How to Cite:
Rajkumar, S., Jeevananth, J., & Kumar, V. R. (2022). Hospital health monitoring on cloud using blockchain technology. *International Journal of Health Sciences*, *6*(S6), 1350–1359. https://doi.org/10.53730/ijhs.v6nS6.9746

Hospital health monitoring on cloud using blockchain technology

Rajkumar S.
Assistant Professor in Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu, India
Email: rajkumars@ksrct.ac.in

Jeevananth J.
Students in Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu, India
Email: jeevaslm2000@gmail.com

Vasantha Kumar R.
Students in Computer Science and Engineering, K.S.Rangasamy College of Technology, Tiruchengode-637 215, Namakkal District, TamilNadu, India
Email: vasanthakumarraj2018@gmail.com

***Abstract*---**Block chain is being used to invest in innovation and address trust issues more effectively. It is at the front of a wide-ranging hunt for position to develop and commercial breakthroughs. A wide range of businesses could profit from blockchain-based technology solutions. It demonstrates how blockchain technology could be utilised in the healthcare industry to share medical data and analysis among institutions and research organisations based on patient-defined access policies. In order to protect confidential data, the project involves the use of two types of chains: A private one is the side chain it will keeps the information about the patients, and A public one is the main chain it which stores information about patients health data marked with a ID temporary. Hospital Health Monitoring deals with the hospital branch and patients management. We are using the cloud computing for delivers the convenient, on-demand access and sharing the data, applications and hardware over the internet, it provides the unlimited infrastructure to store and execute the patient data and program. The project applies that blockchain technology which is a decentralized network, where the entire database of health care management is being handled by many users. All of the records are hashed as blocks and added to the blockchain, allowing for proof of contract for all previous and current transactions. The entire transactions are said to be valid using the

above concept. The application for Hospital Enterprise the designed to using Microsoft Visual Studio .Net 2010 as frontend. The coding language is used in that project is Visual C# .Net. The web technology used for project is ASP .Net 2010. MS-SQL Server 2008 is used for backend database.

***Keywords*---**hospital, health monitoring, blockchain technology.

Introduction

Now-a-days People's daily lives are increasingly taking on digital forms. It also relates to hospital administration, where a range of health-related problems are generated and information from different sources by hospitals and clinics. During their life time, where people want a interact with medical specialists, Doctors that storing data in their Database systems, It lead to a fragmented system they are not interconnected. Blockchain technology that supports the sharing of values. In recent times, it was used in a variety of areas, the most prominent of which would be finance. Blockchain is a technology that preserves all of the activities that have been completed. It creates a continually increasing list of sorted records called blocks using a distributed, friend network. Every block contains a set of sign a transaction and is validated for the network itself, by means of a consensus mechanism. That copies of the blockchain is distributed on each participating node in the networks. Blockchain is considering a permanent database because the implemented algorithms prevent alteration in the already stored information.

Any system that handles and stores medical data must follow current legislation, like the European General Data Protection (GDPR) EU 2016/679 on personal data protection. GDPR applies to any institution based inside the EU which receives personal or health data, as well as any corporation situated outside the EU which processes the data of EU individuals. Because most blockchain implementations are built as an immutable ledger, applying such restrictions in blockchain technology is extremely challenging. This proposal suggests a revolutionary health-care information technology system that places a premium on privacy. Users are acknowledged as data owners who have complete control over their data. They can apply various security policies, such as sharing data with specific clinics or institutions and can contribute anonymously to certain statistics. The blockchain employs public key cryptography to construct an immutable, append-only, time-stamped chain of material. Two types of blockchains are proposed in this project design: a public mainchain and a private sidechain. Every node has a version of the process from the initial, or both blockchains, depending on what type of network (trusted or untrusted).

The content of the nodes is built only by a set of links to health data, permissions, and other auxiliary information, because to privacy concerns and the vast volume of data supplied by all collaborating institutions and devices. The data (medical analysis) could be stored locally or on the cloud, depending on the institution that generated it. A number of blockchain-based solutions have been proposed in the healthcare industry to integrate clinics, doctors, and patients in order to provide better quality services in a timely manner. In general, public key infrastructure is

used to represent individuals' digital identities in a health care blockchain–based architecture. To ensure that people with the corresponding private key may log in, identities are stored directly in the blockchain. These identities are established for clinicians to help them share data and make better decisions for their patients, but they violate data privacy laws. This article provides an overview of related research in the field of blockchain-based healthcare solutions. It also goes into the proposed system design in depth, including the transactions and security measures used. Patients may be assured that their data, as well as their privacy, is well safeguarded with this strategy. Patients come first in the proposed system, therefore medical data can only be accessed through security policies, and policy transactions can be retrieved through a publicly available blockchain. However, because the public blockchain only stores the patient's temporary ID, it cannot be used to trace the patient's medical treatment history. Furthermore, patients are regarded owners of their own medical analyses, with complete authority over them, even if they are held in clinic datacenters, according to the system design.

Literature Review

Data sharing that is both secure and scalable is critical for collaborative healthcare decision making. However, traditional clinical data efforts are frequently soloed, creating barriers to efficient information interchange and obstructing appropriate treatment decisions for patients. This paper makes four contributions to the research of utilising blockchain technology to clinical data sharing in the context of technical requirements outlined in the Office of the National Coordinator for Health Information Technology's "Shared Nationwide Interoperability Roadmap" (ONC). They began by looking at the ONC regulations and how they affect blockchain-based solutions. Second, they introduced FHIR Chain, a blockchain-based architecture meant to meet ONC criteria by encapsulating the HL7 Fast Healthcare Interoperability Resources (FHIR) standard for shared clinical data. Third, they present an FHIR Chain-based decentralised software that uses digital health IDs to authenticate users in a case study of collaborative decision making for remote cancer care. They also emphasised significant takeaways from their case study.

Secure and scalable data exchange is required to make effective joint treatment and care decisions for patients. Throughout their lives, patients visit a variety of healthcare practitioners' offices. These service providers must be trustworthy.It can exchange health information on their patients in a fast and secure manner to guarantee they have the most up-to-date knowledge about their health status. For example, in Berman and Fenaughty's telemedicine practise, where patients are diagnosed and treated remotely, the ability to safely and scalably communicate data is critical for facilitating clinical conversations regarding remote patient cases. The sharing of data aids in the improvement of diagnostic accuracy. By obtaining confirmations or recommendations from a number of medical specialists, Castaneda et al are able to avoid shortcomings Singhetal and drug errors. Kaushaletal. Schiffetal is a place in Germany where you can find a lot of different Similarly, intelligence and insights gathered from a variety of sources Taichmanetal.Warren Geifmanetal assists professionals in better understanding their patients' requirements and, as a result, providing more effective in-person

and remote treatments. Data sharing is especially critical in cancer care, where tumour boards are made up of doctors with various expertise.
These committees meet on a regular basis to review cancer cases, share information, and work together to develop appropriate treatment and care programmes for each patient Gross. Telemedicine Ricke and Bartelink are also being used to set up regional virtual tumour boards. The Bitcoin blockchain Nakamoto, which is a public distributed ledger meant to allow financial transactions using the Bitcoin cryptocurrency, is the most well-known implementation of blockchain. All transactions are disseminated to each network maintainer node (referred to as a "miner") for verification and admission onto the blockchain in this peer-to-peer blockchain. As indicated in Figure 1, these miners validate available transactions and organise them into blocks.

Miners then compete to solve a computationally costly cryptographic puzzle known as "proof-of-work," in which a targeted hash value connected with the chain's last valid block is determined. The first miner to solve this riddle is rewarded (in the form of Bitcoin) and their block of validated transactions is added to the blockchain sequence. The Bitcoin blockchain achieves consensus (agreement on the shared state and order of transactions) by incentivizing miners to contribute powerful hardware and electricity to the network in exchange for small amounts of crypto currency and discouraging rogue actors from attempting to manipulate or maliciously control the system through the "proof-of-work" process outlined above. Cryptography protects a block's transaction history against manipulation after it is uploaded to the blockchain. The Bitcoin blockchain is the most extensively used distributed ledger technology. When specific circumstances are met, smart contracts allow code to run independently. They can also save data as internal state variables and build custom functions to manipulate or update that data. Smart contract operations are published as transactions and thus occur in a globally sequential manner, as seen in Fig. 1

Figure 2.1: The Blockchain Structure: A Permanently Growing And Immutable List Of Ordered And Validated Transactions

Miners on the Ethereum blockchain can verify that these operations are deterministic and legitimate. The methods explained above make a blockchain decentralised and unchangeable, eliminating the need for a single authority. These characteristics make blockchain technologies appealing to certain health IT researchers and practitioners as a way to improve therapeutic interactions while maintaining patients' privacy. They concluded by describing the FHIRChain prototype they created to provide patients with more collaborative healthcare decision support through the use of blockchain technology and the FHIR data standards. Their FHIRChain design addressed five key requirements provided by the ONC interoperability roadmap, including user identifiability and authentication, secure data exchange, permissioned data access, consistent data formats, and system modularity, and was enhanced by the use of public key cryptography. The important lessons they gained from building and implementing the D App based on FHIR Chain are as follows: The FHIR Chain can enable secure, decentralised storage for Meta data and audit logs. By utilising its blockchain component as a decentralised repository of critical reference

information as secure entry points into such databases, FHIR Chain alleviates proprietary vendor-lock inherent in traditional health IT systems.

It allows doctors to share clinical data without establishing trust, offering secure and scalable collaborative care decision support. Furthermore, each public key issued for a user is maintained in the blockchain via a smart contract that links healthcare participants' digital identities to their public keys. Permission authorizations generated between those participants are also documented in a smart contract, resulting in a traceable permission database with a history of data exchange audit log. Storing this information on the blockchain assures that our programme has no single point of failure or record corruption, and that it is always accessible to healthcare participants. FHIR Chain enables data interchange without requiring data to be uploaded or downloaded, preserving data ownership. The FHIR standards provide resource APIs that allow users to refer to specific pieces of structured data while retaining ownership of the original material. FHIR Chain creates lightweight reference links to siloed databases and exchanges these pointers via the blockchain component instead of actual data by adopting FHIR and combining it with blockchain technologies. This strategy can help telemedicine clinics or clinics in remote locations overcome network limits by allowing scalable data exchange without requiring data to be uploaded to a centralised repository where it can be shared and accessed by others. Furthermore, this strategy decreases the danger of data compromise and assures that original data ownership is maintained. To grant data access, the reference pointers are encrypted with the intended recipient's public key, i.e., digital identity. When the data is successfully verified (i.e., reference pointers are appropriately decrypted), it is downloaded directly from the source and presented to the user in the proper manner.

Public key cryptography can help manage digital health identification while exchanging data. FHIRChain generates public keys, which serve as digital health identities for each participating care entity (provider or organisation administrator). This technique has the following advantages: simple authentication, as a clinician simply needs to supply their private key connected with their identification, Integrity, because FHIRChain can easily check that the exchanged reference pointers were provided by the signed provider and have not been modified, and Remedy for lost or stolen keys, because a new key can be readily established to replace the old key and associated with the same user. However, in a general healthcare situation, adopting digital identities for patients has a disadvantage.

Furthermore, each public key issued for a user is maintained in the blockchain via a smart contract that links healthcare participants' digital identities to their public keys. Permission authorizations generated between those participants are also documented in a smart contract, resulting in a traceable permission database with a history of data exchange audit log. It is difficult to share healthcare data among institutions. Compatibility may be hampered by distinct data architecture, while data comprehension is hampered by disparate healthcare terminology. Even if structure and semantics could be agreed upon, there are problems about data security and consistency. Cyber-attacks are attracted to centralised data storage and authority providers, and maintaining a consistent

image of the patient record throughout a data sharing network is difficult. A Blockchain-based solution to exchanging patient data is presented in this paper. This strategy foregoes a single centralised source of confidence in favour of network consensus, which is predicated on structural and semantic interoperability proofs. Sharing healthcare data between institutions is a difficult task that has the potential to improve research and clinical efficacy significantly.

First and foremost, institutions are typically hesitant to share data due to privacy concerns, as well as a fear of giving others a competitive advantage by doing so. Next, even if privacy concerns could be resolved, there is no widespread agreement on the technical infrastructure required to enable such a mission. Finally, healthcare data is complicated, and transmitting it across institutional borders necessitates a shared knowledge of both data formats and meaning. Even if data can be shared efficiently and securely, if interoperability difficulties are not addressed, the data's utility will be limited. Despite proof of the high value of healthcare data exchange, the challenges listed below remain significant roadblocks.

Proposed Methodology

The suggested solution uses blockchain technology to store records in a website database. All transactions or digital events are recorded and shared in this database or public ledger. Every transaction in the public ledger is double-checked by a majority of the system's members. Data could never be deleted once it was entered. It does, however, have a precise and verifiable record of every single transaction that has ever taken place. The history of transactions can be tracked, such as which patients are seen by which doctors, what prescriptions are written for them, and how much money they receive. Storage transactions and policy transactions are preserved in the main blockchain. Following a patient's encounter with a medical institution, storage transactions are made. Following the patient's approval, information about her or his medical analysis is published on the mainchain, and the results are recorded in the clinic's internal database.

So, just a reference (pointer) to the patient's health data is stored in the mainchain, whereas the data is securely stored in dedicated storage infrastructure, protected by suitable security methods, both in terms of access control and anomaly detection. Each mainchain transaction includes a one-of-a-kind temporary ID that can be used to identify the patient in a discreet manner. Only trusted nodes manage and disseminate the sidechain. Untrusted nodes are denied access to this ledger to protect personal information. Because operations are carried out in encrypted message format, third-party cloud storage space is kept more secure. The present technology makes it easy to consolidate data for inter-branch patient visit information. Personal information is protected to the greatest extent possible because the information saved on the sidechain is required to link the patients' temporary ID found within mainchain transactions to the patients' true identity.

Because the mainchain is a permissioned blockchain, any entities can send requests and browse the ledger, but only trusted nodes can add new blocks, the blockchain is based on majority confirmation.Database (With patient master data

only) management in hospital Server. The hospital server is kept up to date with the results of their daily transactions. Only unencrypted data should be stored in the data owner's (hospital) space because the server requirements are minimal (because the cloud manages all data (here the hardware resources are kept to a bare minimum)). This is done to ensure data integrity across many cloud areas that have been duplicated redundantly. Both venues will hold data that is heavily encrypted.

Add Doctor

Doctor information such as doctor ID, name, address, city, phone number, email address, age, gender, qualification, experience, specialisation, and password are entered by the administrator.

View Doctors

The doctor's ID, name, address, city, phone number, email address, age, gender, qualification, experience, and specialisation are all visible to the administrator.

Patient Registration

The administrator enters information such as the patient's ID, name, address, city, phone number, age, gender password, and symptoms.

Database (With all regular visits, prescription data) Management in Cloud Space

The cloud server is kept up to date with the data of their daily visits, prescriptions, and receipts. Data is managed by the cloud provider (here the hardware resources are kept to be maximum). Users who As the number of people who have access to data grows, different privileges must be allocated to them in order to avoid unauthorised data change or theft. All users (except the content owner) are unable to examine the actual data because the data is encrypted and stored.

Patient visit entry/view

Module allows the user to enter and examine information such as the patient's ID, doctor's ID, date, disease, treatment, charge, and other details.

Patient prescription entry/view

In that module allows the user to enter and view patient and doctor IDs, dates, tablets, tablet advice, and other information.

Hospital and Patient Login Provision

Different privileges are provided to different users so that they can view and access data as needed. The key arrangements are such that the content owner has complete control over all material, while the users can only view it.

Login

The 'Admin' table contains information on the administrator's login and password. The administrator logs into the website using one of the username and password.

Blockchain

To protect personal data we are using two types of nodes: trusted and untrusted, as well as two types of blockchains, to secure personal data. Depending on their degree of trust, nodes can access either the public mainchain (untrusted nodes) or both blockchains, specifically the mainchain and the private sidechain (trusted nodes) (trusted nodes). Trusted nodes (authorised medical institutions) validate transactions and decide whether or not a new transaction should be added into the blockchain; and untrusted nodes (all other entities wishing to access medical data).This module creates the solution which involves the existence of two types of ledgers: a mainchain that is accessible by all the nodes and a sidechain that is accessible only by the trusted nodes. Each type of blockchain is represented as an immutable linked list. In that module creates a solution that includes two types of ledgers: a mainchain that all nodes can access and a sidechain that only trustworthy nodes may access. An immutable linked list represents each form of blockchain.

Conclusion

It is expected that nearly all of the system objectives set forth at the start of software development have been met, and the project's implementation phase has been completed. The system has been put through its paces and is producing positive results. The processing methods are straightforward and organised. The procedure of preparing blueprints was overlooked, which might be taken into account for future application modifications. The project efficiently saves and retrieves data from the cloud database server. To ensure the security of the records, they are encrypted and decoded when needed.

Scope for future development

Future upgrades should include the following. The records can be used by multiple applications if the programme is implemented as a web service. The next time you come to see me. Patients can receive information by SMS. During the implementation, the website and database can be hosted in the cloud.

References

1. Peng Zhang, Jules White, Douglas C. Schmidt, Gunther Lenz, S. Trent Rosenbloom: “FHIR Chain: Applying Blockchain to Securely and Scalarly Share Clinical Data”. Elsevier, 2018.
2. Kevin Peterson, Rammohan Deeduvanu, Pradip Kanjamala, Kelly Boles: “A Blockchain-Based Approach to Health Information Exchange Networks”. ONC/NIST Use of Blockchain for Healthcare and Research Workshop, 2016.
3. Dubovitskaya A. et al. “Secure and trustable electronic medical records

sharing using blockchain:, Proceedings of the AMIA 2017, American Medical Informatics Association Annual Symposium; Washington, DC, USA. 4–8 November 2017.
4. X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC), Montreal, QC, 2017, pp. 1-5. doi: 10.1109/PIMRC.2017.8292361
5. M. A. Rahman et al., "Blockchain-Based Mobile Edge Computing Framework for Secure Therapy Applications," in IEEE Access, vol. 6, pp. 72469-72478, 2018. doi: 10.1109/ACCESS.2018.2881246
6. Berman M, Fe naughty A. Technology and managed care: patient benefits of telemedicine in a rural health care network. Health Econ 2005;14:559–73.
7. Castaneda C, Nalley K, Mannion C, Bhattacharyya P, Blake P, Pecora A, et al. Clinicaldecision support systems for improving diagnostic accuracy and achieving precision medicine. Journal of Clinical Bioinformatics 2015;5:4.
8. Singh H, Giardina TD, Meyer AN, Forjuoh SN, Reis MD, Thomas EJ. Types and origins of diagnostic errors in primary care settings. JAMA Intern Med 2013;173:418–25.
9. Kaushal R, Shojania KG, Bates DW. Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. Arch Intern Med 2003;163:1409–16.
10. Schiff GD, Hasan O, Kim S, Abrams R, Cosby K, Lambert BL, et al. Diagnostic error in medicine: analysis of 583 physician-reported errors. Arch Intern Med 2009;169:1881–7
11. Buterin V, et al. Ethereum white paper; 2013.
12. Johnston D, Yilmaz SO, Kandah J, Bentenitis N, Hashemi F, Gross R, et al. The general theory of decentralized applications, dapps, GitHub, June 9; 2014.
13. Yaorong Ge, David K Ahn, Bhagya Shree Unde, H Donald Gage, and J Jeffrey Carr. Patient-controlled sharing of medical imaging data across unaffiliated healthcare organizations. Journal of the American Medical Informatics Association, 20(1):157–163, 2013.
14. Chris Clifton, Murat Kantarcio˘glu, AnHai Doan, Gunther Schadow, Jaideep Vaidya, Ahmed Elmagarmid, and Dan Suciu. Privacy-preserving data integration and sharing. In Proceedings of the 9th ACM SIGMOD Workshop on Research Issues in Data Mining and Knowledge Discovery, pages 19–26. ACM, 2004.
15. Joshua R Vest and Larry D Gamm. Health Information Exchange: persistent challenges and new strategies. Journal of the American Medical Informatics Association, 17(3):288–294, 2010.
16. Paul C Tang, Joan S Ash, David W Bates, J Marc Overhage, and Daniel Z Sands. Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. Journal of the American Medical Informatics Association, 13(2):121–126, 2006.
17. Jan Walker, Eric Pan, Douglas Johnston, Julia Adler- Milstein, et al. The value of health care information exchange and interoperability. Health Affairs, 24:W5, 2005.
18. L. J. Kish and E. J. Topol, “Unpatients-why patients should own their medical data,” Nature biotechnology, vol. 33, no. 9, pp. 921–924, 2015.

19. J. H. Clippinger, “Why Self-Sovereignty Matters,” https://idcubed.org/chapter-2-self-sovereignty-matters/,[Online; accessed 7-March-2017].
20. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
21. X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, “Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability,” in International Symposium on Cluster, Cloud and Grid Computing. IEEE/ACM, 2017.
22. D. K. Tosh, S. Shetty, X. Liang, C. A. Kamhoua, K. A. Kwiat, and L. Njilla, “Security implications of blockchain cloud with analysis of block withholding attack,” in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, ser. CC Grid ’17. Piscataway, NJ, USA: IEEE Press, 2017, pp. 458–467. [Online]. Available: https://doi.org/10.1109/CCGRID.2017.111
23. T. O. of the National Coordinator for Health IT (ONC), the National Institute for Standards, and T. (NIST), “Use of blockchain in healthcare and research workshop,” 2016. [7] C. Cachin, “Architecture of the hyper ledger blockchain fabric,” in Workshop on Distributed Cryptocurrencies and Consensus Ledgers, 2016. [8] R. C. Merkle, “
24. Gede Budasi, I. & Wayan Suryasa, I. (2021). The cultural view of North Bali community towards Ngidih marriage reflected from its lexicons. *Journal of Language and Linguistic Studies*, *17*(3), 1484–1497
25. Suryasa, I. W., Rodríguez-Gámez, M., & Koldoris, T. (2022). Post-pandemic health and its sustainability: Educational situation. *International Journal of Health Sciences*, *6*(1), i-v. https://doi.org/10.53730/ijhs.v6n1.5949
26. Parmin, P., Suarayasa, K., & Wandira, B. A. (2020). Relationship between quality of service with patient loyality at general polyclinic of kamonji public health center. International Journal of Health & Medical Sciences, 3(1), 86-91. https://doi.org/10.31295/ijhms.v3n1.157