International Journal of Computing and Digital Systems
ISSN (2210-142X)
Int. J. Com. Dig. Sys. 16, No.1 (Jul-24)

http://dx.doi.org/10.12785/ijcds/160123

Enhancing Trust between Patient and Hospital using Blockchain based architecture with IoMT

Deepa Pavithran[1], Charles Shibu[2] and Sudheer Madathiparambil[3]

[1]*Information Security Engineering Technology, Abu Dhabi Polytechnic, Abu Dhabi, United Arab Emirates*
[2]*Beacon Red, Abu Dhabi, United Arab Emirates*
[3]*Department of Paediatrics, Ahalia Hospital, Mussafah, Abu Dhabi, United Arab Emirates*

Received 5 Dec. 2023, Revised 20 Apr. 2024, Accepted 23 Apr. 2024, Published 1 Jul. 2024

Abstract: This paper addresses a critical issue within the healthcare industry, where concerns regarding transparency and accountability have surfaced following certain instances of potential misconduct. In particular, there have been allegations in certain countries, asserting the situation where some healthcare institutions prolong the use of intensive care services for deceased patients to generate additional revenue, leading to a severe erosion of trust between the families of patients and these institutions. To mitigate these concerns, we offer insights into how a blockchain-based system integrated with the Internet of Medical Things (IoMT) can help in solving such problems. This approach seeks to enhance trust and transparency by capturing patient data and ensuring its immutability through blockchain technology. Based on the use-case, the architecture of IoT-Blockchain can vary. The system adopts a decentralized framework for combating the addressed concerns with efficacy. The system will provide a secure, tamper-proof, and accountable mechanism that can alleviate trust issues and uphold the highest ethical standards in healthcare. Upon deploying the system the stakeholders, especially the patient's relatives, will be able to access patient data in real-time and gain insights into the patient's condition.

Keywords: Blockchain, architecture, IoMT, IoT, Trust, consensus, healthcare, patient monitoring

1. INTRODUCTION

The healthcare industry stands as a cornerstone of the society, founded on the principles of patient care, ethical practice, and unwavering trust. However, recent revelations of potential misconduct within certain healthcare institutions have cast a shadow over these noble ideals. Reports of patients being maintained in intensive care beyond medical necessity, to extract additional financial revenue have raised serious concerns about transparency, integrity, and the ethical underpinnings of healthcare [1], [2], [3].

At the heart of this issue lies a crisis of trust—a trust that forms the very bedrock of the patient-doctor relationship and the entire healthcare system. The erosion of this trust poses not only an immediate challenge but also a profound threat to the entire healthcare ecosystem. It is imperative that we respond with innovative solutions that not only address the immediate concerns but also shape the future of healthcare data management and ethical practices.

In this context, we provide a solution that leverages the convergence of two transformative technologies: blockchain and the Internet of Medical Things (IoMT). This paper outlines on how this combination can be used to restore trust in healthcare institutions and also to provide secure, transparent, and ethical patient data management.

Blockchain has gained popularity due to the fact that 'trust' can be attained without human intervention but through cryptographic techniques. Due to this reason, it makes it hard for a user to falsify/ tamper/ delete the data [4], [5]. Internet of Things (IoT) has witnessed explosive growth, with billions of devices and sensors being deployed across various industries and sectors. These devices, collect large amount of data and communicate with each other, through a network. The integration of blockchain and Internet of Things (IoT) technology signifies a revolutionary and creative frontier within the digital connectivity landscape. This fusion of technologies could revolutionize the inherent capability to transform the manner in which devices engage, exchange and safeguard data ensuring the integrity and authenticity of information. Hence blockchain for IoT is a promising field in several applications like energy management [6], [7], [8], supply chain [9] asset tracking [10], [11], healthcare [12], [13], [14], smart city [15], [16], industrial devices [17], and home automation [18].

Even though Blockchain and IoT have several use-cases, there is no one-stop solution considering the implementations. We are integrating this technology to offer an effective

E-mail address: deepa.pavithran@actvet.gov.ae

solution for a specific scenario where healthcare institutions are managing deceased patients in intensive care, leading to trust concerns. Whether the patient arrived at the hospital alive or not remains uncertain. This is a primary concern while the other concern is the institutional restrictions in intensive care units making it impossible for the family members to assess the patient's condition. The latter is unarguably due to safety protocols.

2. MOTIVATION

The motivation behind this research work is deeply rooted in the fundamental principles of healthcare: trust, transparency, and the ethical treatment of patients. The allegations levelled against certain healthcare institutions exploiting patients and their families for financial gain have created a crisis of confidence within the healthcare industry. To address these concerns, it is imperative to build a patient-centric care [19], to lay the foundation of trust between patient and doctor [20], to provide data security and privacy [21] and to maintain ethical practices.

1. Patient-Centric care: Healthcare is fundamentally about patient well-being, and any action that undermines this core principle must be rectified. The allegations of prolonged ventilator usage on deceased patients go against the very essence of patient-centric care, and dignity of life. By addressing this issue, we aim to reaffirm our commitment to the highest ethical standards in healthcare.

2. Rebuilding trust: Trust is the foundation of the patient-doctor relationship and the healthcare system as a whole. When the factor of trust diminishes, it poses a severe threat to patient care and outcomes. By implementing a system that ensures transparency and accountability, we can restore reliability or atleast initiate the process of rebuilding the trust that has been damaged.

3. Data security and privacy: In an era of advancing technology, security and privacy of patient data should be protected. Hence there is a need to protect sensitive patient information and safeguard it against any form of manipulation or unauthorized access.

4. Technological innovation: The integration of blockchain and IoMT represents a significant leap in the forward direction in healthcare technology. It offers an opportunity not only to address the immediate issue but also to create a model for the secure, tamper-proof, and ethical management of medical data.

5. Ethical imperative: As a society, we hold ourselves accountable for the ethical treatment of patients in the healthcare system. It is our moral obligation to ensure that medical practices are conducted with highest standards of integrity. This motivation is deeply rooted in our collective commitment to medical ethics and patient well-being.

6. Future of healthcare: The successful implementation of blockchain and IoMT could serve as a blueprint for future healthcare systems, not just in terms of patient data management but in rebuilding the trust that is vital to the practice of medicine. It paves the way for a healthcare system that is patient-focused, technologically advanced, and, above all, built on a foundation of trust and transparency.

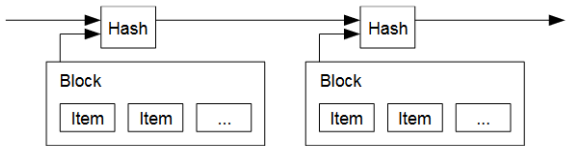

Figure 1. Block Structure: Blocks in Blockchain linked to the previous block

The motivation for this research work is driven by a commitment to the highest standards of patient care and medical ethics. By addressing the issues at hand and embracing innovative technology, we seek to restore trust, ensure data integrity, and contribute to the evolution of a healthcare system that places the welfare of patients at its core.

3. BACKGROUND

Blockchain is a system which records transactions across computers in a peer-to-peer network. The initial implementation of blockchain was mainly for cryptocurrencies which was proposed to solve the double-spending problem. The main components in a blockchain system are transaction data, distributed ledgers, consensus and peer to peer network. Data is organized into blocks and each block is linked to its previous block as shown in Figure 1. This helps in preventing data tampering. Validating and verifying the transactions are done through a consensus mechanism. Verified data is then distributed to multiple nodes within the network. Proof-of-Work (PoW) [4] is a common consensus adopted in many blockchain applications including Bitcoin. It has high energy usage and is more suitable for public blockchains [22]. A public blockchain is a permissionless blockchain where anyone can take part in the consensus process and can be added as a node in the network. These types of blockchains are predominantly used in cryptocurrencies. While extending the use of blockchain to applications like IoT, mostly permissioned blockchains are used where nodes participating in the process is added by a trusted entity [23]. The consensus used for such type of blockchain also varies. An example is PBFT (Practical Byzantine Fault Tolerance) [24].

Another consensus that is used in blockchain is Proof-of-Authority (PoA) [25]. It is more energy efficient and provides better scalability. The validators are nodes in the blockchain that are added by a trusted entity. The algorithm operates in rounds during which an elected party acts as validator. The selected validator will be chosen for creating the block. The validator can be chosen using round-robin fashion or weighted random fashion. PoA has better

performance as less message exchanges are conducted.

The Internet of Things (IoT) are the physical devices in a network such as medical devices, home appliances, RFID tags, sensors used in industry, sensors in vehicles etc. The health customized version of IoT also called the IoMT which is a subdomain of IoT, employs sensors to measure various parameters from patients body such as heart rate, blood pressure, respiratory rate, oxygen saturation, temperature etc. They can be used for various applications such as medical implants, patient monitoring, where real-time patient data can be made available to users. Much like IoT devices, they utilize sensors and machine intelligence to reduce the human intervention in medical field. This helps in reducing cost, time and effort spent on patients by medical professionals. However, these sensors generate patient data, which should be handled in a highly secure manner. The traditional way of handling IoT data is through a centralized database. It has several disadvantages [26],

1. Centralized database system stores all data in one node. Even though it makes it easier to manage data, it is a single point of failure. If any system failure occurs, it is hard to recover the data.

2. Centralized databases are targeted by attackers. The data can be modified by internal or external threats.

While dealing with sensitive personal data, it is crucial to comply with regulations such as the General Data Protection Regulation (GDPR) in Europe, and the HIPAA in the USA to safeguard personal information. These regulations necessitate that systems guarantee the confidentiality of patient data. Leveraging technology in a healthcare environment can support patients and medical professionals in facilitating the management of electronic health records, developing tools for diagnosis of diseases, facilitating pharmaceutical delivery and enhancing Bio-medical research and Genomics [27], [28].

Major advantages of IoMT based Health care system are

1. Effective Remote Monitoring: allows healthcare providers to monitor patient's health data and vital signs outside of traditional clinical settings, such as hospitals or clinics. It involves the use of various electronic devices and technology to collect, transmit, and store patient health information. Healthcare providers, such as doctors or nurses, can access the patient's data through the platform in real-time or at scheduled intervals. They can monitor vital signs, review trends, and make informed decisions about the patient's health.

2. Reduction in cost: This reduces hospital expenses as the patient does not have to stay in the hospital for continuous monitoring. Patients can be monitored even from outside and the collected data can be transmitted to the healthcare provider.

3. Improved health services in the Hospital: Doctors can monitor the health of the patient through his/her phone from a convenient location and provide suggestive treatment and consultations without any delay.

4. Health alerts. The system can be programmed to send alerts or notifications to healthcare providers/patients/ relatives when certain thresholds or abnormal readings are detected. This allows for early intervention in case of deteriorating health [29].

In addition, Table1 provides existing challenges in ventilator based IoMT system and how blockchain based system can address these challenges.

4. RELATED WORK

The majority of blockchain and IoMT applications available in literature focus on remote patient monitoring, wireless capsule endoscopy and telemedicine systems.

The authors in [30] have employed smart contracts for patient monitoring and for sharing the results with health care providers. They have onChain and OffChain data. Patient data is not stored in blockchain, whereas it is forwarded to EHR storage database. The blockchain transactions are linked to the EHR. This will allow the modification of data in EHR. Authors in [31] have utilised Hyperledger Fabric platform to create a private blockchain to analyse the storage and data authorization. They have used both public and private data. To ensure data privacy and integrity during data retrieval from a cloud-based blockchain database, they employed a consensus mechanism that combines Proof of Integrity (PoI) and Proof of Validity (PoV). The system is used for remote patient monitoring.

Authors in [32] proposed blockchain-based smart contracts for authorizing sensor devices and supports the registration of patients and healthcare workers in a healthcare facility. They used IPFS for data storage. In [33] protocol using directed acyclic graphs called GHOSTDAG is proposed for remote patient monitoring. They have also used a hybrid storage where patient data gets stored in a EHD storage unit whereas blockchain stores only the transaction events. Authors in [34] proposed system for remote patient monitoring. They used smart contract for access control and IPFS for storing the data as off-chain.

Wireless Capsule Endoscopy (WCE) is an imaging technology, that uses a pill camera for imaging internal body parts to recognize stomach infections. Authors in [35] use blockchain based approach with convolutional neural network (CNN) model for classifying stomach infections. The authors in [36] offer solutions for teleconsultation service through blockchain. They use an interface layer for communication purposes, a DApp layer that includes smart contracts for providing security and scalability and a Blockchain layer. IPFS is used for distributed storage.

FHIRChain [37] provides authentication using public

TABLE I. Challenges in Ventilator based IoMT system

Challenge	Existing challenges in Ventilator based IoMT system	How Blockchain can address these challenges
Unauthorized Access and Control	Unauthorized device access by individuals gaining access to the ventilator system is a primary concern. These malicious actors could manipulate settings, control ventilation parameters, or disrupt the system's operation	Blockchain can support identity management and access control mechanisms.
Data Privacy and Confidentiality	Inadequate protection of patient data and medical records. Unauthorized access to patient information can lead to privacy breaches and compromise patient confidentiality. This includes vulnerabilities relevant to storage facilities, network infrastructure, transmission protocols, etc	Certain blockchain platforms enables secure and direct communication between devices. This can be obtained by establishing a direct and encrypted channel between the ventilator and smart devices.
Data Tampering and Manipulation	Physical or remote tampering with the ventilator system can lead to malfunctions, system integrity issues leading to erroneous data, incorrect treatment, or disruption of critical care services	Application of Blockchain provides a tamper-proof ledger where each transaction (data exchange) is recorded in a block. Once a block is added to the chain, it cannot be altered. Ensures that crucial patient data transmitted between the ventilator and smart devices remains unchanged and trustworthy.
Network Vulnerabilities	Insecure network connections and communication channels attribute to infrastructure security. Vulnerabilities in network protocols or devices can be exploited for unauthorized access or data interception	Blockchain uses decentralized network, eliminating single point of failures. Data is distributed across nodes, enhancing system resilience. Blockchain improves system reliability by reducing the risk of disruptions due to a single point of failure or malicious attacks.
Insufficient Authentication and Authorization	Weak or inadequate authentication and authorization mechanisms. Unauthorized users may gain access to sensitive functions or information	Participants in the network can be authenticated, and access permissions can be defined through smart contracts. Implementation of Blockchain makes sure that only authorized personnel and devices have access to patient data and controls who can interact with the blockchain.
Interoperability Challenges	Lack of standardized communication protocols while transmitting prioritized information are well known interoperability challenges. Interoperability issues with other healthcare systems may lead to data integrity problems or delayed patient care.	Using an appropriate consensus mechanism can guarantee the accuracy and validity of patient data exchanged between devices by requiring consensus among network participants.

key cryptography and a smart-contract based system is used. The patient data is stored off-chain.

In this paper we provide how blockchain based system with IoMT can be used for developing trust between patient and hospital, for a certain context where hospitals use deceased patients to make additional revenue.

5. SYSTEM ARCHITECTURE

A. *Overview*

The patient is affixed with a ventilator device that can sense patient's vitals with sensors such as Temperature sensor, SPO2 (oxygen concentration), Pulse Oximeter. In addition to these, other sensors required are EEG (Electroencephalogram), ECG (Electrocardiogram), Blood Pressure Monitor, Heart rate Sensor, ET-CO2 (End-tidal carbon dioxide) sensor. The generated data is sent to a smart device within the hospital. The smart device is capable of creating transactions with the data generated by the sensors. The hospitals are provided with a smart device capable of generating anonymous patient ID, possessing its own public-private Key pair and capable of creating smart contracts. Each hospital is added to the blockchain through a trusted entity. This trusted entity could be a governmental entity that manages the department of health. This entity adds the hospitals in the area as nodes in the blockchain. Each node can store a copy of the transactions. Figure 2 provides overview of the network architecture.

B. *Key generation*

The public-private key pair is generated through public key cryptographic algorithms, specifically elliptic curve

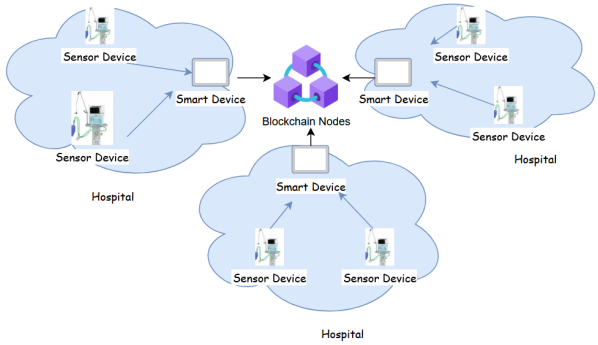

Figure 2. Overview of network architecture

cryptography (ECC). A private key is a 256-bit (64-character hexadecimal) number which should be kept confidential. The public key can be derived from the private key. The patient's anonymous address is then obtained from the public key. Even though both keys are mathematically related, deriving the private key from public key is hard. However, the reverse is a straightforward process. The security of the system is provided through this one-way relationship.

The private key is used to create signature and the signature could be verified by its corresponding public key without revealing the private key. Initially, the private key is generated using pseudorandom number generation technique, by randomly selecting a 256-bit number less than 'n', where n is a constant defined as the order of the elliptic curve.

$$Pu = Pk * R$$

where Pk is the private key, R is the generator point, and Pu is the public key [38].

It is easier to find the public key from private key but the reverse is hard due to the one-way property. From the public key 'Pu', anonymous address can be generated using algorithms such as SHA256 and the RIPEMD160.

Anonymous ID= RIPEMD160(SHA256(K))

C. Registration phase

Device Registration: Each healthcare center will possess smart devices that are capable of performing cryptographic functions. Smart device is incorporated with sensors in the ventilator along with other required sensors. The smart devices are initially registered with the trusted entity. Each smart device collects data from sensors, process it further, initiate smart contract and follow the blockchain process.

Patient Registration: Patients are registered with the smart device to generate the anonymous ID.

D. Consensus

Byzantine Fault Tolerant (BFT) based consensus algorithms are mostly adopted for permissioned blockchains. Proof of Authority (PoA) [25] is a kind of BFT algorithm used in Parity [39]- the Rust-based Ethereum client and Geth [40]- the GoLang-based Ethereum client. As it is used for permissioned network, the nodes in the blockchain are called authorities. Authorities are identified by an identifier and at least N/2 +1 is assumed to be honest, where 'N' is the number of trusted nodes. All nodes in the network are assumed to be synchronized with the same UNIX time 't'. The leader is selected by

$$l = S \, mod N$$

Where the index S is computed by each authority as

$$S = t/step\_duration$$

Where step_duration is a constant determining the duration of the step.

Authorities collect transactions in a transaction queue, and a selected leader broadcasts these transactions to other authorities during the Block Proposal Round.

Each authority then sends the received block to others. This is called Block Acceptance Round. In this round, if authorities do not agree on the proposed block, a voting is triggered to determine whether the current leader is malicious or not. A leader may exhibit malicious behavior under the following conditions:

1) it fails to propose any block
2) it proposes an excessive number of blocks beyond the expected amount, or
3) it puts forth distinct blocks to different authorities

By this way malicious nodes can be identified and removed [41].

E. Block creation and Data storage

Smart device invokes the smart contract and creates transaction. The transaction is signed by the smart device. Unconfirmed transactions are broadcasted to the mempool. Miners (Selected validators based on consensus algorithm) confirm the transactions and add it to the blockchain. Users (Patient's relatives) can view the transactions using their private key.

Figure 3 shows the sequence diagram. Initially, the patient is registered with the smart device. The device provides an anonymous ID (public- private key pair) to the patient. Sensors gather the data from patient which gets added to the smart device. The smart device then creates a smart contract to include the transactions. Miners confirm the transactions and confirmed transactions are added to the

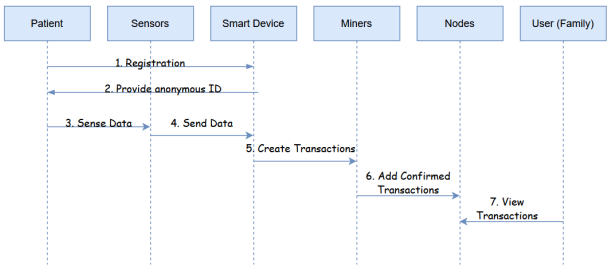

Figure 3. Sequence Diagram

block. Users (relatives of patient) can view the real-time data through a cloud-based system.

A major challenge in implementing blockchain for healthcare system is the impracticality of storing large amounts of data in the blockchain. This will create high latency in the network and large storage space is required in each node. Hence healthcare blockchain applications use hybrid storage methodology where healthcare data is moved to cloud and blockchain nodes contains pointer to it [30]. This is represented in Figure 4.

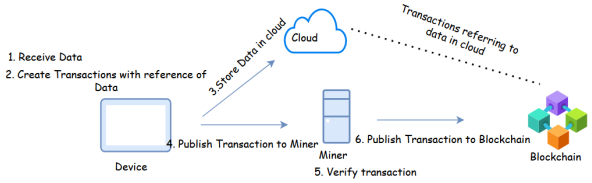

Figure 4. Blockchain process with Hybrid storage

However, if the data to be added is of a significantly smaller size, it is possible to store the data in the blockchain database as shown in Figure 5. For the mentioned cause, the data will not be large as it is applicable only for patients who are in intensive care units.

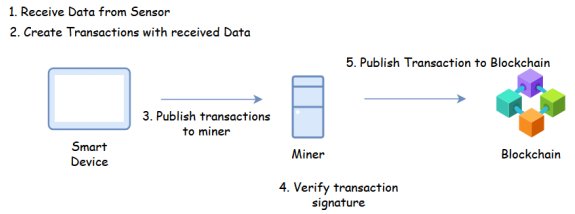

Figure 5. Blockchain Process with data stored in Blockchain Nodes

As per the HIPPA rule "There are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis to identify an individual" [42]. For the mentioned cause, instead of creating encryption overhead, providing pseudo-anonymous address that would not link to the identity of the patient can provide privacy for the patient data. This is accomplished through one-way cryptographic function.

6. IMPLEMENTATION DETAILS

Ethereum [40] is an opensource blockchain-based platform, which features smart contract. Smart contracts are programs that run on the Ethereum network and executes automatically when certain conditions are met. The advantage of using smart contracts is that it doesn't need a central authority to control the process. The system operates as a state machine, wherein each transaction undergoes a series of state transitions. Consequently, the subsequent state is determined by both the data from the prior state and the current transaction. Ethereum employs a specific language, Solidity, designed for crafting smart contracts. Transactions in Solidity involve invoking methods written in the code.

Truffle is an Ethereum development framework, that provides a suite of tools that can be used during development, testing and deployment phases. We used Ganache [43] to set up an Ethereum blockchain to deploy smart contracts. Remix IDE [44], which is a web browser-based IDE is used to create smart contracts in Solidity. Data from the ventilator is stored in the blockchain by invoking the smart contract. Figure 6 shows the smart contract created using Remix IDE. Various IoMT sensors collect the patient's vitals such as Blood Pressure, ET-CO2, Heart rate, Pulse Oximeter, SPO2 and temperature. The smart contract created in Ethereum is invoked, which add these data to the blockchain.

Figure 6. Smart contract Data

Gas represents the cost associated with executing transactions on the Ethereum blockchain, with users paying gas fees in ether to the Ethereum network. These fees are deducted from the user's account during interactions with smart contracts, covering each operation, transaction, or function call within the contract. The gas limit is a fixed value indicating the maximum amount of gas allocated for a transaction, paid upfront before any computation occurs and cannot be increased later. A higher gas limit typically

implies an expectation of more computational work. Meanwhile, the gas price denotes the cost per unit of work performed, representing the payment per unit of gas for all computational expenses incurred during the transaction's execution [45]. We conducted the experiment by calculating the Gas usage based on two scenarios: Sensor data stored in separate transactions, and Sensor data stored in the same transaction. While deploying the transactions as individual transactions as shown in Figure 7, the gas used for each transaction is 21,204. Hence the total gas usage for all the transactions will be 127224. However, when we added all the data into one transaction, the gas usage was found to be 21288. This gas usage does not include the gas usage for contract creation. Figure 7 provides the graph between No: of patients and the Ethereum gas required for executing the smart contract transaction. X-Axis shows the number of patients and Y-Axis shows the gas required when sensor data is separated into multiple transactions and when data is added to a single transaction.

Figure 7 clearly indicates that it is possible to add all the collected data in single transaction which can drastically reduce the execution cost. While Ethereum does not impose restrictions on the size of content, it is not considered efficient for storing large volumes of data [46]. Hence a common way to deal with this limitation is to use Inter Planetary File System (IPFS) [47]. IPFS functions as a decentralized file system where data is distributed across a peer-to-peer network. Each data instance possesses a distinct address that directs to the specific data. Hence many blockchain based IoMT applications use IPFS. The mentioned cause is limited only to emergency patients. Hence our result shows that it is capable to store the data in the Ethereum blockchain.

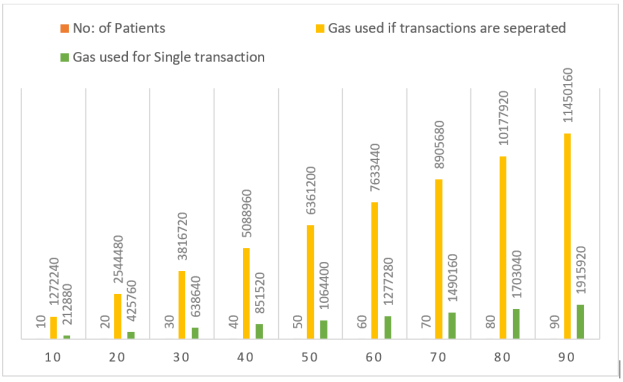

Figure 7. Gas used when data are separated in multiple transactions and when data is added to single transaction

7. SECURITY ANALYSIS

Table II shows how the blockchain based system provides security. The use of pseudo-anonymous address provides privacy without disclosing the patient identity. An adversary will not be able to link to the real identity of the patient. Blockchain ensures that transactions are shared among multiple nodes in the system which protects from single point of failure and ensures data availability. Data integrity is provided through hash functions where each block is linked to previous block through hash. Transactions are recorded in blocks and linking of blocks helps to create immutable transactions. Transactions are authenticated through digital signatures. The system also provides transparency in a controlled way without revealing the identity of the patient.

TABLE II. Security Analysis

Confidentiality	Provides Pseudo anonymity. The use of anonymous addresses safeguards the privacy of patients, preventing any linkages between individuals and their respective data.
Availability	Transactions are recorded on all nodes on the blockchain providing Availability.
Immutability	Transactions are recorded in blocks and blocks are linked to previous blocks. Hence modifying a transaction necessitate multiple changes.
Traceability	Transactions on the blockchain can be tracked from their point of creation, ensuring immutability, and are authenticated by the verifier through digital signatures.
Transparency	Provide Transparency to the data while maintaining privacy and control.
Privacy	The use of anonymous addresses safeguard the privacy of patients, preventing any linkages between individuals and their respective data.

8. CONCLUSION

In this research work, we outlined how blockchain based system can be used for a certain cause that elevated the trust between patients and hospitals. The approach followed in the research is more patient-centric and hence only authorized users have access to patient data. Privacy is provided through anonymity. Patient's condition is easily verifiable for the relatives and patient/authorized representative can grant or revoke permissions of patient data to the parties who would like to access the data. Authorized representative of the patient can trust the hospital and the medical care received by the patient as the patient data is available to them in real time. Compared with the traditional centralized database, the use of blockchain prevent data tampering and single point of failure. The system provides privacy through anonymity and the experiment results show that data can be stored within the blockchain nodes as a single transaction for all vitals. As a future work, the system can be implemented using other blockchain platforms such as Hyperledger Fabric and performance can be measured and compared.

REFERENCES

[1] lakshminm, "Kerala hospitals 'treat' dead body for five hours, charges 9000 — web.archive.org," https://web.archive.org/

web/20210927154830/https://newsable.asianetnews.com/south/kerala-hospitals-treat-dead-body-for-five-hours, [Accessed 15-03-2024].

[2] Piyush.Rai, "Kin claim hospital put patient on ventilator after death to 'extort' money, home ministry official intervenes — Meerut News - Times of India — web.archive.org," News Article Link, 2021, [Accessed 15-03-2024].

[3] M. Khan, "Moradabad's pvt hosp accused of putting dead patient on ventilator to 'extort money' from family; probe ordered — Bareilly News - Times of India — web.archive.org," News Article Link, 2021, [Accessed 15-03-2024].

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized blockchain for iot," in *Proceedings of the second international conference on Internet-of-Things design and implementation*, 2017, pp. 173–178.

[6] M. Yan, F. Teng, W. Gan, W. Yao, and J. Wen, "Blockchain for secure decentralized energy management of multi-energy system using state machine replication," *Applied Energy*, vol. 337, p. 120863, 2023.

[7] J. Li, M. S. Herdem, J. Nathwani, and J. Z. Wen, "Methods and applications for artificial intelligence, big data, internet of things, and blockchain in smart energy management," *Energy and AI*, vol. 11, p. 100208, 2023.

[8] L. Wang, S. Jiang, Y. Shi, X. Du, Y. Xiao, Y. Ma, X. Yi, Y. Zhang, and M. Li, "Blockchain-based dynamic energy management mode for distributed energy system with high penetration of renewable energy," *International Journal of Electrical Power & Energy Systems*, vol. 148, p. 108933, 2023.

[9] T. Bocek, B. B. Rodrigues, T. Strasser, and B. Stiller, "Blockchains everywhere-a use-case of blockchains in the pharma supply-chain," in *2017 IFIP/IEEE symposium on integrated network and service management (IM)*. IEEE, 2017, pp. 772–777.

[10] A. B. Tran, Q. Lu, and I. Weber, "Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management." in *BPM (dissertation/demos/industry)*, 2018, pp. 56–60.

[11] D. Verma, N. Desai, A. Preece, and I. Taylor, "A block chain based architecture for asset management in coalition operations," in *Ground/Air Multisensor Interoperability, Integration, and Networking for Persistent ISR VIII*, vol. 10190. SPIE, 2017, pp. 223–231.

[12] J. Almalki, W. Al Shehri, R. Mehmood, K. Alsaif, S. M. Alshahrani, N. Jannah, and N. A. Khan, "Enabling blockchain with iomt devices for healthcare," *Information*, vol. 13, no. 10, p. 448, 2022.

[13] A. D. Dwivedi, G. Srivastava, S. Dhar, and R. Singh, "A decentralized privacy-preserving healthcare blockchain for iot," *Sensors*, vol. 19, no. 2, p. 326, 2019.

[14] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi, and M. Abid, "Healthblock: A secure blockchain-based healthcare data management system," *Computer Networks*, vol. 200, p. 108500, 2021.

[15] P. K. Sharma and J. H. Park, "Blockchain based hybrid network architecture for the smart city," *Future Generation Computer Systems*, vol. 86, pp. 650–655, 2018.

[16] R. Paul, P. Baidya, S. Sau, K. Maity, S. Maity, and S. B. Mandal, "Iot based secure smart city architecture using blockchain," in *2018 2nd international conference on data science and business analytics (ICDSBA)*. IEEE, 2018, pp. 215–220.

[17] S.-H. Jang, J. Guejong, J. Jeong, and B. Sangmin, "Fog computing architecture based blockchain for industrial iot," in *Computational Science–ICCS 2019: 19th International Conference, Faro, Portugal, June 12–14, 2019, Proceedings, Part III 19*. Springer, 2019, pp. 593–606.

[18] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for iot security and privacy: The case study of a smart home," in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*. IEEE, 2017, pp. 618–623.

[19] A. A. Seyhan and C. Carini, "Are innovation and new technologies in precision medicine paving a new era in patients centric care?" *Journal of translational medicine*, vol. 17, no. 1, p. 114, 2019.

[20] V. Gopichandran, "Trust in healthcare: an evolving concept," *Indian Journal of Medical Ethics*, vol. 10, no. 2, pp. 79–82, 2013.

[21] W. Wilkowska and M. Ziefle, "Privacy and data security in e-health: Requirements from the user's perspective," *Health informatics journal*, vol. 18, no. 3, pp. 191–201, 2012.

[22] K. J. O'Dwyer and D. Malone, "Bitcoin mining and its energy footprint," 2014.

[23] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[24] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.

[25] "POA Network Whitepaper — github.com," https://github.com/poanetwork/wiki/wiki/POA-Network-Whitepaper, [Accessed 15-03-2024].

[26] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with iot. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[27] E. J. De Aguiar, B. S. Faiçal, B. Krishnamachari, and J. Ueyama, "A survey of blockchain-based strategies for healthcare," *ACM Computing Surveys (CSUR)*, vol. 53, no. 2, pp. 1–27, 2020.

[28] T. Justinia, "Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences," *Acta Informatica Medica*, vol. 27, no. 4, p. 284, 2019.

[29] M. Wazid and P. Gope, "Backm-eha: A novel blockchain-enabled security solution for iomt-based e-healthcare applications," *ACM Transactions on Internet Technology*, vol. 23, no. 3, pp. 1–28, 2023.

[30] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, "Healthcare blockchain system using

smart contracts for secure automated remote patient monitoring," *Journal of medical systems*, vol. 42, pp. 1–7, 2018.

[31] M. A. H. Wadud, T. A.-U.-H. Bhuiyan, M. A. Uddin, and M. M. Rahman, "A patient centric agent assisted private blockchain on hyperledger fabric for managing remote patient monitoring," in *2020 11th International Conference on Electrical and Computer Engineering (ICECE)*. IEEE, 2020, pp. 194–197.

[32] H. S. Z. Kazmi, F. Nazeer, S. Mubarak, S. Hameed, A. Basharat, and N. Javaid, "Trusted remote patient monitoring using blockchain-based smart contracts," in *Advances on Broad-Band Wireless Computing, Communication and Applications: Proceedings of the 14th International Conference on Broad-Band Wireless Computing, Communication and Applications (BWCCA-2019) 14*. Springer, 2020, pp. 765–776.

[33] G. Srivastava, R. M. Parizi, A. Dehghantanha, and K.-K. R. Choo, "Data sharing and privacy for patient iot devices using blockchain," in *International Conference on Smart City and Informatization*. Springer, 2019, pp. 334–348.

[34] 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, 2022.

[35] M. A. Khan, I. M. Nasir, M. Sharif, M. Alhaisoni, S. Kadry, S. A. C. Bukhari, and Y. Nam, "A blockchain based framework for stomach abnormalities recognition," *Comput. Mater. Contin*, vol. 67, pp. 141–158, 2021.

[36] H. Kordestani, K. Barkaoui, and W. Zahran, "Hapichain: a blockchain-based framework for patient-centric telemedicine," in *2020 IEEE 8th International Conference on Serious Games and Applications for Health (SeGAH)*. IEEE, 2020, pp. 1–6.

[37] P. Zhang, J. White, D. C. Schmidt, G. Lenz, and S. T. Rosenbloom, "Fhirchain: applying blockchain to securely and scalably share clinical data," *Computational and structural biotechnology journal*, vol. 16, pp. 267–278, 2018.

[38] A. M. Antonopoulos, *Mastering Bitcoin: Programming the open blockchain*. " O'Reilly Media, Inc.", 2017.

[39] "Home — parity.io," https://www.parity.io, [Accessed 15-03-2024].

[40] "Home — go-ethereum — geth.ethereum.org," https://geth.ethereum.org/, [Accessed 15-03-2024].

[41] S. De Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri, V. Sassone *et al.*, "Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain," in *CEUR workshop proceedings*, vol. 2058. CEUR-WS, 2018.

[42] https://www.hhs.gov/ocr/hipaa./index.html, [Accessed 15-03-2024].

[43] "Ganache - Truffle Suite — trufflesuite.com," https://trufflesuite.com/ganache/, [Accessed 15-03-2024].

[44] "Remix - Ethereum IDE — remix.ethereum.org," https://remix.ethereum.org, [Accessed 15-03-2024].

[45] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project yellow paper*, vol. 151, no. 2014, pp. 1–32, 2014.

[46] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[47] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

Deepa Pavithran Dr. Deepa has more than 10 years experience in the field of Information Security and Computer Science. She has Ph.D. in Computer Science, Master's in Cyber Security and Bachelor's in Computer science and Engineering. She holds more than 10 Professional certifications including CISSP and OSCP. Her research interests are in Cryptography, Blockchain and Quantum Computing.

Charles Shibu Charles Shibu, Masters in IT, CISA, CRISC, CISM, CHFI, CEH, CEI, ISO 27001:2013, He is a seasoned cybersecurity expert with over 15 years of experience. He holds industry-leading certifications across various domains and is known for delivering innovative solutions to combat emerging threats. With a passion for staying ahead of the curve, Charles continues to shape the future of cybersecurity with his diversified expertise and commitment to excellence.

Dr. Sudheer Madathiparambil Dr. Sudheer Madathiparambil is a Consultant Paediatrician and Medical Director at Ahalia Hospital Mussaffah, Abu Dhabi. His qualifications include MBBS, MD Paediatrics and DNB Paediatrics from India. He then went on to the UK for further specialized training, during which he completed his DCH and MRCPCH qualifications. He worked as a Paediatrician in the NHS, UK for six years, in tertiary teaching University hospitals. One of his last jobs in the UK was in the Neonatal intensive care at Leicester Royal Infirmary, England. In 2018, he completed the PG Diploma in Respiratory Medicine from University of South Wales, UK. His special interests include Neonatology and Paediatric asthma. He has many international publications to his credit. He is well known for his clinical skills and excellent communication with patients and families.