Integration of Blockchain and Edge Computing in Healthcare: Accountability and Collaboration

Rakshit Kothari[1,*]

[1]Geetanjali Institute of Technical Studies, Udaipur, Rajasthan

[*]rakshit007kothari@gmail.com

Received 15 July, 2023; Revised 4 August, 2023; Accepted 5 August, 2023
Available online 5 August 2023 at www.atlas-journal.org, doi: 10.22545/2020/00230

Abstract:*A decentralized, safe, and effective ecosystem is created in the healthcare industry through the integration of blockchain and edge computing. Secure data interchange, real-time analytics, enhanced privacy, and patient-centered treatment are all made possible. Realizing the full potential of integrating blockchain and edge computing for health care will need accountability and collaboration. It will make it possible to create reliable, secure, and cooperative healthcare organizations that will increase patient care, protect the confidentiality of information, and support cutting-edge applications for healthcare. Our Solution is to share data safely and cooperatively, improve patient confidentiality, and support healthcare data ethical and accountable use. In this paper, we propose that combining blockchain technology with edge computing in healthcare is intended to improve accountability and teamwork. The methodologies used in integrating deep learning deploy various models on edge devices such as Q-Learning and Deep Q-Networks (DQN), SVM, etc. In conclusion, the application of edge computing and blockchain in the healthcare sector offers fascinating possibilities for cooperation and accountability. Healthcare systems may improve data security, privacy, interoperability, and real-time analytics by combining the advantages of the two technologies. The delivery of healthcare might change as a result of this integration, which could also foster cooperative research and eventually enhance patient outcomes.*

Keywords:Blockchain, edge computing, security, privacy, medical research, sharing

1 Introduction

Accountability in healthcare systems is ensured by the transparent and unchangeable database that blockchain technology offers. It permits the safe and decentralized storage of private information [1], including that related to patients, research, and medical study. Blockchain's distributed architecture guarantees

that no single party retains authority over the data, minimizing the possibility of data manipulation or unauthorized access. An audit trail that may be readily followed and validated is produced by recording every transaction or data modification in a separate block. The promotion of trust among those involved, such as patients, healthcare workers, and investigators, is made possible by this degree of responsibility [2 – 6].

By enabling real-time data processing and analysis at the edge of the network, nearer the data source, edge computing enhances blockchain technology. With this strategy, data interchange and collaboration among healthcare stakeholders are more effective and have lower latency [3, 4]. Wearable sensors and Internet of Things (IoT) devices are examples of edge computing devices that may gather and analyse data locally before safely passing it to the blockchain network. This decentralized data processing capacity improves collaboration by enabling the exchange of crucial information between various researchers and healthcare professionals. The Integration of blockchain and edge computing in healthcare represents various factors [5, 7] with the preference for accountability and collaboration in Figure 1.

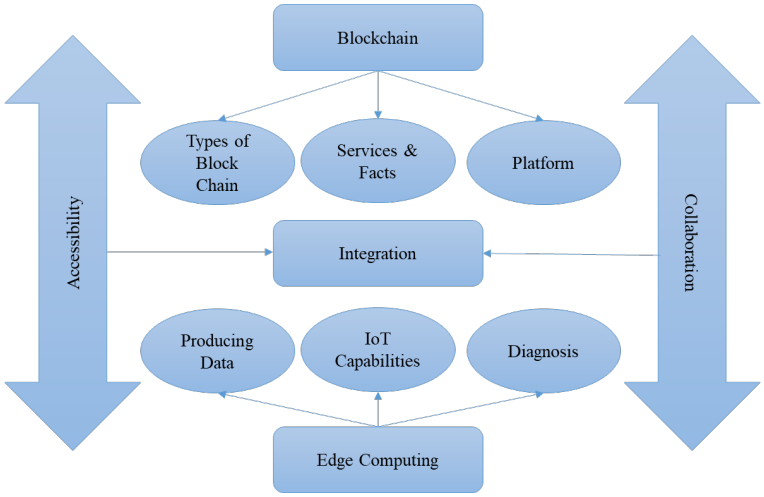

Figure 1: Representation of Accountability and Collaboration.

Data Sharing and Interoperability: Blockchain technology has been investigated to address the problems with data sharing and interoperability in the healthcare industry. Healthcare professionals may easily access and share patient information since it facilitates secure and consistent data transmission across many platforms. By enabling local data preparation and real-time data synchronization with the blockchain network, edge computing [8 – 12] improves this procedure.

Clinical Trials and Research: Clinical trials and medical research can be more transparent and ethical when edge computing and blockchain are used together. The technology allows auditable and tamper-proof records by securely documenting every step of the trial or research process on the blockchain, including participant recruiting, data gathering, and analysis. In order to lessen dependency on centralized systems and increase data accuracy [9 – 14], edge computing devices can gather and analyze data directly from trial participants.

Internet of Medical Things (IoMT): A significant quantity of healthcare data is produced by the IoMT, which comprises wearable technology and remote monitoring systems. Edge computing and blockchain integration make it possible to store, process, and analyse data securely and effectively. With this connectivity, real-time health monitoring can be more accurate, personalized treatment plans can be created, and patient and healthcare provider remote cooperation is made easier.

Data Privacy and Security: Through safe key management, blockchain's cryptographic protocols provide patients ownership over their health data, ensuring data privacy and security. By keeping sensitive data localized and lowering the possibility of unauthorized access or data breaches, edge computing further

increases security.

2 History

Due to its promise to address data security and interoperability issues in a variety of industries, including healthcare, blockchain technology became more well-known in 2017. It has been acknowledged that the decentralized and open nature of blockchain technology offers a way to enhance data integrity and accountability in healthcare systems. Edge computing gained popularity around this time as a means of processing and analyzing data closer to its source, lowering latency and increasing efficiency. With the emergence of wearable technology and the Internet of Things (IoT) in healthcare, the requirement for real-time data processing and analysis became clear.

Since then, blockchain and edge computing has been actively integrated to improve accountability and collaboration in the healthcare industry by technology businesses, research organizations, and healthcare organizations [10]. To test and improve this integration, several pilot projects, research studies, and collaborations have been started. These programs have concentrated on a variety of topics, including clinical trials, the Internet of Medical Things (IoMT), secure data exchange, interoperability, patient consent management, and so on. The difficulties of data privacy, security, fragmentation, and the requirement for real-time data processing and cooperation have all been addressed by efforts to merge blockchain with edge computing.

2.1 Scope

The healthcare sector has a great deal of potential to be revolutionized by block and edge computing. By guaranteeing the safe storage of healthcare data and enabling frictionless data transmission across healthcare stakeholders, blockchain technology can improve data security, privacy, and interoperability [10]. Additionally, it may streamline the procedures for clinical trials, supply chain management, and billing, enhancing patient outcomes, lowering costs, and avoiding fraud. Edge computing, on the other hand, makes it possible to monitor patients in real-time, practice telemedicine, and provide treatment from a distance. This technology enables prompt interventions, expands access to healthcare in under-served regions, and guarantees continuity of care in emergency situations.

There are several applications for edge computing and blockchain in the healthcare industry. It can strengthen consent management, provide patients with more control over their health data, and improve data security and privacy. Healthcare systems may improve data accuracy, minimize administrative hassles, and speed up operations by incorporating these technologies. Furthermore, by providing openness, traceability, and correctness of outcomes, integration can revolutionize clinical trials and medical research.

3 Overview of Blockchain and Edge Computing in Healthcare

This section presents an overview of blockchain and edge computing respectively.

3.1 Blockchain

Blockchain's technology of distributed ledgers makes it easier to transfer patient medical records securely, improves healthcare data security, controls the medication supply chain, and aids genetic code study in the medical field. It's hardly surprising that the most well-liked blockchain healthcare use at the moment is safeguarding medical data. Security is a significant problem in the healthcare sector. From July 2021 to June 2022, 692 significant healthcare data breaches were disclosed. Health and genomic testing records, as well as banking and credit card information, were stolen by the offenders [11]. Blockchain is a technology that is perfect for security-related uses because it can maintain an incorruptible, distributed, and transparent log of all patient data. Additionally, blockchain is both private and transparent, obscuring

any person's identity with intricate and secure protocols that can safeguard the sensitivity of medical data. The technology's distributed nature also makes it possible for patients, physicians, and other healthcare professionals to easily and securely share comparable information. Figure 2 shows the various versions of blockchain.

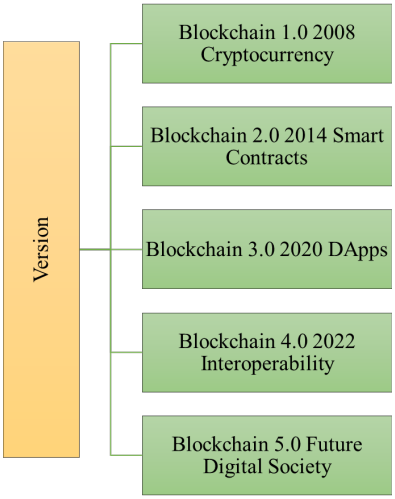

Figure 2: Version of Blockchain.

Blockchain has advanced greatly over time. We categorize the five versions of blockchain into versions 1.0 through 5.0. The most fundamental kind of decentralized ledger for recording transactions and storing data across several devices is this one. It is known as Blockchain 1.0 and was first published by Nakamoto. The data in the first blockchains, to put it simply, was limited to the values of a "thing" that saw ownership changes over time [18]. Usually, the "thing" we're talking about is a type of virtual money like Bitcoin, ripple, and so on. Blockchain 2.0 is sometimes referred to as the emergence of Ethereum, the upgraded cryptocurrency suggested by Vitalik Buterin in 2014.

Due to the inability of traditional health information exchange (HIE) and personal health record (PHR)-based exchanges to deliver on their promise of a shared coalescent, blockchain technology has a lot of potential in the healthcare business. The trust deficit present in traditional health information exchange intermediations continues to be exposed by electronic health records (EHR), conflicting interests, and a number of other reasons. As a result, blockchain technology has lately gained attention and has emerged as a top option in the healthcare industry. A Description of Blockchain technology in the healthcare industry [12]. The healthcare professionals and patients who provide the data, the medical cloud, and the blockchain network with distributed ledger and smart contracts are the components of the healthcare blockchain. The global Google trends for the term "Blockchain - Healthcare" are shown in Figure 3. This clearly demonstrates how the research community's interest has grown.

3.2 Edge Computing

Edge computing and AI go hand in hand. Patients' data must be gathered, but doctors must also analyse it and provide real-time responses. This is becoming increasingly viable thanks to edge computing. Currently, edge computing systems with embedded AI are in place to quickly identify abnormalities and other important results from X – rays and other scans, including potentially life-threatening disorders. By delivering information more quickly at the imaging point, this technology enables clinicians to prioritize exams in a timely and economical manner. Because of this, edge computing and AI have a lot of promise for use in the healthcare industry. Across sectors, edge computing provides a number of advantages. Reduced latency is a key benefit. Edge computing reduces the amount of time data must travel to centralized

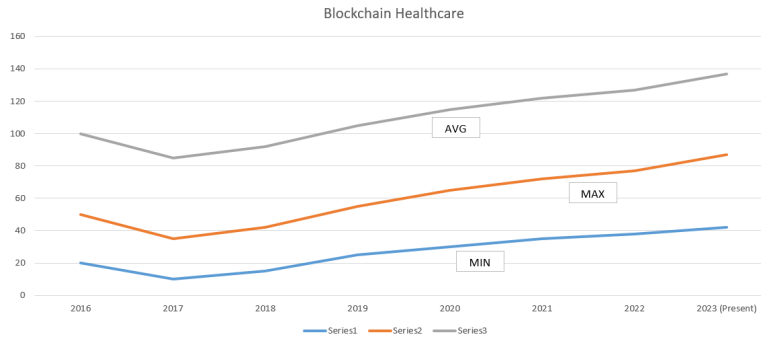

Figure 3: Blockchain Healthcare.

cloud servers by processing data closer to the source, allowing for real-time replies. This is essential for applications that demand quick responses, such as Internet of Things devices or driverless vehicles. Edge computing further improves real-time capabilities by processing data locally, facilitating quicker reaction and decision times. By sending only pertinent data to the cloud and lowering network traffic [14 – 15], it also improves overall network performance and bandwidth utilization which explores the benefits of Edge Computing in Figure 4.

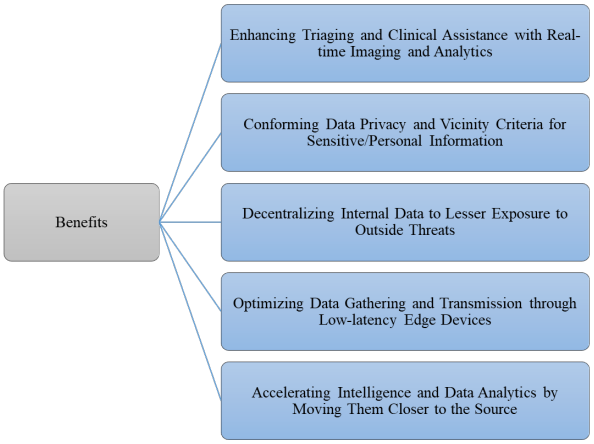

Figure 4: Benefits of Edge Computing.

Additionally, by preserving sensitive data within the local network and lowering the likelihood of data breaches, edge computing improves privacy and security. Additionally, it offers higher dependability since edge devices may keep running even when cloud access is interrupted or lost. Overall, edge computing gives businesses more power through quicker processing, more effectiveness, improved privacy, and increased dependability.

4 Methodology

Blockchain and Edge Computing may be used in the healthcare industry to improve responsibility and cooperation while preserving the confidentiality, privacy, and transactional integrity of data. Although blockchain technology itself has built-in accountability characteristics, specialized algorithms and processes may be used to meet the particular needs of the healthcare industry. LSTM algorithms can also be used to analyse and predict market trends in blockchain-based cryptocurrencies [14]. By processing historical

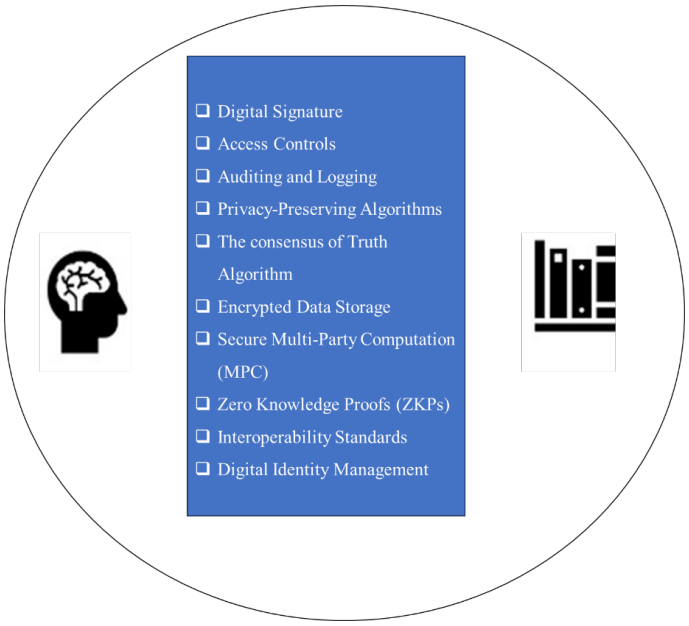

Figure 5: Methods of Accountability and Collaboration in Blockchain.

transaction data, an LSTM model can learn patterns and trends, allowing for the creation of predictive models to forecast price movements. With a plug-and-play design (modular) that enables a high degree of security, privacy, and secrecy of the data, Blockchain is a source that creates the distributed ledger. Peers who are endorsing each other validate the transaction, carry it out, and produce the read-and-write sets. The client is then informed of the response. The client gathers all peer responses, and then sends them to the "order." In this instance, the order places all transactions in ascending order, which is followed by the formation of a block.

Each committer verifies this block, and as a consequence, adds a new block to their own copy of the ledger.

A unique form of deep learning called recurrent neural networks uses the output from one stage as the input for the next. Recurrent neural networks can learn the long-term dependencies of data thanks to a unique form known as LSTM. The repeating module of the LSTM, which consists of a mixture of four separate layers coupled to one another, facilitates this form of learning. The character classification step uses the dataset for training and testing. In LSTM Training curves start at 83.6% and increase to 85% after 30 epochs. The testing curve begins at 84% and drops to 86% before rising to 87.4%.

4.1 Blockchain for Accountability and Collaboration

Due to its transparency and immutability, blockchain technology by default promotes accountability. The employment of certain methods and algorithms can, however, improve accountability in blockchain systems [15]. Here are several essential blockchain accountability and collaboration algorithms and methods in Figure 5.

Digital Signatures: In order to confirm the legitimacy and integrity of healthcare data stored on a blockchain, digital signatures are essential. Participants can sign transactions and data with their private keys using asymmetric cryptographic techniques like RSA or elliptic curve cryptography (ECC), allowing verification of the sender's identity and guaranteeing non-repudiation.

Access Controls: The blockchain may be used to construct access control techniques and algorithms to manage the rights and privileges of healthcare stakeholders. The blockchain can impose accountability by

regulating the visibility and modification rights of sensitive healthcare data by setting access regulations and applying cryptographic techniques like attribute-based access control (ABAC) or role-based access control (RBAC).

Consensus Algorithms: The integrity of healthcare data in a blockchain network must be preserved using consensus algorithms in order to guarantee responsibility. Consensus systems, such as Proof-of-Work (PoW), Proof-of-Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), allow for agreement among network users, limiting criminal activity and the alteration of medical information [16].

Auditing and Logging: Healthcare systems built on blockchain technology may keep meticulous audit trails and event logs to record and manage network activity. These logs could provide details on medical transactions, data access, and modification activities. Blockchain solutions enable openness, traceability, and accountability in healthcare operations by preserving thorough audit trails.

Privacy-Preserving Algorithms: To preserve sensitive healthcare data while enabling analysis and accountability, privacy-preserving algorithms can be connected with the blockchain. These algorithms include differential privacy and secure multi-party computation (MPC). While providing aggregated insights and analysis for accountability reasons, these algorithms ensure that patient information is kept private.

Consensus of Truth Algorithms: Consensus of truth algorithms can be used in the healthcare industry, where numerous parties may have conflicting accounts of events. These algorithms try to establish a single source of truth by bringing together contradictory evidence. Techniques like reputation-based consensus or weighted voting can be used to make sure.

Encrypted Data Storage: It is possible to encrypt healthcare data on the blockchain using symmetric or asymmetric encryption techniques. In order to ensure that only persons with the necessary decryption keys may access and read the healthcare data [17], encryption adds an extra degree of protection and secrecy.

Secure Multi-Party Computation (MPC): Collaboration on encrypted data is made possible via secure multi-party computing. Without disclosing the sensitive material below, it enables many parties to calculate shared data. Through the use of MPC algorithms in healthcare blockchain, aggregated patient data may be collaboratively analysed and researched while maintaining privacy and confidentiality [17, 18].

Zero-Knowledge Proofs (ZKPs): Participants in zero-knowledge proofs can demonstrate the accuracy of particular facts or calculations without disclosing the real data. ZKPs can be used in healthcare cooperation to verify the accuracy of certain data or calculations without disclosing private patient data. Collaboration is made possible while retaining secrecy and privacy.

Interoperability Standards: In order for healthcare organizations to collaborate on the blockchain, interoperability standards and protocols like HL7 and FHIR are essential. These standards make sure that various healthcare systems may communicate data without any problems, encouraging cooperation and data sharing between various organizations and stakeholders.

Digital Identity Management: For safe and dependable cooperation in healthcare blockchain networks, digital identity management algorithms and protocols are crucial. Only persons who have been given permission to do so may take part in collaborative activities and access healthcare data thanks to these algorithms, which monitor and verify participants digital identities.

4.2 Edge Computing for Accountability and Collaboration

Edge computing, as opposed to merely depending on centralized cloud servers, refers to the discipline of processing and analysing data closer to its source or at the edge of the network. While the general architecture and protocols of edge computing are largely responsible for accountability, there are several algorithms and strategies that can improve accountability in these contexts. Collaboration between distributed edge devices and entities is essential for effective data processing and decision-making in edge computing. While numerous protocols and frameworks are utilized to promote collaboration in edge computing, specialized algorithms and approaches are employed to assist collaborative operations in Figure 6.

Secure Communication Protocols: For edge computing to remain accountable, secure communication protocols like Transport Layer Security (TLS) or Secure Shell (SSH) are crucial. In order to secure

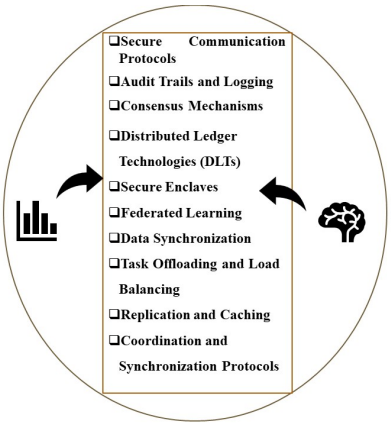

Figure 6: Methods of Accountability and Collaboration in Blockchain with Edge Computing

communication channels between edge devices, gateways, and central servers, these protocols make use of techniques for encryption, authentication, and data integrity. Secure communication protocols encourage accountability in edge computing environments by guaranteeing the confidentiality and integrity of data while it is being sent [15 – 18].

Audit Trails and Logging: In edge computing, keeping thorough audit trails and records is crucial for accountability. It is possible to track actions and identify any unauthorized or questionable behaviour by capturing activities, transactions, and events inside the edge environment. Reconstructing and analysing events using audit trails and logging algorithms enables accountability and, if necessary, forensic investigations.

Consensus Mechanisms: For accountability in edge computing, preserving complete audit trails and records is essential. By recording activities, transactions, and events inside the edge environment, it is feasible to keep track of actions and spot any unapproved or dubious behaviours. Accountability and, if necessary, forensic investigations are made possible by reconstructing and evaluating events using audit trails and logging algorithms [16 – 19].

Distributed Ledger Technologies (DLTs): Edge computing can make use of DLTs, such as blockchain or Directed Acyclic Graph (DAG) technology, to improve accountability. These innovations offer a decentralized and impenetrable ledger that keeps track of and authenticates data transfers or transactions [13]. In order to ensure accountability and data integrity, edge computing systems can use DLTs to keep an immutable and transparent record of actions.

Secure Enclaves: To safeguard delicate calculations and data in edge computing, secure enclaves like Intel Software Guard Extensions (SGX) or Trusted Execution Environments (TEEs) offer hardware-based security capabilities. Accountability may be improved by ensuring that computations are carried out in a trustworthy and tamper-resistant environment by isolating important activities within secure enclaves [9, 12].

Federated Learning: A collaborative machine learning approach called federated learning enables edge devices to jointly train a single model without sharing their raw data. A central server receives just the model updates from each edge device, which trains the model locally using its own data. A global model is collectively learned through training iterations and model update aggregation. While protecting data privacy and minimizing transmission overhead, federated learning enables collaborative model training in edge computing [14].

Data Synchronization: For collaborative data sharing and consistency in edge computing, data synchronization methods are crucial. These techniques make a guarantee that data is consistently synchronized and current among scattered edge devices or nodes [27]. Data synchronization techniques facilitate cooperation by offering a consistent picture of shared data among participating entities by effectively propagating and

Table 1: Blockchain and Edge Computing Survey.

Characteristics Covered	(2020)	(2021)	(2022)	Current Survey
Overview architecture	✓	✓	✓	✓
Consensus Protocol	✓	✓	✓	✓
Health care features	✓	✓	✓	✓
Healthcare applications	✗	✓	✗	✓
Privacy and Security issues	✓	✗	✓	✓
Standards for healthcare	✗	✗	✗	✓
Security and privacy threats Comparison	✗	✗	✗	✓
Blockchain and Edge Computing security and privacy	✗	✗	✗	✓
Performance of Blockchain and Edge Computing	✗	✗	✗	✓

reconciling data modifications.

Task Offloading and Load Balancing: Algorithms for task offloading and load balancing assist in distributing computational workloads and jobs across edge devices cooperatively. These algorithms decide what operations should be carried out locally on edge devices, what operations may be delegated to other devices, and how to distribute the computing burden among the edge network's devices. job offloading and load balancing techniques allow for effective teamwork in edge computing by optimizing job allocation and resource use.

Replication and Caching: In edge computing, replication and caching methods are used to improve data availability and decrease latency. These techniques facilitate cooperative data sharing and quicker access to shared resources by duplicating frequently requested data or storing computation results at edge devices. The availability of pertinent data at the edge for local processing is ensured by replication and caching methods, which facilitate collaborative operations [22, 24].

Coordination and Synchronization Protocols: Edge computing uses coordination and synchronization protocols, such as the Message Passing Interface (MPI) or Publish-Subscribe models, to make it easier for distant entities to work together and share information [17, 18]. The cooperation, coordination, and sharing of data and events throughout the edge network are made possible by these protocols, which specify communication patterns, message-carrying methods, and synchronization primitives.

5 Literature Review

Recent blockchain and Edge Computing survey literature is compared with this survey feature by feature. As we see in Table 1 [15, 16, 19] which shows various survey categories in reference to Blockchain and Edge computing in the healthcare sector.

5.1 Performance Matrix of Blockchain and Edge Computing

Transaction Throughput (TT): The number of transactions that are completed in a certain amount of time is known as transaction throughput. The time it takes to add valid data to blocks is measured using this metric. This influences how quickly the process transactions. The total number of records that have been authenticated and committed is divided by the time (in seconds) required to validate and save all of those records [5, 21].

$$TT = \frac{TotalTransaction}{TimeTaken} \tag{1}$$

Developers employ a variety of tactics, including roll-ups, sidechains, country channels, new consensus processes, and longer blocks, to enhance the throughput. The transaction throughput of a decentralized protocol is determined by the consensus algorithm on the platform. For instance, a proof-of-stake (PoS)

blockchain has a higher throughput than a proof-of-work (PoW) blockchain like Bitcoin. The length of a block in a blockchain, website traffic, edge computing, and transaction complexity are other factors that influence throughput [19].

Transaction per Second (TS): The number of records or transactions that have been submitted and stored each second is measured using the metric known as Transactions per Second (TS). It is used to calculate a network's processing capacity and scalability requirements [12 – 20]. The quantity of data kept in the ledger and the number of entries transferred to the various network are often counted separately. The block size and block time should both rise in order to enhance the number of transactions per second.

$$TS(n) = Count\left\{\frac{Transfrom(x,y)}{y-x}\right\} * \frac{Trans}{s} \tag{2}$$

If the time periods x and y are, is the number of transactions, is the duration in seconds, and TPS n designates the specific node for which the TPS is computed. As a result, the average TS may be used to compute TS for all nodes (N), as shown below.

$$TS = \left\{\sum n\frac{Transn}{N}\right\} * \frac{Trans}{s} \tag{3}$$

Transaction Latency (TL): The time it takes for a transaction to be verified and delivered to the blockchain network to be written to the ledger (or denied) is measured using the Transaction Latency (TL) [12] metric. This statistic is determined by contrasting the timestamps on the submitted transactions with the timestamps on the verified and stored transactions [15, 20, 23]. This metric can also show how rapidly consensus-building strategies are being used. Transaction latency is the interval between when a transaction is submitted to a various networks and edge computing when it is first validated. Additionally, it denotes the amount of time that must pass between pushing the submit button and seeing the transaction display on the screen.

$$TL = Net * Trans - Transst \tag{4}$$

where Transit, indicates the transaction submission time, Transact, denotes the transaction confirmation time, and Net represents the network threshold.

Transaction per CPU (TC): When they are being executed, smart contracts use a lot of CPU power. How much CPU is consumed is dependent on the business logic that was incorporated into the contract [23]. Loops will use a significant portion of the CPU resources when encryption is used. It requires a lot of CPU time to commit the block and calculate the global state's hash. Transaction per CPU applications employs different encryption techniques, hashing formulas, and consensus techniques. We will thus require a metric to monitor CPU use while smart contracts are in operation, where F is the frequency of a single CPU core and CPU(t) is the amount of CPU used by a blockchain program from a to b [25, 26]. Then, the following formula can be used to determine TC for the entire blockchain network of N nodes: **Transaction per second per memory:** TMS is a measurement that illustrates how much physical and virtual memory is used by the software. The TMS of a node (n) connected to a blockchain network between time periods a and b with the execution of a certain number of transactions (Trsac) was calculated using the following formula. The following formula may be used to compute the TMS of the whole blockchain network.

$$TCn = \frac{\sum TCn}{N\left\{\frac{Trans}{GHz.s}\right\}} \tag{5}$$

Transaction per disk INPUT/OUTPUT: Blockchain apps will have a dedicated storage space to keep data and the status of the world. TDIO [4] is a metric that keeps track of the input/output measurements made during certain processes including contract execution and block commits. In the blockchain network,

the TDIO for a particular node n is determined as follows:

$$TMS = \frac{\sum nTMSn}{N\left\{\frac{Trans}{MB.s}\right\}} \tag{6}$$

Edge computing performance evaluation may be theoretically approached utilizing many metrics and modeling methodologies [5, 6, 9, 27].

$$TDIO = \frac{\sum nTDIO}{N\left\{\frac{Trans}{kbs}\right\}} \tag{7}$$

(i) Queuing Theory: Edge computing system performance may be modeled and examined using queueing theory. It makes use of mathematical models that record the pace at which jobs arrive, the rate at which edge devices are serviced, and the total number of servers in the system. Performance measures like queue length, waiting time, and reaction time may be determined by analyzing these models.

(ii) Markov Chains: The state transitions and performance characteristics of edge computing systems may be examined using Markov chains. The probability of existing in various states and the transitions between states may be calculated by modeling the system as a stochastic process. This makes it possible to assess performance indicators like reaction time, availability, and dependability [15 – 20].

(iii) Network Theory: For evaluating the performance of linked edge devices and their communication network, network theory offers mathematical methods. The architecture of the network may be modeled, network latency can be examined, and the data routing between edge devices can be optimized using methods like graph theory and optimization techniques.

(iv) Simulation Modeling: Building computational models that imitate the behavior of edge computing systems is known as simulation modeling. These models represent the arrival of tasks, task processing by edge devices, and device-to-device communication. Performance indicators like latency, throughput, and resource utilization may be assessed by conducting simulations with various situations and settings [17, 20].

(v) Machine Learning Techniques: Large datasets gathered from edge computing devices may be analysed using machine learning methods. Performance patterns may be discovered and future system behaviour predictions can be established by training models using previous data. This can aid in enhancing performance overall, forecasting system problems, and optimizing resource allocation.

6 Results

When blockchain and edge computing are combined, they significantly improve accountability and teamwork in the healthcare industry. Healthcare systems can achieve improved accountability by utilizing the irreversible and transparent features of blockchain and combining it with edge computing's capacity to analyse data at the edge of the network. The blockchain may be used to record patient data acquired and securely kept by edge devices, creating an auditable trail of data access and usage. Encouraging accountability among healthcare professionals assures legal compliance. Additionally, this connectivity makes it possible for healthcare stakeholders to collaborate securely and effectively. With edge devices serving as nodes in the blockchain network, real-time data access and sharing are made possible without the use of middlemen. Effective collaboration between healthcare professionals, researchers, and patients can result in better care coordination, data sharing, and decision-making.

When blockchain and edge computing are combined, real-time data exchange and analytics are made possible. Without depending on centralized cloud servers, edge devices locally process and analyse data to produce insightful results. This makes decision-making possible in a rapid manner, especially in urgent medical situations where quick action is essential.

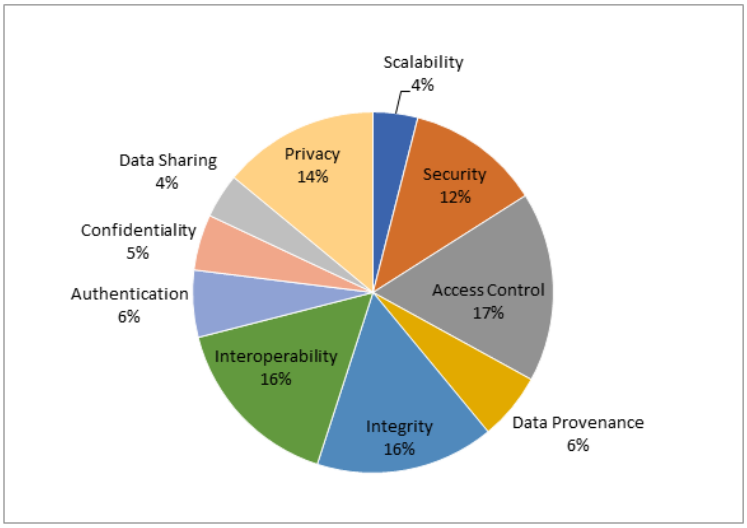

Figure 7: Blockchain and Edge Computing.

This integration also benefits consent management and privacy protection. By utilizing the decentralized design of the blockchain, patients have more control over their data. Through smart contracts, they may immediately give or cancel access permissions, protecting user privacy and data security. Edge devices reduce the dangers associated with centralized data storage by enforcing data privacy standards and keeping sensitive data inside the local network.

Additionally, edge computing and blockchain integration enhance healthcare supply chain management. Stakeholders can trace and instantly confirm the legitimacy and provenance of medicines, medical equipment, and supplies by logging supply chain transactions on the blockchain. Figure 7 depicts the representation of Blockchain and Edge Computing in Healthcare based on various factors. Edge devices are crucial in the collection and verification of supply chain data at multiple points, ensuring transparency and lowering the dangers of fake or sub-par goods. In conclusion, the use of edge computing and blockchain in healthcare produces measurable improvements in accountability. It improves data accountability, makes it possible to collaborate securely and effectively, makes it easier to share and analyze data in real time, improves consent management and privacy protection, and streamlines supply chain management. By promoting openness, reliability, and effectiveness in data management and decision-making processes [19, 20] these results revolutionize healthcare. Finally, experimental results show that the LSTM outperforms the other models in terms of precision, recall, and F1 score in Figure 8. This work is practically possible but the maintenance cost is more when compared to the traditional model.

Enhancing accountability and collaboration within the healthcare sector is made possible by the integration of blockchain technology with edge computing. Healthcare systems may attain new levels of openness, security, and efficiency by integrating the characteristics of these technologies. Blockchain technology creates a strong foundation for accountability due to its decentralized and unchangeable nature. Patient data may be securely gathered and stored by edge devices, and the access, use, and sharing of that data can be the subject of blockchain-based transactions. So that healthcare providers, researchers, and other stakeholders are held responsible for their actions, this generates an auditable record of data activity. Patients can more easily see how their data is utilized and shared thanks to the openness offered by the blockchain, which promotes trust and confidence in the system.

Collaboration among stakeholders in the healthcare industry is made possible by the combination of blockchain and edge computing. In the blockchain network, edge devices serve as nodes to enable seamless cooperation and real-time data exchange. Patients, healthcare professionals, and researchers may work together to develop treatment plans, discuss research findings, and exchange data in a safe and effective

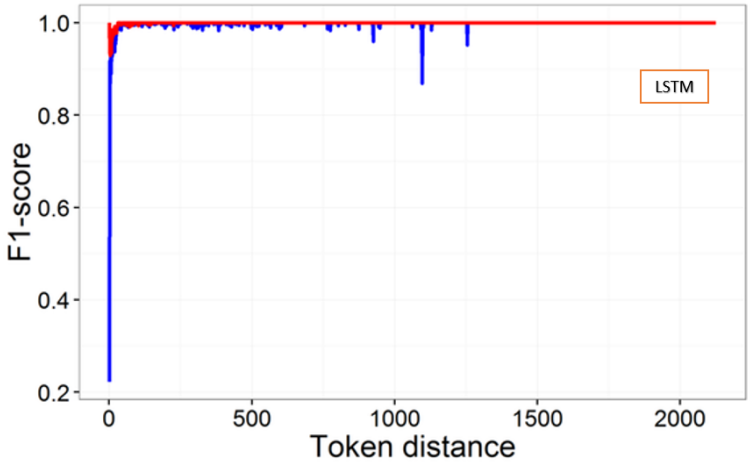

Figure 8: LSTM in Healthcare.

manner. This encourages efficient care coordination, multidisciplinary study, and the creation of novel medical treatments [17].

By allowing quick analysis and decision-making, edge computing's real-time data processing capabilities further improve cooperation. In order to reduce latency and enable quick reactions, edge devices have the ability to process and analyse data at the time of collection. This is especially helpful in challenging healthcare situations when real-time information can have a big influence on how patients are treated. Additionally, privacy preservation and consent management are ensured by the combination of blockchain and edge computing. Through blockchain-based processes, patients have ownership over their data and may give or remove access permissions as needed. Edge devices protect sensitive information by enforcing privacy regulations and keeping it on the local network, reducing the dangers of centralized storage and unauthorized access. Overall, the adoption of edge computing and blockchain in the healthcare sector strengthens accountability in the sector. It creates a framework for data management that is visible and auditable, allows for direct and secure communication between stakeholders, makes it easier to analyse data in real-time and make decisions, and manages privacy and permission. By encouraging trust, effectiveness, and creativity in the provision of patient care, this integration has the potential to revolutionize healthcare.

7 Conclusion

In conclusion, the application of edge computing and blockchain in the healthcare sector has enormous prospects for improving accountability and teamwork. Healthcare systems may reach a new level of trust, security, and efficiency by utilizing blockchain's transparency and immutability as well as edge computing's real-time data processing capabilities. By creating an auditable trail of data activity, the combination of these technologies makes it possible for enhanced accountability. Patient data is securely collected and stored by edge devices, and the blockchain keeps track of all data access and usage activities. This promotes openness and confidence in the handling of patient data by guaranteeing that healthcare practitioners and other stakeholders are accountable for their actions. Additionally, smooth communication across healthcare stakeholders is made possible by integration. By functioning as nodes in the blockchain network, edge devices allow for safe and direct communication, doing away with the need for middlemen. In order to improve care coordination and research efforts, healthcare professionals, researchers, and patients may work together in real time by exchanging data and ideas. This cooperative setting encourages creativity and information exchange, which improves healthcare results. By allowing quick analysis and decision-making, edge computing's real-time data processing capabilities enhance the blockchain's transparency.

By processing data at the moment of collection, edge devices may cut down on latency and enable quick replies. Real-time insights may significantly improve patient care in time-sensitive healthcare circumstances; thus, this is very helpful. Additionally, privacy preservation and consent management are ensured by the combination of blockchain and edge computing. Through blockchain-based processes, patients have more control over their data since they may give or remove access permissions as necessary. In order to reduce the dangers associated with centralized data storage, edge devices enforce privacy regulations and preserve sensitive data on the local network.

The potential for blockchain and edge computing to improve cooperation and accountability in the healthcare industry is exciting. The benefits and capabilities of this integration may be increased through developments in data governance, interoperability, scalability, AI integration, and regulatory compliance. The healthcare sector may increase efficiency, transparency, and collaboration by using these upcoming developments, which will eventually enhance patient outcomes and healthcare delivery.

Authors' Contribution: RK established the proposed concept, developed the theory, and carried out the computations. RK also validated the analytical techniques, encouraged the investigation of real-world issues, and oversaw the results of this work.

Funding Statement: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services,* 14(4), 352-375.
2. Fernandez-Aleman, J. L., Seor, I. C., Lozoya, P. O., & Toval A. (2013). Electronic health record security and privacy: A thorough overview of the literature. *Journal of Biomedical Informatics,* 46(3), 541-562.
3. Kuo, T. T., & Pham, A. (2022). Detecting model misconducts in decentralized healthcare federated learning. *International journal of medical informatics, 158,* 104658.
4. Yang, Y., Xu, R., Zhang, J., & Qian (2018). Design and implementation of a blockchain-based access control system for medical records. *3rd International Conference on Crowd Science and Engineering Proceedings,* 182-188.
5. Zhang, X., Poslad, S., & Ma, Z. (2018, December). Block-based access control for blockchain-based electronic medical records (EMRs) query in eHealth. In 2018 *IEEE Global Communications Conference (GLOBECOM)* (pp. 1-7). IEEE.
6. Farooq, M. S., Ahmed, M., & Emran, M. (2022). A survey on blockchain acquainted software requirements engineering: model, opportunities, challenges, and future directions. *IEEE Access, 10,* 48193-48228.
7. Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K. K. R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security, 97,* 101966.
8. Iqbal, R., Salah, & Chakraborty, S. (2019). Healthcare IoT with Blockchain and Edge Computing: Opportunities, Problems, and Solutions. *IEEE Access, 7,* 10254–10267.

9. Zeng, Z., Sheng, Q. Z., & Qin, Y. (2019). Blockchain in healthcare: A thorough evaluation of the literature, a framework for synthesis, and a research plan for the future. *International Journal of Information Management, 49,* 128–144.
10. Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling of develop a blockchain technology in healthcare application: taxonomy, substantially analysis, motivations, challenges, recommendations and future direction. *Journal of medical systems, 43,* 1-35.
11. Kothari, R., Choudhary, N., & Jain, K. (2021). CP-ABE scheme with decryption keys of constant size using ECC with expressive threshold access structure. In *Emerging Trends in Data Driven Computing and Communications: Proceedings of DDCIoT 2021*(pp. 15-36). Springer Singapore.
12. Rahman, M. A., Hossain, M. S., Loukas, G., Hassanain, E., Rahman, S. S., Alhamid, M. F., & Guizani, M. (2018). Blockchain-based mobile edge computing framework for secure therapy applications. *IEEE access, 6,* 72469-72478.
13. Alotaibi, E. F., AlBar, A. M., & Hoque, M. R. (2016). Mobile computing security: issues and requirements. *Journal of Advances in Information Technology Vol,* 7(1).
14. Ahad, M. A., Tripathi, G., Zafar, S., & Doja, F. (2020). IoT data management—Security aspects of information linkage in IoT systems. *Principles of internet of things (IoT) ecosystem: Insight paradigm,* 439-464.
15. Abu-Elezz, I., Hassan, A., Nazeemudeen, A., Househ, M.,& Abd-Alrazaq, A. (2020). The benefits and threats of blockchain technology in healthcare: A scoping review. *International Journal of Medical Informatics, 142,* 104246.
16. Xiao, K., Shi, W., Gao, Z., Yao, C., & Qiu, X. (2020). DAER: A resource preallocation algorithm of edge computing server by using blockchain in intelligent driving. *IEEE Internet of Things Journal,* 7(10), 9291-9302.
17. Lin, X., Wu, J., Mumtaz, S., Garg, S., Li, J., & Guizani, M. (2020). Blockchain-based on-demand computing resource trading in IoV-assisted smart city. *IEEE Transactions on Emerging Topics in Computing, 9*(3), 1373-1385.
18. Wang, S., Ye, D., Huang, X., Yu, R., Wang, Y., & Zhang, Y. (2020). Consortium blockchain for secure resource sharing in vehicular edge computing: A contract-based approach. *IEEE Transactions on Network Science and Engineering, 8*(2), 1189-1201.
19. Hammoud, A., Sami, H., Mourad, A., Otrok, H., Mizouni, R., & Bentahar, J. (2020). AI, blockchain, and vehicular edge computing for smart and secure IoV: Challenges and directions. *IEEE Internet of Things Magazine, 3*(2), 68-73.
20. Aggarwal, L., Sachdeva, S., & Goswami, P. (2023). Quantum healthcare computing using precision based granular approach. *Applied Soft Computing, 144*, 110458.
21. Xiong, Z., Zhang, Y., Niyato, D., Wang, P., & Han, Z. (2018). When mobile blockchain meets edge computing. *IEEE Communications Magazine, 56*(8), 33-39.
22. Tanwar, S., Parekh, K., & Evans, R. (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications, 50*, 102407.
23. Attaran, M. (2022). Blockchain technology in healthcare: Challenges and opportunities. *International Journal of Healthcare Management, 15*(1), 70-83.
24. Khan, F., Kothari, R., Patel, M., & Banoth, N. (2022, April). Enhancing non-fungible tokens for the evolution of blockchain technology. In *2022 International conference on sustainable computing and data communication systems (Icscds)* (pp. 1148-1153). IEEE.
25. Hofert, A. (2023). Converging Technologies and Business Models That Will Transform the Healthcare Sector Exponentially. In *Digital Identity in the New Era of Personalized Medicine* (pp. 46-64). IGI Global.
26. Mantey, E. A., Zhou, C., Srividhya, S. R., Jain, S. K., & Sundaravadivazhagan, B. (2022). Integrated blockchain-deep learning approach for analyzing the electronic health records recommender system. *Frontiers in Public Health, 10*, 905265.

27. Gupta, R., Tanwar, S., Al-Turjman, F., Italiya, P., Nauman, A., & Kim, S. W. (2020). Smart contract privacy protection using AI in cyber-physical systems: tools, techniques and challenges. *IEEE access, 8*, 24746-24772.

About the Author

Mr. Rakshit Kothari is working as an Assistant Professor in the Department of Computer Science and Engineering at Geetanjali Institute of Technical Studies, Dabok, Udaipur, Rajasthan. He has done B.Tech in Computer Science and Engineering at Rajasthan Technical University, Kota with first division honours. He secured Master of Technology in Computer Science and Engineering at College of Technology and Engineering, Maharana Pratap University of Agriculture and Technology, Udaipur, Rajasthan, India. He is in teaching profession for more than 2 years and published varieties of books. He has presented number of papers in National and International Journals, Conference and Symposiums. He is currently a member in Soft Computing Research Society. His main area of interest includes Internet of Things, Cryptography and Blockchain.