Deep Learning, blockchain based multi-layered Authentication and Security Architectures

Hariket Sukesh Kumar Sheth
School of Computer Science and Engineering
Vellore Institute of Technology, Chennai
Chennai, Tamil Nadu, India
0000-0001-5283-7716

Ilavarasi A K
Centre for Healthcare Advancement, Innovation and Research. School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, 600127, Tamil Nadu, India.

Amit Kumar Tyagi
Centre for Advanced Data Science
Vellore Institute of Technology, Chennai
Chennai, Tamil Nadu, India
0000-0003-2657-8700

***Abstract*— Because of its ability to make educated judgments, deep learning has gained massive attention in recent years. Many of today's deep learning systems rely on centralized servers and lack operational transparency, traceability, depend- ability, security, and trustworthy data provenance. Furthermore, using centralized data to train deep learning models exposes them to the single point of failure issue. The relevance of combining blockchain technology and deep learning is highlighted in this study. Deep-learning (DL) techniques are used to authenticate and identify abnormalities and provide security for systems (in cryptographic and biometric systems). Confidentiality and effectiveness must be balanced since network sensors are energy- constrained devices, which is the most crucial idea to consider when establishing a security system that relies on deep-learning techniques and blockchain. Centralized systems have several flaws. Mostly, a network with significant demand for smart devices creates a prodigious amount of data. There is always the possibility that one or more of the centralized network's major components would fail, causing a catastrophic (or full) system failure. The data acquired by the centralized cloud storage frequently necessitates third-party modification. This may result in data breaches, jeopardizing the privacy of the end-user. In this paper, we primarily draw the attention and focus on the security models proposed in terms of authentication and security using Blockchain, Deep Learning, or the integration of both based on certain characteristics to identify and organize the literature, in-clouding type, models, consensus protocols, applications, services, and deployment goals.**

***Index Terms*—Authentication Methods, Deep Learning, Blockchain, Multi Layered Security Architecture, Health, IoT, Deep Q Learning**

I. INTRODUCTION

Deep learning's promise has been seen in practically every industry area. In the healthcare industry, clinicians employ deep learning models to identify a patient's ailment, based on their symptoms properly. Deep learning models were used to predict the disease spread rate in a specific region during the recent pandemic caused by the spread of coronavirus disease (COVID-19) and assist authorities in managing the pandemic using the forecasted results during the recent pandemic caused by the spread of coronavirus disease (COVID-19).

Furthermore, utilizing a dataset of CT (computed tomography scan) and X-ray pictures, new deep learning approaches have aided health practitioners in identifying COVID-19 patients.[7] Blockchain is gaining traction as a technology that can help global supply networks become more sustainable. Blockchain is a public, distributed ledger technology that provides new methods for protecting and distributing data in a peer-to-peer setting using permanent and verifiable transaction records. By improving security, accountability, and efficiency, the technology is said to offer tremendous promise for supply chain sustainability.[6] Deep learning models can aid authorities in spotting any physical threats in real-time using biometric authentication and facial recognition capabilities.[5] The data quality utilized even during the model training phase determines a deep learning system's efficacy and efficiency. The bulk of deep learning algorithms relies on centralized storing and analysis for model training, which is vulnerable to a single point failure and data manipulation by adversaries. Any change to the data used in deep learning operations has the potential to damage the training model. Blockchain is a decentralized system that can manage the integrity of data, security, and secrecy effectively.[2][3] Blockchain technology is being positioned as a possible Sustainability-Oriented Innovation in this regard (SOI) [1]. The combination of deep learning with blockchain can provide several advantages, including autonomous and trustworthy decision making, efficient data market adminis-tration, data security, improved model building for prediction, model sharing, and increased resilience of deep learning-based systems.

II. MOTIVATION AND STRUCTURE OF WORK

Unethical hackers will find it incredibly difficult to edit, manipulate, or destroy anything stored on the blockchain. It is a decentralized system that [4] stores and processes transactions and data using a peer-to-peer (P2P) architecture. It is made up of a large number of nodes that validate and store transactions in the block form. Every block in the chain contains a set of transactions, and the old blocks are connected appropriately to the newly formed block to build the chain of blocks. To guarantee data consistency, once a miner adds a block to its local chain, the newly added block is disseminated to all participating nodes. Artificial intelligence and machine learning are both supersets of deep learning. A model can learn the latent space representation of all the most fundamental kinds of data, such as pictures, text, and audio signals, in existing deep learning systems. Deep learning enables the hardware to execute numerous tasks with human-like precision, or even better than humans in some circumstances. Image classification, object identification, self-driving cars, illness predictions, [9] and voice recognition are just a few examples of deep learning applications in many industries. The structure of this paper

is as follows: Section 3 would be discussing the integration of blockchain and Deep Learning mostly and what are the notable pros and cons of the same. Section 4 and 5 would be highlighting the various models proposed by several authors and the applications of Blockchain and Deep Learning in various domains. Section 6 would be stating the open issues in terms of authentication, Multi-Layered Security architectures. Section 7 would be a discussion on the scope of the integration of Blockchain, Deep Learning in future technologies, and the authors would be concluding the paper, along with focusing more on research gaps and future work.

III. INTEGRATION OF DEEP LEARNING AND BLOCKCHAIN

Different entities construct, utilize, and train deep learning models. The authenticity of deep learning models may be established via blockchain technology, resulting in trusted artificially intelligent (AI) systems. It records the many stages of the model throughout its development, modification, or use and captures the overall progression of deep learning models as they advance. Specifically, it aids in identifying the owner of deep learning algorithms, datasets, data sources, participants, the base model, and procedures involved in model generation utilizing the record of immutable transactions in the blockchain.

The reusability and trustworthy distribution of deep learning models is a criterion that blockchain technology can meet. Similarly, the main objectives for the inclusion of blockchain with deep learning are audibility, verification, attestation of findings, provenance, ownership traceability, utilization, and assurance of fairness. Deep learning models take instances, which the models utilize to master the features and provide an output with probabilistic vectors. Even though deep learning models perform remarkably well on raw data, the data quality still counts in many real-world settings when it comes to prediction. Blockchain and Deep learning can work together to create a robust, durable, and decentralized infrastructure for the data that deep learning applications would gather, analyze, and use.

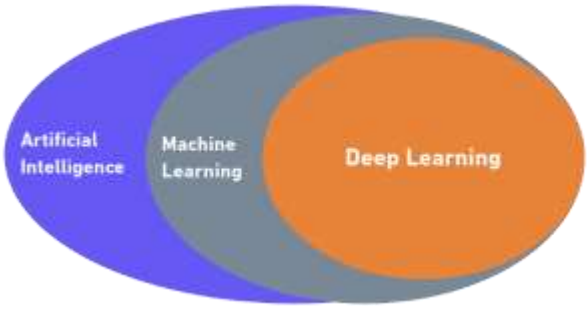

Fig. 1. explains how different domains such as Deep Learning (DL), Artificial Intelligence, and Machine Learning (ML)are interrelated. This interrelation even helps understand the complexity and analysis of how useful each of the domains could be in solving real-world issues. To provide visibility, production, security, and compliance checks, organizations are now depending on smart contracts and bitcoin blockchain-based procedures as part of the manufacturing process.

Machine learning prediction algorithms are utilized to develop flexible plans rather than typical set machine maintenance schedules.

A. Pros for the Integration of Blockchain based Deep learning Models

Quality control and product testing have also become more automated**. Fig. 2** explains Deep learning areas such as Image Recognition, Voice Recognition, text prediction, Intelligent Data Interpretation, Optical Character Recognition (OCR), and Sensory Data Analysis. These are used in today's world for future predictions, analysis. All of the processes include data acquisition and gathering a sufficient amount of data to export. Produce accurate yet reliable results. With added integration of Blockchain, such areas can flourish because of the added advantages such as the Increased and Enhanced Data Security, Cumulative and Smart Judgements, Accurate Predictions, Automation, and Improved Robustness.

Figure 2: Deep Learning Techniques and Benefits from Blockchain integration

The blockchain is a distributed, decentralized, and verified global database where all network nodes [8] may store and exchange data. Deep learning and blockchain, when combined, can provide a robust, durable, and decentralized infrastructure for the data that deep learning-driven applications will gather, analyze, and use.

Table I illustrates some of the major characteristics of blockchain and deep learning. This gives a brief overview of how certain features of both the technologies – Blockchain and Deep Learning could be used extensively for contouring the open challenges in various domains.

The bulk of anti-malware software programmers employ signature-based detection to protect legitimate traffic against attacks. A signature is indeed a short string of characters that is distinctive to each identified piece of malware and allows future samples to be classified effectively and with a low rate of error. Malware attackers, on the other hand, may readily resist this technology using tactics like encryption, polymorphism, and obfuscation. Additionally, rogue files are being distributed at a pace of thousands each day, making this signature-based strategy ineffective. Intelligent malware detection solutions must be researched in order to combat malware attacks. Different types of classification algorithms, such as Artificial Neural Networks (ANNs), Decision Tree (DT), Support Vector Machines (SVM), Nave Bayes (NB) [11] are used to build models to identify malware based on different feature representations. The majority of these techniques rely on learning - based architectures. Shallow learning architectures have seen some progress in malware detection, but they are still unsatisfactory for malware detection challenges.

entire chain is the

TABLE I

ILLUSTRATES SOME OF THE MAJOR CHARACTERISTICS OF BLOCKCHAIN AND DEEP LEARNING. THIS GIVES A BRIEF OVERVIEW OF HOW CERTAIN FEATURES OF BOTH THE TECHNOLOGIES – BLOCKCHAIN AND DEEP LEARNING COULD BE USED EXTENSIVELY FOR CONTOURING THE OPEN CHALLENGES IN VARIOUS DOMAINS.

Deep Learning	Blockchain	Outcomes
Integration of Data-Intensive Approaches and Big Data Analytics	Cybersecurity	Fights hacking with immutability of ledger. It provides validity with data integrity. Decreased IP-Based DDoS (Distributed Denial of Service) Attacks and No Single Point of Failure
Model with a Large Number of Layers, Application of Resource -Intensive Property	IoT, Insurance	Application across various industries such as the supply chain integrity, Trucking, transportation; Streamline risk contract efficiency, Streamline Claims adjudication, increase in transparency with shared data
Supervised, Semi-Supervised or Unsupervised	Forecasting	Combined with machine Learning Algorithms and features of both blockchain and deep learning, this could lead to an efficient decentralized forecasting tool
Diagnosis and Scalability	Legal, Immutability	Maintaining smart contracts with certain defined rules, expiration and accessibility for relevant parties Because of the features like scalability and immutability, the system could be highly reliable and secure for legalities and high prioritized works.
Optimized prioritized and corner parameters, Fault Tolerance	Banking, Financial and FinTech, Transparency	Payments streamlining with increased and improved efficiency. This will not only minimize auditing complexity but also help in empowering global transactions which can help removing the national currency borders.

- **Data Security:** Because blockchain is a decentralized system, the information saved on it is extremely safe. For processing and storing privacy and confidentiality, private blockchain systems are used. The nodes' private keys must be kept secret since they may be the sole method to retrieve the blockchain data. [12] Deep learning algorithms can be executed on the blockchain's stable data, resulting in more reliable, accurate, and dependable decision-making.

- **Automated Decision - making process:** Blockchain is the well technology that facilitates peer-to-peer transactions. The traceability feature makes it simple to validate the judgments produced by deep learning models. It also assures that throughout the human-assisted auditing step, the papers have still not been tampered with.

B. Limitations of Deep learning and Blockchain

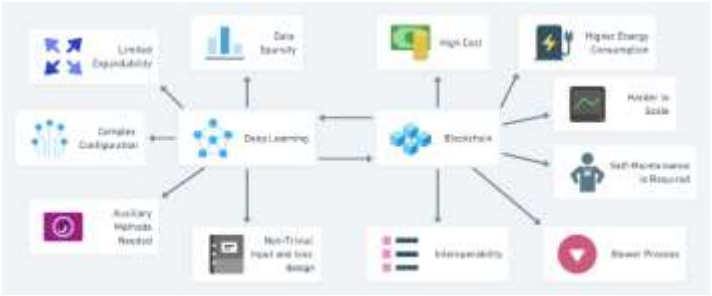

Figure 3: Overview of Cons of Deep Learning and Blockchain

Fig.3 gives a heads-up into the combined Cons of the integrated Deep Learning and Blockchain that either are faced by certain section and rest are expected Cons that could arise at a later point of development process.

- **Usability of Blockchain Nodes:** [12] The ability to split Blockchain's next issue. Endpoints that are still running the outdated software would refuse to acknowledge transactions from the new chain. This chain follows the same path as the last software-based chain. It is referred to as the fork.
- **High Dependency on Energy:** The Blockchain's main disadvantage is that it uses a lot of energy. The usage of energy is required to keep a real-time ledger. Every time a major node is established, it simultaneously links to the existing nodes. [13].
- **Guarantee Factor:** Decision Trees are less predictive and therefore can lead to overfitting. When using logical regression, however, it is possible that it will suffer from multicollinearity. It's challenging to manage mixed-type data in models like the k-nearest neighbor (k-NN) classifier, rendering it vulnerable to linked inputs and irrelevant characteristics.
- **Computational Scalability:** The intuitive handling of varying complexity and computational scalability are both lacking in models like the Support vector machine (SVM). When expanding the number of training dataset in approaches such as Nave Bayes, they are subject to bias.
- **Interpretation of the Result:** It's difficult to evaluate the results of models like k-nearest neighbor (k-NN), and the success of these kind of models is highly reliant on a variety of factors. In the Nave Bayes model, however, all characteristics are considered to be independently and equally essential, which is exceedingly implausible in real-world situations. Even the most data in support algorithms cannot provide the worldwide optimum decision tree. Deep Learning methods such as Decision can handle both categorical and numerical input, but even the most based on cognitive algorithms cannot revert back the globally ideal decision tree. It can't even deal with linear features

combinations.

- **Neural Networks:** On one hand, Neural Networks [14] are strong predictors in general, with appropriate tolerance for coupled inputs. The predictive value of diverse combinations of inputs is also included into neural networks. However, irrelevant traits are extremely sensitive to neural networks. Dealing with massive data and complicated models becomes inconveniently challenging.
- **Deep Learning Classification Framework:** Deep Learning Frameworks [15] such as PyTorch, have drawbacks, such as a lack of server architecture flexibility. TensorFlow, but at the other hand, has concerns with code complexity, poor input channels, and rapid interface changes. Theano is a limited framework with sparse support for pre-trained models, similar to the framework.

IV. UNDERSTANDING APPLICATIONS OF BLOCKCHAIN BASED DEEP LEARNING MODELS

The primary benefits that may be accomplished by combining blockchain and deep learning technologies include efficient decision, information security, accurate forecasting, effective data market management, and increased system robustness. Based on a set of factors, this section proposes a thematic taxonomy for classifying current literature linked to the unionization of blockchain & deep learning techniques. Blockchain & Machine Learning (ML) technology is gaining traction and popularity all over the world today. With the introduction and trade of cryptocurrencies, blockchain, a revolutionary technology, made a significant sensation. ML, on the other hand, is making significant waves in utilizing existing data to find patterns and acquire insights, thanks to predictive and descriptive algorithms. Bringing the two technologies together can only make them more disruptive! Both have the ability to speed up data exploratory data analysis while also increasing transaction security. Furthermore, distributed blockchain technologies can be an excellent and well-proven input for machine learning, which requires large data sets to generate accurate predictions.

- Many of the applications and services provided by deep learning techniques have time limits; as a result, the blockchain's time-specific modalities aid in the improvement of such services. Blockchain platforms examined by state-of-the-art deep learning frameworks may be categorized into public, private, and Consortium/Federated categories [16] based on their design, characteristics, and policies.
- A trained model analyses the data and creates patterns that may be used to make decisions in a variety of situations. Deep learning methods used for decision-making in a variety of applications are divided into five categories based on the structure of neural network layers: Convolution Neural Networks, Deep Reinforcement Learning, Generative Adversarial Networks, Recurrent Neural Networks, and Geometric Deep Learning.[18]

A. Development of smart contract security analysis technologies [17] — When a smart contract is compromised, the programmed reasoning and Blockchain records are exposed, which might be disastrous, and gateway threats could also be used to steal data from the Blockchain. Techniques for assessing the semantic trustworthiness of smart contracts even between two entities are also required. Detecting faults in smart contacts, dealing with malfunctioning smart contracts, and updating them with suitable code without disturbing the running network are some of the other major research problems. Line with regulatory organizations and procedures like HIPAA and GDPR necessitates enclosing all created security assessments for smart contracts with various degrees of secrecy, security, and privacy concerns.

Fig.4 in detail explains the process that is followed in training and re-training and formulation of deep learning models. The results obtained from Consensus Protocols and Methods such as GAN, DBN, RNN, DTL should be able to process and handle the big data but at the same should satisfy all the development goals.

B. Development of smart contract security analysis technologies— If a smart contract is hacked, the coded logic and Blockchain data are revealed, which might have fatal repercussions, and backdoor attacks could be used to steal information from the Blockchain. Techniques for measuring the semantic reliability of smart contracts amongst interacting parties are also needed. Other open research challenges include detecting defects in smart contacts, engaging with misbehaving smart contracts, and upgrading them with proper code without disrupting the operating network. Compliance with regulatory organizations & mechanisms such as HIPAA and GDPR requires encapsulating all produced security evaluations for smart contracts with confidentiality, security, and privacy considerations at several levels.

C. Cybersecurity: (Intrusion Detection System) - Approaches such as signature-based recognition, sector specific network analysis, and statistical packet analysis. The IDS categorizes requests as benign or malicious, with benign referring to normal searches and malevolent referring to anomalous or incursion requests. IDSs are also utilized to recognize a specific type of attack, such as a distributed denial-of-service (DDoS) attack.[10] Artificial Intelligence-based systems, on the other hand, have their own set of problems; false positives can be far more common than genuine threats. Based on imbalanced data and attributes available in the datasets used to train the algorithm, the algorithms may be biased toward specific attacks. Intrusion detection systems that are inaccurate and biased have little hope of securing patient information. [19]

D. Healthcare: Deep learning models may be trained using healthcare data to forecast [7] illness transmission rates and provide appropriate preventative actions. The healthcare data contains information about the illnesses and patient profiles, and it aids the model in forecasting the patients' medical conditions. The centralized storage of data relating to illnesses and patient profiles might result in a single point of failure. Blockchain ensures that data is protected from intentional or unintentional loss.

E. Cloud Storage - Due to load imbalances, disruption from background processes such as data cleaning, backfilling, and restoration, and the variation in processing capacity of coordinating services in a datacenter, cloud storage services are frequently linked with numerous performance difficulties.[39] This has a substantial influence on a variety of applications that have large working sets and strict time limitations. However, hand-tuning multiple control knobs in an online storage cluster for maximum performance under a variety of workload scenarios is difficult and time-consuming for human operators. The information of the client is divided into small chunks using blockchain distributed storage solutions. This is possible because to Blockchain features such as hashing power, encryption keys, and transaction records. Each bit of information is saved in a separate location. [20]

F. Transactional, FinTech and Banking – The Ledger contains a record of all previous transactions in Blockchain. The Blockchain ledger is a tamper-proof data structure that is constantly evolving and contains blocks that include batches of transactions made. [21] The finished blocks are included in the order that they were completed. In the last decade, blockchain through Bitcoin has had quite a significant influence on the globe, and it's reasonable to conclude that it will persist, especially with many individuals working diligently to eliminate the numerous constraints that prevent blockchains from becoming widespread. [22] The high computational and electricity expenses associated with the Proof-of-Work consensus methodology are one such constraint. TML's effectiveness in the implementation of AutoML to data flows for increased business insight and impact has been studied in numerous domains. Given that rapid information is here to remain and will become even more prevalent, businesses have a chance to utilize it and utilize it to bring value to their operations. [23]

G. Internet of Things (IoT) – Data Analytics: IoT sensors create large amounts of data for a variety of applications, including smart homes, smart healthcare, advanced manufacturing, transportation, microgrid, smart agriculture, and so on. Processing such data in order to improve decision-making, productivity and accuracy, and income is a vital step that makes IoT a valuable business idea and a paradigm that improves people's lives. Although obtaining hidden information and conclusions from IoT data has the potential to improve our quality of life, it is a difficult process that cannot be achieved using traditional paradigms. Deep Learning would be critical in the development of smarter IoT.

H. Internet of Vehicles (IoV) - The adoption of the Internet of Things (IoT) as a vehicle instrumentation technology has significantly boosted current device networking capabilities. Modern transportation systems typically outfit cars with gadgets, detectors, and intelligent software that allow them to communicate and share data with one another. [26] Data may be safely transferred across entities by bringing blockchain to the Internet of Vehicles (IoV) [24] [25] network. Next-generation vehicle networks, including IoV, carry with them a slew of cybersecurity issues. In order to properly handle these problems, in addition to current authentication approaches, it is necessary to identify the network's offending entities.

The automobiles in the Internet of Vehicles system use wireless communication technologies to create Vehicular Ad Hoc Networks [25] and dynamically deliver multiple services based on real-time driving information broadcasted by the vehicles.

I. Law Enforcement and Legal related matters: [27][28] Following AI's advancements, law enforcement organizations are increasingly turning to data analysis methods centered on symbolic AI & deep learning.

- **Face Recognition**, in relation to its use of mugshots taken during the usual practice of gathering a person's frontal and profile photographs, fingerprints, and personally identifiable information.
- **Fingerprint recognition**, and in particular, the retrieval of minutiae, or distinguishing characteristics utilized in fingerprint matching;
- **Violence Recognition,** with the purpose of relieving law enforcement of the strain of manually reviewing hours of video material to detect small occurrences.

Despite the fact that these disciplines appear to be unrelated, the computerization of related jobs has origins in Computer Vision and is quickly growing thanks to deep learning. While these (and related) algorithms achieved high accuracy on datasets with fixed characteristics like as position, lighting, and expression, they are unable to extract stable identification features that are invariant to real-world changes. [29]

V. ANALYSIS OF PROPOSED BLOCKCHAIN BASED DEEP LEARNING MODELS

Deep learning models with hospital information management and resource-friendly architecture have become more important in pharmacogenomics research. [30] proposes a decentralized approach for providing pharmacogenetic information to deep learning techniques for ovarian cancer prediction. The blockchain is utilized to share patient details as well as the model's ovarian cancer forecasts with collaborating organizations. These standard ds are useful for evaluating encryption and decryption techniques based on the time it takes to encrypt and decrypt information. The suggested model, on the other hand, has only been evaluated with a small lot of incidents per class and provides predictions for data not yet seen that belongs to the learnt classes.

i. **Arrhythmia Classification:** [31] used a blockchain platform

to build deep learning models to categorize arrhythmia illness. Arrhythmia is a condition characterized by disturbances in the patient's heartbeat. During the first phase of a research suggested in [31], two-layered stacked denoising auto-encoders (SDA) are employed to extract features and detect abnormal heartbeats. In addition, the SDA is retrained during the testing phase to reduce the output classification's false-positive rate. The information acquired after training can be saved in hardware and accessible via pointers recorded in a ledger. The Hyperledger blockchain protects the user's privacy and identity on the network. This is used to differentiate patients from clinicians, as well as to securely link patients to the electronic signatures. The suggested architecture maintains the real data in a cloud drive (cloud or offline database), while the blockchain network merely stores pointers/links to the data's location. This improves scalability by reducing the system's storage restriction. Smart contracts, which are a mechanism to securely perform logic inside a blockchain context, are used to set access policies to authenticate patient read/write access in Hyperledger.

ii. **Blockchain Based Deep Learning Model in IoT:** [32] The Internet of Things is a huge network of nodes in the network, sensing, and other digital nodes that are all connected. The data collected from the sensors is communicated amongst peers and also a central server device. The main threats to the IoT network are security issues and denial of service (DoS) attacks Blockchain plays a significant role in securing the IoT network by removing the primary key from the network. An adaptive user-based healthcare system is created by retraining a set of user information and behaviors. In this study, we employed DL approaches to trace the transaction of public keys between mutually connected parties. In comparison to the benchmark models, our proposed strategies are also more efficient. The concept of DL was concerned with human associated with brain cells known as neurons. The human brain is split into layers, resulting in a deep network. Multi-layer neural networks are used to build privacy-preserving solutions based on DL. [32]

iii. Currency Supervision using DL and Blockchain: [33] With the rapid emergence of digital currencies such as Bitcoin, collecting valuable information from vast amounts of data and assessing the value of digital items using current approaches has become challenging. The digital asset is employed as the research area in this study, and deep learning technology is used to construct a digital valuation analysis model. The permission mechanism is then taken from the DPOS (Delegated Proof of Stake) technique and applied to the precise backward error tracking (PBET) algorithm, which itself is based on the current consensus algorithm. As a consequence, a transient delegated practical byzantine fault tolerance (DDPBFT) mechanism that is blockchain compatible is proposed. Finally, a controlled digital money system is created using upgraded blockchain technology.

iv. Ovarian Cancer Prediction using DL and Blockchain: [30] A one-shot algorithm has been designed to produce an early diagnosis tool for ovarian cancer using pharmacogenomic and deep learning methodologies. The genetic fingerprints driving the disease's proneness were discovered using pharmacogenomic study. From the picture, the trained model will forecast the mutation that is causing the cancer. On iterations, the model has an efficiency of 86 percent. The blockchain-based security solution built for patient-specific data aids in the secure exchange of data across research organizations, hospitals, and medical practitioners. A comparison of encryption methods such as Genetic encryption, AES (Advanced Encryption Standard), and DES (Data Encryption Standard) was conducted, with AES proving to be more efficient predicated on the CRYPTO++ criteria.

VI. OPEN CHALLENGES AND ISSUES TO BE ADDRESSED IN BLOCKCHAIN INTEGRATED DEEP LEARNING MODELS

While research into combining blockchain with deep learning technology is still in its early stages, there are a number of unresolved difficulties and obstacles that future initiatives must carefully address. In addition, numerous additional strategies are influencing the development of blockchain and deep learning technology. Both of them may have significant effects on each other at the same time. In this part, we'll go through some of the most pressing outstanding concerns and research difficulties for improving blockchain and DL performance. Then, with a larger view, we highlight some research prospects in adjacent fields.

i. Based on a developed Deep Autoencoder Neural Network, the suggested smart contracts construct a mutual traffic control agreement (by computer programming) to identify abnormalities. Without the involvement of a single centralized power, this design allows for the establishment of a secure platform that can govern and finish connected transactions in key infrastructure networks. It's a revolutionary method to incorporating artificial intelligence into the Blockchain network, not as a supporting framework that increases the network's capabilities, but rather as an active structural member that's required for its completion.[34]. However, when new blocks are added to the current network, blockchain represents forever record. As the blockchain grows in size, the network's efficiency suffers significantly. Deep learning techniques may be used to compress data while also aiding in the reduction of unnecessary data. Because data recorded on the blockchain is irreversible, the ledger's expanding size is a major challenge that must be managed appropriately.

ii. The widespread use of blockchain will result in a number of issues, mostly related to user demand for internet access, data speed, speed, and number of transactions made by participants. Given the ever-increasing storage and computing needs of the blockchain ledger, the number of nodes and transactions introduced to the blockchain should be drastically decreased in order to meet users' projected requests. However, many existing compression methods are unable to deliver the suitable ratio required to reduce the cost of large-scale deployment of deep learning-based applications using blockchain.

iii. The use of DL-based methods requires both privacy and security preservation. DL systems currently have a centralized design, which makes them vulnerable to hacking because any bad node only has to get into a unified system to modify the instructions. Because training data typically contains a considerable quantity of personal information, data breaches may result in personal data privacy problems. The question of how to keep the training data used in DL models safe from hackers is crucial.

iv. Big data processing [40] is extremely beneficial for a diverse range of industries, including cybersecurity, spam detection, IoT, and healthcare analytics,[35] as it is a vital aspect in today's networks. In the near future, processing collected data could make data highly useful. Bigdata is used extensively in blockchain and machine learning applications, where vast amounts of data are gathered, sorted, and stored in blocks, then processed as training dataset for machine learning models. Blockchain technology offers a new way to store data more securely, with protection from tampering, deletion, and other types of attacks. [36] Furthermore, blockchain allows users to monetize their data, allowing them to genuinely own and manage their data.

v. To harness the potential of blockchain and DL, engineers must correctly organize and plan resources in the underlying networks, such as computation, storage, and communication. Because many heterogeneous resources may be shared across multiple users and suppliers using blockchain technology, efficient coordination and practical incentive systems should be created correctly. Consensus protocols [40] [37] must also be properly included into these processes. To cope with certain difficult difficulties, resource allocation solutions should, for example, identify how to choose mining nodes and distribute limited resources optimally.

Fig.5. gives a broader view of the open challenges and issues present, not discussed extensively and are awaiting an appropriate attention from the academicians and researchers.

When diverse IoT devices share a connection condition, Blockchain can improve spectral efficiency and enable far better 5G traffic optimization while maintaining privacy in 5G applications communications networks and beyond. Despite all of the benefits given by Blockchain technology and the related suggested frameworks based on it to improve the security components, there is no envisaged framework that can provide a comprehensive secured solution that provides the confidentiality, integrity, and availability (CIA) [38] triad, preserves privacy, and offers multi-factor or remote authentication, to the best of our knowledge. As a result, we predict that researchers will have a significant difficulty in the future in securing Blockchain-based IoT systems.

VII. FUTURE SCOPE FOR DEEP LEARNING AND BLOCKCHAIN INTEGRATION AND CONCLUSION

The combination of blockchain, deep learning, and the Internet of Things (IoT) offers several potential opportunities and benefits, and it plays an essential role in a variety of ways. IoT will be practically required to link multiple kinds of DL applications, and it will be much more crucial in supplying large-scale information in real streams for learning algorithms and making decisions. It may gather, disseminate, and analyses bigdata in a variety of ways, including financial, educational, and healthcare services, by combining vast global IoT technologies and adaptive DL technologies. In addition, using Bluetooth signals, motion detectors, or facial-recognition technologies, DL approaches with IoT can analyses human behavior and provide predictions and answers. In the meanwhile, as blockchain-based apps become more common, the volume of transactional data recorded in deep learning grows exponentially. Traditional data storage solutions are unable to store such massive amounts of data at a reasonable cost.

In this research paper, authors have focuses and discussed the importance on the integration with blockchain and deep learning, which is quickly becoming a required solution for intelligent, safe, and decentralized data and model sharing, as well as the efficient functioning of communications and networking systems. We began by providing a brief explanation of blockchain and deep learning technology, including basic principles, taxonomies, and common applications. Furthermore, authors have focused on discussing about the major models that have made an attempt to use such an integrated model or have proposed an architecture for the same based on certain parameters. In addition to this, the paper also specifies usability of Blockchain and deep learning on each other, how DL and Blockchain benefit each other in terms of security, efficiency, immutability and implementation of smart contract systems. Moreover, authors have also specified various open issues, challenges and research gaps present in the same interest that could take up various researchers for future researches.

After analysis and reviewing the domains extensively, research in terms of using blockchain based deep learning models in Healthcare, Communications and Legal Systems is vast. As a result, researchers who are motivated or eager in researching on/against the challenges stated are permitted to continue their study (in near future).

REFERENCES

[1] Nicola Friedman, Jarrod Ormiston, Blockchain as a sustainability-oriented innovation: Opportunities for and resistance to Blockchain technology as a driver sustainability in global food supply chains, Technological Forecasting and Social Change, Volume 175, 2022, 121403, ISSN 0040-16 https://doi.org/10.1016/j.techfore.2021.121403.

[2] Ismaeel Al Ridhawi, Moayad Aloqaily, and Yaser Jararweh. 2021. An Incentive-based Mechanism for Volunteer Computing Using Blockchain. ACM Trans. Inter Technol. 21, 4, Article 87 (November 2021), 22 pages. DOI: https://doi.org/10.1145/3419104

[3] Cao, X., Zhang, J., Wu, X. et al. A survey on security in consensus and smart contracts. Peer-to-Peer Netw. Appl. (2022). https://doi.org/10.1007/s12083-021-012 2

[4] Webb, M.E., Fluck, A., Magenheim, J. *et al.* Machine learning for human learners: opportunities, issues, tensions and threats. *Education Tech Research Dev* **69,** 210 2130 (2021). https://doi.org/10.1007/s11423-020-09858-2

[5] Shafay, Muhammad & Hassan, Taimur & Velayudhan, Divya & Damiani, Ernesto & Werghi, Naoufel. (2021). Deep Fusion Driven Semantic Segmentation for Automatic Recognition of Concealed Contraband Items. 10.1007/978-3-030-73689-7_53.

[6] Berman, Daniel S., Anna L. Buczak, Jeffrey S. Chavis, and Cherita L. Corbett. 2019. "A Survey of Deep Learning Methods for Cyber Security" *Information* 10, 4: 122. https://doi.org/10.3390/info10040122

[7] Ahmad, R. W., Salah, K., Jayaraman, R., Yaqoob, I., Ellahham, S., & Omar, M. (2021). The role of blockchain technology in telehealth and telemedicine. *International journal of medical informatics*, *148*, 104399. https://doi.org/10.1016/j.ijmedinf.2021.104399

[8] Fran Casino, Thomas K. Dasaklis, Constantinos Patsakis, A systematic literature review of blockchain-based applications: Current status, classification and op issues, Telematics and Informatics, Volume 36, 2019, Pages 55-81, ISSN 0736-5853, https://doi.org/10.1016/j.tele.2018.11.006.

[9] Abhishek Gupta, Alagan Anpalagan, Ling Guan, Ahmed Shaharyar Khwaja, Deep learning for object detection and scene perception in self-driving cars: Surv challenges, and open issues, Array, Volume 10, 2021, 100057, ISSN 2590-0056, https://doi.org/10.1016/j.array.2021.100057.

[10] K. Arulkumaran, M. P. Deisenroth, M. Brundage and A. A. Bharath, "Deep Reinforcement Learning: A Brief Survey," in *IEEE Signal Processing Magazine*, vol. no. 6, pp. 26-38, Nov. 2017, doi: 10.1109/MSP.2017.2743240.

[11] Maldonado, A.D.; Morales, M.; Navarro, F.; Sánchez-Martos, F.; Aguilera, P.A. Modeling Semiarid River–Aquifer Systems with Bayesian Networks and Artific Neural Networks. Mathematics 2022, 10, 107. https://doi.org/10.3390/ math10010107

[12] Ziaee Adib, Seyed Morteza & pour, Amir & Ghahfarokhi, Farzaneh. (2019). The impact of blockchain mega-trend on the tourism indust 10.13140/RG.2.2.25803.34083.

[13] W. Fauvel, "Blockchain Advantages and Disadvantages" August 2017. Available from: https://medium.com/nudjed/blockchain-advantage-and-disadvantag e76dfde3bbc0

[14] L. Račić, T. Popović, S. čakić and S. Šandi, "Pneumonia Detection Using Deep Learning Based on Convolutional Neural Network," *2021 25th International Conferer on Information Technology (IT)*, 2021, pp. 1-4, doi: 10.1109/IT51528.2021.9390137.

[15] Zhang, Dehai & Cui, Menglong & Yang, Yun & Yang, Po & Xie, Cheng & Liu, Di & Yu, Beibie & Chen, Zhibo. (2019). Knowledge Graph-Based Image Classificati Refinement. IEEE Access. PP. 1-1. 10.1109/ACCESS.2019.2912627.

[16] Jabbar, S., Lloyd, H., Hammoudeh, M. *et al.* Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia Systems* **27,** 787–806 (202 https://doi.org/10.1007/s00530-020-00687-0

[17] Huang, Yongfeng & Bian, Yiyang & Li, Renpu & Zhao, J. & Shi, Peizhong. (2019). Smart Contract Security: A Software Lifecycle Perspective. IEEE Access. 7. 1 10.1109/ACCESS.2019.2946988.

[18] Dunne, Robert. (2006). A Statistical Approach to Neural Networks for Pattern Recognition. A Statistical Approach to Neural Networks for Pattern Recognitio 10.1002/9780470148150.

[19] M. Kumar and A. K. Singh, "Distributed Intrusion Detection System using Blockchain and Cloud Computing Infrastructure," *2020 4th International Conference Trends in Electronics and Informatics (ICOEI)(48184)*, 2020, pp. 248-252, doi: 10.1109/ICOEI48184.2020.9142954.

[20] A. Mughal and A. Joseph, "Blockchain for Cloud Storage Security: A Review," *2020 4th International Conference on Intelligent Computing and Control Syste (ICICCS)*, 2020, pp. 1163-1169, doi: 10.1109/ICICCS48265.2020.9120930.

[21] R. R. Noel, R. Mehra and P. Lama, "Towards Self-Managing Cloud Storage with Reinforcement Learning," *2019 IEEE International Conference on Cloud Engineeri (IC2E)*, 2019, pp. 34-44, doi: 10.1109/IC2E.2019.000-9.

[22] Maurice S. (2021) Evolution and Opportunities for Transactional Machine Learning in Almost Every Industry. In: Transactional Machine Learning w Data Streams and AutoML. Apress, Berkeley, CA. https://doi.org/10.1007/978-1-4842-7023-3_8

[23] N. S. Akhilesh, M. N. Aniruddha and K. S. Sowmya, "Implementation of Blockchain for Secure Bank Transactions," *2020 International Conference on Mainstreami Block Chain Implementation (ICOMBI)*, 2020, pp. 1-10, doi: 10.23919/ICOMBI48604.2020.9203095.

[24] Alladi, Tejasvi & Kohli, Varun & Chamola, Vinay & Yu, F. (2021). Securing the Internet of Vehicles: A Deep Learning-Based Classification Framework. IE Networking Letters. PP. 10.1109/LNET.2021.3058292.

[25] Tianhong Su, Sujie Shao, Shaoyong Guo, Min Lei, "Blockchain-Based Internet of Vehicles Privacy Protection System", Wireless Communications and Mob Computing, vol. 2020, Article ID 8870438, 10 pages, 2020. https://doi.org/10.1155/2020/8870438

[26] Yang, T., Nazir, S. A comprehensive overview of AI-enabled music classification and its influence in games. *Soft Comput* (2022). https://doi.org/10.1007/s00500-02 06734-4

[27] S. Raaijmakers, "Artificial Intelligence for Law Enforcement: Challenges and Opportunities," in *IEEE Security & Privacy*, vol. 17, no. 5, pp. 74-77, Sept.-Oct. 20 doi: 10.1109/MSEC.2019.2925649.

[28] Mei Wang, Weihong Deng, Deep face recognition: A survey, Neurocomputing, Volume 429, 2021, Pages 215-244, ISSN 0925-23 https://doi.org/10.1016/j.neucom.2020.10.081.

[29] Mishra S., Tyagi A.K. (2022) The Role of Machine Learning Techniques in Internet of Things-Based Cloud Applications. In: Pal S., De D., Buyya R. (eds) Artific Intelligence-based Internet of Things Systems. Internet of Things (Technology, Communications and Computing). Springer, Cham. https://doi.org/10.1007/978-3-0 87059-1_4

[30] Abraham, Misha & Am, Hima & Srinivasan, Chungath & Namboori, Dr. Krishnan. (2019). Healthcare security using blockchain for pharmacogenomics. Journal International Pharmaceutical Research. 6. 529-533.

[31] A. Juneja and M. Marefat, "Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification," *2018 IEEE EM International Conference on Biomedical & Health Informatics (BHI)*, 2018, pp. 393-397, doi: 10.1109/BHI.2018.8333451.

[32] Ali, Aitizaz, Muhammad F. Pasha, Jehad Ali, Ong H. Fang, Mehedi Masud, Anca D. Jurcut, and Mohammed A. Alzain. 2022. "Deep Learning Based Homomorpl Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography" *Sensors* 22, no. 2: 5 https://doi.org/10.3390/s22020528

[33] Huiling Fan, The digital asset value and currency supervision under deep learning and blockchain technology, Journal of Computational and Applied Mathemati 2022, 114061, ISSN 0377-0427, https://doi.org/10.1016/j.cam.2021.114061.

[34] Demertzis, K., Iliadis, L., Tziritas, N. *et al.* Anomaly detection via blockchained deep learning smart contracts in industry 4.0. *Neural Comput & Applic* **32,** 1736 17378 (2020). https://doi.org/10.1007/s00521-020-05189-8

[35] S. AVRP and P. K. Baruah, "Blended Learning-Assimilating Authentic Data Into Deep Learning Models," *2018 IEEE 25th International Conference on Hi Performance Computing Workshops (HiPCW)*, 2018, pp. 75-80, doi: 10.1109/HiPCW.2018.8634015.

[36] C. H. Liu, Q. Lin and S. Wen, "Blockchain-Enabled Data Collection and Sharing for Industrial IoT With Deep Reinforcement Learning," in *IEEE Transactions Industrial Informatics*, vol. 15, no. 6, pp. 3516-3526, June 2019, doi: 10.1109/TII.2018.2890203.

[37] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang and Y. Qian, "Resource Trading in Blockchain-Based Industrial Internet of Things," in *IEEE Transactions on Industr Informatics*, vol. 15, no. 6, pp. 3602-3609, June 2019, doi: 10.1109/TII.2019.2902563.

[38] E. Hegland Hjort Kure, P. Engelstad, S. Maharjan, S. Gjessing and Y. Zhang, "Distributed Uplink Offloading for IoT in 5G Heterogeneous Networks Under Priv Information Constraints," in *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6151-6164, Aug. 2019, doi: 10.1109/JIOT.2018.2886703.

[39] Sheth, H.S.K., Tyagi, A.K. (2022). Mobile Cloud Computing: Issues, Applications and Scope in COVID-19. In: Abraham, A., Gandhi, N., Hanne, T., Hong, TP., Nogueira Rios, T., Ding, W. (eds) Intelligent Systems Design and Applications. ISDA 2021. Lecture Notes in Networks and Systems, vol 418. Springer, Cham. https://doi.org/10.1007/978-3-030-96308-8_55

[40] Y. Liu, F. R. Yu, X. Li, H. Ji and V. C. M. Leung, "Blockchain and Machine Learning for Communications and Networking Systems," in *IEEE Communicatic Surveys & Tutorials*, vol. 22, no. 2, pp. 1392-1431, Secondquarter 2020, doi: 10.1109/COMST.2020.2975911.