A Study to Create Secure E-Healthcare Framework using Blockchain Technology: A Case of Tertiary Hospitals of Punjab

Prikshat Kumar Angra
Lovely professional University, Phagwara

Pritpal Singh
Lovely professional University, Phagwara

Abstract

Blockchain technology enables a decentralized and distributed state without the need for a central authority. Because of the use of cryptographic standards, exchanges are still reliable and dependable. Blockchain technology has recently become popular and has made inroads into a variety of industries, owing to the popularity of cryptographic forms of currency. The need for a more persistent oriented way to deal with human services systems and to interface different processes, as well as increasing the accuracy of electronic social insurance records, is one area where blockchain innovation has colossal potential (EHRs). A study of cutting-edge blockchain research in the field of human services is currently underway. The aim is to highlight the future applications of the technology as well as the challenges and implications of blockchain research in the medical field. First, some background information is presented, followed by a description of the current philosophy in use. Exploratory analysis, probe gathered information including properties, and aftereffects writing finitude assessments are among the study's outcomes. In the end, analysis leads to discussion. According to findings, blockchain technology research in the human services sector is growing, with the technology being used primarily for knowledge sharing, health record management, and access control. There are many transactions conducted in the electronic health records (EHR) system, and the data travelled in the transactions is stored on many peers across the network. The study incorporates a security mechanism that is used to provide security in the transactions of the electronic health records (EHR) system. The aim of this study is to create a protection system for electronic health records (EHR) and to use blockchain technology to enforce a consensus mechanism. A consensus algorithm was used to secure e-healthcare data obtained from Punjab's tertiary hospitals. To protect healthcare data, the Python programming language is used to enforce a proof of work consensus process. We used 10000 data base rows with 7 attributes data from tertiary hospitals in Punjab for our study, which shows that blockchain is a revolution in providing protection in healthcare data.

Keywords: Distributed Systems; Healthcare; Exploratory; Blockchain

Introduction

Since there are many peers in healthcare where transactions are performed and data is accessed, this research focuses on implementing blockchain technology to provide protection to healthcare data. The enormous value growth of digital forms of money and enormous speculations of investment in blockchain new businesses have largely guided the premium and advancement of this innovation. The demand for blockchain innovation is expected to develop until 2021, according to estimates. As of now, there are approximately 1500 crypto coins that were created just a few years after the introduction of bitcoin. Bitcoin was the first computerised cryptocurrency. It ensures that exchanges are carried out in a localised manner, eliminating the need for a confided in focal point. There is no compelling need to discover someone's personality when open keys are used. Diggers, who receive coins for their fractional work to verify and exchanges (installations) in the Bitcoin blockchain, are an essential part of the Bitcoin arrangement. More information about Bitcoin can be found for those who are interested.

Electronic health care increases the social, health benefit and reduces medical errors. Electronic health record (EHR) is an electronic version of patient's medical records that are conserve using database technologies. Electronic Health Record is electronic patient's health information which is produced by more Care Delivery Organization. The EHR provides the complete record of the patient, which is supported by the different Care Delivery Organization via the interface. Health information like prescriptions, lab reports, patient's medical history etc. With EHRs, patients' wellbeing data is accessible in one spot, when and where it is required. Suppliers approach the data they need, at the time they need it to settle on a choice. Solid admittance to finish persistent wellbeing data is fundamental for protected and successful consideration.

The blockchain enables substance transactions without the need for a (trusted) third-party. Validators (commonly known as excavators) take the place of outsiders and authorise transfers in a decentralised manner. This is done through a dispersed agreement—the capacity to come to an agreement on something among disparate groups who don't trust one another. In the cryptographic money environment, this computational problem is known as the twofold payment question, which certifies that a certain amount of an advanced coin has not yet been spent without the approval of a trusted outsider (usually a bank) who monitors all exchanges and client adjustments.

As opposed referenced papers, this work presents an exploratory survey & examination cutting edge blockchain inquire about in the yard of social insurance. The point of our paper is additionally demonstrate chance utilization blockchain in social insurance furthermore, viewing the difficulties & chance bearings of blockchain look into. Our methodical survey just incorporates investigate that presents another solution, algorithm, strategy, approach, or engineering for the yard of social insurance. Survey findings, inactivity potential utilizations of blockchain, outer large distributions are avoided.

Literature Review

The advantages of a dispersed database hold the guarantee of overseeing information in the social insurance industry. Because of the multifaceted nature as far as the partners engaged with the human services organize, a monstrous measure of information must be moved in reverse and advances. The use of blockchain gets significant in managing the need of an assortment of included gatherings to access a similar sort of data. Clinical treatment forms are organized while considering the additional worth made by blockchain. A pilot venture, in light of the Ethereum stage, which is known as the Gem Health Network, gives distinctive human services master viders full access to treatment data. Such a biological system handles the issues of simultaneous openness, in this way restricting the opportunities for carelessness brought about by obsolete information. Furthermore, operational expenses brought about from keeping up past various databases can be diminished. The sys-tem grants parental figures to follow patients' clinical data on a frequent premise, just as to survey the memorable association between clinical specialists and patients, which consequently improves the straightforwardness and nature of the whole clinical condition.

A dispersed agreement convention characterizes how a system figures out which companion will get ready and seal the most up to date hinder with still unsubstantiated and non-designed information. The most straightforward route

is to decide it haphazardly, however such a methodology isn't successful as far as system life span and can even be perilous for the system, since companions could choose to assault the entire system.

The PoW agreement convention is utilized in bit-coin mastermind. Its uses figuring energy as a segment to choose the picked peer. The rivalry betwixt peers depends on hashing unverified exchanges. Along these lines, a companion's possibility of being picked is in relation to its computational force.

The PoS agreement convention depends on the benefits a companion has. A companion's possibility of being picked to affirm another square is with respect to its advantages. Practically speaking, acknowledged include a friend store a predefined least count advantages. Opposition right now not founded on the computational intensity of the companions, which means there is negligible vitality utilization in contrast with the PoW. In any case, such a methodology is like an investor company, where the rich have a bit of leeway.

Blockchain—Distributed Ledger Technology

Each trade finished by a center point is set apart before it is imparted to the framework for afterward attestation. The propelled checking of a trade utilizing the private key engages confirmation and gives decency trade. The first is a result of the way solitary customer having particular secret key can sign the trade furthermore, a result way that a bumble during transmission of the information realizes the disappointment disentangling.

The essential assignments of a blockchain hub are:

- interfacing with the blockchain arrange
- putting away cutting-edge record
- tuning in to exchanges
- passing on legitimate exchanges into the system

Variety of blockchain

By and large, there are various sorts of block chains relying upon oversaw information, on the client's ability to access certain knowledge and what tasks he or she may perform This include the following:

- open permission less,
- cartel,
- snobbish

Everyone has access to and can see all of the details in the free permission less blockchain. Regardless, a few bits of the blockchain may be encoded to compensate for the lack of meaning in a particular part. In an open permission less blockchain, anyone can enter the blockchain and act as a simple hub or an excavator without any approval (hub). These kinds of blockchains are normally given a monetary impetus, for example, in digital currency systems.

Blockchain in Healthcare

To improve medical usefulness, the focus should be on data management, which can benefit from the ability to link different systems and improve EHR precision. Blockchain technology can be used to help calm down solutions and development networks around the board, pregnancy and any hazard information the executives just as to help find a good pace, regulating of clinical activities. Social protection organizations are changing to enable a patient-driven approach. Block-chain based social protection automated-system may upgrade safety & dependability of person's information from person's authority over their therapeutic administrations data sets. Those systems could in like manner help combine tolerant data, enabling the exchanging of clinical records across various restorative administrations establishments.

Taking care of the clinical data of patients is significant in human administrations. These data are very delicate also, right now a practical objective for advanced assaults. It is essential to make sure about each fragile datum. Right now, and finding a good pace of patients' human administrations data is another usage section may benefit by bleeding core current day promotion. Block-chain advancement is hearty against assaults and disappointments, and deliver various simulations for get to control. Right now way, block-chain gives a better than average structure to human administrations data.

Healthcare information necessitates a high level of security and confidentiality. The term "privacy" applies to people who have the legal authority to authorize or reveal personal details to others. This necessitates collaboration between healthcare providers and regulators, as well as the creation of agreed-upon policies and procedures. The first step in deciding who should have access to confidential patient information is to consider privacy. Numerous security

standards, such as HIPAA, COBIT, and DISHA, have been established in response to this problem, and have been used to protect patients' health information. Healthcare providers must also priorities confidentiality in order to protect the privacy of their patients' health details. This involves maintaining patient information access control, securing patient data from unauthorized users, and modifying and destroying stored data, among other things. As the scale of healthcare data expands, security measures to protect the data are needed. As a result, the US and other countries have established security standards and regulations to safeguard their healthcare data.

In e healthcare distinct security requirement are mentioned in table 1.1. Every security concept takes place numerous transactions in e healthcare. In common cloud based architecture data as directly send to the system is stored in the data base. But using blockchain we can secure data in e healthcare system

Table 1.1 Users Security Requirements in E healthcare

S. No.	Security concept	Requirements
1	Registration	Verify the authenticity of user
2	Non-repudiation of user action	It is required in e -healthcare that verification one user transaction never deny other user's transaction
3	Non-repudiation of emergency access	E healthcare gives emergency access to users (doctors, patient), due to provide secur ity to one side transaction other transaction not denied
4	Verify user actions	It access user's identity and allowed access
5	Access in transactions	To check the privileges only to the authorized users, allow users to make transactions to the system.

Research Mathodology

Electronic Health Record is electronic patient's wellbeing data which is created by more Care Delivery Organization. The EHR gives the total record of the patient, which is upheld by the distinctive Care Delivery Organization through the interface. This interface having many pathways to get data. Health information like patients registration, approval of their appointments, medical history of patient, doctor's prescription, and progress notes etc. stored directly into data base from different GUI (Graphical User Interfaces). The Electronic Health Record (EHR) with patient's data is viewed as exceptionally delicate in Healthcare association. Delicate data to patients in medical services must be overseen with the end goal that it is free from any and all harm from unapproved access. Electronic Health Record is electronic patients prosperity information gives the absolute record of the patient, which is maintained by the unmistakable Care Delivery Organization through the interface. The National Alliance connects the sharing of Electronic health records between different providers for health Information Technology.

In tertiary hospitals of Punjab, trillions of transactions executed on the network in seconds. Using blockchain technology we create and implement security framework on e healthcare system of Punjab using consensus mechanism. In our study we implements proof of work algorithm for secure e healthcare records.

Proof of Work

The prover (requestor) and verifier are two separate parties (nodes) in a Proof of Work (PoW) mechanism (provider). The prover completes a resource-intensive computational

task with the aim of achieving a goal and then presents it to a verifier or a community of verifiers for validation. The central concept is that the asymmetry in resource requirements between proof generation and validation acts as an inherent barrier to any device misuse. Within this aim, the idea of PoW was first presentedy Dwork and Naor in their seminal article in 1993. They proposed that PoW be used to prevent email spamming. According to their plan, an email sender will be expected to complete a resource-intensive mathematical puzzle and attach the solution to the email as proof of completion. The email recipient can only approve an email if the solution can be checked successfully.

Our study is to examine e-Healthcare security challenges in order to address the emerging needs of a national digital healthcare solution. New security concerns arise in transmitting and processing of electronic medical records, personal healthcare records, and patient billing records, as well as public health alerts, across many parties with varying security, privacy and trust levels.

Blockchain has numerous potential for healthcare. EHR systems are used to maintain electronic healthcare records. Our research is to secure e-healthcare using blockchain technology. In figure-1 we gives an idea that clearly defines our work.

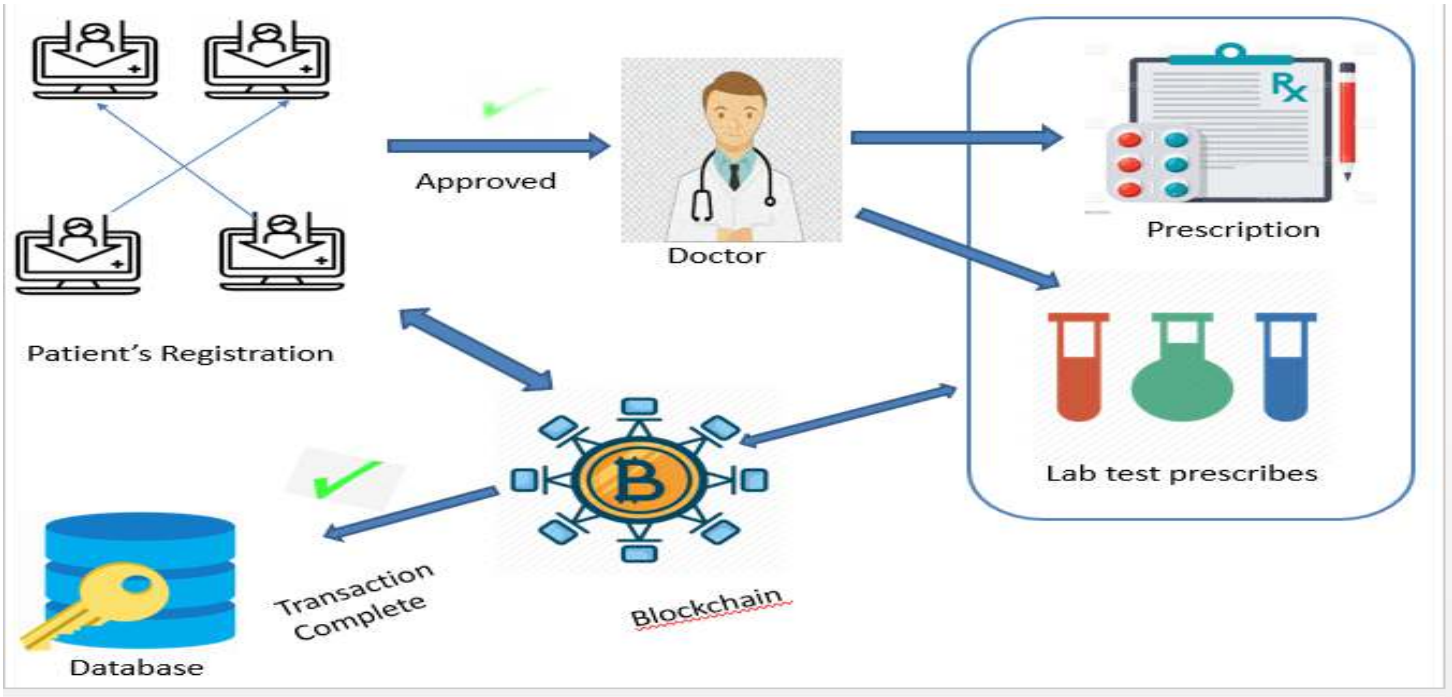

Figure 1:- Implement Blockchain in E-healthcare

Patient's register themselves after successfully registration there details are send to doctor after appointment approval. When doctor got details of patients day wise, according to schedule there patients visit to hospital for their treatments. Doctor gives prescription and lab test according to case. There are different transactions done in this complete work. Our research is emphasis to secure these transactions using blockchain technology.

We are using python for create blockchain in healthcare. For secure data transaction in blockchain in both patient and doctor side we implement consensus algorithm proof of work. A Proof of Work algorithm (PoW) is how new Blocks are created or mined on the blockchain. The goal of PoW is to discover a number which solves a problem. The number must be difficult to find but easy to verify-computationally speaking-by anyone on the network. This is the core idea behind Proof of Work.

In our study we using python to create blockchain. We processing blockchain with proof of work consensus algorithm. Healthcare as an industry has unique requirements associated with security and privacy due to additional legal requirements to protect patients' medical information. The aim of this study is to identify and analyses the security threats that exist for Electronic Health Records health care system.

Proposed system secure transactions using blockchain technology using consensus mechanism, records in e healthcare system is encrypt using cryptography and then transfer from one peer to another peer.

Conclusion

Our examination explored flow block-chain investigate slants inside social insurance. The blockchain innovation instant federalized system viewed extraordinary potential for use in medicinal services, due to the touchy idea of information being prepared and overseen. The point examination recognize the flow status of block-chain research and technology in social insurance. To accomplish this goal, we have characterized look into questions and utilizing the predefined approach. These were then additionally dissected.

Our discoveries demonstrate that blockchain advancement research and its work in human administrations is extending. EHR are now protected using blockchain reason behind that is all transaction in healthcare are secured using consensus algorithm. Moreover, frequently specialized insights regarding the utilized blockchain components aren't give such as, blockchain stage, accord calculation, blockchain type or the utilization of brilliant agreements. Especially, keen agreements could be increasingly utilized as they empower the mechanization of procedures inside a blockchain stage. Most research could likewise give a model usage or if nothing else talk about some execution subtleties of their recommendations.

References

- Swan, M. Blockchain: Blueprint for a New Economy; O'Reilly Media: Newton, MA, USA, 2015.
- Singh, S.; Singh, N. Blockchain: Future of financial and cyber security. In Proceedings of the 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I), Noida, India, 14–17 December 2016; pp. 463–467.
- Tschorsch, F.; Scheuermann, B. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. IEEE Commun. Surv. Tutor. 2016, 18, 2084–2123.
- Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. In Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress), Boston, MA, USA, 11–14 December 2017; pp. 557–564.
- Park, J.; Park, J. Blockchain Security in Cloud Computing: Use Cases, Challenges, and Solutions. Symmetry 2017, 9, 164.
- Yin, S.; Bao, J.; Zhang, Y.; Huang, X. M2M security technology of CPS based on blockchain. Symmetry 2017,9, 193.
- Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In Proceedings of the 2017 IEEE Technology Engineering Management Conference (TEMSCON), Santa Clara,CA, USA, 8 June 2017; pp. 137–141.
- Conoscenti, M.; Vetro, A.; Martin, J.C.D. Blockchain for the Internet of Things: A systematic literature review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), Agadir, Morocco, 29 November–2 December 2016; pp. 1–6.
- Yli-Huumo, J.; Ko, D.; Choi, S.; Park, S.; Smolander, K. Where Is Current Research on Blockchain Technology?—A Systematic Review. PLoS ONE 2016, 11, e0163477.
- Tama, B.A.; Kweka, B.J.; Park, Y.; Rhee, K.H. A critical review of blockchain and its current applications. In Proceedings of the 2017 International Conference on Electrical Engineering and Computer Science

(ICECOS), Palembang, Indonesia, 22–23 August 2017; pp. 109–113.

- Mettler, M. Blockchain technology in healthcare: The revolution starts here. In Proceedings of the 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 14–17 September 2016; pp. 1–3.
- Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain Technology Use Cases in Healthcare. In Advances in Computers; Elsevier: Amsterdam, The Netherlands, 2018.
- Kuo, T.T.; Kim, H.E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J. Am. Med. Inform. Assoc. 2017, 24, 1211–1220.
- vAngraal, S.; Krumholz, H.M.; Schulz, W.L. Blockchain Technology: Applications in Health Care. Circ. Cardiovasc. Qual. Outcomes 2017, 10, e003800.
- Mackey, T.K.; Nayyar, G. A review of existing and emerging digital technologies to combat the global trade in fake medicines. Expert Opin. Drug Saf. 2017, 16, 587–602.
- Giungato, P.; Rana, R.; Tarabella, A.; Tricase, C. Current Trends in Sustainability of Bitcoins and Related Blockchain Technology. Sustainability 2017, 9, 2214.
- Engelhardt, M. Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector. Technol. Innov. Manag. Rev. 2017, 7, 22–34.
- [18] Alhadhrami, Z.; Alghfeli, S.; Alghfeli, M.; Abedlla, J.A.; Shuaib, K. Introducing blockchains for healthcare. In Proceedings of the 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA), Ras Al Khaimah, UAE, 21–23 November 2017; pp. 1–4.
- Sater, S. Blockchain Transforming Healthcare Data Flows. SSRN Electr. J. 2018.
- Aste, T.; Tasca, P.; Di Matteo, T. Blockchain Technologies: The Foreseeable Impact on Society and Industry.Computer 2017, 50, 18–28.
- Raval, S. Decentralized Applications: Harnessing Bitcoin's Blockchain Technology, 1st ed.; O'Reilly Media, Inc.:Sebastopol, CA, USA, 2016.
- Roehrs, A.; da Costa, C.A.; da Rosa Righi, R.; Alex, R.; Costa, C.A.; Righi, R.R. OmniPHR: A distributed architecture model to integrate personal health records. J. Biomed. Inform. 2017, 71, 70–81.
- Sleiman, M.D.; Lauf, A.P.; Yampolskiy, R. Bitcoin Message: Data Insertion on a Proof-of-Work Cryptocurrency System. In Proceedings of the 2015 International Conference on Cyberworlds (CW), Visby, Sweden,7–9 October 2015; pp. 332–336.
- Aumasson, J. Serious Cryptography: A Practical Introduction to Modern Encryption; No Starch Press: San Francisco,CA, USA, 2017.
- Ferguson, N.; Schneier, B. Practical Cryptography, 1st ed.; John Wiley & Sons, Inc.: New York, NY, USA, 2003.
- Greenspan, G. Blockchains Vs Centralized Databases; MultiChain: London, UK, 2016.
- Lewis, A. A Gentle Introduction to Blockchain Technology. Bits on Blocks. 2018. Available online: https:// bitsonblocks.net/2015/09/09/gentle-introduction-blockchain-technology/
- Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here.Paper presented at the e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference.
- Chen L, Lee WK, Chang C-H, Raymond Choo K-K, Zhang N. Blockchain based searchable encryption for electronic health record sharin.Fut Gener Comput Syst 2019;95:420–9
- Dwork, Cynthia and Naor, Moni "Pricing via processing or combatting junk mail". Annual International Cryptology Conference, 139–147, 1992.