International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Using Blockchain in healthcare services

Prof. Dr. Shankar Patil[1], Bhushan Babar[2], Prathmesh Sable[3],Yogesh Sonawane[4]

[1]*Prof Dr. Shankar Patil, Professor, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India*
[2]*Bhushan Balasaheb Babar, Student, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India*
[3]*Prathmesh Madhukar Sable, Student, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India*
[4]*Yogesh Rajendra Sonawane, Student, Dept. of Information Technology, Bharati Vidyapeeth College of Engineering, Maharashtra, India*

Abstract - *Everyone in this world is having some health issues. In today's world, everyone wants the privacy of their health. nobody wants to expose their weakness to others. To tackle this problem Electronic health records (EHR) Came into the picture. but some authors have identified problems in EHR like financial issues, loss of data integrity, security concerns, and some other consequences.In this paper, we will discuss how blockchain will replace EHR and other systems regarding health care records. Blockchain is a type of register that keeps a record of every transaction; each transaction generates a hash value and each block refers to the previous block together they make the blockchain. As blockchain is gaining popularity in the healthcare domain. blockchain guarantees privacy, storage, security, control, and managing of patient health records*

1. INTRODUCTION

Current healthcare systems are struggling to provide desirable outputs. In this pandemic of COVID-19 healthcare systems do not perform as well making vaccination, disease monitoring, child health, etc. current healthcare systems process slow or mainly fail to deliver these outputs. Blockchain is the answer to this all. Blockchain was introduced by a person (Group of people) using the name Satoshi Nakamoto's name is still unknown to date. Blockchain was invented for ***bitcoin, the*** first digital currency to solve the problem of double-spending without any need for any centralized server/system. Before this advanced technology medical institutes and health departments were using paper to note down the patient details and other classified details about any vaccine or disease. This leads to a loss of integrity and lots of mistakes (i.e. Due to handwritten documents were written by humans).due to this healthcare and other departments were forced to shift to EHR systems. Which were more secure and cost-effective than paper-work. EHR was the answer to every problem in the healthcare sector. Which were used to store patient's details in acentralized server, billing, lab testing, sharing patient's details with other hospitals or doctors, etc. this EHR system was used around the globe by almost every health sector. As the EHR system is gaining popularity around the globe it has some major issues regarding its use and data handling. Users were having an issue with the EHR system as it was not much user-friendly and it was not stable. The EHR system was also having some major issues like Sharing of data was a bit too difficult, research [4] was done to know the data leak or breach in the EHR system around 173 million*(approximately)* patient's details were compromised since October 2009. In a recent study, the biggest healthcare data breach of 2018(so far) [5] analyzed that attackers will continue to breach data from this industry.As EHR systems are not so reliable and safe, the Healthcare industry should move to the new system as soon as possible and BLOCKCHAIN can be the answer as to its more reliable and safe and user-friendly behavior. As both doctor and patient's confidential data are safe and easy to share.

2. LITERATURE REVIEW

(khzer et al) They have presented the current research on healthcare using distributed ledger technology with some possible medical use cases where blockchain technology can play a significant role to make the process efficient. They discussed various issues of the healthcare management system and how they could be resolved using blockchain technology. They have also proposed the IoMT delivery system using networking protocols.

Healthcare Data Security and Privacy using Blockchain (Litchfield et al). By using blockchain improved the security and privacy of healthcare data and overcame issues. They discussed issues regarding healthcare data security and privacy and suggested blockchain to overcome these issues besides surveying healthcare issues.

(Rouhani et al) They have used an instance of the Hyperledger platform for patient-controlled healthcare data management. They came up with an approach to address the limitations of permission and permissionless

blockchain.

(Wu and Tsai) They suggested using a distributed system for healthcare data management and establishing regulations for healthcare data. They did a literature review on healthcare management systems and proposed two algorithms for providing network security.

(Anuraag et al) In their study, they included various types of studies and most of the work among this study was discussing the potential benefits and limitations of blockchain technology for healthcare without being provided any proof or system evaluation. They studied blockchain as a way to manage healthcare information efficiently.

(Mian Zhang and Yuhong Ji) They have suggested that Most people realize and understand the hard problems in the current healthcare industry. However, blockchain is no elixir. To power blockchain applications, we need to continuously improve low-level blockchain protocols that are equivalent to the backbone of current internet services such as TCP/IP and HTTP. We also need to improve trust and decision-making processes in blockchain so that the system is more scalable with higher transaction throughput without sacrificing security. One way that has been used is that blockchain networks could assign more weight to trusted nodes to expedite the computation of the block.

(T. Mikula and R. H. Jacobsen) authors explain that Blockchain has proved itself to be tamper-resistant and secure. It is increasingly getting attention from companies changing from centralized to decentralized systems. This paper proposes a system for identity and access management using blockchain technology to support authentication and authorization of entities in a digital system. A prototype demonstrates the application of blockchain in identity and access management using the Hyperledger Fabric framework. It provides a proof of concept based on a use case concerning Electronic Health Records from the healthcare domain where an immutable and auditable history is desired for data concerning patients. Basic authentication and authorization operations can execute in 2-3 seconds with an initial size of blockchain of about 3.8 MB covering physicians in Denmark

(M. Zarour et al) They explain that Blockchain technology is among the most significant developments and revolutionary innovations of the Information Technology industry. It corners a crucial space in the present digital era and has already made significant differences in human life. Moreover, it is anticipated that Blockchain technology will improvise the existing IT facilities in the next several years in many domains. Recent technological developments are allowing for a major advancement in the Healthcare sector. Information security and accessibility are critical considerations for the integration and communication with Electronic Healthcare Record (EHR) systems when sharing private medical information. In this context, selecting the most effective blockchain model for secure and trustworthy EHRs in the healthcare sector requires an accurate mechanism for evaluating the impact of different available blockchain models for its features. The present study uses a scientifically proven approach for evaluating the impact of blockchain technology and provides a novel idea and path to future researchers. This research analysis garnered the feedback of 56 domain experts in healthcare management for assessing the impact of different blockchain models. To eliminate the ambiguities that arose due to multiple opinions of these experts and for the externalization and organization of information about the selection context of the blockchain model, the study used a decision model. The fuzzy Analytic Analytical Network Process (F-ANP) method was used to calculate the weights of the criteria, as well as the Fuzzy-Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) technique, was used to evaluate the effect of alternative solutions. Further, the results obtained through this empirical investigation will be an instrumental reference for choosing the most appropriate Blockchain model for maintaining breach-free EHRs.

(Y. Wehbe, M. A. Zaabi and D. Svetinovic) they state that Healthcare-related technology has been growing exponentially, from electronic healthcare records (EHRs) and personal health trackers to population health management tools. Currently, data from these sources is largely archived, analyzed separately, or using only cursory integration with other data sources. In this study, we propose a coupled AI-Blockchain EHR management system. The goal is to provide a platform that leverages blockchain and artificial intelligence (AI) for (i) secure EHR management, (ii) efficient data integration, and (iii) reliable computer-aided diagnosis. A goal-oriented modeling approach with the Constrained Goal Model (CGM) is used to elicit the system requirements. Questionnaire results for a case study in Abu Dhabi, UAE served for model validation and refinement for maximizing the number of system users

(Khandakar Ahmed, Hua Wang, Frank Whittaker, Zhenxiang Chen) The privacy of Electronic Health Records (EHRs) is facing a major hurdle with outsourcing private health data in the cloud as there exists the danger of leaking health information to unauthorized parties. EHRs are stored on centralized databases that increase the security risk footprint and require trust in a single authority that cannot effectively protect data from internal attacks. This research focuses on ensuring the patient's privacy and data security while sharing the sensitive data across the same or different organizations as well as healthcare providers in a distributed environment. This research develops a privacy-preserving framework viz Healthchain based on Blockchain technology that

maintains security, privacy, scalability, and integrity of the e-health data. The Blockchain is built on Hyperledger Fabric, a permissioned distributed

3. EXISTING TECHNOLOGY

Technical and social framework that permits data to maneuver electronically between organizations. Using associate degree EMR to browse and write a patient's record isn't solely doable through a digital computer however, betting on the kind of system and health care settings, may additionally be doable through mobile devices that area unit handwriting capable, tablets and smartphones. Electronic Medical Records might embody access to private Health Records (PHR) that makes individual notes from associate degree EMR pronto visible and accessible for customers

3.1 DRAWBACKS OF EXISTING SYSTEM

- Each care setting functions otherwise, typically in vital ways that. it's tough to make a "one-size-fits-all" EHR system.
- Additionally, issues regarding long storage of electronic health records are sophisticated by the chance that the records may sooner or later be used longways and integrated across sites of care. Records have the potential to be created, used, edited, and viewed by multiple freelance entities.
- These entities embrace, however don't seem to be restricted to, medical aid physicians, hospitals, insurance firms, and patients.
- Possibility of information breach of user's

4. PROPOSED SYSTEM

- Patient can access his/her data anytime anywhere through the web portal.
- Patient can grant/revoke access to Doctors. Doctor can access the records of the patients who he/she is treating anytime.
- Doctor needs to request other patients if they wants to access their records.
- Patients can grant access to doctors by sharing special key/OTP with doctors.
- The records are encrypted and stored in the form of Hash values in the ledger.

5. HARDWARE & SOFTWARE REQUIREMENT

- **Hardware Requirement**
  - 4 GB RAM.
  - 200 GB HDD.
  - Intel 1.66 GHz Processor Pentium.
- **Software Requirement**
  - Operating System: Microsoft Windows 7,8,10.
  - Microsoft . Net Framework
  - Visual Studio 2013
  - Database : MS Sql 2008

6. IMPLEMENATION

We are developing a reliable and more secure healthcare system by implementing blockchain technology in our web application. We have developed this system using ASP.net for the front end and SQL for the database.

The basic work of this system is to add patients as well as doctor's details in which blockchain will be implemented.

Patients can access their data anytime, anywhere. Another feature of this system is that patients can grant or revoke access to doctors for viewing or adding their details. The records are ***encrypted*** and stored in the ***hash*** format in the ledger. Once data added cannot be altered it makes integrity and availability of data.

- **FRONT-END (HTML,CSS)**

1. First, we have designed the front end using HTML(hypertext markup language) and CSS(cascading style sheet).
2. Every form inside the web portal is designed using HTML and CSS.
3. Patient module, doctor module, view report, login, logout,new register, etc are done using HTML and CSS

- **DATABASE**

1. Next, we have created a database for storing various data intothe database.
2. SQL Server **2008** Express is a free edition of SQL Server that isan ideal data platform for learning and building desktop and small server applications.
3. In ASP.net there is a Web. config file to connect with the database and web application.

- **CONNECTION STRING OF OUR PROJECT**

1. Next, we have created a connection string to Connectour web application with the database.
2. This configuration is done on the web. config file underYour project folder which is created by default.
3. After opening the web. config file in an application, add sample dB connection in connection Strings section like this.

- **BACK-END(C#)**

1. For data handling and processing we have used C# i.e.(C-sharp).
2. C# is a programming language developed by Microsoft that runs on the. NET Framework. **C#** is used to develop web apps, desktop apps, mobile apps, games, and much more.
3. C-sharp connects web applications with databases.
4. Every user request and data preprocessing is done using C#.
5. Pre-defined class, function, and all other back-end tasksare performed using C#.

- **SHA-256**

1. Secure Hash Algorithm 256 or SHA 256 is defined as one of the most secure ways to protect digital information. SHA 256 is a mathematical process that generates a 256 bit (64 characters long) random sequence of letters and numbers (hash) out of any input.
2. Step 1 we have created a PUBLIC class Block. Then we declare all data types that are required.
3. Step 2 we declare a function called CalculateHash() which will perform the hash algorithm by taking input Encoding ASCII and converting to base 64 string.

- **CREATING A BLOCKCHAIN**

1. Step 1 we have created Blockchain. By creating a *PUBLIC* class called Blockchain. Next, we declare a function called *Blockchain().*
2. Step 2 we created a function called *public void AddBlock().* This function will create a block and will add an index every time a new block iscreated.
3. Next *Chain.Add(block)* will add the next block to the chain.

- **AES**

1. The **AES algorithm** is a symmetrical block **cipher algorithm** that takes the plain text in blocks of 128 bits and converts them to ciphertext using keys of 128, 192, and 256 bits.
2. AES has two algorithms called Encryption and Decryption.

- **ENCRYPTION**

1. To perform encryption first we have created a *PUBLIC* Static class called Encryption.
2. Inside the encryption class, we have created a function called Encrypt
3. This will perform encryption on file and write the data on file
4. *WriteByte((byte)data).*

- **DECRYPTION**

1. Decryption is inverse to Encryption first we created a *PUBLIC* class called Decryption.
2. In the next step it will decrypt the data and write the data on the outputfile
3. *fsOutput.WriteByte((byte)data);*

- **BLOCK DIAGRAM**

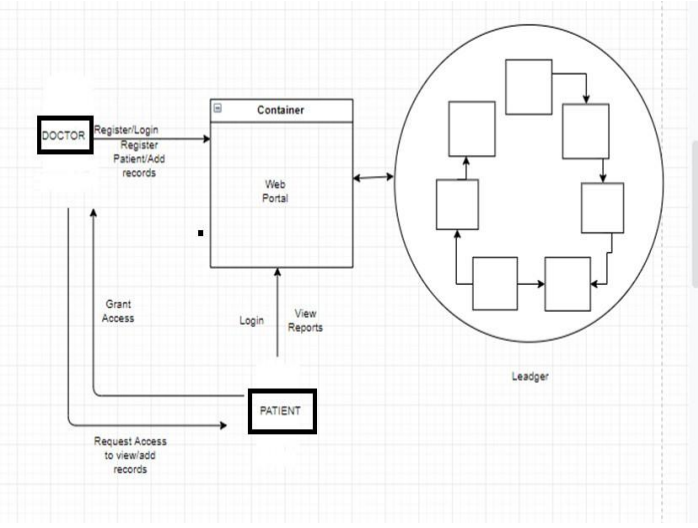

Fig: Block diagram of how the system will work

The above diagram shows how our system works. There are three main modules of our system: the doctor, patient, and container (.i.e. Web portal). The container module is attached to the ***ledger***[6]. A ledger is a collection of transactions or contracts maintained in decentralized form across different people or locations

7. CONCLUSIONS

In this paper, we have discussed how blockchain will change the entire healthcare system. Even the advanced technology and innovation in the current EHR system have some issues regarding data and privacy. Our system will use blockchain and solve privacy and data-related issues which will make the system more secure and reliable. The main purpose of our system is to be cost-effective and its easy use structure.

For future scope, we are planning to add a payment system in this service and live update of patients' health e.g. Their Heart rate, blood pressure, BMI, SPO2, etc. as blockchain technology is gaining attention and its day-to-day evolve in the future blockchain may have variations. There may be different blockchain systems as per the industrial requirement. Blockchain technology is not yet ready for big-scale use but in the future blockchain will be used in daily transactions and big sectors like health care. We need technology like blockchain.

8. REFERENCES

1]M. Kassab, J. DeFranco, T. Malas, V. V. Graciano Neto, and G. Destefanis, "Blockchain: A Panacea for Electronic Health Records?," 2019 IEEE/ACM 1st International Workshop on Software Engineering for Healthcare (SEH), Montreal, QC, Canada, 2019, pp. 21-24, DOI: 10.1109/SEH.2019.00011.

[2]N. Kshetri, "Blockchain and Electronic Healthcare Records [Cybertrust]," in Computer, vol. 51, no. 12, pp. 59-63, Dec. 2018, DOI: 10.1109/MC.2018.2880021.

[3]A. Shahnaz, U. Qamar, and A. Khalid, "Using Blockchain for Electronic Health Records," in IEEE Access, vol. 7, pp. 147782-147795, 2019, DOI: 10.1109/ACCESS.2019.2946373.

[4]Zhang M, Ji Y. 2018. Blockchain for healthcare records: A data perspective. *PeerJ Preprints* 6:e26942v1 https://doi.org/10.7287/peerj.preprints.26942v1

[5]T. Mikula and R. H. Jacobsen, "Identity and Access Management with Blockchain in Electronic Healthcare Records," 2018 21st Euromicro Conference on Digital System Design (DSD), Prague, Czech Republic, 2018, pp. 699-706, DOI: 10.1109/DSD.2018.00008.

[6]M. Zarour et al., "Evaluating the Impact of Blockchain Models for Secure and Trustworthy Electronic Healthcare Records," in IEEE Access, vol. 8, pp. 157959-157973, 2020, DOI: 10.1109/ACCESS.2020.3019829.

[7]Y. Wehbe, M. A. Zaabi and D. Svetinovic, "Blockchain AI Framework for Healthcare Records Management: Constrained Goal Model," 2018 26th Telecommunications Forum (TELFOR), Belgrade, Serbia, 2018, pp. 420-425, DOI: 10.1109/TELFOR.2018.8611900.

Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z (2020) Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE 15(12): e0243043. https://doi.org/10.1371/journal.pone.0243043

Damiano Di Francesco Maesa, Paolo Mori, Blockchain 3.0 applications survey, Journal of Parallel and Distributed Computing, Volume 138, 2020, Pages 99-114, ISSN 0743-7315, https://doi.org/10.1016/j.jpdc.2019.12.019. (https://www.sciencedirect.com/science/article/pii/S0743731519308664)