International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Trustworthy Healthcare Data Systems: The Role of Blockchain in IoT, Edge and Cloud Environments

Sheeba Kuriakose[1], Dr. K. P. Malarkodi[2]

[1]Research Scholar, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, India
Email: *sheebaobey[at]gmail.com*

[2]Assistant Professor, Department of Computer Science, Sri Krishna Arts and Science College, Coimbatore, Tamil Nadu, India
Email: *malarkodikp[at]skasc.ac.in*

Abstract: ***Healthcare technology is now undergoing a digital transformation that incorporates cloud computing, Internet of Things (IoT) devices and edge computing, in order to enhance medical data management, enable remote healthcare delivery, and track patients in real time. In healthcare, IoT devices are constantly gathering complex and sensitive patient information, and frequently storing and processing it in the cloud to retrieve and analyse information quickly for easy access by the user. The centralization part of the cloud-based computing has its own security issues of data security, data privacy, data integrity, unauthorized access, and single point of failure. Edge computing is a potential solution to address these challenges as it involves processing data closer to its source, reducing latency and bandwidth, and minimizing the need for centralized infrastructures. While these are some advantages, there are still significant challenges to the safe and reliable transmission of information in decentralized healthcare systems. Healthcare applications seek to realize unprecedented data security, transparency, traceability, and access control through an integration of blockchain technology that is difficult to gain using traditional centralized systems. By integrating blockchain with IoT, edge computing and cloud networking, healthcare institutions can ensure secure data transfer, enhanced privacy measures, and effective Electronic Health Record (EHR) management. Most recently, there have been several examples indicating the potential of blockchain architectures for both improved cybersecurity and providing affordable healthcare. Healthcare systems that use blockchain technology are the focus of this study, which also assesses their architectures, security protocols, advantages, and disadvantages that incorporate the concepts of IoT, edge computing, and cloud computing, offering some insights into creating secure, scalable, and trustworthy healthcare data systems.***

Keywords: Blockchain, Edge Computing, Cloud Computing, Privacy Preservation, IoT, Healthcare Data, Data Security.

1. Introduction

The healthcare sector has experienced extensive technological advances, particularly in the last decade, with rapid adoption of cloud computing, edge computing, IoT and blockchain technology [1]. Smart healthcare settings, made possible by these technological advancements, allow for remote diagnosis, individualized treatment plans, effective administration of medical data, and real-time patient monitoring. The explosion of the medical IoT has led to vast amounts of health data being gathered from wearable sensors, smart medical devices, mobile healthcare applications, and remote monitoring systems, which must be handled securely while stored, processed, and transmitted [2].

Medical imaging, medications, patient information, insurance details, clinical histories, laboratory findings, and Electronic Health Records (EHRs) [3] are all examples of healthcare data. This type of data is both of the utmost sensitivity and very sensitive to security, privacy and integrity issues. In a contemporary healthcare system, each healthcare service requires the adoption of electronic health records for efficiency. In an updated health system, every health service needs to use electronic health records to enhance efficiency.

There is a higher demand in the healthcare sector to gather patient data every minute of the day with the increasing number of IoT devices [4]. IoT technologies have heavily been integrated in healthcare devices, such as wearable fitness trackers, heart rate monitors, glucose monitoring systems, as well as blood pressure and electrocardiogram (ECG) devices and smart medical equipment [5]. Safeguarding the usage of these gadgets would enable healthcare staff to remotely monitor patients' health state and initiate actions promptly. An illustration of the advantages of the IoT in healthcare is shown in Figure 1.

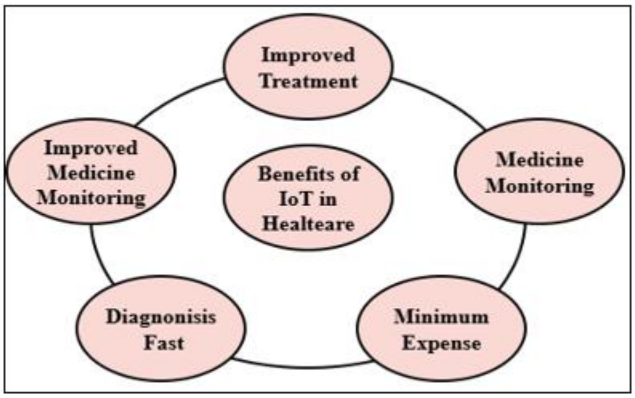

Figure 1: Benefits of IoT in Healthcare

Common uses of IoT in health care are:
- Elderly care monitoring
- Smart hospital management
- Remote patient monitoring
- Emergency healthcare services
- Telemedicine and virtual health care
- Chronic disease management

While these are benefits, healthcare data generation presents multiple security and privacy concerns. Health information is commonly moved from one network to another and held in centralized centres, making it easy for cyber criminals to target it for unlawful intrusion, data entry, data manipulation and data breaches.

Figure 2: Role of Cloud Computing in Healthcare (tekkiwebsolutions.com)

The most significant security issues of healthcare systems fall under the following categories:

- Data Privacy Violations: Improper access to confidential patient information.
- Data Integrity Attacks: Altering, or tampering with, medical records while they are being sent or stored.
- Unauthorized Access: When unauthorized individuals or unauthorized users can access information about healthcare.
- Identity Theft: Patients' identities being used and medical credentials being misused.
- Single Point of Failure: Service outages caused by failures in a central health service.
- Lack of Transparency: inability to monitor data accesses and modification actions.

Cloud Computing has long been used to handle health care data due to its flexibility, cost-efficiency and scalability. It offers healthcare service accessibility, storage space as well as computational power in large quantities across different locations [6]. It allows medical professionals to easily access and manage patient records, and facilitate seamless data exchange between healthcare institutions, such as between hospitals, clinics, laboratories, and insurance companies. Cloud computing in the healthcare industry is seen in Figure 2.

There are essentially four types of cloud computing in the healthcare industry [7]:

- **Public Cloud:** Services are provided over public cloud infrastructures handled by third party providers. Public clouds can be beneficial for non-critical healthcare application needs, because they're cost-effective, can be scaled easily, and are readily accessible.
- **Private Cloud:** Private cloud infrastructure is used by just one healthcare organization. They can offer better security, more oversight over health-related data, and fulfill regulatory specifications, which makes them ideal for handling sensitive patient-related information.
- **Hybrid Cloud:** The attributes of both public and private cloud converge on a hybrid cloud. Certain workloads and applications may be spun up in a cloud public facing framework and other less critical healthcare information is stored on a private cloud. This will ensure flexibility, scalability and optimum use of resources.
- **Community Cloud:** Community clouds can be shared, as long as they share the same security needs and needs to operate in the same community as one another- as is the case with multiple healthcare institutions, hospitals, research centers or government agencies.

While cloud computing provides many benefits, the centralized cloud architecture has a number of drawbacks. Healthcare data centralizing within one infrastructure makes the probability of data breaches, in-sider attacks, service downtime and privacy violations higher. Besides that, large amounts of health-care data sent to remote cloud servers may cause communication delays and demand higher bandwidth.
Edge computing is a highly useful solution that tackles these challenges. The concept of edge computing is that it reacts to the data source it collects when processing instead of the data source it generates. When used in a healthcare context, edge devices can perform local data processing and filtering before uploading the selected data for further analysis or prediction to the cloud [8]. Edge devices can do the processing, filtering and initial analysis in healthcare settings, with deeper analysis or prediction applied in the cloud. Figure 3 shows the edge computing in IoMT devices.

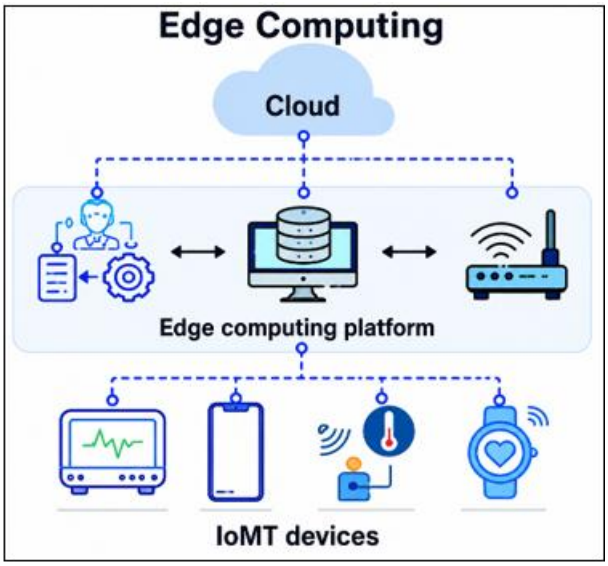

Figure 3: Edge Computing in IoMT devices [36]

Edge computing offers the following benefits:
- Reduced communication latency.
- Quick reaction time of critical health systems.
- Lower bandwidth utilization.
- Improved system reliability.
- Improved capabilities in real time patient monitoring.
- Improved Healthcare Services.

While edge computing enhances the efficiency of the system, it doesn't necessarily ensure secure data sharing and reliable handling of health data. Hence, stringent security measures are needed to ensure that vital patient data is safeguarded within the healthcare landscape.

Blockchain has become an exciting paradigm in the healthcare sector for secure data management. A decentralised Distributed Ledger Technology (DLT), blockchain records transactions in an immutable ledger that cannot be altered [9,10]. Unlike the traditional centralized approach, blockchain technology does not require reliance on a single administrator and rather ensures that the data is safely and transparently maintained and records are verifiable and tamper-proof. The use of blockchain technology to secure healthcare data is illustrated in Figure 4.

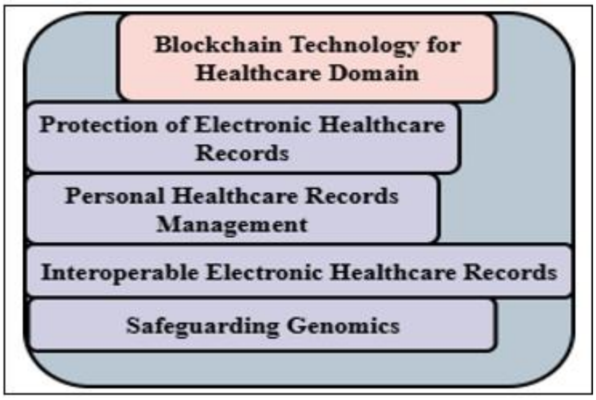

Figure 4: Implementing Blockchain Technology for Healthcare Data Security

Among the primary parts of blockchain technology are:
- **Blocks:** Containers that contain transaction information.
- **Block Cipher:** A cryptographic system that is performed on blocks of data.
- **Distributed Ledger:** Shared database running across many nodes.
- **Payment Systems:** Payment systems for transactions.
- **Smart Contracts:** Automated agreements which can be triggered by certain conditions.

To ensure the safety, confidentiality, and authenticity of health care records, several blockchain technologies have been adopted in this industry. Consensus methods, like as Proof of Work (PoW), are built into blockchain systems to guarantee the authenticity of data. Proof of Stake (PoS) is a more energy-efficient alternative to Proof of Work (PoW) that uses the notion of assigning validators based on their stake in the network. Perfect for a permissioned healthcare setting, Proof of Authority (PoA) relies on a network of verified users to validate transactions. Practical Byzantine Fault Tolerance (PBFT) helps maintain a system's reliability and trustworthiness against the attacks of Byzantine or faulty nodes so that the system does not rely on high risks [11].

Moreover, smart contract systems automatically manage consent and healthcare policies to ensure access to this sensitive and critical healthcare information is granted to only authorized users. There are several sectors in the healthcare industry that can benefit from the use of blockchain. They range from better data security to improved patient privacy, immutability of medical records, and the addition of audit trails that can be tracked as well as a decentralised trust management system and the secure exchange of healthcare data between patients, providers and other parties.

This blended integration of IoT, edge computing, blockchain, and cloud can be a sensible and secure healthcare system. The edge layer is designed to streamline latency, the blockchain layer enhances security and trust, while the cloud-layer provides sample storage and service provision. These technologies complement each other to enable safe handling of medical data, along with privacy, integrity and access to medical information.

This report describes ongoing developments in this space as illustrated with examples drawn from the IoT, edge computing, cloud computing and healthcare information systems based on the blockchain. Section 2 introduces existing approaches of blockchain use in health care and security. The compared analysis of the reviewed models is offered in section 3. In Section 4, the approaches will be evaluated for their security and performance. Section 5 presents future research directions, while Section 6 concludes the study.

2. Review of Blockchain-Based Models for Healthcare Data Management

Jayabalan & Jeyanthi [12] presented a scalable blockchain model that allows for safe storage, sharing and retrieval of Healthcare Data Security via the IPFS. The model resorts to off-chain storage on IPFS, thereby providing both privacy and security in the storage and retrieval of data, and utilizes digital signatures and hashing through the use of RSA encryptions and AES encryption, while allowing for the scalability of the blockchain. The patient-centric access control mechanism empowers patients to give and take access to healthcare providers for them suit their needs improving their control over personal health data. However, interoperability among heterogeneous healthcare systems is not extensively addressed.

Dammak et al., [13] implemented LoRaChainCare- an IoT-based healthcare monitoring architecture with the combination of blockchain, LoRa communication, edge computing, fog computing, and IPFS for the safe storage and administration of individual health records. By combining architecture with reliable and low-power transmission of health care data in LoRa networks and data security, privacy, and controlled access by blockchain and IPFS, the initiative enhances data reliability and security. Additionally, with the help of IPFS as well as blockchain to ensure data security, privacy, controlled access, and the architecture, the initiative provides reliable data transmission and properties. However, the architecture primarily focuses on secure data communication and storage, with limited support for intelligent healthcare analytics and disease prediction.

Jaishankar et al., [14] introduced an Efficient Blockchain Network for Securing Healthcare Data Utilising the Multi-Objective Squirrel Search Optimisation Algorithm (MOSSA). Using blockchain technology, the model offers decentralized, secure, and trustworthy storage of healthcare information via digital signatures, consensus algorithms, and hashing methods. By optimising blockchain parameters including block size, transaction size, and the total amount of blockchain channels, MOSSA enhances blockchain security and scalability. Yet, the blockchain initiative mainly aims to optimise its performance and security, with minimal support for intelligent clinical decision-making and real-time healthcare analytics.

Ali et al., [15] created a block chained-based secure searchable encryption an approach based on Industrial IoT (IIoT) and neural networks in Health-care systems. The idea combines the blockchain technology, homomorphic encryption, and trust-chain mechanisms to enable secure access to healthcare data of the patient based on keywords while ensuring privacy and data integrity. To improve intrusion detection and better monitor healthcare data security, a method called Group Theory-based Binary Spring Search (GT-BSS) is implemented utilising a Hybrid Deep Neural Network. In addition, there exist key revocation mechanisms and policy update mechanisms for enhancement in access control. However, incorporating various cryptographic and neural network elements can complicate the computational process.
Rani et al., [16] introduced lightweight privacy and security preserving blockchain approach for cloud-based administration of health records. Using cryptography, smart contracts, encryption, and pseudonymization, it allows for the safe transfer and storage of medical records without sacrificing patients' right to privacy or control. The decentralized ledger model helps to decrease transparency, auditability, and privacy and security risks in cloud situations. However, discussing benefits of scalability of growing number of transactions in health care is not done to its full extent.

Azbeg et al., [17] developed BlockMedCare, safe data management with remote patient monitoring through the integration of the IoT, blockchain technology, and IPFS into a healthcare system. To safeguard healthcare data, the system employs proxy re-encryption and employs blockchain technology; to regulate access to available entities, it makes use of smart contracts. A Proof-of-Authority (PoA) consensus mechanism is utilised to provide quick data processing, while IPFS is utilised as an off-chain storage option to optimise for scalability and minimise storage overhead. But not fully discussed the interoperability with external healthcare systems and standards.

Lodha et al., [18] presented a Blockchain-based IoMT Security System (BC-IoMT-SS) to safeguard electronic healthcare monitoring and the administration of patient data. To ensure the confidentiality, authenticity, and integrity of healthcare data during transmission and storage, this framework integrates IoMT with blockchain technologies. It allows secure electronic access to medical records and provides alerts to authorized health care practitioners, using blockchain as the basis for authentication. But the whole framework concentrates on aspects of data security and monitoring, while diminishing value to the advanced healthcare analytics and intelligent disease forecast.

Rani et al., [19] suggested a safe HealthCare on IoT using Blockchain, IPFS and smart contracts for safe monitoring of patients remotely. The framework combines the benefits of blockchain technology for data security and integrity, IPFS for decentralized content storage and sharing of patient records, and decentralized applications (DApps) for the process of collecting data and sharing it across different nodes. Health data and permissions may be automated between healthcare actors using smart contracts. But the framework doesn't have any sophisticated prediction analytics or intelligent diagnostics algorithms.

Chaturvedi [20] presented an IoT-based secure framework of healthcare systems using blockchain technology, Safe transfer and analysis of medical pictures using a Simplified Swarm-Optimized Bayesian Normalised Neural Network (SSO-BNNN). The use of blockchain ensures decentralized and secure data sharing, and the introduction of the SSO-BNNN model augments the processing and usefulness of healthcare data for decision-making. The hash value is further encrypted using a Neighbourhood Indexing Sequence (NIS) approach to further increase data security. However, the framework provides only basic support for interoperability and secure transmission of medical images and may not support healthcare data interoperability in multi-healthcare systems.
Meisami et al., [21] created a decentralised system for managing healthcare data that is built on blockchain technology and the IoT in order to improve the safety, privacy, and management of patient healthcare information. The protocol reduces network cost and improves efficiency by using a blockchain design that does not rely on a heavy consensus process. This makes it ideal for IoT devices that have limited resources. Also, the patient is able to control access to patient information and against any such disclosure is offered an access control mechanism that respects privacy. However, it cannot solve the real-time healthcare analytics and intelligent disease prediction capability.

Ali et al., [22] suggested blockchain-based healthcare system for improved scalability, security, and healthcare decision-making using a combination of DL methods. Interoperability in health care provider communication and secure storage of private information are both made possible by the permission-based blockchain. The hybrid deep learning approach challenges the traditional machine learning and deep learning approaches by analyzing complex healthcare data to assist diagnosis, treatment recommendation, and disease prediction. But it might have challenges in practice in a big medical setting, because of its computational complexity or regulatory compliance.

Sharma et al., [23] introduced a Distributed Application (DA) and smart contracts based blockchain privacy protection technique for healthcare systems enabled by the IoT. With such an approach, the secure issuance, management and validation of healthcare certificates become possible and privacy and transparency of certificates are preserved, along with attacks including collusion, phishing and masquerading. Smart contracts are applied to implement security policies and manage the interactions between healthcare centers, authorities and verifiers. But the consideration of interoperability does not reach the level of heterogeneous health-care platforms in a great amount.

Taloba et al., [24] created a blockchain-based hybrid platform for processing multimedia data in healthcare contexts enabled by the IoT. Secure storage, processing, and transfer of healthcare multimedia data—including medical photographs, audio recordings, and text records—is ensured by the app's reliance on blockchain technology. The echo retagging system produces a hash for all healthcare information, thus guaranteeing that the data hasn't been modified without permission or violated. However, the management of big data covering multimedia healthcare information is difficult.

Bhaskar et al., [25] introduced a lightweight blockchain system to improve data security in IoT sensor networks. The model incorporates measures to safeguard patient data, including encryption, access control, secure authentication, and blockchain technology. These measures help to prevent unauthorised access and cyberattacks. New technology possibilities, such as blockchain and AI, are also covered, along with healthcare system cybersecurity concerns, regulatory mandates, and interoperability. However, practical aspects and deployments in real world health care environments are not much benchmarked.

Kothari [26] introduced that blockchain technology and edge computing are being integrated in the field of healthcare to enhance transparency, collaboration and information security. They have now been combined to establish distributed security features of a blockchain and real-time processing capabilities of an edge computing system, offering a secure data sharing up-to-date privacy, interoperability, and patient-focused healthcare solutions. Furthermore, application of machine learning methods such as Q-Learning, Deep Q-Networks (DQN) and SVM are integrated to achieve smart edge healthcare analytics. Implementation complexities as well as resource concerns in case of heterogeneous healthcare settings are however unaddressed.

Ganapathy et al., [27] designed a communication system in Healthcare IoT networks that enables secure communication by implementing an IoT Federated Learning model based on Blockchain (BFL-hIoT). It combines blockchain technology with federated learning, helping to ensure trust and privacy while securely sharing data across various healthcare devices and systems. It recognizes the typical activities of users and distinguishes them from malicious actions, further enhancing the protection and maintenance of sensitive healthcare information. However, seamless integration and sharing of healthcare data across different medical platforms remain unexplored.

Babu and Jothi [28] designed a multi-tenant cloud infrastructure, zero-knowledge proofs (zk-SNARKs), and blockchain technology to create a secure architecture for healthcare analytics that preserves patient privacy. The framework's ability to securely compute health-related information without revealing sensitive patient data contributes to better healthcare record security. Blockchain is used to create a secure, transparent ledger, and anonymized healthcare information and zk-SNARKs are used to preserve privacy during analytics processing. The framework also enables secure data sharing and computation for telemedicine apps. However, creating and verifying ZKPs might come with high computational costs, which could impact the efficiency of systems.

Verma [29] suggested healthcare data security in the cloud using a blockchain-based privacy protection architecture. Using blockchain technology, the system provides a safe and reliable way to store and share medical records. Equine Herding Optimisation with Opposition-Based Learning (EHO-OBL) is employed for key generation, and an improved Blowfish model of encryption is employed for enhanced data security, secrecy, authentication, and integrity. However, there is still no support for real-time health care monitoring and intelligent healthcare analytics.

Anjum et al., [30] introduced an Opportunistic Access Control Scheme (OACS) to enhance security in healthcare settings that are IoT-enabled and utilise blockchain technology and machine learning. Depending on the specific access needs for a user, its previous access pattern and the sequence of access permissions delegated over the blockchain, the scheme dynamically grants and revokes access permissions. To improve the safety of electronic health records, a machine-learning algorithm is employed to decipher blockchain suggestions and make smart access decisions. However, it doesn't support real-time healthcare monitoring or predictions of disease analytics.

Mallick et al. [31] introduced a secure, trusted data-sharing solution for smart healthcare that combines blockchain, IoT, smart contracts, and IPFS. The architecture provides secure storage and sharing of health records, enhancing data privacy and interoperability for patients and healthcare providers while offering scalability benefits. This is embedded with a device proxy, which can detect any event on vulnerable devices and use cryptography to keep critical health data secure from adversarial users. The extra layer of proxy, though, could bring added complexity to the system.

Regalado and Han [32] presented a secure, expandable structure for IoT-Mixed Reality (IoT-MR) for constant performance and well-being verification. The framework features a 3-tiered design with intelligent sensors, wearable devices, and mixed reality interfaces, providing a range of immersive visualization possibilities, real-time feedback, and AI-driven healthcare analytics. The combination of edge computing and adaptive compression technologies boosts data processing capabilities, interoperability, and decision making in critical healthcare environments. The ability to adapt compression and work at the edge will increase in data processing capabilities, interoperability, and decision making in critical health care environments. However, reliance on specific MREs could make things more expensive and more difficult to deploy.

Mythili and Gopalakrishnan [33] introduced AdaSec-Health, a sharded blockchain-based protocol for secure healthcare

Paper ID: SR26711122439 DOI: https://dx.doi.org/10.21275/SR26711122439

data transfer in cloud-IoT contexts, and scalability. Combines IPFS nodes, blockchain, and an Enhanced Coati Optimization Algorithm (ECOA) to optimize shard configuration, minimize orphan blocks or even forks and enhance the security of Electronic Health Records (EHRs). Its user-centric design ensures a high level of interactivity, while simultaneously delivering robust network security and scalability. However, optimization process could make implementation more complicated in large scale health care networks.

Bose et al. [34] presented a cloud-based health-care security architecture called Secure health-care data processing via Quantum-Secure HealthChain, which integrates blockchain technology with quantum computing. It uses Quantum Key Distribution (QKD) protocol, quantum resistance and quantum biometric authentication to enhance data confidentiality, access control and prevent future quantum attacks. The technology of the blockchain is used to maintain the integrity, transparency and secure storage of healthcare records, and multi-layered encryption protects patient privacy. But the demand for specific infrastructure is quantum may hinder actual use of the technology and pose deployment costs.

Ali et al., [35] implemented the validation and storage of safe health data using an IoMT framework based on blockchain technology. By combining IoMT devices, edge computing and Hyperledger Fabric, the framework can provide the safe transfer of sensitive medical information in real-time without compromising its security, privacy, and interoperability of data across any health care system. Edge computing is being used to lower latency and boost processing efficiency, to provide better clinical decision-making and remote patient monitoring. However, the framework mainly focuses on secure data storage and validation, with limited attention to intelligent data analytics, predictive healthcare modelling, and automated disease detection capabilities.

3. Comparative Analysis

The examined healthcare data management methods based on blockchain are compared in Table 1, highlighting their merits and demerits along with their techniques and datasets used as well as their performance metrics.

Table 1: Summary of Blockchain-Based Healthcare Data Management Models

Ref No.	Techniques Used	Merits	Demerits	Dataset	Performance Metrics
[12]	Blockchain	Secure and decentralized EHR sharing, patient-centric access control, highly scalable on-chain / off-chain with IPFS storage.	Complex management of cryptographic functions, higher complexity of implementation, not completely validated real-time performance.	Health Data Transactions Dataset	Compression rate = 99.14%
[13]	IoT, Blockchain, LoRa, Edge computing, Fog computing	Enhances secure sharing of health-related data, facilitates low energy long-range communication.	Low level of focus on interoperability of healthcare data.	Real-Time Data	Transmission Time Determination = 3.36s
[14]	MOSSA, Blockchain	Improves transaction size and block size optimization on blockchain, which enhances security, scalability, throughput and storage management	Has limited real-world healthcare validation and it has only been evaluated in a simulation environment.	Monitoring devices (MM) and the Service providers	Throughput = 26.87%, Higher efficiency = 34.67%, Lowest delay = 22.97%, Lesser computational overhead = 37.03%, Higher storage cost = 34.29%
[15]	IoT, Blockchain, NN	Supports safe, searchable encryption, intrusion detection and privacy preserving access to healthcare data.	Prolongs the algorithm's processing time, an increase in the encryption overhead that arises when using it to process a data set.	Personal Health Records System	No. of people 300: FPR = 0.002%, FNR = 0.029%, FDR = 0.035%, ACC = 0.87%
[16]	Blockchain, IoT, Cloud System	Improves the privacy, security and cost-effective sharing of healthcare information in a cloud environment.	Limited Evaluation against large-scale healthcare datasets/real world understandings	EHR system (Patient Data)	Encryption time = 98.2 ms, Decryption time = 9 ms
[17]	Blockchain, IoT	Safely Distributes Healthcare Data on the Internet of Things, Blockchain, and Secure Inter-Protocol File Sharing.	The complex architectural design because of using more than one technology.	Off-chain database based on IPFS	Block creation = 5000 ms, Physician registration = 10482 ms, Patient registration = 10648 ms, Device registration = 9625 ms, Send data = 19747 ms
[18]	BC-IoMT-SS	Efficiently manages data while assuring secure and privacy-preserving IoMT-based healthcare monitoring. Improvement:	Restriction in scale for large-scale real-time deployments of IoMT is addressed.	Dataset search: From 10 patients are selected for clinical study	High precision ratio = 94%, Efficiency ratio of 94%, Shorter delay = 0.63s
[19]	Blockchain, IoT	Supports secure decentralised IoT monitoring of healthcare, offering robust privacy and access control.	Implementation complexity is high because it has multiple integrated technologies.	Dapp, IPFS (Inter Planetary file system) for patient data	Time taken for consensus: PoA = 7.5 s, PoS = 8.3 s, PoW = 17.3 s
[20]	SSO-BNNN, Blockchain, IoT	Secure and accurate health care data transmission via	Needs lots of computational expenses and training data.	Medical Image Data	For SSO-BNNN:

		optimized neural networks and blockchain through IoT.			Accuracy = 99%, Sensitivity = 98%, Specificity = 98%
[21]	Blockchain, IoT	Facilitates safe, streamlined and patient-managed access to health information with less reliance on third-party solutions.	Few evaluations of large-scale real-time deployments of IoT devices.	Off-chain storage in IPFS	Network's computing power = 50%
[22]	IoT, Decentralized applications, Blockchain, Hybrid DL	Enables scalable and secure healthcare data management with real-time intelligent decision support.	Integration of hybrid deep learning is relatively expensive in terms of computation.	Healthcare datasets (medical records, images, sensor data)	For 10 nodes: Latency = 4000 ms, Encryption Time = 5 ms, Transaction Count = 120, Computing Time =55, Execution Time = 5 ms
[23]	IoT, Blockchain, DA	Efficient and secured data sharing over the IoT via smart contracts as well as distributed tasks on blockchain.	Limited scalability and transaction cost associated with blockchain operations.	Ethereum platform (Public Blockchain)	Latency = 600 secs, Throughput = 5500 tps, Response Time = 2200 secs
[24]	Blockchain, Multimedia, IoT	Provides secure and efficient multimedia healthcare data processing using IoT and blockchain.	Large Size of the Multimedia Datasets (high storage & complexity of the system).	IoT healthcare multimedia data (images, text, audio simulation)	Accuracy = 86%
[25]	Lightweight blockchain, IoT	Excellent information protection, confidentiality and integrity, secure healthcare data sharing.	It is costly in terms of computation, incompatible, it requires a complex infrastructure.	Medical Data Security with 20 participants	Treatment A: Average = 84.3%, Treatment B: Average = 86.7%
[26]	Blockchain, Edge computing, DQN, SVM	To guard against data security, privacy, real-time healthcare data analytics, collaboration and accountability.	Complex systems, integration issues, higher price for implementation.	Healthcare Transaction Data	Accuracy = 87.4%

4. Performance Evaluation

This section assesses the accuracy and throughput of healthcare frameworks that utilise blockchain, IoT, ML, DL, cloud computing, and edge computing. Figure 5 illustrates the accuracy achieved by the different frameworks, while Figure 6 presents their throughput performance. The analysis highlights the capability of these frameworks to provide reliable healthcare security with efficient data processing and communication.

Figure 5 shows that the article [23] has better throughput performance, among the proposed blockchain-based healthcare frameworks. The framework emphasizes secure and efficient healthcare data sharing, with a particular emphasis on blockchain, IoT, and decentralized applications, to enhance the efficiency of transactions and communications. Furthermore, the article [33] shows great throughput performance in healthcare applications using the AdaSec-Health framework, which improves scalability and transaction handling capabilities. The higher throughput indicates the systems' capacity to handle healthcare transactions efficiently, enhancing the performance and scalability of healthcare networks.

Figure 6 shows the accuracy of various healthcare security frameworks based on blockchain and IoT technologies with machine learning. The results show that the selected models can be used for prediction and classification of protection and attack in healthcare data with varying performance. SSO-BNNN [20] are found to perform best among the compared approaches which is very important to provide secure and reliable healthcare services. According to the analysis, using smart learning methods along with blockchain can substantially enhance the accuracy of health care security systems.

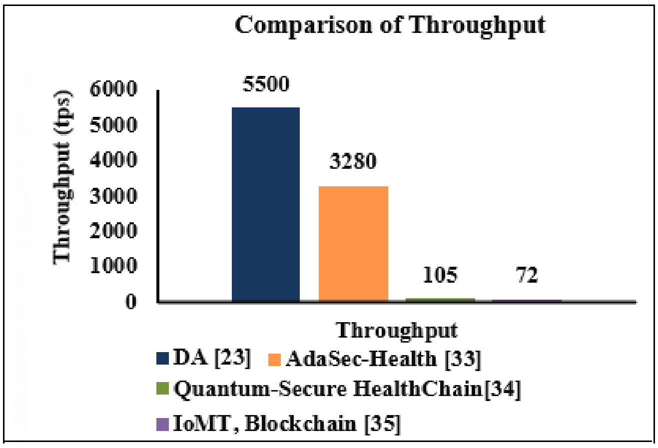

Figure 5: Comparative Evaluation of Throughput for Blockchain-Based Healthcare Frameworks

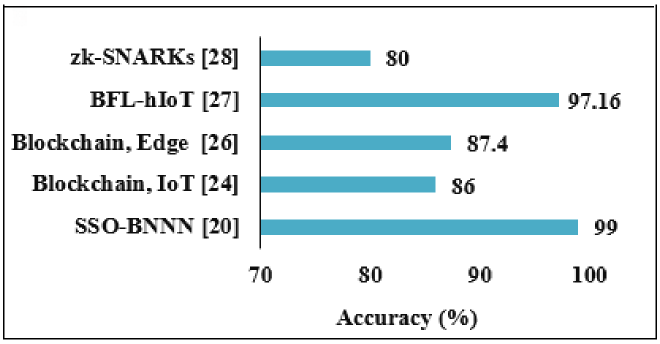

Figure 6: Comparative Evaluation of Accuracy for Blockchain-Based Healthcare Frameworks

5. Conclusion

Healthcare systems are turning to blockchain, IoT, cloud computing, edge computing, federated learning, and quantum-secure technologies to tackle issues of data security, privacy, interoperability, and effective healthcare data management. In this study, different healthcare frameworks with their strengths and weaknesses, datasets and performance measures were identified. While these technologies have the potential to revolutionize data security, real-time monitoring, and the delivery of healthcare services in decentralized settings, there are also several challenges that remain to be addressed, such as scalability, computational requirements, implementation, and the need for broad testing in real-world applications. Future studies should aim at the development of intelligent and adaptive healthcare architectures that combine multiple technologies in order to improve the whole system's security, scalability, interoperability, and performance in next-generation healthcare settings, as no one solution can meet all of the healthcare industry's demands.

References

[1] Z. J. Al-Araji, M. S. AlKhaldee, A. A. Mutlag, Z. A. Abdulkadhim, S. S. S. Ahmad, N. N. Hikmat, & A. H. Ali, “Healthcare security in edge-fog-cloud environment using blockchain: A systematic review. Mesopotamian”, Journal of CyberSecurity, vol. 5, no. 2, pp. 606-635, 2025.

[2] M. Osama, A. A. Ateya, M. S. Syed, M. Hammad, P. Pławiak, A. A. Abd El-Latif, & R. A. Elsayed, “Internet of medical things and healthcare 4.0: Trends, requirements, challenges, and research directions”, Sensors, vol. 23, no. 17, pp. 7435, 2023.

[3] M. M. Pai, R. Ganiga, R. M. Pai, & R. K. Sinha, “Standard electronic health record (EHR) framework for Indian healthcare system”, Health Services and Outcomes Research Methodology, vol. 21, no 3, pp. 339-362, 2021.

[4] B. Pradhan, S. Bhattacharyya, & K. Pal. “IoT-based applications in healthcare devices”, Journal of healthcare engineering, vol. 2021, no. 1, pp. 6632599, 2021.

[5] Z. Yang, Q. Zhou, L. Lei, K. Zheng, & W. Xiang, “An IoT-cloud based wearable ECG monitoring system for smart healthcare”, Journal of medical systems, vol. 40, no. 12, pp. 286, 2016.

[6] V. Mamidala, & A. RS. “Energy-efficient cloud computing solutions for healthcare systems using genetic algorithms”, International Journal of Business Management and Economic Review, vol. 2, no. 5, pp. 71, 2016.

[7] S. Goyal, “Public vs private vs hybrid vs community-cloud computing: a critical review”, International Journal of Computer Network and Information Security, vol. 6, no. 3, pp. 20-29, 2014.

[8] G. Matsumura, S. Honda, T. Kikuchi, Y. Mizuno, H. Hara, Y. Kondo, & K. Takei, “Real-time personal healthcare data analysis using edge computing for multimodal wearable sensors”. Device, vol. 3, no. 2, 2025.

[9] E. P. Adeghe, C. A. Okolo, & O. T. Ojeyinka, “Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes”, Open Access Research Journal of Science and Technology, vol. 10, no. 2, pp. 013-020, 2024.

[10] A. Thakur, “A comprehensive study of the trends and analysis of distributed ledger technology and blockchain technology in the healthcare industry”. Frontiers in Blockchain, vol. 5, pp. 844834, 2022.

[11] A. A. Al-awamy, N. Al-shaibany, A. Sikora, & D. Welte, “Hybrid consensus mechanisms in blockchain: a comprehensive review”, International Journal of Intelligent Systems, vol. 2025, no. 1, pp. 5821997, 2025

[12] J. Jayabalan, & N. Jeyanthi, “Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy”. Journal of Parallel and distributed computing, vol. 164, pp. 152-167, 2022.

[13] B. Dammak, M. Turki, S. Cheikhrouhou, M. Baklouti, R. Mars, & A. Dhahbi, “Lorachaincare: An iot architecture integrating blockchain and lora network for personal health care data monitoring”. Sensors, vol. 22, no. 4, pp. 1497, 2022.

[14] B. Jaishankar, S. Vishwakarma, P. Mohan, A. K. S. Pundir, I. Patel, & N. Arulkumar, “Blockchain for securing healthcare data using squirrel search optimization algorithm”, Intelligent Automation & Soft Computing, vol. 32, no. 3, pp. 1815-1829, 2022.

[15] A. Ali, M. A. Almaiah, F. Hajjej, M. F. Pasha, O. H. Fang, R. Khan, & M. Zakarya, “An industrial IoT-based blockchain-enabled secure searchable encryption approach for healthcare systems using neural network”, Sensors, vol. 22, no. 2, pp. 572, 2022.

[16] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, & D. Kumar, “Simulation of the lightweight blockchain technique based on privacy and security for healthcare data for the cloud system”. International Journal of E-Health and Medical Communications (IJEHMC), vol. 13, no. 4, pp. 1-15, 2022.

[17] K. Azbeg, O. Ouchetto, & S. J. Andaloussi, “BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security”, Egyptian informatics journal, vol. 23, no. 2, pp.329-343, 2022.

[18] L. Lodha, V. S. Baghela, J. Bhuvana, & R. Bhatt, “A blockchain-based secured system using the Internet of Medical Things (IOMT) network for e-healthcare monitoring. Measurement”, sensors, 30, 100904, 2023.

[19] D. Rani, R. Kumar, & N. Chauhan, “A secure framework for IoT-based healthcare using blockchain and IPFS”, Security and Privacy, vol. 7, no. 2, pp. e348, 2023.

[20] S. Chaturvedi, “IoT-based secure healthcare framework using blockchain technology with a novel simplified swarm-optimized bayesian normalized neural networks”, International Journal of Data Informatics and Intelligent Computing, vol. 2, no. 2, pp. 63-71, 2023.

[21] S. Meisami, S. Meisami, M. Yousefi, & M. R. Aref, “Combining blockchain and IOT for decentralized healthcare data management”, arXiv preprint arXiv:2304.00127, 2023.

[22] A. Ali, H. Ali, A. Saeed, A. Ahmed Khan, T. T. Tin, M. Assam, & H. G. Mohamed, “Blockchain-powered healthcare systems: enhancing scalability and security

with hybrid deep learning", Sensors, vol. 23, no. 18, 7740, 2023.

[23] P. Sharma, S. Namasudra, N. Chilamkurti, B. G. Kim, & R. Gonzalez Crespo, "Blockchain-based privacy preservation for IoT-enabled healthcare system", ACM Transactions on Sensor Networks, vol. 19, no. 3, pp. 1-17, 2023.

[24] A. I. Taloba, A. Elhadad, A. Rayan, R. M. Abd El-Aziz, M. Salem, A. A. Alzahrani, & C. Park, "A blockchain-based hybrid platform for multimedia data processing in IoT-Healthcare". Alexandria Engineering Journal, vol. 65, pp. 263-274, 2023.

[25] T. Bhaskar, M. N. Narsaiah, & M. Ravikanth, "Central Medical Centre Healthcare Data Security with Lightweight Blockchain Model in IoT Sensor Environment", Journal of Sensors, IoT & Health Sciences, vol. 1, no. 01, pp. 15-26, 2023.

[26] R. Kothari, "Integration of blockchain and edge computing in healthcare: accountability and collaboration", Transdisciplinary Journal of Engineering & Science, no. 14, pp. 14, 2023.

[27] G. Ganapathy, S. J. Anand, M. Jayaprakash, S. Lakshmi, V. B. Priya, & S. Pandi, "A blockchain based federated deep learning model for secured data transmission in healthcare IoT networks". Measurement: Sensors, no. 33, pp. 101176, 2024.

[28] S. B. Babu, & K. R. Jothi, "A secure framework for privacy-preserving analytics in healthcare records using zero-knowledge proofs and blockchain in multi-tenant cloud environments", IEEE Access, no. 13, pp. 8439-8455, 2024.

[29] G. Verma, "Blockchain-based privacy preservation framework for healthcare data in cloud environment", Journal of Experimental & Theoretical Artificial Intelligence, vol. 36, no. 1, pp. 147-160, 2024.

[30] M. Anjum, N. Kraiem, H. Min, A. K. Dutta, Y. L. Daradkeh, & S. Shahab, "Opportunistic access control scheme for enhancing IoT-enabled healthcare security using blockchain and machine learning". Scientific Reports, vol. 15, no. 1, pp. 7589, 2025.

[31] S. R. Mallick, S. Sobhanayak, & R. K. Lenkar, "Secure and trusted data sharing in smart healthcare using blockchain and IoT integration". Discover Internet of Things, vol. 5, no. 1, pp. 90, 2025.

[32] P. H. Regalado, & T. Han, "MediVerse: A secure and scalable IoT-MR framework for real-time health and performance monitoring". IEEE Access, 2025.

[33] J. Mythili, & R. Gopalakrishnan, "Improving data transmission through optimizing blockchain sharding in cloud IoT based healthcare applications". Egyptian Informatics Journal, no. 30, pp.100661, 2025.

[34] R. Bose, S. Mondal, S. Sutradhar, S. Das, M. Faheem, S. Roy, & A. Ahmad Khan, "Enhancing Cloud-Based Healthcare Security With Quantum-Secure HealthChain: A Quantum Computing and Blockchain Integrated Framework". Health Science Reports, vol. 9, no. 5, pp. e72367, 2026.

[35] A. S. M. Ali, S. Ali, K. Ziaullah, M. I. Joo, & H. C. Kim, "Iomt and blockchain synergy: a novel approach to health data validation and storage". IEEE Access, 2025.

[36] R. Chengoden, N. Victor, T. Huynh-The, G. Yenduri, R. H. Jhaveri, M. Alazab, & T. R. Gadekallu, "Metaverse for healthcare: a survey on potential applications, challenges and future directions". IEEE access, vol. 11, pp. 12765-12795, 2025.