architecture for the research key techniques integrations and detail the interconnection between them.

2 BACKGROUND

2.1 SMART GRID

The SG is a modern electrical grid that integrates smart systems with existing infrastructure. This system can establish its own robotic mode of electricity delivery that would make the grid smarter and more automated.[8] Its main objectives are increasing the energy efficiency and promoting the effective electricity demand management and grid protection through self-healing. Smart grid systems can even out supply and demand, store surplus power for use at a more convenient time, and efficiently incorporate renewable energies like sun and wind, and they can identify problems fast and automatically route power around them, cutting down on outages and making the lives of consumers more dependable [9].

Due to their manual management and slow reaction time, traditional interconnection networks are not ideal. The advent of smart grids has revolutionized electricity management by doing away with the inefficiencies and rigidity of conventional grid systems. The responsive and stable low-carbon backbone of the grid allows for dynamic technology to stabilize and defend it. As a major improvement over conventional electrical grids, SG enhances energy generation, distribution, and transmission through the integration of contemporary communication and computational architecture [10].

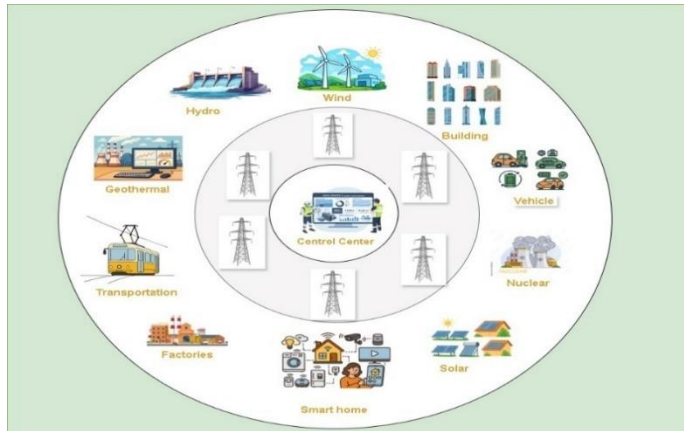


Figure 1. Smart grid architecture linking multiple energy sources to a central control center for efficient management

The SG generates electric power sustainably and reliably from a variety of interconnected renewable energy sources, including wind, solar, hydro, and geothermal power. Energy storage systems have a pivotal and crucial role to play in smart energy management systems, particularly while managing renewable energy sources to maintain the efficiency of the energy supply. One of the merits of the smart grid is energy storage [9].

Figure 1 illustrates the architecture of a modern smart grid ecosystem that integrates diverse energy sources and intelligent end-user applications through a centralized control centre. It highlights the grid’s cyber-physical nature, allowing for real-time communication, energy efficiency, and environmentally friendly power management.

2.2 Artificial Intelligence

AI has emerged as one of the most transformative technologies of the 21st century, revolutionizing industries and reshaping human-machine interaction .AI refers to the development of systems capable of performing tasks that typically require human intelligence, such as learning, reasoning, decision-making, and understanding natural language [11].

However, AI could create some problems relating to issues of decisions being taken with moral reasoning, learning to adapt, and information privacy decisions being explained to users [1] .ML is a specialized domain within AI that enables computational systems to learn from data and autonomously improve their performance over time, unlike traditional programming, which relies on explicit rule-based instructions. ML leverages probabilistic and statistical techniques to extract meaningful patterns from datasets. The growth of ML as an area of research has been driven by the ease of availability of data on a mass scale, reduced costs of data storage, and the increase in processing speed made possible by the IoT [11]. Data forms the backbone of ML systems and comes from a variety of sources, including system logs, social media platforms, blogs, and sensors that measure parameters such as temperature, current, and humidity [2], [3] .Globally, scientists categorize the mechanisms for ML algorithms into four divisions, starting with supervised learning models, where labelled data is supplied in prior tasks related to disease classification . Unsupervised Learning is about learning on untagged data and tries to figure out relationships between the features with other tasks as clustering, outlier detection, rule discovery, and reduction of

dimensionality. Semi-Supervised Learning (SSL) is the part where we have only a small fraction of labelled data[8]. It is based on both supervised and unsupervised methods to enhance model predictions.

DL has emerged as a significant evolution within ML, designed to handle complex, high-dimensional, and non-linear data more effectively than traditional algorithms. DL algorithms use deep, multi-layered neural network architectures to extract and learn hierarchical feature representations from complex data. Many specialized DL architectures have been developed to meet the needs of various data types and tasks [12].

Recurrent Neural Networks (RNNs) and Long Short-Term Memory (LSTM) networks are designed for sequential data, making them well-suited for tasks like time-series forecasting and language modelling. Convolutional Neural Networks (CNNs) have been designed keeping in mind the nature of spatial data and images. They apply convolutional filters for finding local patterns. The Transformer Network has given a new dimension to sequence-level work by applying self-attention mechanisms. The Autoencoders (AENs) help in unsupervised learning of higher-level representations as well as dimensionality reduction. The Generative Adversarial Networks (GANs) help in generating novel simulated data by adversarial training. GNNs extend deep learning to graph-structured data, helping applications in social network analysis, molecular chemistry, and suggestion system [13]. Collectively, ML and DL represent a fundamental technological shift, providing the

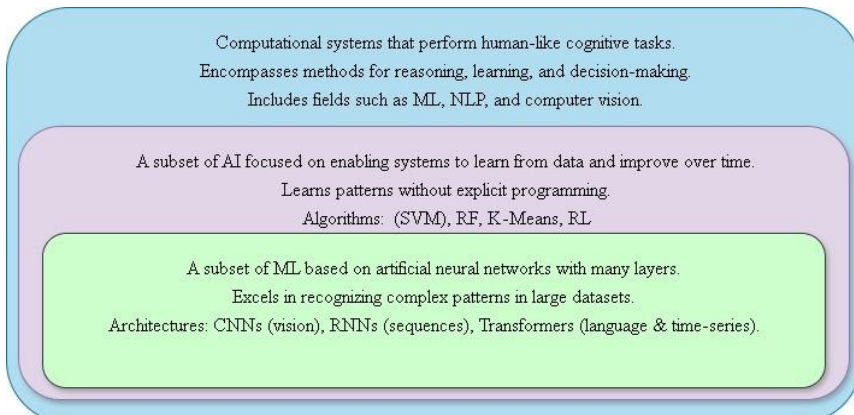


Figure 2. Hierarchical relationship among (AI), (ML), and (DL)

algorithmic processing foundation for intelligent, adaptive, and autonomous systems. Its integration continues to power more domains of new development, and has also become a key component for next-generation intelligent applications. This hierarchical relationship is shown in Figure 2. It is indicative of the way deep learning further develops machine learning methods, while machine learning constantly draws on a broader AI platform as its background work. It is a layered structure built up with intelligent computational methodologies.

2.3 BLOCKCHAIN

Blockchain is a shared and decentralized digital ledger technology designed to record transactions in a secure, transparent, and tamper-resistant manner [2]. Interconnected blocks of data mean that after a certain date, the data collected and certified cannot be altered. Beyond this stage, each node connecting to the network records a complete history of user transactions across the Blockchain [3]. A blockchain network can act as a large autonomous shared DB recording and logging transactions till they are needed. Ensuring the protection of

all transactions from the beginning and initiation of the network; transparency for updates on stored data; and fault tolerance above all else. Any transaction, once made and sent from the sender, has to be checked by the whole network [3].

In blockchain, the security of devices and the integrity of data are ensured through cryptographic methods and consensus algorithms. These include many algorithms, such as Proof of Work and Proof of Stake algorithms, which validate a transaction before it is permanently recorded and stored on the blockchain. The decentralized nature of blockchain significantly reduces and tries to prevent the risk of fraud, and further enhances trust among all participant [8].

Additionally, blockchain technology has quickly developed into other standalone platforms and real-world uses. Their fundamental blockchain architectures, solutions for increased scalability, and specialized use cases for different industries' needs are slightly different [2]. The initial implementation, Bitcoin, came into being in 2008. After that, Ethereum brings the idea of "smart contracts," which simplify the process of building DAOs. Among the many designed blockchains, Hyperledger Fabric is worth mentioning. Faster than earlier versions, Hyperledger runs on similar protocols. From basic transactions, these systems show blockchain evolving - into active, custom-built solutions [5].

A different angle ties into how blockchains are shared. When it comes to open networks, individuals stay anonymous using code that hides identities while every transaction shows up for everyone to see. In contrast, secret blockchains might lighten the load on computers since access is locked down to approved members - yet that setup often narrows who takes part and widens control over the chain [2]. One look at Table 1 shows how centralized setups compare to blockchain-based ones - structure, control, security. Though fast and streamlined, central authority systems can falter at one weak spot. On the flip side, blockchain spreads power widely; transparency grows alongside immutability. Yet heavier loads on networks remain a sticking point. Security trades off against raw speed more than expected. Figure 3 breaks down the process: a transaction begins it, then nodes across the network check its validity through methods like Proof of Work, agreeing on outcomes without central oversight. After checking, the block becomes part of the chain - a permanent piece of history stored on every node.

Table 1. Centralization and Decentralization Difference

Aspect	Blockchain System	Centralized System
Architecture	Decentralized, peer-to-peer network with a distributed ledger replicated across nodes.	Client-server model with a single authoritative database controlled by a central entity.
Control & Governance	Decisions made collectively through consensus; no single point of control.	Central authority makes all decisions, simplifying management but creating dependency.
Data Integrity	Transactions are cryptographically hashed and immutable once recorded, ensuring tamper-resistance.	Data can be altered by authorized administrators; vulnerable if the central database is breached.
Transparency	All participants can verify transactions (especially in public blockchains).	Only authorized users have visibility into stored records.
Fault Tolerance	A high network continues operating even if some nodes fail.	A single point of failure can disrupt or halt system operation.
Performance	Slower transaction throughput due to consensus and replication overhead.	High performance, faster execution since processing is centralized.
Scalability	Challenged by network size and the complexity of consensus mechanisms.	Easier to scale vertically by upgrading server resources.

Security	Resistant to single-point attacks but susceptible to 51% or Sybil attacks in some cases.	Relies heavily on perimeter security; once breached, the entire system may be compromised.
Cost	Higher computational and energy costs (e.g., Proof of Work); lower trust overhead.	Lower operational costs but high expenses for server maintenance and cybersecurity.

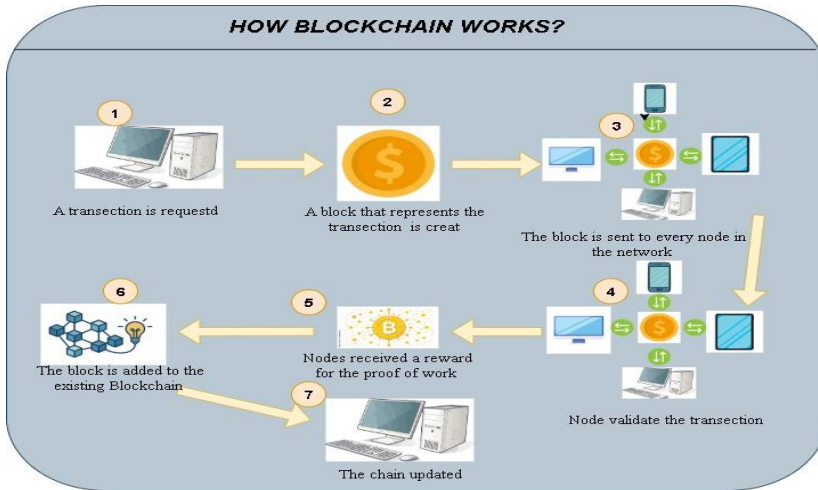


Figure 3. Blockchain Transaction Mechanism

3 Key Techniques Integration Taxonomy

3.1 Smart Grid and Deep Learning Integration

The SG is an important piece of technology since it allows for better tracking of both buyer and seller actions by combining cutting-edge computer and internet methods with improved monitoring. More efficient energy management is made possible by its ability to allow the bidirectional movement of electricity and information, in contrast to traditional grids [9]. Even with these improvements, SGs still confront a lot of problems. An adversarial attack could compromise the system if its connectivity is increased. When different devices and protocols need to be coordinated, interoperability problems emerge. The power supply becomes more unpredictable and variable as a result of renewable energy integration.

In the study, the authors have developed a hybrid deep-learning framework that combines Gated Recurrent Units (GRU), Temporal Convolutional Network (TCN), and focuses on the load forecasting by capturing long-term and dependent variable relationships (temporal multi-scale patterns) and prioritizing related features [11]. The results of their study indicate that their approach outperforms the three individual models in predicting loads as well as accurately handling nonlinear and seasonal loads, supporting real-time forecasting and Smart Grid Optimization.

The study presents a method for enhancing the detection of theft precursors and the prediction of theft occurring in real-time using a model which is based on real-world datasets, including datasets from the Republic of Ireland and Sustainable Energy Authority of Ireland, with precision, recall, and F-1 score [6]. The authors of [6] caution, though, that although the use of a guide is of significance in their study, privacy and confidentiality of data are still open questions that cannot be answered currently.

The study proposes a lightweight Theft Detection Deep Learning (DL) model [2] in that the authors will use Feature Engineering and Dimensionality Reduction to re-sample training data and increase the accuracy and usefulness of their models in resource-constrained environments. As the authors note, the challenges associated with applying AI to Smart Grids are attributed to existing infrastructure, the standardization of smart grid systems, as well as the capital investment in developing intelligent systems.

As shown in reference [9], there are many approaches to developing AI based Intrusion Detection Systems (IDS) for IIoT Smart Grids. Machine Learning, Deep Learning, and Neural Networks are all integral parts of these systems, and by optimizing the selection of features, the combination of different types of machines to create hybrid model systems leads to improved accuracy of theft detection. In addition, even though PSO, GWO, GA, and Deep Networks achieve high detection rates, all require a significant amount of computational power, indicating a clear trade-off between efficiency and accuracy in the context of real-time IIoT environments.

3.2 Smart Grid and Blockchain Integration

Cyberattacks, ineffective communication between connected devices, and security flaws in the data kept by the grid are among the major issues with smart grids [14]. Blockchain technology is useful for these kinds of issues. Utilizing an immutable distributed ledger, it validates network transactions. Through the establishment of transparent, immutable, and autonomous P2P (peer-to-peer) transactions. Implementing blockchain technology into a smart grid can greatly enhance its scalability, security, reliability, and efficiency in energy exchange. Plus, with the aid of interaction that does not require thrust [3]. On the other hand, the purpose of the research in [7] is to solve the scalability problem once and for all. More precisely, it aims to explain why more efficient consensus methods are needed, as larger block sizes resulted in a linear increase in processing time. Smart grids enabled by blockchain, P2P energy trading, distributed energy storage, and AI-powered intelligent and dynamic optimization of energy use are all demonstrated to be feasible by the experiments.

3.3 Blockchain and Deep Learning Integration

Smart grids, industrial healthcare systems, and Vehicular Ad-Hoc Networks (VANETs) are just a few examples of distributed intelligent systems that could benefit greatly from DL and BC integration efforts to improve data privacy, integrity, and security [5, 8]. Blockchain provides decentralized trust, immutable ledgers, and authentication through smart contracts, often combined with Inter Planetary File System (IPFS) for off-chain storage and scalability. For instance, a study in [10] suggested a framework combining Digital Twin, Software Defined Networking (SDN), DL, and blockchain to secure IoT-enabled smart grids against DDoS and (Man-in-the-Middle) MiTM attacks. It uses blockchain-based authentication and a DL-based IDS (self-attention + Bi-GRU) with SDN as the backbone, achieving 99.73% accuracy on the N-BaIoT dataset. The model uses SegCaps and CNNs for feature extraction, as it then uses a Capsule Networks approach that can improve generalization. To manage a heterogeneous global data source, it uses data normalization. The FL technology is used as it involves the cooperation among the various models to train the single model, and blockchain technology is used to ensure trust during the collection of the gradient data [8].

Another works in [4] proposed AI model for forecasting power usage in smart grid-smart city setups. The process involves Z-Score normalization, Spatial-Temporal Correlation (STC) to pull out features, Distributed Authentication and Authorization (DAA) with blockchain for safe storage, LSTM-RNN enhanced by the Improved Sparrow Search

Algorithm (ISSA) to predict load, and Blockchain-Based Smart Energy Trading with Adaptive Volt-VAR Optimization (BSET-AVVO) for immediate energy trading. Simulation outcomes showed better results in mean squared error, delay, and throughput when compared to standard approaches.

Figure 4 from [1] shows a general approach for a blockchain-based deep learning framework where devices train local models and share only parameters via blockchain, ensuring data privacy. A registration module authenticates devices, and a model manager aggregates updates into a global model, with blockchain providing transparency, immutability, and trust for smart grid and IoT applications.

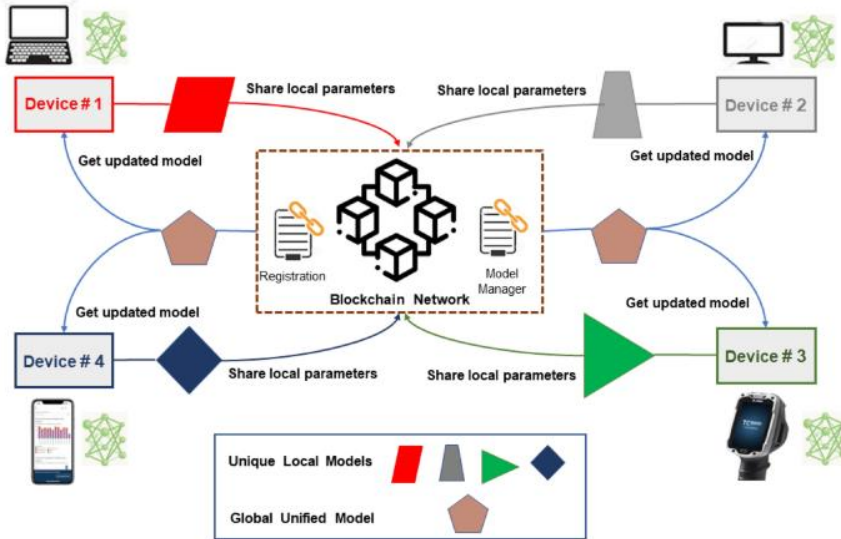


Figure 4. Illustration of Blockchain Contribution to Deep Learning Systems [1].

3.4 Smart Grid, Blockchain, and Deep Learning Integration

In accordance with what was presented in previous integration methods, it seems that existing smart grids could struggle with some bottlenecks because they may not meet the growing need for quality of service aspects [8]. In addition, the industry is becoming more diverse in terms of how production and sales are handled, which makes it even more complicated. The fluid nature of supply and demand is another nail in the coffin for traditional systems. Hence, there is a need for intelligent grids that can easily support high energy flows and respond to rapid changes.[3], [6]. Future smart grid success depends on DL and BC working together. Put another way, the massive amounts of data gathered from meters and sensors may be understood by deep learning thanks to its ability to identify intricate relationships within them. Here, errors/metering crimes detection and load prediction have both made excellent use of deep learning [5]. Moreover, blockchain technology provides a trustworthy and open system for data storage and transmission. A use of smart contracts for smart grid transaction validation is detailed here, along with the use of blockchain technology and peer-to-peer energy trading [15].

The synergy between deep learning and blockchain creates complementary benefits that can be listed as follows:

- They can process data in real time, identify anomalies, and flag cyber-attacks.
- Results are managed by blockchain to avoid changes to decisions or events.

- Smart contracts on blockchain can be automatically activated once certain conditions are met, linking intelligent predictions with operational execution.

The integration of BC technologies to Smart Grid is catching attention in academic research, resulting in different theoretical models and first case studies for several markets, notably traditional power system modernization. One of these uses that is widely studied and recognized for its ability to let active consumers share surplus power and reduce peak consumption effectively is the P2P energy trading [4].

Integrating DL and Blockchain in Smart Grids comprises different kinds of challenges in technical, security, and operational dimensions. Technically, the highly limited scalability as well as large latencies and overheads limit the real-time efficiency and overall performance dramatically; the low bandwidth data transmission and heterogeneous environmental data quality bring challenges to learning a high-accuracy deep neural network[10]. Security-wise, smart grids are still vulnerable to cyber-attacks such as false data injection (FDI), distributed denial-of-service attacks, and insider threats. Furthermore, blockchain also adds new challenges, including weak key management, insecure smart contracts, and the difficulty in interpreting threat detection results driven by DL [5]. There are also fundamental and cost obstacles like a lack of awareness gap, higher cost of high-power energy and hardware consumption, no standardized market and price model for the computing services provided by quantum technologies (if there are any), as well as reliance on central controllers for their management, and new risks associated with quantum computing [9].

Table 2 provides a summary of most of the above-discussed solutions in terms of objectives, algorithm used, dataset used, if any, and adopted performance metrics.

Table 2. Summary of Discussed Solutions

Ref	Objective	Algorithm/Fram ework	Dataset	Key Performance Metrics
[13]	Short-term power load forecasting	GRU + TCN + Attention	GEFCom2014, ERCOT Load, AEMO Load, NYISO	Accuracy, RMSE, MAE, MAPE
[6]	Automated electricity theft detection	Hybrid CNN-RF	SEAI, Low Carbon London	Precision, Recall, F1-score
[12]	Theft detection from monthly readings	Lightweight DNN + PCA/t-SNE/UMAP	Power Grid Corporation of China	Accuracy, Precision, Recall, F1-score
[2]	Protection from FDIA & DDoS attacks	Blockchain (Ethereum PoA) + LSTM + CNN	MatPower simulated data	Detection Accuracy, Response Time

4 Discussion

The approach that involves the use of deep learning and blockchain technologies proves to be the most effective and efficient way for handling modern smart grid challenges. In other words, the capacities to provide the desired level of data privacy and an opportunity to perform all functions in real time are a priority if risk biases are inevitable. Moreover, the acquisition and use of deep learning and blockchain-based technologies for the development of distributed energy networks is associated with the use of accurate forecasts, independent control, and safe record-keeping that cannot be tampered with as to deals and operational data.

Another issue that also associated with the computation is that required for deep learning in heavy tasks like a load prediction analysis. This problem becomes more challenging when

the algorithm in the use is like LSTM, or CNN. All these issues will even take up more system resources when you move it to real-time calculations on multiple machines.

The cyberattacks are another ongoing issue in the smart contract despite the key technique above integration. Injections of arbitrary data, distributed denial-of-service attacks that throttle networks, congesting them so massively they fail to work altogether--all these spoils by proxy serve to yet further hurt the given smart grid. Another issue is that occurs in certain applications relating to key management, and calls are relevant for smart contracts-based solutions.

Operational and economic barriers also remain substantial. Interoperability gaps among heterogeneous devices, especially in terms of data format, high energy and hardware costs, and the lack of standardized market mechanisms and pricing models, impede effective deployment. Emerging and evolved threats, such as quantum computing, further increase the weakness in the security of blockchain networks and the integrity of smart grid operations. Considering all the above factors, this research underscores the necessity for adaptive, efficient, and secure frameworks that integrate DL and blockchain technologies, ensuring scalable, reliable, and resilient operation of next-generation smart grids.

4.1 Future Conceptual Framework

This paper suggests a novel framework that brings in a blockchain and deep learning-based framework to achieve secure, transparent, and intelligent data handling of the smart grid. Every piece of information produced and transmitted from the smart meter is labelled with a unique label for the device number and associated metadata in this construction. This tag assists the blockchain to readily recognize the details and associate them with a distinct physical tool in the block of batteries. Vital parts of the system – in this case, power-generating units and monitoring tools – are hooked up to the blockchain network. As a consequence, there is a wide and decentralized base upon which consensus may be formed about the system.

An Authentication Smart Contract keeps a continuously updated authentication list that records legitimate and authorized devices. This mechanism prevents unauthorized access and ensures that only validated sources are permitted to communicate and share data within the network. In order to remove the risk of single points of failure and guarantee data integrity, the Authentication Sharing API handles data source verification and transfers information to decentralized storage when a device submits data. In order to do complex analytics, such as fraud detection, energy theft identification, and abnormal behavior recognition, the stored data is utilized by the deep learning module. A combination of time-series and pattern-based learning models does this. The findings are sent to the Policy Enforcement Smart Contract, which subsequently updates the authentication records, isolates suspicious nodes, or alerts administrators according to the established operational and security regulations. This feedback loop, which enables continuous system improvement, enables cyber defenses to react to new threats as they appear. By integrating blockchain technology with authentication, decentralized storage, and deep learning analysis, the framework provides a reliable, versatile, and intelligent solution for managing smart grid data. These qualities make this solution strong, auditable, and effective.

5 Conclusion

Development of Smart Grids is an important progression to create secure, intelligent, self-healing power ecosystems that can serve the growing global energy demand and support large scale renewable energy integration. The use of Artificial Intelligence, particularly Deep Learning, has addressed several aspects of big data challenges (load forecasting, fault

detection, energy theft analyses). However, AI alone cannot solve the issues of trust, transparency, and data integrity in decentralised energy networks. When combined with the use of blockchain technology, however, these two technologies offer a practical solution for the current difficulty in controlling energy networks decentralised, managing data using an immutable ledger, executing energy trading using smart contracts. In this paper, we described the recent developments in Blockchain-AI platforms and identified several gaps and provided a framework for future growth and development of Blockchain-AI systems. As stated in this paper, Blockchain-AI development for future smart grids must address the combined area of computational and communications systems, along with establishing trusted infrastructure and real-time decentralisation. As Blockchain and AI research grows, and as Blockchain and AI systems are developed within a field setting, it is expected the current smart grid prototypes will be transitioned to complete energy ecosystems.

References

- [1] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Comput.*, vol. 26, no. 1, pp. 197–221, Feb. 2023, doi: 10.1007/s10586-022-03582-7.
- [2] Y. Ishaq, A. S. Prince, G. G. J. Claude, and T. M. Di Bebe, "Decentralized Framework for Securing Smart Grids Using Blockchain and Machine Learning," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 13, no. 1, pp. 679–685, Jan. 2025, doi: 10.22214/ijraset.2025.66079.
- [3] H. Khan and T. Masood, "Impact of Blockchain Technology on Smart Grids," Oct. 01, 2022, *MDPI*. doi: 10.3390/en15197189.
- [4] E. Aljarrah, "AI-based model for Prediction of Power consumption in smart grid-smart way towards smart city using blockchain technology," Dec. 01, 2024, *Elsevier B.V.* doi: 10.1016/j.iswa.2024.200440.
- [5] M. Alabadi and A. Habbal, "Next-generation predictive maintenance: leveraging blockchain and dynamic deep learning in a domain-independent system," *PeerJ Comput. Sci.*, vol. 9, 2023, doi: 10.7717/peerj-cs.1712.
- [6] S. Li, Y. Han, X. Yao, S. Yingchen, J. Wang, and Q. Zhao, "Electricity Theft Detection in Power Grids with Deep Learning and Random Forests," *Journal of Electrical and Computer Engineering*, vol. 2019, 2019, doi: 10.1155/2019/4136874.
- [7] B. Zafar and S. Ben Slama, "Energy Internet Opportunities in Distributed Peer-to-Peer Energy Trading Reveal by Blockchain for Future Smart Grid 2.0," Nov. 01, 2022, *MDPI*. doi: 10.3390/s22218397.
- [8] W. Hua, Y. Chen, M. Qadrdan, J. Jiang, H. Sun, and J. Wu, "Applications of blockchain and artificial intelligence technologies for enabling prosumers in smart grids: A review," Jun. 01, 2022, *Elsevier Ltd.* doi: 10.1016/j.rser.2022.112308.
- [9] M. M. Abou-Elasaad, S. G. Sayed, and M. M. El-Dakroury, "Smart Grid intrusion detection system based on AI techniques," *Journal of Cybersecurity and Information Management*, vol. 15, no. 2, pp. 195–207, 2025, doi: 10.54216/JCIM.150215.
- [10] M. Z. Gunduz and R. Das, "Smart Grid Security: An Effective Hybrid CNN-Based Approach for Detecting Energy Theft Using Consumption Patterns," *Sensors*, vol. 24, no. 4, Feb. 2024, doi: 10.3390/s24041148.
- [11] X. Wen, J. Liao, Q. Niu, N. Shen, and Y. Bao, "Deep learning-driven hybrid model for short-term load forecasting and smart grid information management," *Sci. Rep.*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-63262-x.
- [12] S. M. Saqib *et al.*, "Deep learning-based electricity theft prediction in non-smart grid environments," *Heliyon*, vol. 10, no. 15, Aug. 2024, doi: 10.1016/j.heliyon.2024.e35167.

- [13] S. Mohsen, M. Bajaj, H. Kotb, M. Pushkarna, S. Alphonse, and S. S. M. Ghoneim, "Efficient Artificial Neural Network for Smart Grid Stability Prediction," *International Transactions on Electrical Energy Systems*, vol. 2023, 2023, doi: 10.1155/2023/9974409.
- [14] R. Soni, M. Kumar Thukral, and N. Kanwar, "A Secure Blockchain Based Smart Contract Framework for Smart Grid Management Using Improved Chaotic Encryption and Decryption Techniques," Aug. 2025. doi: <https://dx.doi.org/10.2139/ssrn.5400533>.
- [15] P. Boopathy *et al.*, "Deep learning for intelligent demand response and smart grids: A comprehensive survey," *Comput. Sci. Rev.*, vol. 51, Feb. 2024, doi: 10.1016/j.cosrev.2024.100617.