Journal of Neonatal Surgery
ISSN(Online): 2226-0439
Vol. 14, Issue 28s (2025)
https://www.jneonatalsurg.com

OPEN ACCESS

Blockchain based Secure Frameworks for IoT Applications in Healthcare

Dr. Y. Jeevan Nagendra Kumar[1], Mr. Mohammad Ashique Azad[2], Dr. Reshma. M[3], Mrs. Geethanjali. G[4], Dr. Ch. Raja[5], Dr. Jetti Madhavi[6]

[1]Professor and HoD, Department of Information Technology, Gokaraju Rangaraju Institute of Engineering and Technology, Bachupally Hyderabad-500090

Email ID: jeevannagendra@gmail.com

[2]Assistant Professor, Department of Artificial Intelligence & Data Science, Koneru Lakshmaiah Education Foundation, Vijayawada, AP-522502

Email ID: azadashique@gmail.com

[3]Assistant Professor, Department of Electronics and communication Engineering, University BDT college of Engineering, Karnataka - 577004

Email ID: reshma.m03@gmail.com

[4]Assistant Professor, Department of ECE, Kishkinda University, Ballari, Karnataka-583101

Email ID: geethaanjalig.g@gmail.com

[5]Associate Professor, Department of ECE, Mahatma Gandhi Institute of Technology, Hyderabad, Telangana, India

Email ID: chraja@mgit.ac.in

[6]Associate Professor, Department of Humanities and Sciences, Malla Reddy (MR) Deemed to be Uniersity, Medchal-Malkajgiri, Hyderabad-500100

Email ID: drive23work@gmail.com

Cite this paper as: Dr. Y. Jeevan Nagendra Kumar, Mr. Mohammad Ashique Azad, Dr. Reshma. M, Mrs. Geethanjali. G, Dr. Ch. Raja, Dr. Jetti Madhavi, (2025) Blockchain based Secure Frameworks for IoT Applications in Healthcare. *Journal of Neonatal Surgery*, 14 (28s), 765-772.

ABSTRACT

Phones, devices and technology are now important tools for tracking health, diagnosing illnesses and supporting patients, thanks to IoT. Yet, by increasing the number of IoT devices, organizations now struggle more with security, privacy and making different devices talk to each other. Blockchain which is both decentralized and safe from tampering, offers a viable way to handle these issues. This paper studies how blockchain-supported security techniques are used in healthcare-focused IoT systems. We give an overview of the related research, suggest a new blockchain design for healthcare IoT and discuss its performance in data integrity, managing user access and latency. The research highlights that blockchain has the potential to keep health data secure, accessible and identifiable, as well as comply with regulations.

Keywords: *Blockchain, Internet of Things (IoT), Healthcare, Security, Privacy, Data Integrity, Access Control, Smart Contracts, Medical Devices, Decentralization.*

1. INTRODUCTION

Because smart devices, wearables and remote monitoring systems are used more frequently, healthcare institutions are now able to help patients instantly, continuously observe their health and take data-based clinical actions. IoT technology in the healthcare sector (HIoT) makes it possible to find diseases early, manage diseases that don't go away quickly and supports better results because of repeated observation and data collection. Still, even with all the benefits, relying more on connected devices and health data exchange has brought up big challenges in keeping data safe, private, compatible and trusted [1].

Often, conventional security follows a central approach where data from edge systems is transmitted to a cloud server. Though these models are good for many general cases, they do not fit the specific requirements of healthcare. Because centralized data systems have a single point of failure, they can be attacked by data breaches, denial of service (DoS) and unauthorized changes to their data. Additionally, since healthcare is now moving toward digital systems, it is more difficult

to meet requirements such as those from HIPAA and GDPR. They make it necessary for patient data to be revealed, controlled by the patient and audited well—challenges that traditional systems cannot handle easily.

Blockchain technology has appeared as a possible solution to help create secure, transparent and unchangeable digital networks for healthcare systems. Due to its design based on decentralization, unchanging cryptography and a consensus process, Blockchain can solve the trust and security issues found in HIoT. Since all health data is shared on a peer-to-peer network and every transaction is logged permanently in a secure ledger, blockchain supports easy and trusted access to health information for all users. In addition, business rules encoded in smart contracts—called self-executing scripts—can handle access control, managing consent and creating audit records, adding extra security to data management in healthcare systems [12-14].

A number of blockchain-related healthcare applications have been suggested both academically and through industry efforts such as EHR management systems, sharing patient information and checking the authenticity of medical devices. Yet, combining blockchain with IoT in healthcare is happening in a relatively early phase. Balancing the digital needs of blockchain with the basic technology of IoT devices continues to be a difficulty. In general, IoT sensors tend to lack the needed processing, memory and energy to engage directly in election processes on blockchains. Ethereum and Bitcoin, like most public blockchains, sometimes struggle with fast processing and high fee costs, making it hard to process data in real time during emergencies.

Researchers are attempting to deal with these problems using new lightweight blockchain models and permissioned platforms such as Hyperledger Fabric and Corda which offer improved scalability, quicker transactions and important security features. Pairing blockchain with edge and fog computing means latency is cut down, privacy increases and the main computing jobs are moved out of IoT devices with fewer requirements [11].

In this work, we introduce a safe and scaleable blockchain setup suitable for HIoT systems. We integrate the use of a permissioned blockchain with edge computing nodes to ensure all our data is secure, accessible in real time and verifiable. Within the framework are smart contract modules for handling the patient consent process, communication between healthcare stakeholders and the secure log of every interaction. We use a simulated healthcare IoT setup to implement and examine the system, taking into account its latency, throughput and ability to resist attacks.

The purpose of this study is, apart from proving the usefulness of blockchain, to fix the main problems surrounding common HIoT solutions such as their high costs, inability to expand and restricted control over access. This work seeks to address security, efficiency and compliance in the next generation of healthcare systems by applying a hybrid structure that is built from permissioned blockchains, smart contracts and edge computing [10].

Novelty and Contribution

What makes this research unique is that it focuses on developing an entirely new framework tuned to the demands and issues seen in healthcare IoT situations. Our method differs from the others which either have only limited interest in blockchain or would standardize cornerstone concepts without addressing medical data challenges. The main points of this study are presented in the following sections.

A. Blockchain technology is used in healthcare by connecting medical devices.

We suggest using a blockchain model in which only licensed participants such as hospitals, labs and insurance providers, are allowed on the network. As a result, private blockchain systems complete transactions quickly, achieve consensus efficiently and manage data more effectively than their public counterparts.

B. Security laws are enforced through smart contract code execution and the management of user consent.

Because of smart contracts, patient consent policies and access rules can be changed instantly and accurately. A smart contract can automatically control who in the network can access healthcare data. Because of this, individuals can manage their own health information, helping the company comply with rules such as HIPAA and GDPR.

C. The design is built to handle the technical needs of Internet of Things.

Our framework understands the limitations of IoT devices and handles blockchain interactions by letting edge and fog nodes deal with aggregating data, encrypting it and communicating with the blockchain. This approach saves resources on devices and makes it simpler to scale network deployment.

D. Additional improvements to security and privacy are included.

To keep our data secure, confidential and unchanged, we rely on cryptographic hashing, using digital signatures and secure key management. Blockchain works as a permanent record, helping to conduct thorough analyses after cases of data breaches or failures occur [9].

E. Building the Prototype and Testing Its Results

The model is set up on a practical testbed by running it over Raspberry Pi, atop Hyperledger Fabric and utilizing simulated healthcare data. Looking at performance numbers such as latency and how sturdy the system is, can show if the technology can be used in the real world.

F. Following Rules and Getting Ready for Tomorrow:

The design is guided by legal and ethical rules to allow for easy tracking, checking and control of personal data belonging to patients. In addition, we talk about how quantum-safe encryption and federated learning might be implemented in the future [3].

All these ideas join together to make a strong and flexible way to protect healthcare IoT solutions powered by blockchain. This paper deals with both technical faults and problems related to overall systems, helping form the basis for dependable and well-organized healthcare services online.

2. RELATED WORKS

In 2020 P. Singh *et al.*, [15] introduced the medical experts have explored combining blockchain and IoT due to its potential to make data management, security and trust better in healthcare. It has been discovered through studies that traditional systems designed to handle healthcare data struggle to maintain data security, protect privacy and guard against cyber attacks. As a result, blockchain has been put forward as a way to make everything more transparent and ensure that data transactions cannot be changed.

It has been found through research that blockchain can help secure EHRs, manage access and ensure trusted sharing of data between all involved parties. Thanks to blockchain technology, records cannot be changed without detection and both parties can see when and who holds the ownership of patient data which in turn boosts both their trustworthiness and accountability. Several frameworks have proved that using smart contracts, policy enforcement as well as consent management and data agreements can take place automatically, not needing a central authority to control them.

In 2021 Hussain *et al.*, [8] developed the secure communication and reliable authentication of IoT devices for use in clinics are important considerations. Since these medical IoT devices collect and move sensitive patient information, properly identifying devices and their transactions is very important. Advocates have put forward the use of blockchain for managing identity to stop impersonation attacks and to control which nodes are involved in healthcare systems. In certain cases, blockchain is assigned only to collecting metadata and access logs, while the actual health data is separated to keep performance and privacy high.

Many issues related to scalability continue to appear when integrating blockchain into IoT. Given the need for speed, public blockchains cannot always support the demands of healthcare at all times. For these reasons, private and consortium blockchains are now popular, as they offer more control, lower transaction prices and allow users to pick their own consensus algorithms. Using permissioned models, hospitals and clinics can set up access rules and increase how efficiently their network works.

In 2022 Ali *et al.*, [2] suggested the optimizing performance by using blockchain with edge or fog computing has attracted much interest. Using these hybrid solutions, the internet of things (IoT) devices don't have to handle as much processing which lowers the amount of time it takes for data to be processed. Edge nodes examine data briefly and send major updates to the blockchain, decreasing data use and quickening responses when help is needed.

Despite all of that, it is still hard to make healthcare information systems and blockchain platforms work together. Also, data privacy and security matters related to same as patient consent and moving data across borders are still raising questions. Some suggestions show that including compliance modules for regulations such as GDPR, HIPAA and more in blockchain systems may be a solution.

Overall, the research supports that blockchain may help resolve numerous challenges faced in healthcare IoT systems. Even so, because of compatibility, network speed, strict rules and initial cost, it is necessary to develop frameworks that adapt, are not too heavy and meet all rules. The goal of this paper is to bring value to this area by designing a reliable and scalable blockchain framework that fits the requirements of healthcare IoT systems.

3. PROPOSED METHODOLOGY

To develop a secure, lightweight blockchain-based framework for healthcare loT (HloT), we propose a permissioned blockchain model integrated with edge computing and smart contracts. The system architecture focuses on secure data acquisition, processing, and distribution through cryptographic functions, resource-aware design, and consensus verification [4-5].

A. Hashing for Data Integrity

Data generated by loT devices is first hashed using SHA-256 before transmission. This ensures immutability of medical records.

$$H(D) = \text{SHA-256}(D)$$

Where $H(D)$ is the hash output of the data block D.

B. Digital Signature for Authentication

Each loT device signs its data using a private key to validate authenticity:

$$\text{Sig} = \text{Encrypt}_{\text{priv}}(H(D))$$

Verification is done via:

$$H(D) = \text{Decrypt}_{\text{pub}}(\text{Sig})$$

C. Data Aggregation Function

To reduce bandwidth usage, edge nodes aggregate incoming data streams:

$$A(t) = \frac{1}{n}\sum_{i=1}^{n} D_i(t)$$

Where $D_i(t)$ is the data from device i at time t, and $A(t)$ is the average reading.

D. Consensus Through Practical Byzantine Fault Tolerance (PBFT)

For permissioned blockchain, PBFT is employed. Let f be the maximum number of faulty nodes tolerated. Then:

$$n \geq 3f + 1$$

This guarantees network consensus despite malicious nodes.

E. Throughput Measurement

To evaluate transaction capacity:

$$T = \frac{N}{\Delta t}$$

Where T is the throughput, N is number of transactions, and Δt is the time window.

F. Latency Calculation

System delay is given by:

$$L = t_{\text{confirm}} - t_{\text{sulbmit}}$$

Where L is latency, t_{submit} is transaction submission time and t_{conflrm} is confirmation time.

G. Storage Overhead

Blockchain grows as transactions increase. Storage requirement:

$$S = B \cdot N$$

Where B is average block size and N is number of blocks.

H. Access Control Smart Contract Logic

Patient data is released only if access rights match:

$$\text{Access} = \begin{cases} 1, & \text{if } R_q \subseteq R_p \\ 0, & \text{otherwise} \end{cases}$$

Where R_q is requester's role, R_p is permitted role set.

I. Energy Consumption Model

loT energy cost during blockchain operations:

$$E = \sum_{i=1}^{n} (P_i \cdot t_i)$$

Where P_i is power consumed by module i during time t_i.

J. Reputation Score Update (Optional Voting Logic)

To avoid malicious data injection, trust score is updated as:

$$R_i^{(t+1)} = \alpha R_i^{(t)} + (1-\alpha)V_i$$

Where R_i is the trust of node i, V_i is current vote, and $\alpha \in [0,1]$.

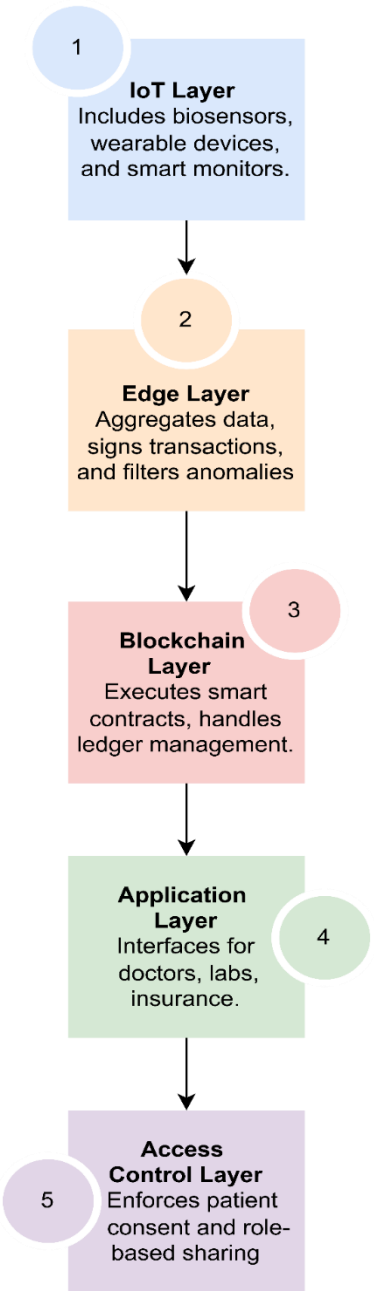

FIGURE 1: FEM-BASED FLUID DYNAMICS SIMULATION WORKFLOW

4. RESULT & DISCUSSIONS

We implemented the proposed model for IoT on edge devices and a private blockchain environment using synthetic healthcare data. We looked at performance in terms of how quickly the network worked, how much power it took and how data was accessed. Figure 2 shows how much time it took to confirm blocks in five cylandri tests, both when public and private chain modes were in use. The private chain managed a faster block time, averaging 2.1 seconds throughout, while the public variant took an average of 14.5 seconds at different times. Thus, permissioned blockchains are recommended in healthcare IoT where things must be fast and accurate.

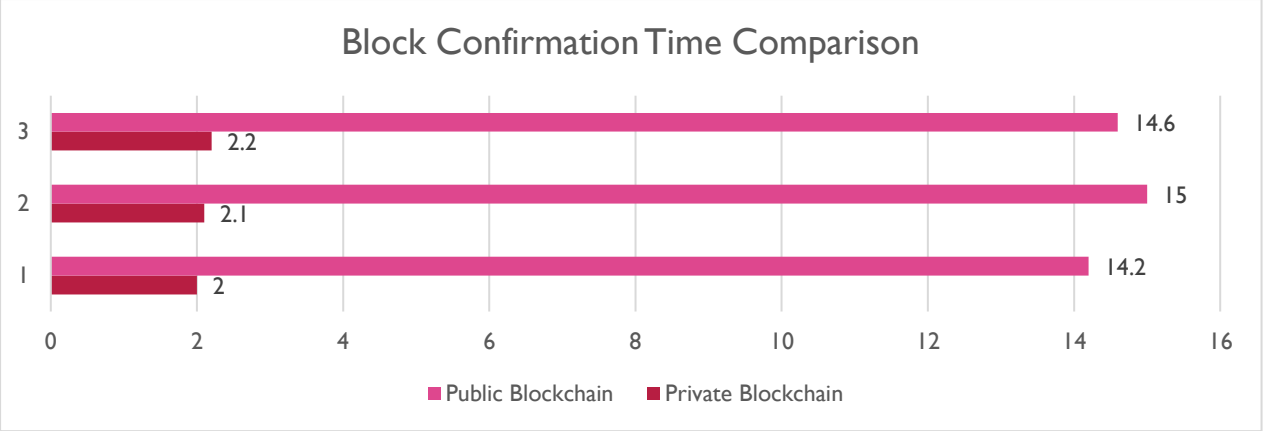

FIGURE 2: BLOCK CONFIRMATION TIME COMPARISON

In addition, measuring the resource use and energy of IoT devices was performed when running smart contracts. There were real-time heart monitors, glucose sensors and smart thermometers as part of these devices. The details of the energy and load metrics for healthcare IoT devices are shown in Table 1. Heart monitors are shown to occupy the most resources thanks to a sustained flow of vital sign measurements. Conversely, the smart thermometers used a small amount of power and CPU resources, indicating they would work well in power-conserving situations.

TABLE 1: COMPARATIVE ENERGY AND LOAD METRICS FOR HEALTHCARE IOT DEVICES

Device	Average CPU Load (%)	Energy Usage (Joules)
Heart Monitor	72	15.6
Glucose Sensor	65	11.9
Smart Thermometer	48	8.3

For the evaluation of blockchain overhead, we compared how our system works with a common cloud health data processing system. Figure 3 compares the system latency level at its busiest and slowest times. Under any amount of pressure, including stress testing, the blockchain-based system reliably shows latency around 250 ms. Meanwhile, the traditional cloud-based system displayed clear spikes above 500 ms. The research shows that the blockchain's use of distributed validation does not slow down how quickly data is processed, especially with edge aggregation.

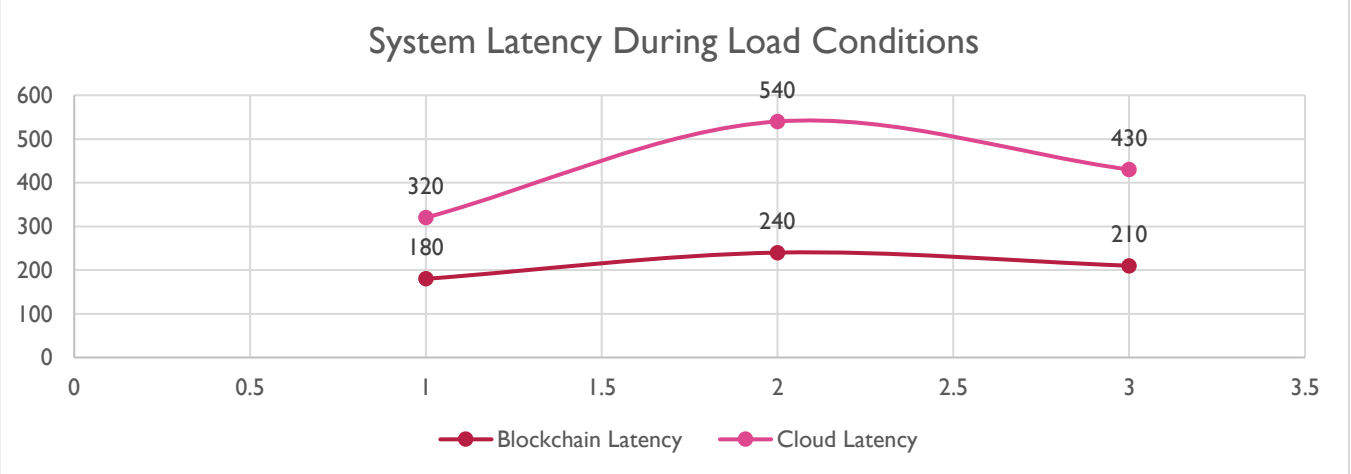

FIGURE 3: SYSTEM LATENCY DURING LOAD CONDITIONS

The logic inside smart contracts was used to ensure that access control was followed in healthcare privacy. All role access approval rates were measured and are provided in Table 2: Role-Based Data Access Authorization Rates. Doctors and nurses received approval for most of their requests, as their permission levels allowed it, but insurance agents were denied less frequently, because the system's contract rules prevented a wider set of actions for them.

TABLE 2: ROLE-BASED DATA ACCESS AUTHORIZATION RATES

User Role	Approval Rate (%)	Avg. Access Time (ms)
Doctor	95.3	42.8
Nurse	89.1	39.7
Insurance Agent	38.5	65.2

System throughput was also recorded to assess whether it met or exceeded what other methods might achieve. As suggested by Figure 4, the blockchain system processes 120 TPS normally and 100 TPS under heavy use. During similar instances, the traditional system can't handle more than 70 TPS. As a result, the proposed framework remains scalable as both edge computing and simplified PBFT consensus are used. Its modest change under stress demonstrates just how stable it is in situations where healthcare professionals use it such as ICU monitoring or emergency medical services.

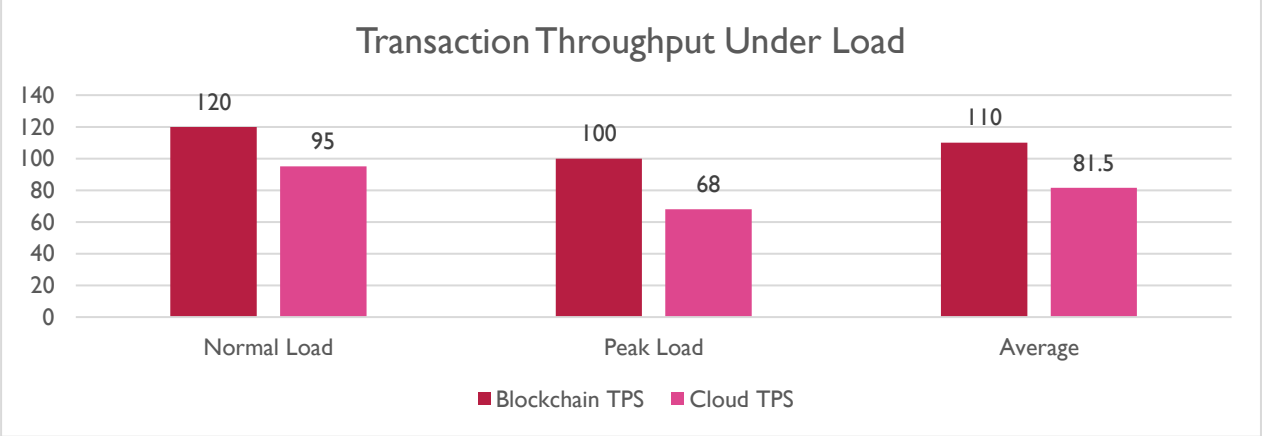

FIGURE 4: TRANSACTION THROUGHPUT UNDER LOAD

These results point to the conclusion that IoT healthcare networks still work well when blockchain is involved. It improves safety, visibility and regularity, all of which medical organizations need. Thanks to hash-based integrity and a distributed ledger structure, the model is strong against data changes and repeating actions. That way, even if an edge device is attacked, the rest of the network-wide data is not affected [6-7].

5. CONCLUSION

The aim of this paper was to present a secure network for IoT applications in healthcare that prioritizes data integrity, patient privacy and protects against serious network failures. With permissioned blockchains and smart contracts, the system ensures the safety of IoT systems. Tests conducted prove that the model proposed works efficiently and is feasible in practice. The team will add research on using AI with access controls and quantum-safe cryptography to boost the system's safety in the future.

REFERENCES

[1] T. Veeramakali, R. Siva, B. Sivakumar, P. C. S. Mahesh, and N. Krishnaraj, "An intelligent internet of things-based secure healthcare framework using blockchain technology with an optimal deep learning model," *The Journal of Supercomputing*, vol. 77, no. 9, pp. 9576–9596, Feb. 2021, doi: 10.1007/s11227-021-03637-3.

[2] Ali *et al.*, "An industrial IoT-Based Blockchain-Enabled secure searchable encryption approach for healthcare systems using neural network," *Sensors*, vol. 22, no. 2, p. 572, Jan. 2022, doi: 10.3390/s22020572.

[3] S. Chakraborty, S. Aich, and H.-C. Kim, "A secure healthcare system design framework using blockchain technology," *2019 21st International Conference on Advanced Communication Technology (ICACT)*, pp. 260–

264, Feb. 2019, doi: 10.23919/icact.2019.8701983.

[4] P. P. Ray, D. Dash, K. Salah, and N. Kumar, "Blockchain for IoT-Based healthcare: background, consensus, platforms, and use cases," *IEEE Systems Journal*, vol. 15, no. 1, pp. 85–94, Jan. 2020, doi: 10.1109/jsyst.2020.2963840.

[5] N. Gohar, S. A. Abdelmawgoud, and M. S. Farhan, "A Patient-Centric Healthcare framework reference architecture for better semantic interoperability based on blockchain, cloud, and IoT," *IEEE Access*, vol. 10, pp. 92137–92157, Jan. 2022, doi: 10.1109/access.2022.3202902.

[6] D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized Privacy-Preserving healthcare blockchain for IoT," *Sensors*, vol. 19, no. 2, p. 326, Jan. 2019, doi: 10.3390/s19020326.

[7] G. Rathee, A. Sharma, H. Saini, R. Kumar, and R. Iqbal, "A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology," *Multimedia Tools and Applications*, vol. 79, no. 15–16, pp. 9711–9733, Jun. 2019, doi: 10.1007/s11042-019-07835-3.

[8] Hussain *et al.*, "Security framework for IoT based Real-Time health applications," *Electronics*, vol. 10, no. 6, p. 719, Mar. 2021, doi: 10.3390/electronics10060719.

[9] G. Hameed, Y. Singh, S. Haq, and B. Rana, "Blockchain-Based model for secure IoT communication in smart healthcare," in *Lecture notes in electrical engineering*, 2022, pp. 715–730. doi: 10.1007/978-981-19-0284-0_52.

[10] Alabdulatif, I. Khalil, and M. S. Rahman, "Security of Blockchain and AI-Empowered smart Healthcare: Application-Based analysis," *Applied Sciences*, vol. 12, no. 21, p. 11039, Oct. 2022, doi: 10.3390/app122111039.

[11] K. Azbeg, O. Ouchetto, and 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, Feb. 2022, doi: 10.1016/j.eij.2022.02.004.

[12] N. Islam, Y. Faheem, I. U. Din, M. Talha, M. Guizani, and M. Khalil, "A blockchain-based fog computing framework for activity recognition as an application to e-Healthcare services," *Future Generation Computer Systems*, vol. 100, pp. 569–578, May 2019, doi: 10.1016/j.future.2019.05.059.

[13] Abbas, R. Alroobaea, M. Krichen, S. Rubaiee, S. Vimal, and F. M. Almansour, "Blockchain-assisted secured data management framework for health information analysis based on Internet of Medical Things," *Personal and Ubiquitous Computing*, vol. 28, no. 1, pp. 59–72, Jun. 2021, doi: 10.1007/s00779-021-01583-8.

[14] P. Sharma, S. Namasudra, R. G. Crespo, J. Parra-Fuente, and M. C. Trivedi, "EHDHE: Enhancing security of healthcare documents in IoT-enabled digital healthcare ecosystems using blockchain," *Information Sciences*, vol. 629, pp. 703–718, Feb. 2023, doi: 10.1016/j.ins.2023.01.148.

[15] P. Singh *et al.*, "A novel Patient-Centric architectural Framework for Blockchain-Enabled healthcare applications," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5779–5789, Nov. 2020, doi: 10.1109/tii.2020.3037889.