Journal of Theoretical and Applied Information Technology
31st December 2023. Vol.101. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENERGY EXCHANGE PROCESS FOR SMART GRID BASED ON INTEGRATING BLOCKCHAIN WITH GCN-LSTM

DR. VUDA SREENIVASA RAO[1], AFSANA ANJUM[2], DR.S.SUMA CHRISTAL MARY[3], IBRAHIM AQEEL[4], DR. S. KOTESWARI[5], SHAMIM AHMAD KHAN[6], MANIKANDAN RENGARAJAN[7]

[1]Associate professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, INDIA.
[2]Lecturer, Dept.of Information Technology & Security, Jazan University Jazan, KSA.
[3]Professor, Department of Information Technology,Panimalar Engineering College, Poonamalle, Chennai.
[4]College of Computer Science & IT, Jazan University, Jazan, Saudi Arabia.
[5]Professor, Pragati Engineering College, Surampalem, Kakinada.
[6]Research scholar, Glocal University.
[7]Vel Tech Rangarajan Dr. Sagunthala R&D Institute of Science and Technology, Avadi, Chennai, Tamil Nadu, India-6000627

[1]vsreenivasarao@kluniversity.in , [2]afsana24sajid@gmail.com, [3]sumasheyalin@gmail.com, [4]iahmed@jazanu.edu.sa, [5]eshwari.ngr@gmail.com, [6]skwarsi@hotmail.com, [7]rmanikandan@veltech.edu.in

ABSTRACT

The energy exchange process lies at the heart of the modern smart grid, a transformative energy infrastructure. This process involves the seamless transfer of electricity among various grid components, including consumers, producers, and storage units, to meet dynamic demand patterns efficiently. Traditional energy exchange systems often lack transparency, building it tough on behalf of clients to track the source of their energy and verify the fairness of prices. By addressing these issues and increasing effectiveness, security, also transparency of energy trading and supply. The modernization of energy systems has ushered in the era of the smart grid, promising enhanced efficiency and resilience. In the pursuit of these goals, this study explores a novel approach by integrating two cutting-edge technologies: Block chain and Graph Convolutional Networks with Long Short-Term Memory (GCN-LSTM). Block chain, renowned for its transparency and security features, is leveraged to enable transparent, tamper-proof energy transactions within the smart grid. Complementing this, GCN-LSTM, a fusion of graph neural networks and deep learning, enhances grid intelligence and decision-making, optimizing energy distribution and consumption patterns. This research delves into the intricacies of this integration, offering insights into its benefits, challenges, and potential applications. By combining the decentralized ledger capabilities of Block chain with the data-driven power of GCN-LSTM, This study hopes to open the door to a more resilient and adaptive smart grid, heralding a new era in energy exchange and management. Overall, the proposed methods are highly effective and have demonstrated their superiority by achieving an impressive classification accuracy of 99.30%, which outperforms several existing state-of-the-art methods in the same task.

Keyword: *Graph Convolutional Networks; Deep Learning; Long Short-Term Memory; Block Chain; Smart Grid;*

1. INTRODUCTION

A dynamic and technologically cutting-edge system for controlling the production, distribution, and use of electricity is represented by the energy exchange process in a smart grid, particularly within the framework of information networks. The substantial use of digital technology, real-time data transmission, and sophisticated decision-making algorithms that define smart grids. These developments make it possible for the grid's different parts, such as power plants, transmission lines, distribution networks, smart meters, and end consumers, to function together seamlessly and effectively [1]This data and energy-related data interchange is made possible by information networks, which also enable better grid resilience, smarter energy management, and the incorporation of renewable energy sources. The act of exchanging energy in this networked world involves more than just supplying power; it also entails optimizing its flow, maintaining sustainability, and adapting quickly to shifting needs and environmental issues. This introduction lays the groundwork for a more in-

depth analysis of how information networks enable the modernization of energy systems and pave the way for a future that is more robust and sustainable, [2].Through remote autonomous metering, the power generator may save expenses and improve the reliability of the grid. Because the maximum demand for electricity is lower, it improves operating efficiency and lowers the amount of money required for the power plant. When the electrical consumption rate is low, consumers can supply energy via the stored energy device. On the other hand, they sell power during periods of strong demand. They therefore transition to being consumer groups [3].Applications built on the block chain may provide answers to smart grid issues with varying degrees of sophistication. Unlike many comparable methods, block chain developed quickly and is already being used in a variety of areas of the modern economy [4]

An overview of the development and application of the technology known as block chain is provided in Many academics think that the development of distributed led to the creation of Block chain. The use of Block chain as an essential tool in the smart grid could provide a way to set up a trade infrastructure there. In an ideal world, the Block chain would be used to facilitate peer-to-peer power trading between festivities, in this sample customers and prosumers contained by the smart grid, without the need for a middleman to maintain trust. Numerous advantages are promised by the implementation of a block chain-based trade system within the smart grid [5] One may consider benefits like the creation of an actual time a more efficient trading system's ability to cut expenses for transactions, and more individual security inside the smart gridAdding computational power may be utilized to construct more complex and intricate applications in addition to utilizing the technology of block chains to build a trading network. [6] As a result, many solutions for smart grids may be offered using a decentralized processing platform that is established. For instance, the smart grid might be controlled by using variable pricing. According to the expanding variety of investigations and study initiatives, block chain's potential in smart grids has just recently been recognized. [7] The growth of renewable energy and how it interacts with block chain technology are examined, and the use of block chain technology is confirmed as a potential alternative to raise the percentage of renewable energy. [8] A unique method for developing a decentralized system that prevents connection with other parties is to use block chain technology. [9] Block chain technology protects against fraudulent manipulation of the money transfer process by acting as a shared ledger amongst network members. The design of the Block chain allows for the generation of additional blocks that may be utilized to continually store data. The smart grid is adaptive and redundant against faults and cyber-attacks because to its architecture. Block chains powered by smart contracts may create and store block of information that are more immune to change and invulnerable to it without the need for human involvement.[10] A crucial infrastructure like a smart grid may be greatly enhanced with block chain technology.

Power grids nowadays are equipped with interaction and management technology thanks to smart grids, which enable substantial advancements in energy efficiency and system security. [11] To effectively control electricity production, distribution, transmission, and use, multiple smart devices are placed throughout a smart grid. The safety and reliability of the electricity system must be maintained while properly managing these smart devices. However, conventional hierarchical methods of managing smart grids confront significant difficulties in a number of areas, including management of energy, electricity trading, security and privacy, micro grid administration, and the control of electric vehicles., [6] They are further explained in the sections that follow. The robust tool provided by block chain technology may encourage people to trade their private data, which is then utilized to create models for neural networks. For AI-based models, the block chain network must exclude duplicate, insufficient, or loud information., therefore keeping machine learning-related data there lowers the likelihood that the model will contain mistakes Integrating the block chain's fundamental values with machine learning The use of data management, inspection, and the addition of fresh values to company processes via automating enabled available by smart contracts are just a few of the benefits of principles for applications. For example, smart contract neural network models can recommend to authorities a request to recall outdated pharmaceuticals.[12] Block chain can document the many stages of the algorithm's construction, usage, or application and can track the growth of machine learning algorithms as it advances. The use of the record of permanent transactions stored on the block chain aids in identifying the owners of the neural network learning algorithms, databases, the origin of the data, individuals, the foundation of the model, and the processes employed throughout model

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

development. A block chain's collaboration algorithm, database permanence, and encrypted hash functions make attacks on AI models such as data, model, and algorithm poisoning difficult. The purpose and applications of systems based on block chains In prior research, a number of machine learning-related fields were carefully examined. In the research stated there, for instance, a brief discussion of the use of blockchain in the fields of artificial intelligence and neural networks was made. No study or research article has, to our knowledge, fully studied how block chain technology fits into the deep learning field.[13] Energy exchange process for smart grid using block chain is shown in FIG:1

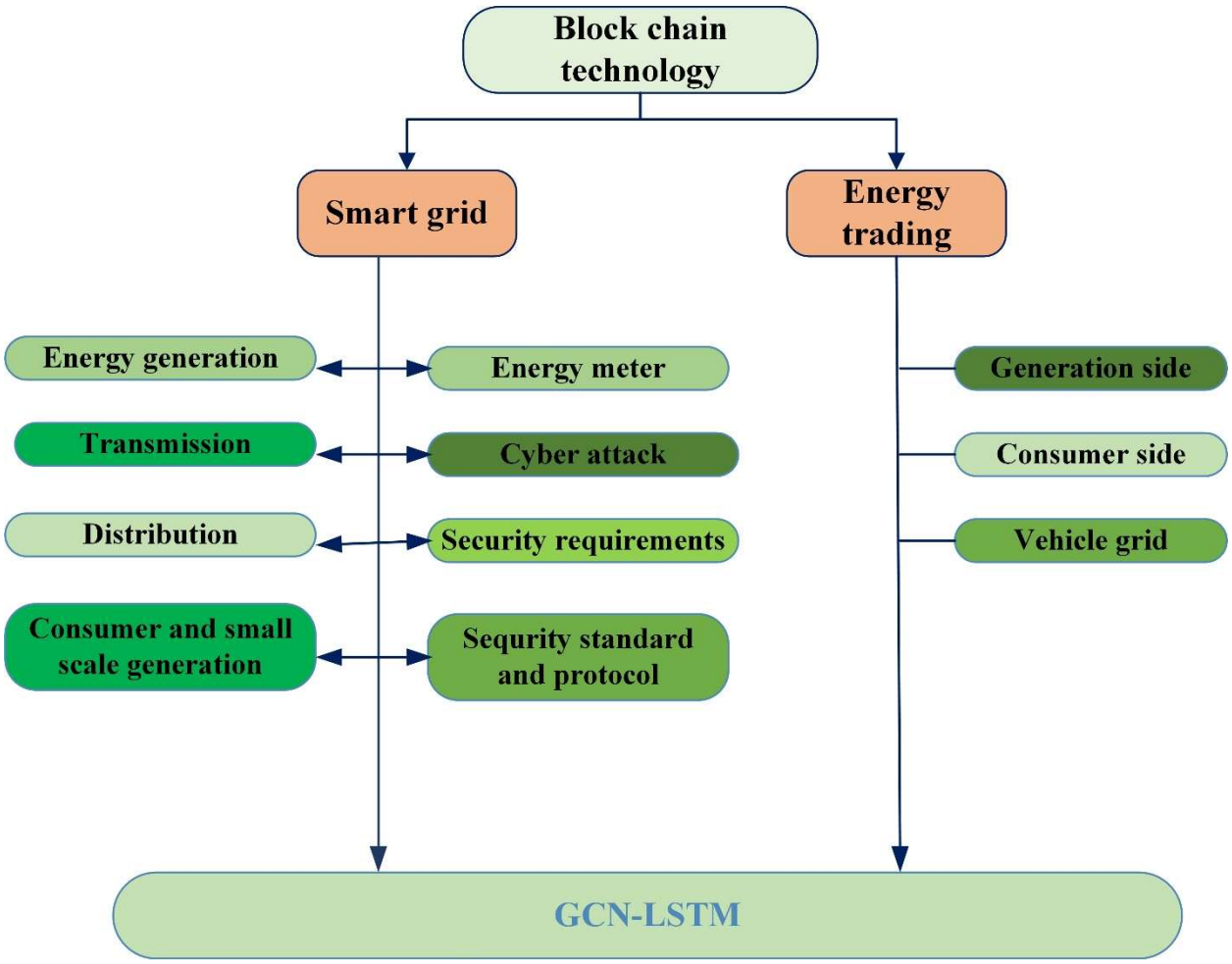

Figure 1: Energy exchange process for smart grid using block chain

The Key Contribution of this work is as follows:

- The block chain method offers a visible and secure ledger for documenting energy transactions. This minimizes the risk of fraud and builds confidence among smart grid participants by ensuring that all transactions are tamper-resistant and verified.
- The integration of GCN enables the smart grid to model complex relationships within the energy network.
- Long Short-Term Memory (LSTM) networks excel at processing time-series data, making them invaluable it can optimize energy distribution, anticipate grid disturbances, and facilitate peer-to-peer energy trading, ultimately leading to more efficient energy utilization.
- For real-time adaptation within the smart grid.
- The combined capabilities of block chain, GCN, and LSTM empower the smart grid to make more informed decisions.
- By integrating these technologies, the smart grid becomes more sustainable and

resilient. It can better incorporate renewable energy sources, adapt to unforeseen challenges, and maintain grid stability, contributing to a greener and more reliable energy ecosystem.

The following is how the investigation progresses: In paragraph 2. Related studies perform a thorough analysis of earlier research, focusing on prediction issues and the wide range of optimization techniques used in such settings. In Section 3, a thorough investigation of issue statements is conducted. Section 4 elaborates on the suggested method or plan of action to deal with these difficulties. The entire topic of performance evaluation metrics and criteria is covered in Section 5. Subsequently. Section 6 serves as the essay's conclusion by summarizing the main findings and learnings from the inquiry.

2. RELATED WORKS

Uddin et al. [14] discusses the advantages and difficulties of the future BCn framework'stechnological architecture it has to do with putting the new SGES components into action. Innovative capabilities like smart meters, peer-to-peer (P2P) energy trading, self-operation, and visibility for the ongoing functioning of SGES are made feasible by this design.Technology advancements in smart grid energy systems are being made with a focus on effectiveness and sustainability over time in order to satisfy the needs of the fourth energy revolution. These frameworks, which will be put into practice in the upcoming years, contain crucial elements like simplifying grid activities, facilitating energy trading, and enhancing energy management. Among these developments, block chain (BCn) has been a hot topic of discussion among academics. Its incorporation into smart grid power systems holds the prospect of more successfully achieving consumption targets. In order to keep pushing the limits of managing energy and sustainability, researchers are actively working to further improve block chain's capabilities with the goal of using it as the basis for the future block chain framework. The scope of this publication may be constrained, and it might not include all pertinent studies in the area.

The awareness of the "smart grid" is a up-to-date redesign of the old-fashioned electrical grid with the goal of maximizing the incorporation of sources of clean energy and storage of energy technology. The convergence of large information and internet connectivity has become a revolutionary force in this evolution, making it possible to realize an intelligent grid that is networked and sometimes recognized as the "power Internet." Due to its intrinsic qualities, which provide workable solutions to solve security issues and trust-related difficulties in the smart grid ecosystem, the block chain system plays a crucial role in this context. A solid foundation is being built for maintaining the integrity and dependability of energy transactions and data inside the smart grid thanks to block chain's dispersed, tamper-resistant ledger, secure encryption techniques, and smart contract functionalities Hasan et al. [15] In addition to details on cyber security and safeguarding of energy information in smart grids, [15] presented an organized examination of block chain applications. This study highlights the main safety issues that big data faces and how block chains might help with them in smart grid situations. A variety of recent block chain-based research projects that have been published in a variety of publications are then highlighted, along with security concerns with smart grid technologies. Explore numerous recently made items, experiments, and useful concepts that are similar here. Finally, go through some of the biggest investigation issues and potential approaches to use blockchain technology to address safety concerns with smart grids.

The software that allows for creating and maintaining such a grid architecture is sought after in block chains. By imagining an electrical grid that relies on the immediate involvement of todays embedded energy devices inside a decentralized structure housing specific coordination mechanisms, it creates an initial structure to satisfy this demand. The platform was created during the course of research that was experimental and was conducted at ABB Laboratories using embedded circuits that are now built as control connection boards for smart inverters Baggio and Grimaccia [16] explain the underlying justification, high-level architecture, and essential element of the Block chain-based framework for grid operation coordination. Here, it is believed that block chain technology is the best option for realizing of a multi-actor energy management platform and facilitating scattered collaboration in electrical networks. The present energy sector is undergoing a change as a result of increased electrification and the integration of distributed assets such as photovoltaic inverters (PvI), EV chargers, and windmill controllers, all of which are furnished with cutting-edge

communication capabilities. While decentralization gives each member greater authority, it additionally renders it more challenging for centrally-managed electrical networks to effectively coordinate these assets. To manage it, a decentralized coordination-and-control system is required. Unlike traditional centralized techniques, it makes it simple to integrate consumers and distributed energy resources (DERs), optimizing the use of green energy and grid flexibility.

The smart grid's four-layered design for energy trading deals with the complications brought on by technological improvements and the incorporation of renewable energy supplies. Communication and information technology (ICT) is fundamentally about improving grid performance and enabling intelligent handling of energy. Energy transmission is made more difficult by the introduction of characteristics like continuous tracking and automatic outage management brought about by the combination of clean sources of energy, energy storage, and modern transmission technology. In the Internet of Things (IoT) age, when situations such micro-grids and vehicle-to-grid networks play a crucial role, this architecture is crucial for building energy trading mechanisms. However, it has difficulties including safety, private consumption of electricity, system dependability, and energy market uncertainty. This structure aims at solving these issues by dividing energy trade into four tiers, enabling translucent, effective, and reliable energy trading processes in the smart grid Yapa et al [17] Afford a thorough grounding on the fundamental ideas behind energy exchanges and the significance of the technologies that enable it that control power imbalances in the smart electricity system. This paper propose an issue classification that utilizes popular methodologies for promotion, numerical, and simulations based on models energy exchange method control and maintenance. Also propose a solution taxonomy including supporting technologies like Energy Internet, software- defined networking (SDN), and block chain based on what we learn from the literature. To give readers profound insights, a synopsis of possible future study directions based on energy trading systems is examined in the conclusion.

In order to facilitate peer-to-peer (P2P) energy trade in the wholesale power market, Han et al. [18] propose offers an overall basis for a block chain platform. The peer-to-peer energy trading method is intended to focus on finding energy-matching pairings from both sides of the equation and to promote energy trading between manufacturers and customers. A whole energy trading procedure is implemented by the multidimensional block chain platform that was built. The privacy and integrity of trading in energy are considerably increased by smart contracts, which precisely implement the trade and payment regulations without involving humans. The extensive advantages of the suggested system for P2P energy trade have been clearly demonstrated by case studies done on the ethereal private chain. It excels at properly representing market quotes, ensuring that the latest information is available to users. And transparent price data. The system also successfully balances the financial gains of all participants, creating a trading environment that is fair and equal and promotes continued participation. Additionally, it supports sustainability goals by simplifying the incorporation of alternative power sources, making it a desirable option for those who care about the environment. Notably, the system's effective gas usage and smart contract calculation speed show that it can manage transactions efficiently even with several players, thus encouraging wider participation in P2P energy trade. Future efforts have to think about expanding the system's capabilities and evaluating it in various settings.

In the contemporary energy landscape, witnessing a significant shift towards increased electrification of various energy end-uses. This transformation is reshaping electricity networks, primarily due to the proliferation of supplies were scattered across the grid's edges. These dispersed assets now include cutting-edge information and communication technology (ICT) capabilities, such as photovoltaic inverters (PvI), electric vehicle (EV) chargers, wind turbine supervisory burdens, and batteries for storing energy.. These assets are no longer restricted to large utility companies; they can now communicate independently and intelligently. They can make decisions either under human guidance or autonomously, responding to real-time conditions or optimizing their operations. This development represents a growing shift towards a more shifting, distributed energy ecosystem that enables better grid supervisors, more grid integration of renewable energy sources, and increased energy efficiency. It develops a preliminary framework to meet this requirement by visualizing an electrical grid that depends on the direct participation of modern integrated energy producers within a decentralized structure housing specialized coordinated processes. The platform, based on embedded devices now designed as controller connector modules for smart

inverters, was developed as a consequence of research done at ABB Laboratories. Zafar and Ben Slama [19] gives a broad overview of peer-to-peer energy exchange. It examines the degree of decentralization, flexibility, and device dependability as well as how block chain might enhance visibility and performance as a whole. The research is expanded to look at outstanding problems and possible future approaches for P2P block chain-based energy sharing. In reality, this study highlights the value of block chain technology and its applications in future smart grid operations. The report also carefully looks at the problems with block chain integration, assuring that autonomous power grids would operate in the future in a decentralized, safe, and scalable manner. A major disadvantage of block chain is its high development cost.

Guan et al.[20] introduces CP-ABE as the primary method to rebuild the financial model. Cipher text-Policy Attribute-Based Encryption. Furthermore, developed PP-BCETS (Privacy-preserving Block chain Energy Trading Scheme), a generic model for shared transactions. Transaction arbitration in the cipher text form allows for fine-grained control of access. With this layout, the confidentiality of user data is protected to the fullest extent possible, and the payment model's security and dependability are greatly enhanced. A credibility-based equity confirmation agreement process is also suggested in PP-BCETS, which has the potential to significantly improve operational effectiveness. To demonstrate the reliability and applicability of our suggested strategy, assessment of experiments and security analyses are carried out. Due to the inherent openness of block chain technology, privacy disclosure is an issue for chain-based trade models in the context of the Energy Internet within intelligent cities. Block chain's decentralized, unchangeable ledger provides integrity and confidentiality, but it additionally stores activities in a way that is open to the public. While important for reliability and confidence, this transparency may unintentionally divulge private data regarding user interactions, transactional data, and energy usage habits. It is crucial for utilizing privacy-enhancing methods and tactics to strike an equilibrium between openness and data security in these block chain-based platforms since it presents a serious risk to the confidentiality of people and companies engaged in the energy trading industry. Block chain systems could have resource-intensive processes, latency in the network, and misalignment with goals for sustainability.

Research Objective

- Examine how blockchain technology might help with security and transparency concerns in the energy exchange.
- Evaluate how GCN-LSTM affects energy distribution and consumption patterns optimization.
- Examine the advantages of an integrated strategy, such as enhanced resilience, flexibility, and efficiency.
- Determine and resolve obstacles in putting blockchain and GCN-LSTM for energy exchange into practice.
- Examine practical uses for the integration in situations involving smart grids.
- Help build a smart grid that is transparent, adaptable, and resilient to transform energy management and trade.Energy transactions in smart grids are transparent and impenetrable.

3. PROBLEM STATEMENT

The current body of research on blockchain-based and smart grid power systems highlights both the potential benefits and difficulties of incorporating blockchain into the changing energy environment. Have looked at a number of ways that block chain might improve the sustainability, efficiency, and security of smart grid operations. The topics of discussion include decentralized coordination, smart meters, peer-to-peer (P2P) energy trading, and block chain's ability to solve security concerns and enable trustworthy and visible energy transactions [11]. The investigations also recognize the difficulties posed by issues including private use, system reliability, security issues, and market for energy uncertainty [21]. An emphasis on the privacy concerns of blockchain technology is also there, along with initiatives to strike a balance between data protection and openness. The literature does, however, also draw attention to issues such high development costs, labor-intensive procedures, network latency, and possible inconsistencies with sustainability objectives. In light of this, the main issue that needs to be addressed is how the smart grid can use blockchain technology to improve security, handle present issues, and maintain a balance between privacy and transparency while avoiding potential problems with cost, resource efficiency, and network latency. In order to overcome this, we proposed an energy exchange process for smart grids that integrates blockchain technology with GCN-LSTM [22].

4. PROPOSED ENERGY EXCHANGE PROCESS FOR SMART GRID BASED ON INTEGRATING BLOCK CHAIN WITH GCN-LSTM

The integration of block chain technology with Graph Convolutional Networks (GCN) and Long Short-Term Memory (LSTM) networks represents a cutting-edge approach to enhancing the energy exchange process within a smart grid. This advanced system leverages the capabilities of block chain for secure and transparent transaction management while harnessing the power of GCN and LSTM for optimizing energy-related data analysis and forecasting. In this innovative setup, block chain provides a tamper-resistant and decentralized ledger for recording energy transactions, ensuring trust and transparency among participants in the smart grid ecosystem. The integration with GCN enables the network to capture and model the complex relationships and dependencies among various grid components, such as power generators, consumers, and energy storage systems. This allows for more accurate predictions of energy demand, supply, and grid conditions. Furthermore, the inclusion of LSTM networks enables the smart grid to process and analyze time-series data effectively. LSTM's ability to capture temporal dependencies is particularly valuable for forecasting energy consumption patterns and adapting to changing conditions in real-time. This integration enhances the grid's ability to make informed decisions, optimize energy distribution, and facilitate peer-to-peer energy trading. Overall, the integration of block chain with GCN and LSTM networks in the smart grid energy exchange process represents a promising step towards a more efficient, secure, and adaptive energy ecosystem. It enhances the grid's ability to manage energy resources, improve sustainability, and meet the evolving demands of a rapidly changing energy landscape.

4.1 Data Collection

The data set from CICIDS2017 collects 78 attributes and 79 labels using CICFlowmeter-V3.0, closely resembling real-world network information (PCAPs). This data set contains the abstract feature attitudes of 25 people according to the HTTP, HTTPS, FTP, SSH, and email protocols. The information is gathered at different points in time. According to the 2016 McAfee Report, the assaults in this dataset are divided into violent FTP, brute force SSH, DoS, heart bleed, web, infiltration, botnet, and distributed denial of service (DDoS) attacks. And aren't included in any of the databases described above. By applying the Alpha template to simulate various multi-stage attack conditions, CICIDS2017 uses the B-Profile system to accomplish a conceptual features assessment of individual inter-actions. Table 1 shows list of file names along with the classes[23]

Table 1: Datasets along with classes

Name of file	Class found
Monday-Hours.pcap_ISCX.csv	Benign(Normal human activities)
Tuesday-HOURS.PCAP_ISCX.csv	Benign, FTP-patator, SSH Patator
Wednesday-.pcap_iscx.csv	Benign. Dos GoldenEye, DoS lowhttptest, DoS SLOW LORIS, Heartbleed
Thursday-WebAttacks.pcap_ISCX.csv	Benign, Brute Force, SQL Injection, XSS.
Thursday-InFilteration.pcap_.csv	Benign, Infiltration
Friday-pcap-Iscx.csv	Benign, Bot
Friday-PortScan.pcap_ISCX.csv	Benign, PortScan
Friday-DDos.pcap_ISCX.CSV	Benign, DDos

4.2 Data Preprocessing

Pre-processing data is regarded as a single of the crucial and critical phases in the identification of intrusions within research and safety system development. When employing a dataset with high dimensions and numerous features that are redundant in addition to associated characteristics, the existence of datasets in multiple representations and dimensions typically affects computation efficiency and reliability of the method of detection. Before the stage of learning, the collected information must be treated to decrease or remove the undesired properties of the data in order to overcome this obstacle. The properties also include conceptual and numerical information, therefore data could also contain the Nigerian News Agency infinite, or fixed amounts that require specific treatment. The following subsections detail how the preparation in was taken into account when implementing the Botnet datasets preparation steps:

4.2.1 Dataset Cleaning

A major issue that impairs the efficiency of a system is the existence of recurrent and undesirable numbers in the collection of data. Repeating values typically waste time with no adding value, so it is vital to remove them. Due to the availability of discovery techniques that do not deal with NAN and

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Infinity values, for instance, these numbers have to be removed or substituted with alternative values.

4.2.2 Removing Zero-Attributes

In your suggested work, attributes with a single non-null value for every entry are referred to as zero-attributes. These can be identified by techniques like summing or finding the minimum and maximum values to check for zeros. When both the lowest and highest values in a dataset attribute are zero, it's categorized as a 0-attributes type. Removing these zero-attributes is expected to enhance model accuracy.The CICIDS2017 dataset contains ten zero-attributes with identical values across all records, including flags and bulk-related attributes. Eliminating these irrelevant connection characteristics from the dataset doesn't affect estimation outcomes but reduces data complexity and improves throughput. Numeric values are preferred for some detection models, so removing non-essential attributes simplifies computations. Also, issues like NaN and Infinity values are addressed by replacing Infinity with the absolute maximum and NaN with the lowest possible value for data consistency.

4.2.3 Data Normalization

The values of the attributes of the CICIDS2017 dataset show a broad range of values. The accuracy and effectiveness of the developed Botnet detection methodology must thus be improved by data normalization. the results of the current study, one normalization approach called Minmax normalization transforms dataset values into a particular processed range associated with every attribute, as shown in the remaining terms of equation (1). Y = Xi X X X (1), where i is the number on the counter of values Xi of an attribute (X), the lowest and maximum values of an attribute (X) are denoted by Xmin and Xmax. The new informational amount would range from 0 to 1.

4.3 Data authentication using smart grid

Generic authentication protocol to construct safe and decentralized certified connections using block chain technology. Registration and login are two of the steps that make up the authentication protocol. Registration. The cryptographic public key of a user is initially initialized as their private key during the registration phase of our authentication system. Then, we put the connection on a block chain so that the purchase can later be validated by other users. Then, a user-defined, distinctive Username is connected to this identifying key. The user creates an identity transaction after the registration process. Type of Transaction The real block chain event is described by the operation type variable and only takes place when certain users sign with their individual private keys. The payment type is kept in the data block once the authentication process is complete and cannot be altered or faked. Usually, the user name is too lengthy or too illogical to be legible by humans. Consequently, for improved user experience, we allow users to choose a specific, accessible to humans Username and tie this name to their account in our protocol. Other users can seek up the user and other data using this special Username. Many block chain technology options available today can put this kind of binding into place. A smart contract employing an EOS, for instance, can predicament to a readable by humans Username in the Block stack project. Additionally, they create a system that is similar to DNS to offer addressing services, and users may access the Usernames of other users and other pertinent data. These techniques are used in our dispersed protocol as well, where any peer with a complete copy of the block chain data may provide consumers a name service. In our protocol, timestamps are utilized to validate every single business best, which can demonstrate the record's legitimacy, much too how transactional contract are certified. The timestamp offers an inherent period highest for the entire business order as an element of the block information.

It's crucial to make sure that signature doesn't change the substance of a transaction. Even if a transaction has not yet been published on the block chain, it is still possible to view it since it is open. Login. After Someone must import their private key into the online application and commit their identification data before they may log in.In this scenario, the private key can be imported either manually or by detecting a QR code, among other methods. The smart grid network's operator receives an inquiry about login from an individual who needs to log in. Take note that the user's secret key is used to sign the login request. The provider of the service analyzes the username and password request, derives the hash, queries the block chain, gathers identification data from a username and password list (uniqueness transactions), and executes the related smart contract as detailed above. The solution provider sends back a request for authentication when the aforementioned procedure is complete. The authentication request includes the user's Username, their, a timestamp (to thwart a

replay attempt), and a signature. Five variables are generated by the user while creating a signature, which include the timestamp, Username, and the names of the end of the service provider. The transaction's header contains the signature, which is used as the user's identification credentials. If what was provided is accurate, the solution provider confirms it; if not, the verification process is unsuccessful, and the user's login request is rejected.

Following the Login procedure, the supplier of services asks the individual for more personal data to create their account, this will be applied later during the permission process. Creation of smart contracts. To go over how to implement our method, we now provide a description of our suggested smart contract algorithms. The first two essential functions we require are "Query Data" and "Send Transaction." These are the smart contract methods. To search for individuals or list of resources on the block chain, employ the "Query Data" function. The CRUD interface was used by this smart contract to streamline coding in a manner comparable to using relational databases to carry out an action. The information about the account or source transactions may be obtained as a list that is kept in a table, and the intended records can then be accessed by a query using the key-value pair "account ID." When a user requests to log in, the service provider runs the "Query Data" function within the decentralized app in order to query the user's identification data.

To submit an operation to the block chain technology, use the "Send Transactions" feature. In the initial setup stage of the authentication protocol, the user can utilize this function to submit their personal data to the block chain. Following receipt of the trade, the block chain system verifies the registration's legitimacy. The data is subsequently posted to the block chain if the identification information is accurate. Then, we need to complete two different kinds of jobs in order to establish decentralized authentication. One requires accessing the block chain system by invoking the aforementioned smart contract, whereas another includes managing interactions among customers and service providers. The "Registration" and "Login" algorithms make up the distributed authentication system. In order to imitate the signing up process, we created users' public keys and identities at random. The distributed ledger system is built to refuse enrollment and increase the number of failures if an account id already exists.[24] Smart grid composed of energy resource is shown in Figure 2

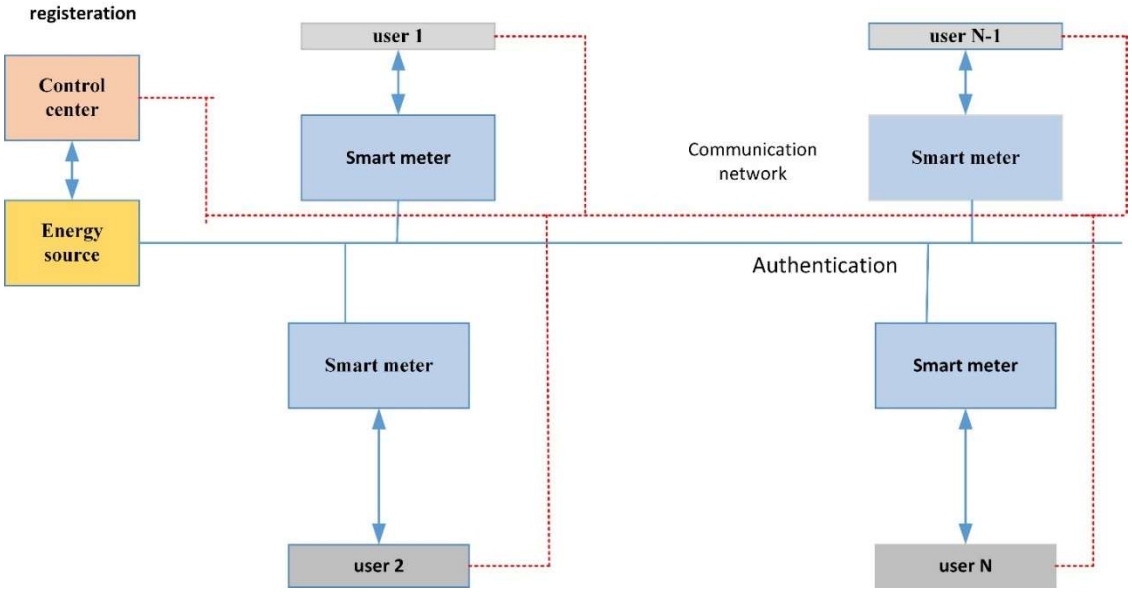

Figure 2. Smart grid composed of energy resource

4.4 Block chain

Block chain is a circulated ledger system that depends on an agreement among participants and communication protocol to protect the ledger's integrity by connecting blocks with cryptographically time-stamped representations of transactions. The Proof of Work (PoW) methodology, used in the creation of bit coin, is where the block chain strategy first emerged.

Trades are included into tree-based blocks by the miner and are encrypted with a predetermined hash range. However, the PoW strategy employing a public ledger has numerous drawbacks in terms of privacy, scalability, transaction volume, and energy usage. In attempt to address the foregoing weakness, several additional block chain-related projects have been launched during the past few years. These innovations include intelligent contracts, consensus mechanisms, and transparency and authorization mechanisms. Below are the specifics of these advances in technology.

4.4.1 Privacy and Permission Mechanism

There are two types of block chains in the block chain system: private and public. The private block chain is an private network that is run and controlled by a group of authorized users. In a block chain that has been granted permission, only parties that have registered can be involved in the block generation process, whereas in an unrestricted block chain, anybody can yield part in agreement building and block creation. Because it relies on participant integrity, the unsupervised block chain is therefore less secure, less secretive, and less visible. Additionally, the authorized block chain has improved access control mechanisms, is highly customizable, and is more secure. In other words, a private chain of blocks is superior to an open block chain in terms of efficiency. As a result, in the framework being demonstrated, we use hyper ledger Fabric, a permissioned block chain that is used for developing blocking network-based services.

4.4.2 Consensus Mechanism

The consensus mechanism is employed in block chain to guarantee consistency and integrity as well as the order of payments across dispersed nodes. The current consensus mechanism, similar to POW, which is utilized by bit coin, uses 47.1 ter a Watt/hour of energy on a yearly basis. Additionally, the PoW consensus mechanism suffers from several transaction count issues that reduce the likelihood of employing the framework in an outstanding performance. Setting. Over the past several years, numerous novel consensus protocols have been created, Some of them use more energy than others, while others help save energy. In this study, we employ PBFT, which reduces the danger of block chain centralization by raising the quantity of payments between each shared additionally, the PBFT reduces energy usage by eliminating the confusion energy required to procedure a block on a block chain.[6]

4.4.3 Smart Contract

An example of a computer program that offers self-execution, self-verification, and impermeable to capabilities is a smart contract. In 1994, Nick Szabo created the leading BondNodules may execute facilities based on the results of processing transactions goal and likewise offer the ability of sophisticated logic thanks to the Turing computer-generated machine and procedure, which are supported by smart contracts. Both consumers and prosumers may conduct energy trading transactions on an efficient and secure platform thanks to smart contracts [25]

4.4.1 Deep learning-based scheme

A robust anomaly detection system is built on a Graph Convolutional Network (GCN) and Long Short-Term Memory (LSTM). This hybrid technique takes advantage of the advantages of both LSTMs and GCNs to efficiently identify anomalies in a variety of data sets, particularly when the data can be shown as a graph or sequential time-series.The GCN component excels in modeling dependencies and connections within graph-based representations of structured data. It works by spreading information throughout the graph's nodes, which enables it to detect complex relationships and patterns. This implies that the GCN can discover anomalies by detecting deviations from the anticipated graph structure or node attributes in the context of anomaly identification.

4.4.1.1 GCN- LSTM Based Anomaly detection system

The method of creating a dynamic graph network from the chosen input data in order to fully represent the connections between properties. The starting organization consists of a matrix of dimensions [mn], whereby each column is randomly chosen from a set of qualities. Utilizing the feature correlation graph G, we provide a straightforward approach for expressing the correlations among characteristics.With the help of this methodology, we may evaluate and comprehend the relationships between the traits that we have chosen.

We used the standard GCN technique to determine the relationship between feature columns since this study concentrates on network intrusion instead of building complex node embed graph models, recognition is used for IDS. A highly complex

embedding of graphs model that has been applied in several graph-based systems is the GCN approach. The layer specification of the GCN neural network is presented in (1)

$$B(l+1)=\mathrm{f}\,(B^{L}),A) \quad (1)$$

Here B^{0} is the starting input in the form of m * n parameters, BL is the graph G's adjacency matrix, and A is the graph G's featured node matrix. The quick estimate convolution on the graph of data may be used to generate the following in layers propagate multilayer graph convolution network (GCN) structure, as indicated in (2)

$$\mathrm{F}(B^{L}),A) =\sigma\,(\hat{C}\text{-}\tfrac{1}{2}\hat{A}\hat{C}\text{-}\tfrac{1}{2}B^{(L)}W^{(L)}) \quad (2)$$

Where, BL, the feature node matrix of graph G, and A, the matrices of adjacency of graph G, are the input data with m * n dimensions. We could also derive the subsequent layer-by-layer propagating multilayer graph convolution network (GCN) formulation using the fast approximation convolution on the graph, as given in (3).

$$\hat{A} =\mathrm{A}+ I_{N} \quad (3)$$

The unstructured graph G has additional self-connections, is the particular adaptable matrix of weights in the layer relationships, and is the unit of matrix. The activation function is represented.

The feature selection module for the GCN (Graph Convolutional Network) is displayed. There are separate specimens test 1, sample, and m more arbitrarily chosen samples on the left side of the picture labeled in (4)

$$\hat{C}_{ij=\Sigma_{j}\hat{A}_{IJ}} \quad (4)$$

The feature selection module for the GCN (Graph Convolutional Network) is displayed. There are separate specimens labeled sample 1, model, and m more aimlessly chosen samples on the left side of the picture. The Batch-Size determines the value of m, and since each sample has n characteristics, the matrix has a size of [mn]. This matrix's columns each correspond to a distinct feature column, which is indicated by the form [m1]. These characteristic columns that were retrieved are regarded as nodes and together make up an evolving graph. A new feature node connected to the node F1 is created on the right side by treating all the other nodes in its vicinity together and averaging their data. Each feature node goes through this procedure again, creating a collection of feature nodes [f1,f2,...,fn]. The true feature node, which is a condensed representation of the [m,n]data matrix, is obtained by averaging these feature nodes.[26]

4.4.1.2 Automatic feature selection module

The method of creating an participation characteristic matrix [MN] by selection data samples at random from a dataset with N features. The computerized feature selection module then receives the feature vector f that was extracted using the GCN characteristic identification module as its input. Every function in this module has a designated agent that evaluates whether to keep it depending on input data and environmental feedback. The autonomous feature selection module uses a reinforcement learning multi-agent framework to create a Markov Decision Process (MDP) that combines representatives, states that actions, rewards, and policy functions [27].The model learns the ideal management function for every state via the agents by defining the MDP, and then it performs activities that optimize the total reward R.GCN feature selection module is shown in FIG:3

Journal of Theoretical and Applied Information Technology
31st December 2023. Vol.101. No 24

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

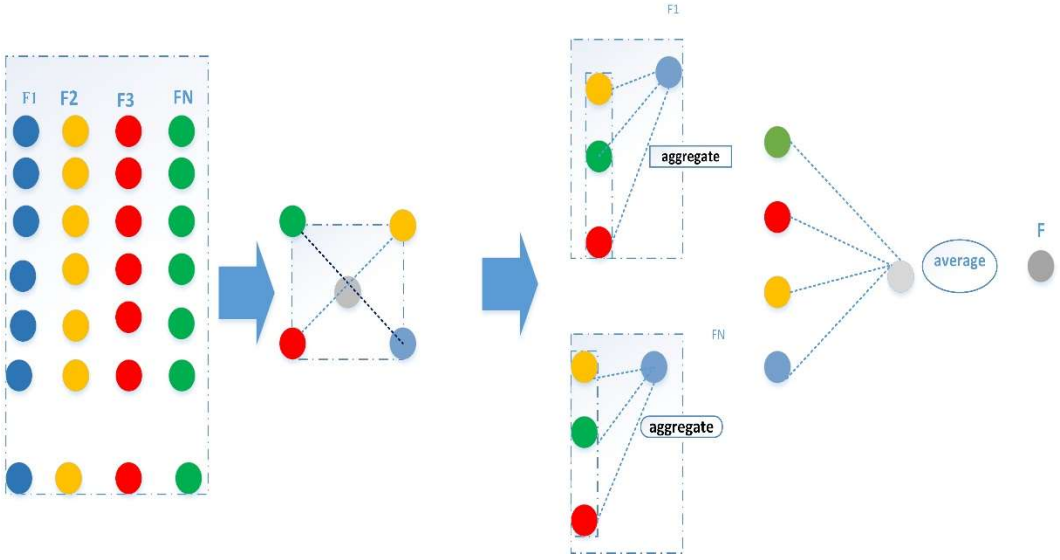

Figure 3: GCN feature selection module

The difficulty of feature categorization in anomaly detection may be effectively overcome by combining Graph Convolutional Networks with Long Short-Term Memory networks. The model can recognize complex relationships, dependencies, and temporal patterns within complex data thanks to this combination of deep learning paradigms, improving the precision and adaptability of anomaly detection systems across a variety of domains. First, the LSTM-based classifier is qualified using the CSE-CIC-IDS2018 dataset. Before sending the data to the classifier, the fingerprint analysis is also done to determine the potential characteristics of known IoT threats. By altering hyper-parameters, the algorithm's detection accuracy is assessed and enhanced. The classifier must be put into use after training if the IoT is to identify anomalies. Setting up a timer is the first step in the procedure. When a host exhibits any kind of harmful behavior, it is placed to a group of suspect hosts named The list is extended until, during a set time frame, its count exceeds a predetermined threshold value. The sites on the list of targets are then put on hold and suspect hosts are assessed once again in order to precisely detect attacks..[28]

among grid participants. Meanwhile, GCN's incorporation has bolstered predictive analytics, enabling the smart grid to model intricate relationships among various grid components. This has notably improved the accuracy of energy demand and supply forecasts, leading to more efficient energy distribution and grid management. Additionally, LSTM networks have empowered the grid to adapt in real-time, particularly crucial when dealing with renewable energy sources' intermittency and fluctuations in energy demand. These improvements have facilitated informed decision-making, allowing for optimized energy allocation and grid stability.

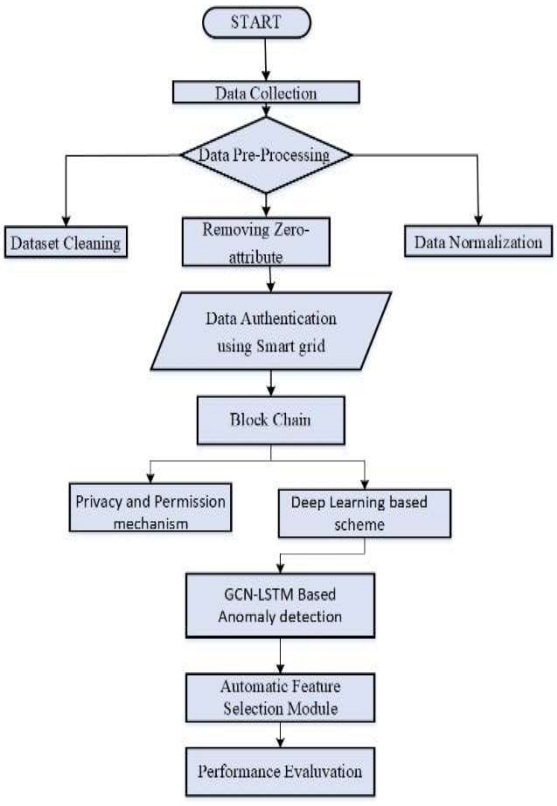

Figure 4: Flowchart of proposed method

5. RESULT AND DISCUSSION

The integration of block chain has significantly enhanced the safety and clearness of energy transactions within the smart grid. Block chain's tamper-resistant ledger ensures that all energy-related data is secure and immutable, reducing the risk of fraudulent activities and enhancing trust

5.1 Evaluating attack detection in different dataset

Attack detection, which aims to find and reduce hostile activity and online threats, is a crucial component of cyber security. Various datasets have been created and used by researchers and security professionals to develop and evaluate attack detection algorithms and models. Below Table:2 shows datasets commonly used for attack detection along with their general characteristics.

Table 2: Attack detection in different datasets

Name of the dataset	Attack model	Finest time era	Ideal value
ISCX-IDS-2012	HIGH VALUE	43	-0.1
CTU-10	HIGH VALUE	43	2.5
CTU-11	HIGH VALUE	12	1.3
CICIDS2017	HIGH VALUE	15.1	-1.5

Table 3. The accuracy assessment of the proposed Anamoly detection

	Accuracy	Training time(s)			Testing time(s)		
		CPU	GPU	TPU	CPU	GPU	TPU
HN=10	95.77	110	14.3	13.8	2.15	1,21	1.20
HN=20	96.88	456.7	30.8	33	1.67	1.87	3.22
HN=30	97.78	921.6	67.98	45	1.78	8.98	16.67
HN=40	98.65	1022.7	56.8	76	17.88	76.8	15.88
HN=60	99.55	1766.6	110.4	89	72.66	87.78	87.33

The accuracy assessment of the proposed Anamoly detection using the CICIDS2017 dataset has been conducted, considering variations in hardware accelerators and hidden node configurations. This assessment attempts to thoroughly evaluate the IDS's functionality and its responsiveness to hardware and neural network architectural decisions. Beginning with a variety of hardware platforms, including Central Processing Units (CPUs), Graphics Processing Units (GPUs), and specialized hardware accelerators like Field-Programmable Gate Arrays (FPGAs) or Tensor Processing Units (TPUs), the IDS has undergone extensive testing. Each hardware accelerator offers distinct attributes in terms of parallelism and computational capacity, which can distinctly influence the IDS's processing speed and, more importantly, its accuracy in detecting network intrusions.

5.2. Evaluation metrics

Accuracy, detection rate (DR), and false alarm rate (FAR), which are specified below, are the three essential gauges of performance that we utilize to evaluate the effectiveness of the suggested IDS model. Of course, let's give a technical breakdown of the metrics used to assess the effectiveness of a system that detects intrusions.A key criterion for evaluating a classification model's ultimate quality is accuracy. It is determined as the percentage of all correct classifications throughout the full dataset (including true positives and true negatives). The definition of correctness in mathematics is (5):

$$\text{Accuracy}=\frac{tp+tn}{tp+tn+fp+fn} \quad (5)$$

The capacity of the system to accurately identify positive cases—in this example, attacks—is measured by the detection rate, also known as sensitivity or recall. It is determined as the ratio of

true positives (attacks that were accurately recognized) to all real attacks (attacks that were both true positives and false negatives). Mathematically,

$$\text{Detection rate}=\frac{tp}{tp+f} \quad (6)$$

The likelihood that the system would issue false alerts or mistakenly identify legitimate data as assaults is quantified by the false alarm rate. It is determined by dividing the percentage of false positives (attacks that were wrongly recognized) by the total number of benign occurrences (including true negatives and false positives). The false alarm rate is described theoretically as (7):

$$\text{False alarm rate}=\frac{fp}{fp+tn} \quad (7)$$

5.3 Training and Testing Accuracy

The graph shows how a usual machine-learning algorithm that was developed using the suggested technique performed throughout a number of training epochs. The quantity of training epochs is shown on the x-axis. showing how the training process is developing. The accuracy values, which range from 0 to 1, are represented on the y-axis and show how well the model's forecasts match the true labels. Illustration in graphics for Training and Validation Precision is provided in Figure 5

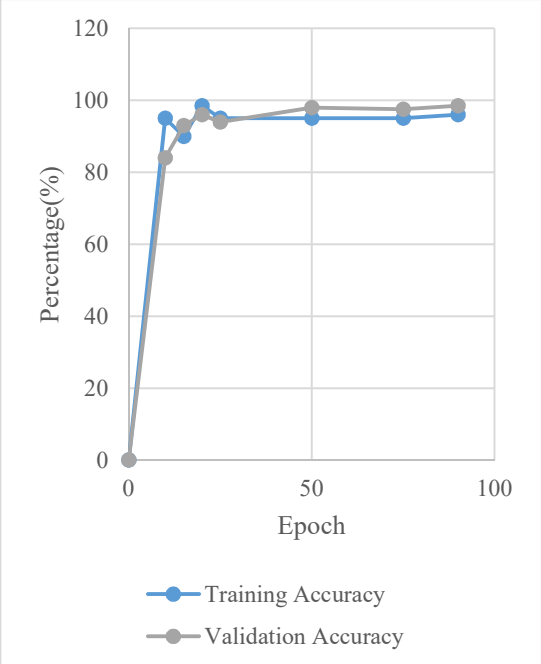

Figure 5: Graphical depiction for Training and Validation Accuracy of proposed method

5.4 Model loss

Visualizing how the loss function varies throughout training epochs is required to provide a graphical depiction of the loss during the training process of the proposed GCN-LSTM model. Here is a description on how to read this type of graph. As a result, the graphs above clearly demonstrate that both our training and testing accuracy are increasing over time, which suggests that the model is getting much better over time. Furthermore, it is clear that the loss of our model is decreasing is given in Figure 6

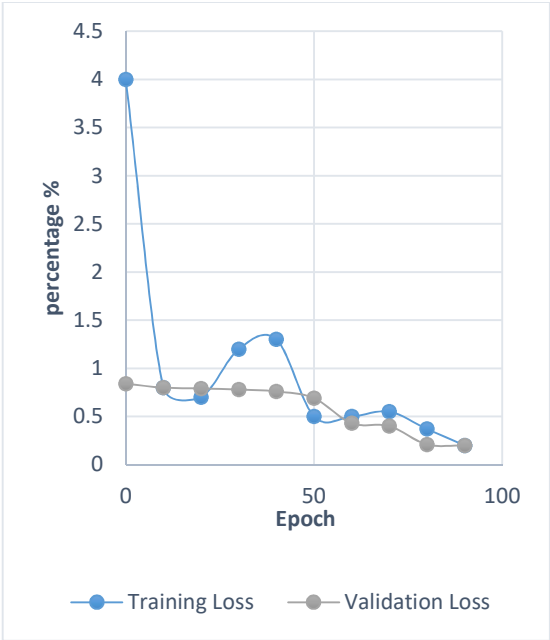

Figure 6: Graphical representation of loss in proposed GCN-LSTM

Table 4 Comparisons of the suggested strategy with certain recent strategies

Method	Dataset	Accuracy
CNN[29]	MNIST	97.32%
LSTM[30]	Power system	96.27%
DBF	D1,D2	98.86%
Proposed GCN-LSTM	CICIDS2017	99.30%

The provided table offers a concise summary of the performance results achieved by various machine learning methods on different datasets, highlighting their respective accuracy percentages. First, the Convolutional Neural Network (CNN) model developed evaluated on the MNIST dataset, where it achieves an impressive accuracy rate of 97.32%. Moving on to the Long

Short-Term Memory (LSTM) model, demonstrates a commendable accuracy of 96.27% when applied to power system data. The Differential Bacterial Foraging (DBF) method, utilized on two distinct datasets labeled as D1 and D2, attains an accuracy of 98.86%. Lastly, the table showcases the performance of the proposed GCN-LSTM model on the CICIDS2017 dataset, where it achieves a remarkable accuracy of 99.30%. This suggests that the combination of Graph Convolutional Networks (GCN) and Long Short-Term Memory (LSTM) architecture is exceptionally adept at detecting and classifying network intrusions in the realm of cyber security. In sum, these accuracy percentages not only reflect the success of each respective method within its specific domain but also serve as crucial benchmarks for assessing the efficacy of machine learning and deep learning models across diverse datasets and applications. Figure 7 shows Comparison of proposed approach with some recent approaches.

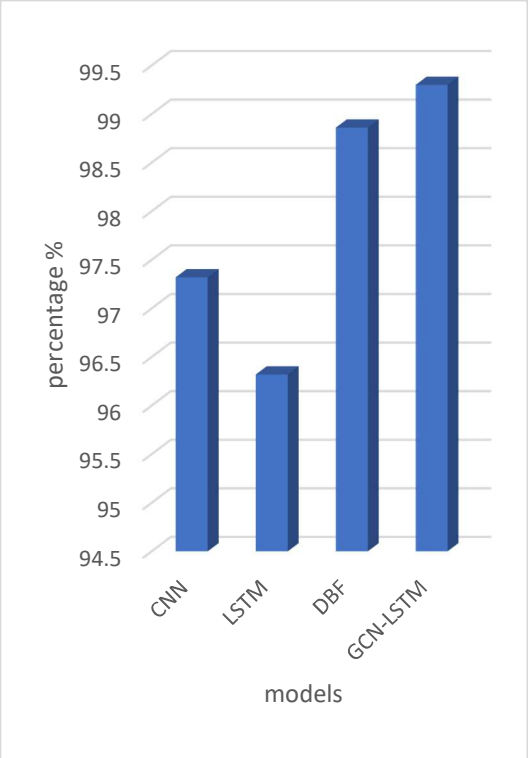

Figure: 7 Comparison of proposed approach with some recent approaches

6. CONCLUSION AND FUTURE WORKS

The integration of blockchain technology Graph Convolutional Networks (GCN) and with Long Short-Term Memory (LSTM) models offers a revolutionary approach to tackle significant obstacles in the energy exchange procedure inside the smart grid. In addition to guaranteeing safe and transparent transaction recording via blockchain, this technological synergy makes use of GCN-LSTM's analytical capabilities to comprehend and improve grid dynamics and energy consumption trends. As a result, the smart grid is now more data-driven, robust, and efficient, better able to adapt to changing energy-related needs.By reducing the risks of fraud and guaranteeing data privacy, the integrated method promotes peer-to-peer trade between producers and consumers through safe and transparent energy transactions. Improved grid management results in better energy distribution and overall grid stability thanks to the data-driven insights produced by GCN-LSTM models. The union of blockchain technology with GCN-LSTM models presents a formidable instrument in the pursuit of sustainability and efficiency in energy systems, hence holding the potential to transform energy exchange, management, and consumption in forthcoming smart grids.But overcoming significant obstacles is necessary for this integrated strategy to be implemented successfully in the real world. Careful consideration of scalability, interoperability, and energy efficiency is necessary to guarantee broad acceptance and smooth integration into current energy infrastructures. Sustained R&D should concentrate on improving the integrated system, investigating realistic deployments, and carrying out extensive testing in various smart grid scenarios. It will need cooperative efforts combining academics, business leaders, and legislators to overcome these obstacles and realize the full promise of this ground-breaking and inventive strategy. By doing this, we may open the door to a future in smart grid energy systems that is more robust, sustainable, and intelligent.

REFERENCES

[1] T. Alladi, V. Chamola, J. J. P. C. Rodrigues, and S. A. Kozlov, "Blockchain in Smart Grids: A Review on Different Use Cases," *Sensors*, vol. 19, no. 22, p. 4862, Nov. 2019, doi: 10.3390/s19224862.

[2] R. Khalid, N. Javaid, A. Almogren, M. U. Javed, S. Javaid, and M. Zuair, "A Blockchain-Based Load Balancing in Decentralized Hybrid P2P Energy Trading

Market in Smart Grid," *IEEE Access*, vol. 8, pp. 47047–47062, 2020, doi: 10.1109/ACCESS.2020.2979051.

[3] S.-K. Kim and J.-H. Huh, "A study on the improvement of smart grid security performance and blockchain smart grid perspective," *Energies*, vol. 11, no. 8, p. 1973, 2018.

[4] J. J. Sikorski, J. Haughton, and M. Kraft, "Blockchain technology in the chemical industry: Machine-to-machine electricity market," *Applied Energy*, vol. 195, pp. 234–246, Jun. 2017, doi: 10.1016/j.apenergy.2017.03.039.

[5] H. T. Doan, J. Cho, and D. Kim, "Peer-to-Peer Energy Trading in Smart Grid Through Blockchain: A Double Auction-Based Game Theoretic Approach," *IEEE Access*, vol. 9, pp. 49206–49218, 2021, doi: 10.1109/ACCESS.2021.3068730.

[6] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *International Journal of Information Management*, vol. 39, pp. 80–89, Apr. 2018, doi: 10.1016/j.ijinfomgt.2017.12.005.

[7] A. S. Musleh, G. Yao, and S. M. Muyeen, "Blockchain Applications in Smart Grid–Review and Frameworks," *IEEE Access*, vol. 7, pp. 86746–86757, 2019, doi: 10.1109/ACCESS.2019.2920682.

[8] A. Kumari, R. Gupta, S. Tanwar, S. Tyagi, and N. Kumar, "When Blockchain Meets Smart Grid: Secure Energy Trading in Demand Response Management," *IEEE Network*, vol. 34, no. 5, pp. 299–305, Sep. 2020, doi: 10.1109/MNET.001.1900660.

[9] A. Hasankhani, S. Mehdi Hakimi, M. Bisheh-Niasar, M. Shafie-khah, and H. Asadolahi, "Blockchain technology in the future smart grids: A comprehensive review and frameworks," *International Journal of Electrical Power & Energy Systems*, vol. 129, p. 106811, Jul. 2021, doi: 10.1016/j.ijepes.2021.106811.

[10] D. Immaniar, A. A. Aryani, and S. Z. Ula, "Challenges Smart Grid in Blockchain Applications," *B-FronT*, vol. 2, no. 2, pp. 1–9, Sep. 2022, doi: 10.34306/bfront.v2i2.150.

[11] X. Chen, J. Shen, Z. Cao, and X. Dong, "A Blockchain-Based Privacy-Preserving Scheme for Smart Grids," in *Proceedings of the 2020 The 2nd International Conference on Blockchain Technology*, Hilo HI USA: ACM, Mar. 2020, pp. 120–124. doi: 10.1145/3390566.3391667.

[12] X. Lu, Z. Guan, X. Zhou, X. Du, L. Wu, and M. Guizani, "A Secure and Efficient Renewable Energy Trading Scheme Based on Blockchain in Smart Grid," in *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*, Zhangjiajie, China: IEEE, Aug. 2019, pp. 1839–1844. doi: 10.1109/HPCC/SmartCity/DSS.2019.00253.

[13] M. Shafay, R. W. Ahmad, K. Salah, I. Yaqoob, R. Jayaraman, and M. Omar, "Blockchain for deep learning: review and open challenges," *Cluster Computing*, vol. 26, no. 1, pp. 197–221, 2023.

[14] S. S. Uddin *et al.*, "Next-generation blockchain enabled smart grid: Conceptual framework, key technologies and industry practices review," *Energy and AI*, vol. 12, p. 100228, Apr. 2023, doi: 10.1016/j.egyai.2022.100228.

[15] M. K. Hasan *et al.*, "Blockchain technology on smart grid, energy trading, and big data: security issues, challenges, and recommendations," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–26, 2022.

[16] A. Baggio and F. Grimaccia, "Blockchain as Key Enabling Technology for Future Electric Energy Exchange: A Vision," *IEEE Access*, vol. 8, pp. 205250–205271, 2020, doi: 10.1109/ACCESS.2020.3036994.

[17] C. Yapa, C. De Alwis, M. Liyanage, and J. Ekanayake, "Survey on blockchain for future smart grids: Technical aspects, applications, integration challenges and future research," *Energy Reports*, vol. 7, pp. 6530–6564, Nov. 2021, doi: 10.1016/j.egyr.2021.09.112.

[18] D. Han, C. Zhang, J. Ping, and Z. Yan, "Smart contract architecture for decentralized energy trading and management based on blockchains," *Energy*, vol. 199, p. 117417, May 2020, doi: 10.1016/j.energy.2020.117417.

[19] 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," *Sensors*, vol. 22, no. 21, p. 8397, 2022.

[20] Z. Guan, X. Lu, W. Yang, L. Wu, N. Wang, and Z. Zhang, "Achieving efficient and Privacy-preserving energy trading based on

blockchain and ABE in smart grid," *Journal of Parallel and Distributed Computing*, vol. 147, pp. 34–45, 2021.

[21] E. S. Kang, S. J. Pee, J. G. Song, and J. W. Jang, "A Blockchain-Based Energy Trading Platform for Smart Homes in a Microgrid," in *2018 3rd International Conference on Computer and Communication Systems (ICCCS)*, Nagoya, Japan: IEEE, Apr. 2018, pp. 472–476. doi: 10.1109/CCOMS.2018.8463317.

[22] V. Hassija, V. Chamola, S. Garg, D. N. G. Krishna, G. Kaddoum, and D. N. K. Jayakody, "A Blockchain-Based Framework for Lightweight Data Sharing and Energy Trading in V2G Network," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5799–5812, Jun. 2020, doi: 10.1109/TVT.2020.2967052.

[23] Z. Wu, H. Zhang, P. Wang, and Z. Sun, "RTIDS: A Robust Transformer-Based Approach for Intrusion Detection System," *IEEE Access*, vol. 10, pp. 64375–64387, 2022, doi: 10.1109/ACCESS.2022.3182333.

[24] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Comput Sci Res Dev*, vol. 33, no. 1–2, pp. 207–214, Feb. 2018, doi: 10.1007/s00450-017-0360-9.

[25] F. Jamil, N. Iqbal, Imran, S. Ahmad, and D. Kim, "Peer-to-Peer Energy Trading Mechanism Based on Blockchain and Machine Learning for Sustainable Electrical Power Supply in Smart Grid," *IEEE Access*, vol. 9, pp. 39193–39217, 2021, doi: 10.1109/ACCESS.2021.3060457.

[26] V. V. Belikov, "Using Deep Reinforcement Learning for Selecting Network Traffic Features in Intrusion Detection Systems," *Program Comput Soft*, vol. 48, no. 6, pp. 359–368, Dec. 2022, doi: 10.1134/S0361768822060020.

[27] A. Savelyev, "Copyright in the blockchain era: Promises and challenges," *Computer Law & Security Review*, vol. 34, no. 3, pp. 550–561, Jun. 2018, doi: 10.1016/j.clsr.2017.11.008.

[28] A. Wani, R. S, and R. Khaliq, "SDN-based intrusion detection system for IoT using deep learning classifier (IDSIoT-SDL)," *CAAI Trans on Intel Tech*, vol. 6, no. 3, pp. 281–290, Sep. 2021, doi: 10.1049/cit2.12003.

[29] J. Weng, J. Weng, J. Zhang, M. Li, Y. Zhang, and W. Luo, "Deepchain: Auditable and privacy-preserving deep learning with blockchain-based incentive," *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 5, pp. 2438–2455, 2019.

[30] M. Keshk, B. Turnbull, N. Moustafa, D. Vatsalan, and K.-K. R. Choo, "A Privacy-Preserving-Framework-Based Blockchain and Deep Learning for Protecting Smart Power Networks," *IEEE Trans. Ind. Inf.*, vol. 16, no. 8, pp. 5110–5118, Aug. 2020, doi: 10.1109/TII.2019.2957140.