Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 4s (2025)

Blockchain-Enabled Patient-Centric Framework for Secure Health Data Exchange

Mr. Shankar Gadhve[1], Dr. Goldi Soni[2]

[1]PhD Scholar, Department of CSE, Amity University ,Raipur, India. shankar_gadhve@yahoo.com

[2]Assistant Professor, Department of CSE, Amity University, Raipur, India. gsoni@rpr.amity.edu.in

Article History:

Received: *24-09-2024*

Revised: *26-11-2024*

Accepted: *04-12-2024*

Abstract:

Information and communication technology (ICT) has become integral to various facets of society, including healthcare, where it supports digitization and the development of sophisticated solutions. The adoption of digital health technologies, such as electronic health records (EHRs), has accelerated with the increasing volume of patient data. However, traditional EHR systems face critical challenges, including potential data loss, concerns about the confidentiality and integrity of medical records, inefficient clinical data retrieval, and the lack of effective communication among participating hospitals.

To address these limitations, blockchain technology offers a decentralized and secure approach to managing healthcare data. It ensures data integrity, enhances privacy, and facilitates seamless sharing across stakeholders. A patient-centric design for a decentralized healthcare management system has been developed using JavaScript-based smart contracts and blockchain-based EHRs. A functional prototype leveraging Hyperledger Fabric and Composer technologies demonstrates how these innovations can transform healthcare by ensuring data security, interoperability, and efficiency.

Keywords: Blockchain Technology, Block code, electronic healthcare records (EHRs), Concept of hyperledger, Patient centric approach.

I.INTRODUCTION

Block chain technology is a developing list of data, called blocks which are connected with the help of cryptography. Each block can have a cryptographic hash of the previous block, a timestamp, and exchange data. Blockchain technology is resistant to alteration of the information. It is "an open, distributed data that can store between two peers effectively and in an undeniable and lasting manner". Blockchain is a distributed record that is managed by a shared network that follows a standard protocol for certifying new blocks and facilitating inter-node communication. Once recorded, no block's data may be altered backwards without also altering every subsequent block, which calls for approval from the majority of the network. The data in are not immutable, blockchain seems to be secure by design and exemplify. The adoption to distributed computing system with high byzantine that result into non- critical failure [1].

In the present scenario as the world is going through the pandemic situation the society need better healthcare system .It is important to have better healthcare system. As the ill health, casualty, emergencies happen each day and the diseases are expected to be analyzed and treated. A health record is an assortment of clinical information identified with the patient's psychological and physical health, gathered from various sources. [2] Health record comprises of a patient's clinical history, assessment, conclusion, treatment, consequences of lab examination, checking reports. This health records can be verseen both manually and digitally. The conventional technique which is followed in a large portion of the emergency clinics for keeping up records is the manual strategy which incorporates papers and books. This method has genuine limitations, for example, a requirement for huge storage area and recovery of records is difficult.

In the current era computerization of clinical records has become famous as the storage and recovery of the records is easy. However, the chances of manipulation without recognizable proof have become a genuine concern. Another major issue is the maintenance of patient records secretly as the patient can hold the doctor and the hospital flippant for breaking the privacy of his medical record also paper-based records are regularly inadequate, giving rise to unwanted repeat testing and prescription. [3]

II. RELATED WORK

The most recent research on these topics is presented in this section. There have been some blockchain applications for healthcare. The development of blockchain technology has brought forth a variety of Authenticity, data security, data sharing, and data privacy were all addressed at different levels in the blockchain-enabled healthcare applications [4]–[5]that have surfaced to demonstrate the relevance and significance of blockchain in healthcare. An enhanced location- and biometric-based access control system, called the automated validation Internet security protocol and application (AVISPA) for secure EHR, was proposed by Hathaliya et al. [4]. A user-centric approach to validation and integrity was explored by Huang et al. [6], but due to sensor limitations, its scalability was severely constrained. Fan et al. presented in Fan.

MedBlock, a healthcare information system, offered an improved consensus method and uses distributed ledgers for effective access. The combined-attribute and identity-based encryption and signature (C-AB/IB-ES) proposed by Wang and Song (24)[7], which explores intrinsic cryptography, could witness to the reliability and traceability of medical data. It should be noted that the work provided here does not seek to define new consensus mechanisms or encryption schemes, but rather assumes that such mechanisms are already present in the suggested system. An agent-based system for quick retrieval of remotely streamed medical data was presented by Ud- din et al. [8]. The primary concerns of [7] were the protection of privacy and the authentication of authenticity with the signer's identity, which also tracked on-chain and off-chain collaborative storage for effective storage and its verification. But these are the elements that have been taken into account for this effort. A permissioned blockchain-based healthcare system has been presented by Tanwar et al.[9] to increase access to data across healthcare providers using an algorithm called access control policy. Synergy exists between the study published by Tanwar et al. [9] and the newly presented material in this article. But in this effort, two new modules—the insurance and chemical modules—have been included, drastically altering how the entire system interacts. Insurance companies will be able to easily and quickly register, approve, verify, and disburse claims with unquestionable legitimacy thanks to such a plan. There may be other such circumstances in addition to this one. In addition, unlike the works of Tanwar et al.[9] and Bhattacharya et al. [10], the entire design of the work is based on a patient-centric design philosophy where the patients' requirements can be made simple. For instance, the creation of patient records can be made accessible across time, hospitals, and other factors, even after a patient has been discharged. The originality of the work provided below rests in this. Access rights to various stakeholders have also been limited at the architecture level by establishing rules in the network. A few works have investigated patient-centric healthcare systems, as seen in the work by Shen et al. [11]. But none of these functions have either been discovered to offer a complete end-to-end implementation or have shown performance. A few noteworthy outliers include [12].[13], and [4], which supported implementation and performance assessment. The implementations of the suggested frameworks [14] lacked any intelligent approaches, and the business logic was implicit. On the other hand, data privacy, a crucial component of the pre-existing EHR systems, was disregarded in the work by Hathaliya et al. [4]. A patient-centric approach, which is required for emerging healthcare industries, is at the complete other end of the spectrum from the technology-centric frameworks given in [13], [14], [15], and [6].Based on the aforementioned works,

it can be said that despite numerous attempts to implement blockchain-based healthcare systems and constituent technologies, none of them were able to fully account for the following properties: smart contracts, data privacy and security, a patient-centric approach, implementation and performance of their proposed schemes. In order to do this, the current effort has a greater chance of addressing the aforementioned problems while also outlining the implementation and performance assessment of the suggested plan. This article's key contributions are as follows:

III.PROPOSED SYSTEM FRAMEWORK

A blockchain-based patient-oriented healthcare paradigm as mention in Figure 1 It illustrates the many functional elements of the suggested blockchain-based, patient-centered healthcare system. System, with a rectangular box used to represent each. The suggested structure offers a single platform for data sharing among various healthcare system stakeholders. Each participant's ledger for storing health data on the network is the blockchain. Each of these components has access to a blockchain application programming interface (API), which facilitates communication between users and controls the status of the blockchain by dealing with updates to ledgers. The five modules that make up the software architecture are further depicted in Figs. A–D. The application's first module focuses on building secure, decentralised, and immutable EHRs.

1) Development of a simple access control system using the Hyperledger blockchain for the healthcare industry, 2) The development of an approved architectural framework for these applications 3) Comprehensive testing to demonstrate the effectiveness of the proposed plan in terms of different performance measures, including throughput, latency, and resource usage, among others.

The other features are covered by the final module, which also makes patient data more transparent and allows for quick verification of prescriptions as well as retrieval of a patient's whole medical history at one time and access to EHRs for research.

Section III-A provides an overview of Section III-B delineates the participants and resources of the different entities, whereas Section III-C delineates the security layers of the five modules.

Systematic Framework

The functionality of the proposed patient-oriented, blockchain-based healthcare framework—which functions both independently and collectively—is traced through descriptions of all modules, assets, and smart contracts. The patient schedules an appointment via the communication network's client interface and chain code. All stakeholders are given access to the completed transaction over the network to ensure security and robustness to prevent unauthorized attackers from modifying or deleting data. The distributed ledger makes this transaction available together with a date and hash value, making it easier to confirm that a patient is actually present. All authorized stakeholders have access to this medical record, and they may ask questions of other authorized stakeholders through the communication network enabled by blockchain technology.

The patient may also ask questions of the physicians regarding his visit, prescription drugs, reports, clinical diagnoses, and a host of other topics.

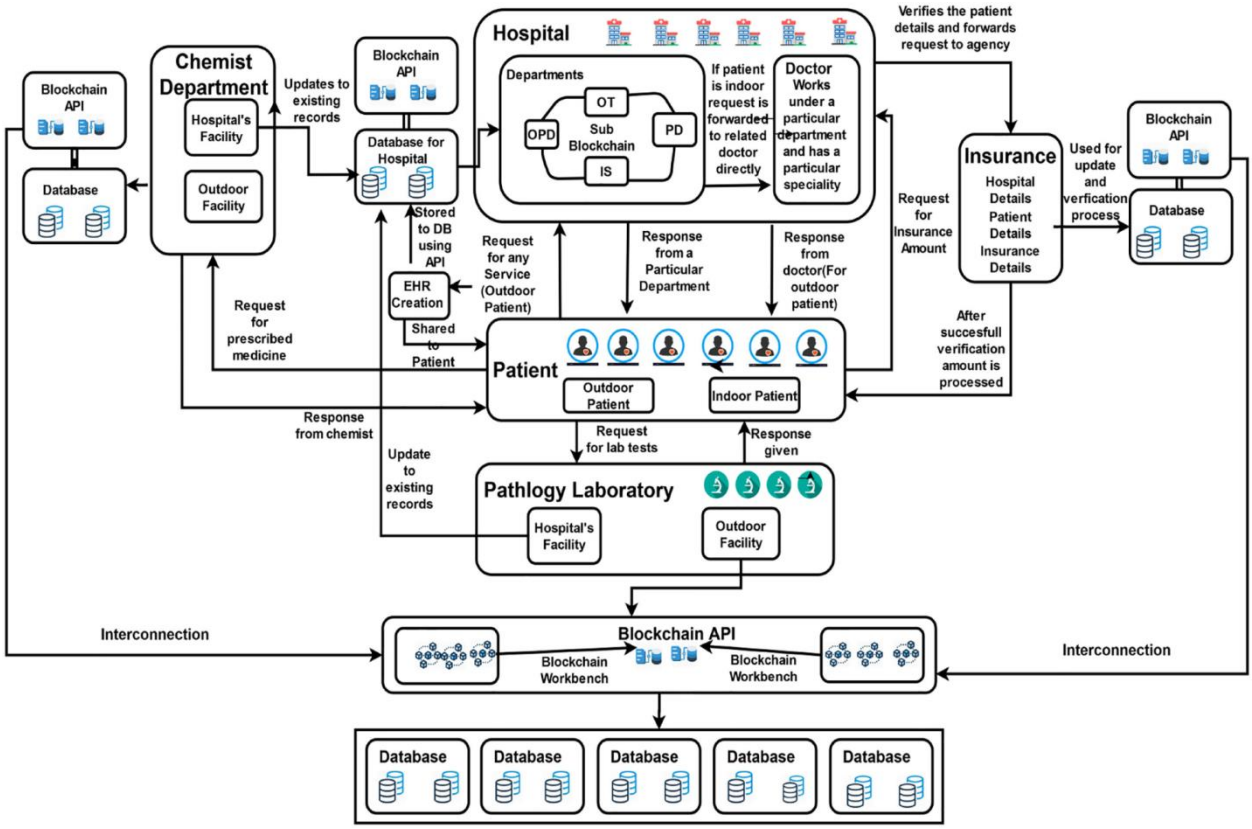

Fig. 1.Patient-oriented architectural framework.

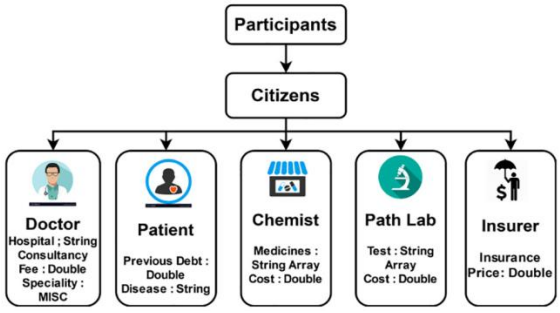

Fig. A. Participant Section

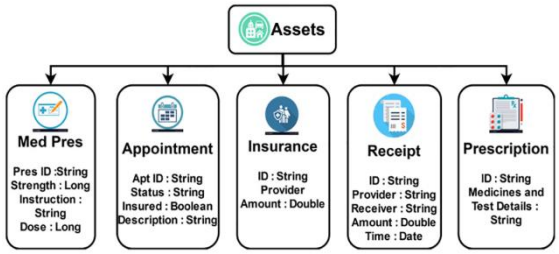

Fig. B. Assets Section

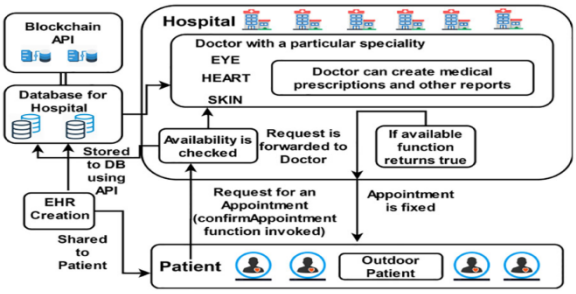

Fig. C. Appointment Section

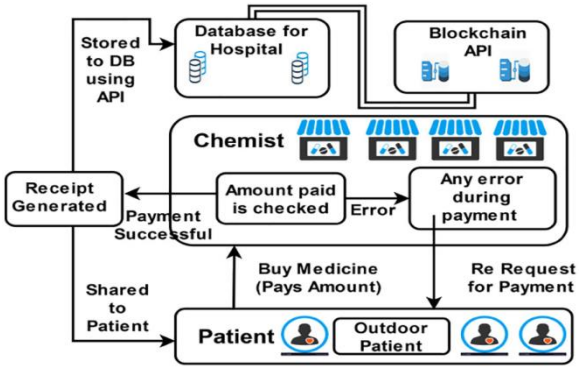

Fig. D. Chemist Section

A. Intended Participants, Assets, and Transactions

A further degree of abstraction for creating technical blockchain-based applications is offered by the hyperledger composer.

Transaction, participants, assets, transactions, and control rules are all entities associated to networks. Together, these elements form a full network. For the envisioned healthcare system, a comprehensive case study has been created, which helps define the participants and resources required to develop the application. It also lists the transactions that need to be completed in order to use a particular capability

1) Participants Section : A participant may be a company or an individual. A person who is a part of the network has the ability to produce assets and trade assets with other users. Fig. A is a list of current application participants.

2) Assets Section: Any material or immaterial object can be considered an asset. A receipt, for instance, is a physical object. You can change these assets by generating new transactions. A list of all the resources connected to our application is provided in Fig. B.

3) Transactions Section: An invoked result that is sent for ordering, confirming, and committing is called a transaction. We have worked on two transactions in our application. When a patient buys medications from a pharmacy, a second transaction is created to generate a receipt. The first transaction is created to confirm the appointment if a doctor is available. Fig.C lists scenarios pertaining to appointment fixing. Here, a non-patient seeks an appointment under a specific illness heading. A doctor who falls into the appropriate category is chosen to schedule a visit. The creation of a receipt is the second feature. A patient receives a receipt if they successfully pay the amount that the chemist has requested. Figure D shows the scenario in its entirety.

C) Roles of Security Layer and Consent Manager

Blockchain security layer provided to secure all the assets like patient registration, Transactional approval, managing record indexing, Doctor Registration, HIP and HIU in fig.2

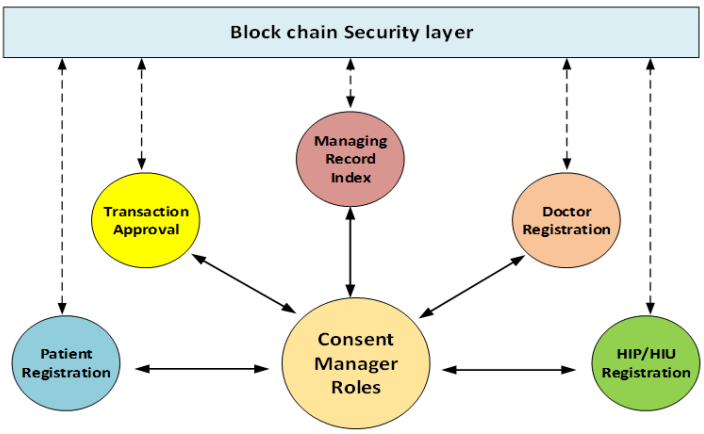

Fig. 2. Blockchain Security Layer

i)Consent Manager

The rationale for data gathering and utilization is referred to as a purpose . It is the primary component of patient permission since the patient chooses to limit the collection and use of their data to a specific scope for a given purpose. In this regard, purpose has its narrow and broad area of coverage, and it can be arranged in a hierarchical tree structure, or "purpose tree," as depicted in Figure 2. The general purpose, which has the broadest scope and is the top node of the tree, contains

its successor purpose nodes. The purpose-tree's connection lines between nodes show how they are related to one another. The shared objective of the organizations for sharing data with one another is represented by given tree.

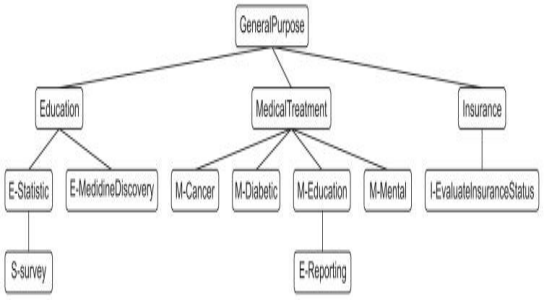

Fig. 3 General Purpose Tree.

The "intended purpose" of data, which governs access to the data, is referred to as the "intended purpose," and the "access purpose" is the reason for accessing the data [16][17]. The intended purpose, which specifies the reason for which the data may be accessed, is typically stated in an advance patient agreement. As a result, when someone requests access to data, they should be clear about why they need it, as this will be compared to the purpose for which the data was collected, as stated in the patient agreement. The system gives the requestor access to the data if the two purposes line up. The consent model states how the patient permission describes the intended-purpose and how a requestor prescribes an access request with the matching criteria. This provides the matching rule.

ii)Consent Model and Consent List

When a patient receives permission for the use of his or her data, it is restricted to the clearly stated intended use. Additionally, depending on their positions, patients typically grant varied levels of consent to healthcare workers. The role reflects the job function or job title in the organization according to the RBAC model [18][19], and it is specified in the role hierarchy. Depending on the job title, access privileges are assigned. It is simpler for data owners to grant access to requestors based on the requestor's role than to refer to the user within the organisation.We modify the RBAC idea and the purpose-based access control system for our consent model. The intended use of data access and the specific user's function are both included in our model's patient permission.

The data access control in our consent model adopts basically white listing with an exception that the patient can make some designated blacklists within a white list.A patient can compile a list of consents for the data in order to react to various requests for data access from various requestors. The patient consent list is created by combining numerous consents with a range of roles and intended uses. Data access is permitted if a request matches one of the listed consents.. In our system, consent together with its hash value and the pertinent patient record metadata are maintained in a blockchain. It can, however, also be kept off-chain with the patient records.

iii). Access Request

A requestor must be properly qualified and specify a suitable reason for the access when requesting access to data. The system grants access within the specified activity on the data after the requestor's role and the access purpose have been successfully validated.

Actually, a requestor sends the system a query with data attributes for a data search together with the access request and any extra useful keywords when attempting to obtain certain patient data for any purpose. Hospital, department, doctor, disease, time and date, demography, and other terms are among the data attributes and keywords. Once the system has the target list, it begins to verify the access request using the patient consent for each of the candidate.

The role and eID of the requestor are often constants among the four basic tuples in our model of patient consent since they are recorded in the organisation or system to which they belong. The only fixed parts in the access request are the access purpose and action. The system uses the eID to verify the requestor's identity and determine their function. If necessary, the system can also consult the participant organizations.

Figure 4 depicts a scenario where a nurse requests access to patient data using the patient's data properties and query phrases. The system generates a list of data as a result, and then verifies that each item in the list has the agreement of the patient. The requestor may have access to the data and take action on it if the access request and the patient's consent are in agreement. She can read data in this case for general purposes, excluding those pertaining to education and mental disease.

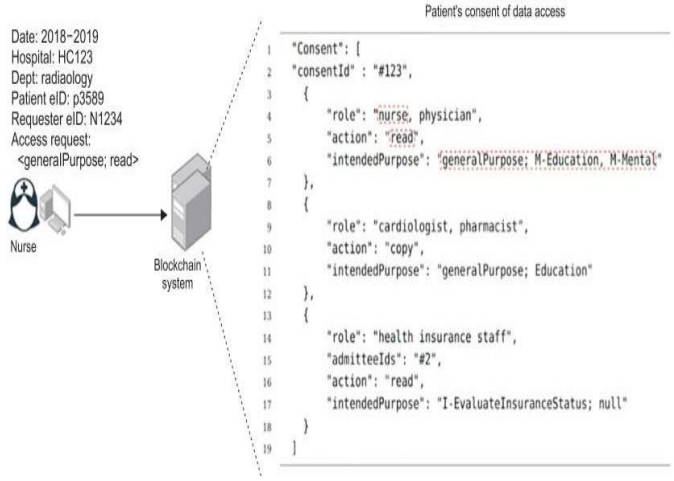

Fig.4 Process of patient's consent list

iv)Blockchain Framework

A blockchain is a collection of blocks that are distributed across network users and contain every transaction in a particular network. As illustrated in Figure 5, each block is connected to the following one [20][21] by the hash value that is recorded in the following block. This structure renders the blockchain unchangeable; if someone wants to change some data in a block, they must replace the blockchains of all other nodes with the forged one and recalculate the block's hash using the forged data, going all the way to the last block

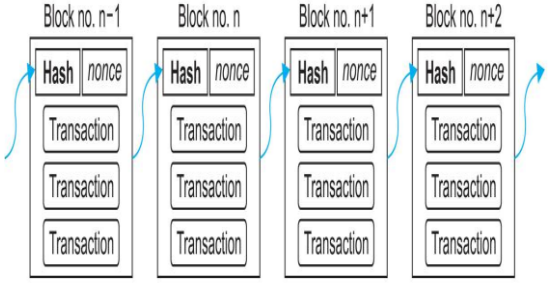

Fig 5 Typical Blockchain Structure

Blockchains are typically split into two categories: public and private, with the latter typically further divided into consortium and private based on the intended usage and characteristics of system participants [22].

We employ HLF [23], a consortium blockchain in which all players are identified in the network of a consortium, as our blockchain platform. A blockchain and a world state database make up the HLF ledger. The former holds the program's chaincodes, or final state of variables, whereas the latter is made up of all transactions that can never be changed after being written.

Additionally, HLF offers the three primary user roles of client, endorser, and orderer. After validating a potential transaction, or so-called proposal, each endorser uses the chaincode to approve it. A block containing endorsed proposals is created by an orderer, distributed among peers, and appended to the blockchain [23].

We use the identical system design from Figure 6 to our earlier studies [24]. It contains a channel designed for sharing patient records between participating hospitals, each of which is linked to a different EHR system. The membership service provider must provide an E-Certificate to each member, and the E-Cert's ID serves as the member's ID in the system that maintains user roles. In that case, it can speak with the participating hospitals. Each proxy of a hospital communicates with other hospitals and is involved in proxy re-encryption to protect patient data.

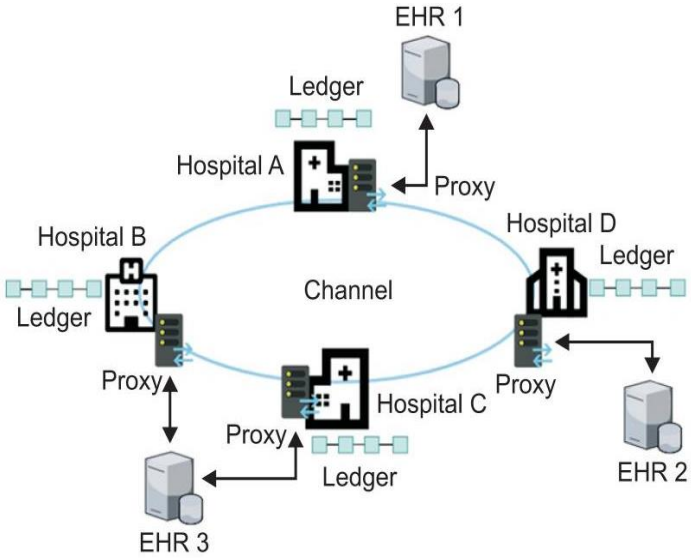

Fig.6 Decentralized Network

IV CONCLUSION

This article provided a foundation for a patient-centered a healthcare system powered by blockchain it addresses the issues of data privacy, authentication, and immutability while also providing a performance analysis and a thorough deployment and execution plan for the suggested scheme. The hyperledger platform was used for the implementation. Hyperledger Calliper was used to evaluate the proposed model's performance and resource usage. Proposed work has presented the design and implementation of an approach towards automation of patients related data transfer through Blockchain Technology. Only the reports of hashes are stored in blockchain for adaptability. Proposed work is totally decentralized in nature dissimilar to the directly accessible concentrated stock piling instrument for information sharing among medical service provider. In addition, the model doesn't depend on third party and offers reasonable assistance to authorized peers. This system

enables the concept of interoperability for healthcare system associated to patient centric information the proposed work is totally decentralized in nature.

References

[1] V M, H., Danai, S., H R, U., &Kounte, M. (2019) Health Record Management through Blockchain Technology. In the Third International Conference on Trends in Electronics and Informatics (ICOEI 2019).
[2] "Preserving Data Confidentiality and Data Integrity in cloud Environment" International Journal of Management, Technology and Engineering(IJMT&E), Vol.09, issue 04, April2019 and ISSN: 2249-7455.
[3] S. Wang, J. Wang and X. Wang,"Blockchain-Powered ParallelHealthcare Systems Based on the ACPApproach", IEEE TRANSACTIONSON COMPUTATIONAL SOCIALSYSTEMS, vol. 5, no. 4, 2018.
[4] J. J. Hathaliya, S. Tanwar, S. Tyagi, and N. Kumar, "Securing electronicshealthcare records in healthcare 4.0: A biometric-based approach," Com-put. Elect. Eng. vol. 76, pp. 398–410, 2019.
[5] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patientagent to manageblockchains for remote patient monitoring," Stud. HealthTechnol. Inf., vol. 254, pp. 105–115, 2018.
[6] H. Huang, T. Gong, N. Ye, R. Wang, and Y. Dou, "Private and secured medical data transmission and analysis for wireless sensing healthcare system,"IEEE Trans. Ind. Informat., vol. 13, no. 3, pp. 1227–1237, Jun. 2017.
[7] H. Wang and Y. Song, "Secure cloud-based EHR system using attribute-based cryptosystem andblockchain," J. Med. Syst., vol. 42, no. 8, 2018,Art. no. 152.
[8] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A patientagent to manage blockchains for remote patient monitoring," Stud. HealthTechnol. Inf., vol. 254, pp. 105–115, 2018.
[9] S. Tanwar, K. Parekh, and R. Evans,"Blockchain-based electronic health-care record system for Healthcare 4.0 applications," J. Inf. Secur. Appl.,vol. 50, 2020, Art. no. 102407.
[10] P. Bhattacharya, S. Tanwar, U. Bodke, S. Tyagi, and N. Kumar,"BinDaaS: Blockchain-based deep-learning as-a-service in Healthcare4.0 applications," IEEE Trans. Netw. Sci. Eng., to be published,doi: 10.1109/TNSE.2019.2961932.
[11] B. Shen, J. Guo, and Y. Yang, "MedChain: Efficient healthcare data sharing via blockchain," Appl. Sci., vol. 9, no. 6, 2019, Art. no. 1207
[12] P. Pasquale et al., "An edge computing, Internet of Things, and Big Data analytics applications for healthcare Industry 4.0," IEEE Trans. Ind.Informat., vol. 15, no. 1, pp. 454–456, Jan. 2019.
[13] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multipleauthorities for blockchain in electronic healthrecords systems," IEEE Access, vol. 6, pp. 11676–11686, 2018.
[14] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain forhealthcare," IEEE Access, vol. 7, pp. 149935–149951, 2019.
[15] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G.Soursou, "Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives," Cryptography, vol. 3, no. 1,pp. 1–16, 2019.
[16] Byun JW, Li N. Purpose based access control for privacy protection in relational database systems. *VLDB J.* 2008;17(4):603–19.
[17] Byun JW, Bertino E, Li N. Purpose based access control of complex data for privacy protection. Proceedings of the 10th ACM Symposium on Access Control Models and Technologies; 2005 Jun 1–3; Stockholm, Sweden. pp. 102–10.
[18] Kabir ME, Wang H, Bertino E. A conditional purpose-based access control model with dynamic roles. *Expert Syst Appl.* 2011;38(3):1482–9.
[19] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. *Computer.* 1996; 29(2):38–47.
[20] Zhang R, George A, Kim J, Johnson V, Ramesh B. Benefits of blockchain initiatives for value-based care: proposed framework. *J Med Internet Res.* 2019;21(9):e13595.
[21] Nakamoto S. *Bitcoin: a peer-to-peer electronic cash system.* Bitcoin.org; 2008.
[22] Viriyasitavat W, Hoonsopon D. Blockchain characteristics and consensus in modern business processes. *J Ind Inf Integr.* 2019;13:32–9.
[23] P. Sajana, M. Sindhu, and M. Sethumadhavan, "On blockchain applica-tions: Hyperledger fabric and Ethereum," Int. J. Pure Appl. Math. vol. 118,no. 18, pp. 2965–2970, 2018.
[24] Tith D, Lee JS, Suzuki H, Wijesundara WM, Taira N, Obi T, et al. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. *Healthc Inform Res.* 2020;26(1):3–12.