International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 30, No. 3, March, 2025, pp. 629-636
Journal homepage: http://iieta.org/journals/isi

A Novel Storage Decision Framework for Managing Healthcare Big Data on Blockchain Platform in IoT Integrated Telemedicine Systems

Babita Yadav[1*], Sachin Gupta[2]

[1] Department of CSE, SOET, MVN University, Palwal 121105, India
[2] Department of CSE, Maharaja Agrasen Institute of Technology, Delhi 110086, India

Corresponding Author Email: 19cs9001@mvn.edu.in

https://doi.org/10.18280/isi.300307

Received: 13 July 2024
Revised: 21 November 2024
Accepted: 9 December 2024
Available online: 31 March 2025

Keywords:
healthcare big data, blockchain, Internet of Things (IoT), telemedicine systems

ABSTRACT

Healthcare is one of the major technical challenges of the 21st century, with the rapid adoption of technologies like the Internet of Things (IoT) to support remote patient access to telemedicine. This domain is highly data-intensive and involves handling large amounts of sensitive personal information, making trust a crucial issue among all involved parties. Blockchain technology, with its decentralized trust management model, offers the potential to transform healthcare data management by removing the need for a trusted third party. However, applying blockchain to telemedicine introduces specific data management challenges. The objectives of this research are to determine the diverse storage needs of healthcare data within a blockchain-based system and to develop a decision framework for managing this data. The study begins with an extensive review of existing blockchain storage solutions across various domains, with a focus on healthcare. This background research underscores the importance of making balanced storage decisions that consider the high costs of on-chain methods and the lower security of off-chain methods to optimize blockchain storage expenses. The methodology involves creating a formal framework that guides storage management decisions for telemedicine data generated through IoT devices. This framework incorporates both on-chain and off-chain storage methods, taking into account factors such as data sensitivity, access frequency, and cost efficiency. Scenario-based validation of the framework is performed to evaluate its practicality and effectiveness in real-world settings. The anticipated results include a robust and adaptable decision framework that simplifies storage management for developers and practitioners in telemedicine and healthcare data management. This framework aims to enhance data security, reduce storage costs, and improve the overall efficiency of blockchain-based telemedicine systems.

1. INTRODUCTION

Healthcare challenges in the 21st century have earned a prominent position among the seventeen sustainable development goals (SDGs) adopted by the United Nations (UN). The vast amount of healthcare data, encompassing patient medical histories, diagnostic reports, prescription records, and hospital records, exemplifies the concept of big data with its volume, variety, and velocity. The COVID-19 pandemic exposed significant weaknesses in global healthcare infrastructure and underscored the urgent need for telemedicine solutions [1, 2]. This period also presented an opportunity for researchers to develop IoT-integrated telemedicine solutions for continuous, non-invasive patient monitoring with remote doctor access. Despite these advances, the integration of wearable sensors and improvements in communication networks and edge processing have introduced new concerns regarding data privacy and security. The potential misuse of personal and sensitive healthcare data and massive security breaches remain significant obstacles to the adoption of IoT-integrated telemedicine systems. Effective management and protection of electronic healthcare records (EHR) and understanding the sensitive nature of this data [3] are critical for developing any Internet of Medical Things (IoMT) [4] framework or solution.

Blockchain technology provides an immutable way to store transactions in a distributed ledger. This immutability is crucial for maintaining trust in many applications. However, the "Right to be Forgotten," as offered by various laws, presents a challenge. With rising awareness of individual data rights and stricter data privacy laws, such as the General Data Protection Regulation (GDPR) in the European Union, the universal use of blockchain becomes problematic. This necessitates customized implementations rather than standard ones.

While several blockchain storage strategies exist, there is no comprehensive framework for blockchain-based data management [5] in IoT-integrated telemedicine solutions [6]. This paper aims to propose a decision framework for blockchain storage tailored to healthcare's diverse data needs.

This paper offers the following contributions:

1. Extensive Literature Review:

Provides a thorough survey of current research to comprehend the range of blockchain solutions for healthcare and the methods for storing medical health records [7].

2. Diverse Storage Needs Identification:

Identifies the varying storage needs of different types of healthcare data in blockchain-based applications.

3. Framework Proposal:

Introduces a formal framework for managing healthcare big data on blockchain within IoT-integrated telemedicine systems, aiming to deliver efficient and cost-effective storage solutions [8].

2. LITERATURE REVIEW

The rapid advancement of IoT-integrated telemedicine systems has highlighted the significant challenge of managing healthcare big data. Researchers have extensively analyzed the application of big data characteristics—volume, variety, and velocity—to patient medical histories, diagnostic reports, and other healthcare records, underscoring the complexities and opportunities this data presents. The COVID-19 pandemic exposed critical weaknesses in global healthcare infrastructures, which in turn emphasized the urgent need for robust telemedicine solutions. In response, researchers have developed IoT-integrated telemedicine systems using wearable sensors and advanced communication networks to enable continuous, non-invasive patient monitoring. However, these innovations have also raised significant concerns about data privacy and security [9, 10].

Blockchain technology has emerged as a promising solution for managing and securing healthcare data due to its decentralized nature and ability to establish trust in multi-party environments. Studies have demonstrated its potential in managing electronic healthcare records (EHR) and other sensitive data within healthcare systems. Beyond healthcare, blockchain applications have been explored in various sectors such as supply chain management, food management, digital marketing, reputation management, and smart cities, each revealing unique challenges and solutions [11, 12].

Despite these advancements, integrating blockchain with healthcare big data in IoT-integrated telemedicine systems presents unresolved challenges. These include ensuring data privacy, preventing security breaches, and developing a versatile storage decision framework that can handle the diverse nature of healthcare data, from streaming information to large diagnostic reports [13, 14]. Addressing these issues is crucial for the effective and secure deployment of IoT-integrated telemedicine solutions.

In response to these challenges, this research proposes a novel decision framework that leverages blockchain technology to manage and secure healthcare big data within IoT-integrated telemedicine systems. This framework aims to provide tailored solutions for different types of healthcare data, enhancing data privacy and security [15-17] while accommodating the specific needs of telemedicine [18-20].

Sonnis et al. [21] discuss creating a secure and interoperable healthcare system using blockchain e-healthcare solutions with wireless body area networks to enhance interoperability. They compare power consumption and usage in their study.

A decentralized storage solution is proposed in the study [22] to use unused personal hard disk space globally via blockchain. The system issues a data integrity certificate to users, allowing storage only after verification through lightning network technology. All related proofs and payment information are stored on the blockchain, ensuring security and credibility.

Data masking technology is explored, and insights are provided into using the Inter Planetary File System (IPFS) to build a secure and cost-effective data-sharing model [23]. The cost of storing IoT data on the blockchain using smart contracts is discussed in the study [24], and it also examines storing numeric data from temperature sensors on the blockchain using a single variable.

The study compares storing data in an array versus storing data from all sensors in one variable. The authors conclude that while storing data on the blockchain is expensive, it provides reliable data integrity and transparency. Two critical challenges in health data sharing are addressed: deploying and installing blockchain software across different hospitals, and protecting sensitive health information. A blockchain-based solution using a distributed microservice architecture is proposed. This approach encapsulates core functions into isolated services that can be independently scaled to meet the needs of different hospitals [25]. The workflow process of blockchain-based healthcare on a global scale is also explored. Using blockchain to prevent healthcare data manipulation while maintaining data transparency is advocated [26].

Blockchain scalability issues are discussed, and off-chaining is presented as a solution. Various off-chaining models are categorized, and it is concluded that off-chain computations are more powerful and scalable than other approaches [27]. A detailed study of IPFS-based secure healthcare storage solutions is also provided. Traditional local storage methods and cloud-based storage are compared, highlighting their respective issues. Various existing solutions are discussed, and improvements for medical record storage are suggested [28]. Additionally, the explosion of public and social sector data is reviewed, emphasizing the big data challenges in healthcare data storage [29].

An integrated project focusing on telemetric health using IoT sensors to monitor bedridden patients is discussed in the studies [30, 31]. The authors propose a virtual nurse that observes patient vitals and generates alerts for any anomalies to the attending doctor. They emphasize that IoMT-based observations, such as ECG and glucose levels, can be monitored and reported in real time.

Additionally, a study of various blockchain solutions available in the literature was conducted to inform the framework's choice of blockchain solutions specifically for healthcare, based on the data characteristics and the commissioning organization. Table 1 presents the key distinguishing features of the most commonly used blockchain platforms.

The table can be referred to by the blockchain application developers to choose a platform based on the priority ranking of blockchain features of the specific use case. For instance, it is apparent from the above table that healthcare applications are better adapted to be developed on Ethereum and Hyperledger [32] platforms.

The choice of consensus algorithm is also significant when making the selection of blockchain platforms for application development. There are over a hundred consensus algorithms available in the literature, of which around twenty are exceptionally significant. Table 2 is a filtered list to summarize the most commonly used consensus algorithms from among all consensus algorithms.

It is worthwhile to mention here that there are several off-chain storage methods available for different blockchains.

Each method has its own cost, pros and cons which the framework does not address. Without the loss of generality, we have used the Interplanetary File System (IPFS) for the off-chain storage cost calculations in the framework validation. The developer may choose any off-chain storage method based on total present and projected storage requirements of the application data, where the storage cost will adjust according to the choice of platform [33]. To make the choice easier for the developer, a comparative analysis of some common off-chain storage [34] methods is presented in Table 3 for reference.

Table 1. The key distinguishing features of the most commonly used blockchain platforms

Aspect	Off-Chain Storage	On-Chain Storage
Cost Efficiency	Significantly lower costs per GB and transaction fees	Higher costs can be prohibitive for extensive data
Scalability	Facilitates scalability; easier to scale operations	Costs can limit scalability; need to manage data volume
Performance	Better performance for large-scale data storage	Potential impact on performance due to higher costs
Security and Integrity	Generally secure; may require additional measures	Higher security and data integrity due to blockchain
Use Cases	Ideal for large volumes of less sensitive data	Best for critical data needing security and immutability
Hybrid Solutions	Common approach to balance cost, performance, security	Often used for critical and less critical data

Table 2. Study of various algorithms from the literature

Type	Lottery Based Consensus Algorithm [35, 36]						Voting Based Algorithm [35]		
Algorithm	Proof of Stake (PoS) [37-39]	Delegated Proof of Stake (DPoS) [40-43]	Leased Proof of Stake (LPoS) [43]	Proof of Work (PoW) [43]	Proof of Authority (PoA) [44, 45]	Proof of Importance (PoI) [35]	Practical Byzantine Fault Tolerance (PBFT)	Paxos [43]	Raft [35]
Blockchain type	Permission-less and permission-ed	Permission-less and permission-ed	Permission-less and permission-ed	Permission-less	Permission-less and permissioned	Consortium	Permissioned	Permission-ed	Permission-ed
Miners Selection	Based on stake	Based on stake	Based on stake	Hash puzzle	Hash puzzle	High priority	Mathematical operation	Number will be proposed	Random timings
Decentraliza-tion followed [45]	Strong	Strong	Strong	Strong [24]	Strong	Strong	Weak	Weak	Weak
Transaction fees	For all miners	For all miners	NA	For all miners	For miners and stakeholders	For all transaction partners	No	No	No
Reward [48]	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
Trust model	Un-Trusted	NA	NA	Un-Trusted	NA	NA	Semi-Trusted	Semi-Trusted	Semi-Trusted
Speed of block creation	High	High	Not Found	Low	High	High	High	High	NA
51% attack [45]	No	No	No	Yes	No	No	No	No	No
Double spending [44]	No	No	No	yes	No	No	No	No	No
Pros	Higher speed, less energy consump-tion [45]	More decentrali-zed and better distribution of rewards [45]	Earn with fewer tokens also, less energy consump-tion [46, 47]	Highly scalable so used in a variety of applications [48]	Highly scalable, guaranteed higher throughput	Reduces hoarding of coins	Less time as multiple confirmations by each node do not require [45]	Optimized for "ease of implementa tion"	Easy to understand and implement as compared to Paxos [45]
Cons	Less decentraliz-ed, less scalability	Cartel formation [49], 51% attack	Possible cartel formation	Energy intensive, notorious 51% attack [50]	The identities of validators are public	Rich get richer syndrome	Sybil attacks [48]	Overhead of request rejection, live lock	Real-life applicability low as no byzantine fault assumption

Table 3. Comparative analysis of off-chain storage methods

Criteria	Filecoin [47]	Sia [48]	Swarm [49]	Storj [51]
Data Replication	The replication factor is configurable by the user	Encoded fragments stored across a network	Encoded fragments stored across the neighborhood	Encoded fragments stored across a network
Availability of data over	Proof-of-Spacetime (PoSt), Pledged collateral recurring payments	Hashed fragments with proof of storage	Recurring payments, Race Raffle, Proof of ownership, Race Raffle	Recurring payments, data fragments audits, revenue withholding

Proof of Data Stored	Proof of Replication	Hashed fragments Proof of Storage	Merkle tree root Hash	Data Fragments Audit
Tracking Storage	Blockchain and node gossip	Blockchain and node gossip	Data Chunks	Satellite Node
Storage Price	$1.33/TB/month (Dynamic according to market price)	$2/TB/month	Not Defined	$4/TB/month
data transmission	Retrieval miners	Users pay as per bandwidth	Using protocol	Payment as per bandwidth usage
Proof of data stored	Proof-of-Replication (PoRep)	Proof of Storage (PoS) of hashed fragments with Merkle Tree	Merkle tree root hash	Audits of Data Fragments

2.1 Limitations of existing literature

Blockchain technology in IoT-integrated telemedicine systems faces several challenges that limit its current effectiveness. Scalability is a significant issue, as blockchains struggle to handle the large volume of data generated by IoT devices, with high transaction costs and limited throughput. Energy-intensive consensus mechanisms, like Proof-of-Work, further exacerbate this problem, making blockchain less sustainable for healthcare applications. Direct storage of healthcare data on the blockchain is impractical due to high costs, and while off-chain solutions like IPFS offer alternatives, they introduce complexities in data retrieval and redundancy management. Latency in blockchain transactions also poses a challenge, especially for real-time telemedicine systems that require immediate responses. The lack of universal standards complicates the integration of blockchain with diverse IoT devices and healthcare systems. Privacy concerns persist, as blockchain's decentralized structure does not inherently safeguard sensitive data, requiring advanced cryptographic techniques that add complexity. Moreover, regulatory frameworks like GDPR and HIPAA may conflict with blockchain's decentralized approach, particularly in areas like data ownership and the "right to be forgotten." Power consumption issues in IoT networks, particularly in wireless body area networks, reduce reliability for long-term use. Finally, decentralized storage solutions face risks of data unavailability, while storing even small amounts of IoT data on the blockchain remains costly, limiting scalability for healthcare systems.

3. METHODOLOGY

3.1 Decision framework for healthcare big data on blockchain

Based on the gaps identified from the literature survey, and security challenges observed by the researchers working with storage of different types of healthcare data on blockchain, the following key criterion for storage decision making were identified. The complete framework with all the criteria consolidated in a single flowchart has been presented visually in Figure 1.

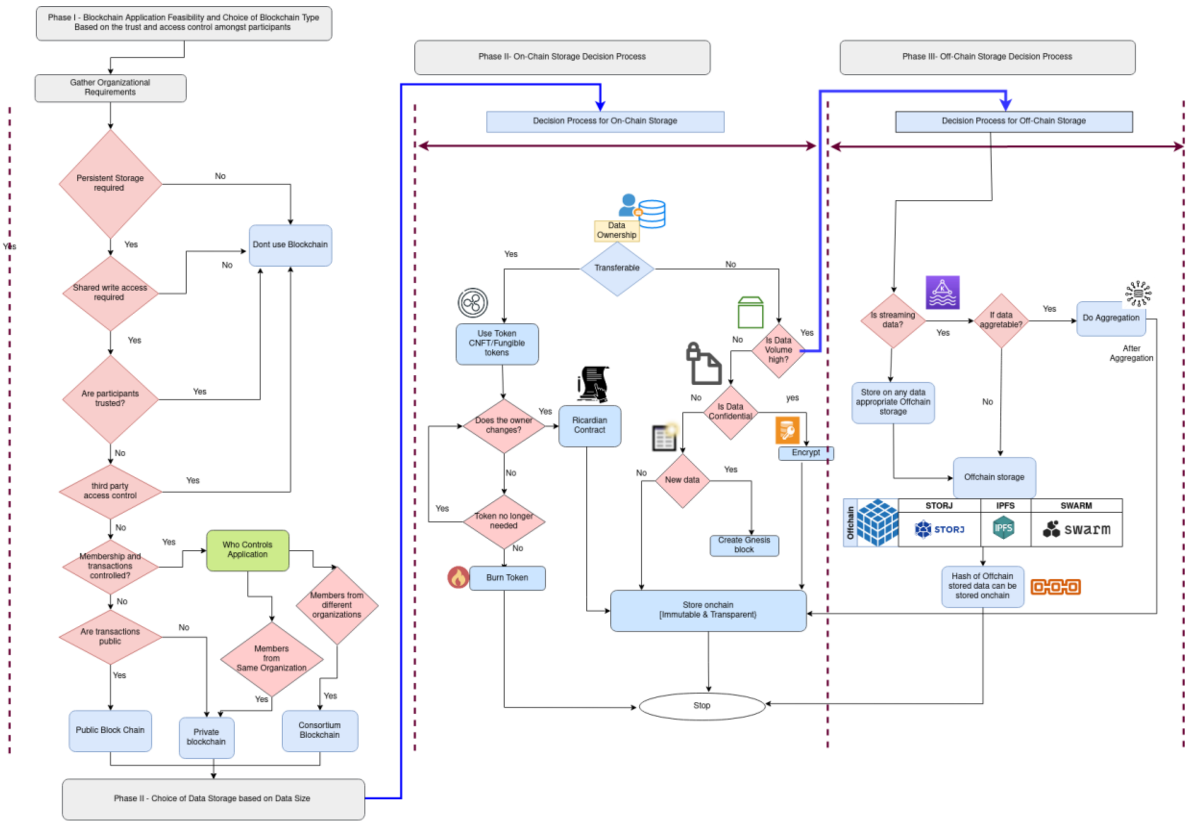

Figure 1. Decision framework for managing healthcare big data on blockchain applications

The decision-making criteria in the framework can be modularized into three distinct phases based on the identified criteria. Phase I covers blockchain use case feasibility and subsequent choice of the type of blockchain based on the use case being discussed. The detailed break-up of the criteria is presented below:

I. Criteria for blockchain use case based on application characteristics

• Requirement of persistent storage (If no, blockchain use is not recommended)

• Write access is shared (If no, blockchain use is not recommended)

• Presence of untrusted parties (If no, blockchain use is not recommended)

• Allowing third party access (If no, blockchain use is not recommended)

II. Criteria for blockchain type based on membership characteristics

• Membership is not controlled (Use public blockchain platform)

• Membership is controlled and members are from same organization (Use private blockchain platform)

• Membership is controlled and members are from multiple organizations (Use consortium blockchain platform)

Phase II and Phase III cover the on-chain vs off chain storage decision making process based on the following criteria:

III. Criteria for blockchain type based on transaction characteristics

• Transactions are public (Use public blockchain platform)

•Transactions are not public (Use private blockchain platform)

IV. Criteria for storage decision based on data characteristics

• Data ownership

• Does the owner of the Data change?

• Data volume

• Data sensitivity and confidentiality

• Data governance by privacy laws

• Data aggregation possibility

V. Criteria for blockchain type based on transaction characteristics

• Transactions are public (Use public blockchain platform)

• Transactions are not public (Use private blockchain platform)

Criteria for storage decision based on data characteristics

• Data ownership

• Does the owner of data change?

• Data volume

• Data sensitivity and confidentiality

• Data governance by privacy laws

• Data aggregation possibility

3.2 Data collection

On-Chain Storage:

Cost per unit of storage: Typically measured in gas costs per byte. This varies based on blockchain platform (e.g., Ethereum, Binance Smart Chain).

Transaction fees: Cost per transaction to store data on-chain.

Other costs: Include any additional costs like contract deployment fees or storage maintenance fees if applicable.

Off-Chain Storage:

Cost per unit of storage: Monthly or annual subscription costs or per GB costs.

Transaction fees: Costs associated with uploading, downloading, or accessing data.

Other costs: Any maintenance fees, retrieval fees, or other hidden costs.

Hypothetical Data:

Define a hypothetical dataset with different sizes (e.g., 1GB, 10GB, 100GB).

Estimate the costs for storing this data both on-chain and off-chain.

The framework should include various medical data collection methods, such as data from wearable devices, imaging systems, and electronic health records, to ensure a broad and comprehensive approach to healthcare data management. Additionally, its credibility can be enhanced by validating the framework with large, real-world datasets that reflect different healthcare scenarios, demonstrating its practicality and ability to scale effectively in real-world applications.

Analysis and visualization

A comparison of on-chain and off-chain storage costs for managing healthcare big data on a blockchain platform in IoT-integrated telemedicine systems is shown in Figure 2.

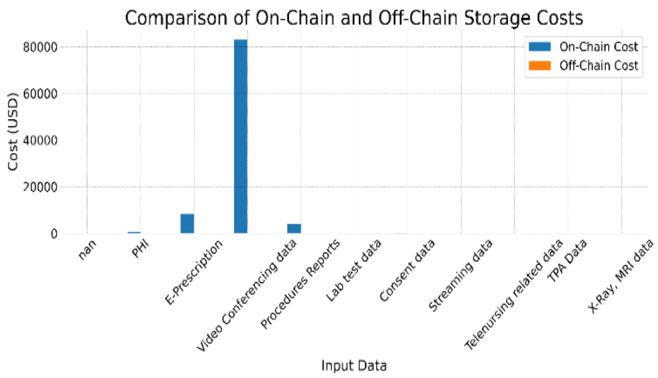

Figure 2. Comparison of on-chain and off-chain data storage costs

3.3 Practical implications and challenges

The cost differences between on-chain and off-chain storage solutions have significant implications for businesses using blockchain for storage in several key areas. table summarizes the implications of using off-chain versus on-chain storage solutions in blockchain applications. It highlights the key differences in cost efficiency, scalability, performance, security, and suitable use cases, as well as the prevalence of hybrid solutions to optimize these factors.

3.4 Adapting blockchain platforms to support future medical technologies

To ensure adaptability to future medical data types and emerging technologies, the framework can be designed with a modular structure, allowing for the seamless addition of new components or functionalities as needed. Integrating machine learning models can enable dynamic analysis and classification of data, ensuring efficient storage and management of novel medical information. The use of interoperable standards and APIs will facilitate smooth integration with evolving telemedicine technologies and IoT devices. A hybrid storage model that combines blockchain with cloud or edge computing can provide the scalability needed to handle diverse and expanding datasets. Lastly, employing advanced cryptographic techniques, including those resistant to future threats like quantum computing, will enhance the framework's resilience and security over time.

3.5 Cost-benefit analysis

The graph above illustrates the cost-benefit analysis of implementing a blockchain-based framework in IoT-integrated telemedicine systems. The red bars show the various initial costs, such as setup, IoT devices, storage, and compliance with regulatory standards. The green bars represent the potential benefits, including enhanced data security, reduced long-term data management expenses, improved healthcare outcomes, scalability, and regulatory compliance. While the upfront costs are considerable, the graph highlights that the long-term advantages, particularly in security and healthcare efficiency, provide significant value over time as shown in Figure 3.

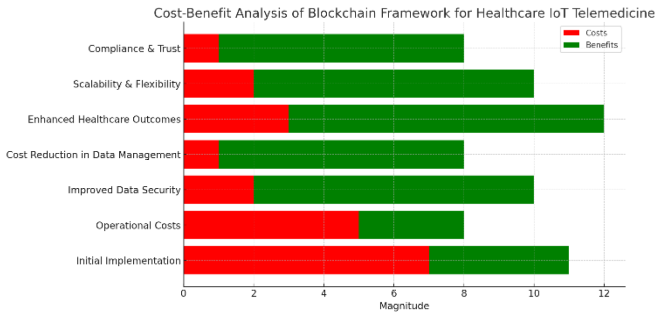

Figure 3. Cost benefit analysis

4. RESULTS AND DISCUSSION

In real-world deployment, several challenges may arise, particularly with the technical aspects of integrating blockchain into healthcare systems. Issues such as the scalability of blockchain, compatibility with existing infrastructure, and the high energy demands of consensus mechanisms can impede smooth implementation. To resolve these, using a hybrid blockchain structure, incorporating edge computing for real-time data processing, and selecting more energy-efficient consensus algorithms could help mitigate these technical hurdles.

Organizational resistance is another potential barrier, often due to concerns about privacy, the complexity of adopting new technology, and disrupting established workflows. To address this, providing thorough training for healthcare providers, demonstrating the security advantages of blockchain, and introducing the system gradually can ease the transition. Gaining early support from key stakeholders and showcasing.

5. CONCLUSIONS AND FUTURE WORK

Telemedicine and healthcare have the widest data variety amongst most of the present day applications, and is also considered the most trust deficit due to the sensitive nature of the data. Blockchain solutions can be considered for data storage in such applications, but no single solution can possibly fit the diverse needs of healthcare data, and thus a storage decision framework has been proposed in this paper, with due validations.

An implementation of the framework is due yet, and should be coincided with measurement of performance characteristics including queries, runtime and real time use cases of data storage and retrieval. New system improves patient care outcomes will also help in reducing resistance and fostering acceptance.

In emergency medical situations, the need for rapid access to patient data is essential, but it must be managed alongside the need for security to protect sensitive information. To address this, the framework could introduce a special protocol for emergency access, allowing healthcare professionals to access critical data quickly while ensuring that security is not compromised. This can include time-sensitive access permissions, ensuring that emergency responders are granted temporary access to necessary medical information. Role-based access controls and multi-factor authentication could further ensure that only authorized individuals are granted access. Additionally, it is important to maintain encryption during emergency access to preserve data confidentiality, with automatic logging for auditing and compliance purposes.

The framework could be enhanced by implementing fine-grained access control using smart contracts, which would allow the definition of specific rules for each participant. These smart contracts would set clear permissions on who can view, modify, or share data, based on their roles or authority level. By embedding these access control mechanisms directly within the blockchain, it ensures secure, transparent, and efficient management of sensitive medical information while maintaining strict data privacy.

REFERENCES

[1] Emokpae, L.E., Emokpae, R.N., Lalouani, W., Younis, M. (2021). Smart multimodal telehealth-IoT system for COVID-19 patients. IEEE Pervasive Computing, 20(2): 73-80. https://doi.org/10.1109/MPRV.2021.3068183

[2] Islam, S.R., Kwak, D., Kabir, M.H., Hossain, M., Kwak, K.S. (2015). The internet of things for health care: A comprehensive survey. IEEE Access, 3: 678-708. https://doi.org/10.1109/ACCESS.2015.2437951

[3] Seh, A.H., Zarour, M., Alenezi, M., Sarkar, A.K., Agrawal, A., Kumar, R., Ahmad Khan, R. (2020). Healthcare data breaches: insights and implications. In Healthcare, 8(2): 133. https://doi.org/10.3390/healthcare8020133

[4] Pandey, R., Gupta, A., Pandey, A. (2022). The internet of medical things (IoMT) and telemedicine frameworks and applications. IGI Global.

[5] Gupta, S., Yadav, B., Gupta, B. (2022). Security of IoT-based e-healthcare applications using blockchain. In Advances in Blockchain Technology for Cyber Physical Systems, pp. 79-107. https://doi.org/10.1007/978-3-030-93646-4_4

[6] Gupta, S., Gupta, B. (2020). Securing honey supply chain through blockchain: An implementation view. In IoT Security Paradigms and Applications, pp. 321-335. https://doi.org/10.1201/9781003054115-15

[7] Yadav, B., Gupta, S. (2022). Healthcare transformation traditional to telemedicine: A portrayal. In Emerging Technologies for Computing, Communication and Smart Cities: Proceedings of ETCCS 2021, pp. 3-14.

https://doi.org/10.1007/978-981-19-0284-0_1
[8] Gupta, S., Yadav, B. (2022). Economics of immutability preserving streaming healthcare data storage using aggregation in blockchain technology. In Smart Trends in Computing and Communications: Proceedings of SmartCom 2022, pp. 611-621. https://doi.org/10.1007/978-981-16-9967-2_57
[9] Aboamer, M.A., Sikkandar, M.Y., Gupta, S., Vives, L., Joshi, K., Omarov, B., Singh, S.K. (2022). An investigation in analyzing the food quality well-being for lung cancer using blockchain through CNN. Journal of Food Quality, 2022(1): 5845870. https://doi.org/10.1155/2022/5845870
[10] Gupta, S., Garg, N., Sinha, D., Yadav, B., Gupta, B., Miah, S. (2022). The emerging role of implementing machine learning in food recommendation for chronic kidney diseases using correlation analysis. Journal of Food Quality, 2022(1): 7176261. https://doi.org/10.1155/2022/7176261
[11] Saini, V.K., Gupta, S., Gupta, B. (2022). Data security in collaborative business intelligence for sustainable super smart society. In Decision Analytics for Sustainable Development in Smart Society 5.0: Issues, Challenges and Opportunities, pp. 113-130. https://doi.org/10.1007/978-981-19-1689-2_8
[12] Wang, J., Han, K., Alexandridis, A., Chen, Z., Zilic, Z., Pang, Y., Jeon, G., Piccialli, F. (2020). A blockchain-based eHealthcare system interoperating with WBANs. Future Generation Computer Systems, 110: 675-685. https://doi.org/10.1016/j.future.2019.09.049
[13] Zhu, Y., Lv, C., Zeng, Z., Wang, J., Pei, B. (2019). Blockchain-based decentralized storage scheme. In Journal of Physics: Conference Series, 1237(4): 042008. https://doi.org/10.1088/1742-6596/1237/4/042008
[14] Wu, S., Du, J. (2019). Electronic medical record security sharing model based on blockchain. In Proceedings of the 3rd International Conference on Cryptography, Security and Privacy, pp. 13-17. https://doi.org/10.1145/3309074.3309079
[15] Kurt Peker, Y., Rodriguez, X., Ericsson, J., Lee, S.J., Perez, A.J. (2020). A cost analysis of internet of things sensor data storage on blockchain via smart contracts. Electronics, 9(2): 244. https://doi.org/10.3390/electronics9020244
[16] Cyran, M.A. (2018). Blockchain as a foundation for sharing healthcare data. Blockchain in Healthcare Today, 1. https://doi.org/10.30953/bhty.v1.13
[17] Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S. (2021). Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, 2: 130-139. https://doi.org/10.1016/j.ijin.2021.09.005
[18] Eberhardt, J., Heiss, J. (2018). Off-chaining models and approaches to off-chain computations. In Proceedings of the 2nd Workshop on Scalable and Resilient Infrastructures for Distributed Ledgers, pp. 7-12. https://doi.org/10.1145/3284764.3284766
[19] Kumar, S., Bharti, A.K., Amin, R. (2021). Decentralized secure storage of medical records using Blockchain and IPFS: A comparative analysis with future directions. Security and Privacy, 4(5): e162. https://doi.org/10.1002/spy2.162
[20] Padgavankar, M.H., Gupta, S.R. (2014). Big data storage and challenges. International Journal of Computer Science and Information Technologies, 5(2): 2218-2223.
[21] Sonnis, O., Sunka, A., Singh, R., Agarkar, T. (2017). IoT based telemedicine system. In 2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI), pp. 2840-2842. https://doi.org/10.1109/ICPCSI.2017.8392239
[22] Babu, B.S., Srikanth, K., Ramanjaneyulu, T., Narayana, I.L. (2016). IoT for healthcare. International Journal of Science and Research, 5(2): 322-326. https://doi.org/10.1007/978-3-319-97016-5_2
[23] Mazzoni, M., Corradi, A., Di Nicola, V. (2022). Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study. Blockchain: Research and applications, 3(1): 100026. https://doi.org/10.1016/j.bcra.2021.100026
[24] Baliga, A., Subhod, I., Kamat, P., Chatterjee, S. (2018). Performance evaluation of the quorum blockchain platform. arXiv preprint arXiv:1809.03421. http://arxiv.org/abs/1809.03421
[25] Carrara, G.R., Burle, L.M., Medeiros, D.S., de Albuquerque, C.V.N., Mattos, D.M. (2020). Consistency, availability, and partition tolerance in blockchain: a survey on the consensus mechanism over peer-to-peer networking. Annals of Telecommunications, 75: 163-174. https://doi.org/10.1007/s12243-020-00751-w
[26] Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. Peer-to-peer Networking and Applications, 14: 2901-2925. https://doi.org/10.1007/s12083-021-01127-0
[27] Buterin, V. (2018). Vyper documentation. Website. https://media.readthedocs.org/pdf/viper/latest/viper.pdf.
[28] Parizi, R.M., Amritraj, Dehghantanha, A. (2018). Smart contract programming languages on blockchains: An empirical evaluation of usability and security. In Blockchain–ICBC 2018: First International Conference, Held as Part of the Services Conference Federation, SCF 2018, Seattle, WA, USA, June 25-30, 2018, Proceedings 1, pp. 75-91. https://doi.org/10.1007/978-3-319-94478-4_6
[29] Siris, V.A., Nikander, P., Voulgaris, S., Fotiou, N., Lagutin, D., Polyzos, G.C. (2019). Interledger approaches. IEEE Access, 7: 89948-89966. https://doi.org/10.1109/ACCESS.2019.2926880
[30] Nizamuddin, N., Salah, K., Azad, M.A., Arshad, J., Rehman, M.H. (2019). Decentralized document version control using ethereum blockchain and IPFS. Computers & Electrical Engineering, 76: 183-197. https://doi.org/10.1016/j.compeleceng.2019.03.014
[31] Böhme, R., Christin, N., Edelman, B., Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2): 213-238. https://doi.org/10.1257/jep.29.2.213
[32] Antwi, M., Adnane, A., Ahmad, F., Hussain, R., ur Rehman, M.H., Kerrache, C.A. (2021). The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain: Research and Applications, 2(1): 100012. https://doi.org/10.1016/j.bcra.2021.100012
[33] Amoussou-Guenou, Y., Del Pozzo, A., Potop-Butucaru, M., Tucci-Piergiovanni, S. (2018). Correctness and fairness of tendermint-core blockchains. arXiv preprint arXiv:1805.08429. http://arxiv.org/abs/1805.08429
[34] Brown, R.G. (2018) R3-Corda platform whitepaper.

https://www.corda.net/content/corda-platform-whitepaper.pdf.
[35] Kaur, S., Chaturvedi, S., Sharma, A., Kar, J. (2021). A research survey on applications of consensus protocols in blockchain. Security and Communication Networks, 2021(1): 6693731. https://doi.org/10.1155/2021/6693731
[36] Lashkari, B., Musilek, P. (2021). A comprehensive review of blockchain consensus mechanisms. IEEE Access, 9: 43620-43652. https://doi.org/10.1109/ACCESS.2021.3065880
[37] Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T., Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. IEEE Access, 7: 85727-85745. https://doi.org/10.1109/ACCESS.2019.2925010
[38] Shifferaw, Y., Lemma, S. (2021). Limitations of proof of stake algorithm in blockchain: A review. Zede Journal, 39(1): 81-95.
[39] Nguyen, G.T., Kim, K. (2018). A survey about consensus algorithms used in blockchain. Journal of Information Processing Systems, 14(1): 101–128. https://doi.org/10.3745/JIPS.01.0024
[40] Luo, Y., Chen, Y., Chen, Q., Liang, Q. (2018). A new election algorithm for DPos consensus mechanism in blockchain. In 2018 7th international conference on digital home (ICDH), pp. 116-120. https://doi.org/10.1109/ICDH.2018.00029
[41] Douceur, J.R. (2002). The sybil attack. In International workshop on peer-to-peer systems, pp. 251-260. https://doi.org/10.1007/3-540-45748-8_24
[42] Wahab, A., Mehmood, W. (2018). Survey of consensus protocols. arXiv preprint arXiv:1810.03357. https://doi.org/10.48550/ARXIV.1810.03357
[43] Lepore, C., Ceria, M., Visconti, A., Rao, U.P., Shah, K. A., Zanolini, L. (2020). A survey on blockchain consensus with a performance comparison of PoW, PoS and pure PoS. Mathematics, 8(10): 1782. https://doi.org/10.3390/math8101782
[44] Conti, M., Kumar, E.S., Lal, C., Ruj, S. (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4): 3416-3452. https://doi.org/10.1109/COMST.2018.2842460
[45] Alibaba Cloud Community. 2021. Paxos, Raft, EPaxos: How Has Distributed Consensus Technology Evolved? https://www.alibabacloud.com/blog/paxos-raft-epaxos-how-has-distributed-consensus-technology-evolved_597127/, Accessed on 9 May 2022.
[46] Jain, M. (2021). EasyChair preprint survey of blockchain consensus algorithms survey of blockchain consensus algorithms.
[47] Filecoin. A decentralized storage network for humanity's most important information. https://filecoin.io/.
[48] Sia. Decentralized data storage. https://sia.tech/.
[49] Swarm. Digital freedom now. https://www.ethswarm.org/.
[50] Yadav, B., Gupta, S. (2022). Comparative cost analysis of on-chain and off-chain immutable data storage using blockchain for healthcare data. In IOT with Smart Systems: Proceedings of ICTIS 2022, Volume 2, pp. 779-787. https://doi.org/10.1007/978-981-19-3575-6_74
[51] Storj | Fast, secure cloud storage at a fraction of the cost. https://www.storj.io/, accessed on Sep. 28, 2022.