SECURE STORAGE AND ACCESS SCHEME FOR E-MEDICAL RECORDS USING BLOCK CHAIN ENVIRONMENT

Sonya A[1], Jeevitha S[2], Vaishnavi M[3]
[1]Assistant Professor, [2,3]UG Scholar
[1,2&3]Department of Information Technology,
B. S. Abdur Rahman Crescent Institute of Science and Technology,
Vandalur, Chennai 600 048, India
Email: [1]sonya.yasmin152@gmail.com

Abstract

Blockchain have been a fascinating exploration region for quite a while and the advantages it gives have been utilized by various different ventures. Additionally, the medical services area stands to profit tremendously from the blockchain innovation because of safety, securityand decentralization. In any case, the Electronic Health Record (EHR) frameworks deal with issues in regards to information security, uprightness and the executives. In the proposed work,to communicate approximately how the blockchain innovation can be applied to alternate the EHR frameworks and solution of those issues. To propose a system that can be applied for the execution of blockchain innovation in scientific offerings location for EHR. The factor of our proposed system is first and to execute blockchain innovation for EHR and moreover to provide stable ability of digital information with the aid of using characterizing granular get right of entry to regulations for the customers. Besides, this system examines the flexibility problem seemed with the aid of using the blockchain innovation average through usage of off-chain stockpiling of the information. This structure offers the benefits of getting an adaptable, stable and vital blockchain-primarily based totally association with usage of PoW (Proof of Work) Algorithm.

Keywords: Block chain, Electronic Health Record, Personal Health Records, Power of Work (PoW) and Cryptographic Algorithm.

I. Introduction

The Bitcoin device proposed with the aid of using Satoshi Nakamoto turned into primarily based totally on cryptology proofing as opposed to trust, allowing or extra events to carry out transactions without a mediator. These events had been called ‘‘depended on 0.33 party’’ (TTP). As a result, this inspiration solved the verification of personal transaction. This

transaction turned into called the double-spending problem [1], which turned into the primary utility of blockchain. Blockchain era is a private, secure, trustworthyand obvious statistics trade completed in a decentralized manner. Therefore, the coordination and validation. Efforts for the decentralized database are simplified because the facts are designed to replace frequently and there may be no distinction withinside the databases. However, hospitals expenses retain to mount, alongside inefficient practices and fitness information breaches are poised to retain. This is one place wherein blockchain generation can enhance the situation. It can do many things, from imparting steady encryption of affected person statistics to managing epidemics. Blockchain's cap potential to maintain an incorruptible, decentralized and obvious log of all affected person information[2]. Additionally, Blockchain is obvious it's also private, concealing the identification of any character with complicated and stable codes that may guard the sensitivity of clinical data. The decentralized nature of the era lets in patients, docs and healthcare vendors to percentage the identical statistics fast and competently Notably, there are demanding situations and possibilities associated with the blockchain primarily based totally utility in healthcare area which desires to be investigated in lots of viewpoints. Blockchain can be used to monitor the patient's healthcare transactions and can ensure authorized access to patient records and compliance based on health information protection laws [3]. In this paper, multilevel blockchain model for the healthcare sector is proposed. The model combines healthcare authorityand private patientfor a tamperproof permission monitoring system which provides increased security and privacy while improving health records and permission redundancy.

II. Related Works

Blockchain is a Peer-to-Peer (P2P) appropriated record technology which rethinks trust in an online entomb state data organization. It was at first concocted for the monetary business, trailed by the possibility of exchanges professional liferating without a middle person. Like governments and partnerships, go between generally assume the part of confided in outsider (TTP), who get, cycle, and store exchanges. In any case, the trustworthy in TTP isn't best due to its opportunity to fall flat or breakdown, lose security, grow to be compromised, or result in the shortfall of the financial framework [4]. From the specialized perspective, blockchain is a dispersed information base which is available in a P2P organization. It comprises of blocks, hubs, and contract basis. The block contains data and the hubs are the mark of association

between members. Each hub stores a nearby mutates, known as the blocks in the blockchain framework. The contract happened when the agreement of hubs concurs upon the exchange's legitimacy.On account of blockchain frameworks, the trustworthy is decentralized. In the interim, the framework and innovation expect a part of the center human beings behind. Significantly, trustworthy in the framework amongst customers is fundamental, that's trailed via way of means of the sharing of keys among members [5]. At present, digital fitness information allow automated extrade and sharing of scientific facts on a given affected person inner a corporation or community of companies completely. Personal Health records (PHRs) [6] are private and fundamental resources for each understanding. There have been presented numerous deals with different parts of overseeing and putting together the PHR up until now. The sharing of individual wellbeing records can assist with improving the precision of the specialist's determination and to advance the advancement of clinical examination. As of now, to decrease the support cost of information, individual wellbeing records are generally moved to an outsider, for example, the cloud specialist co-op. For this situation, patients may lose direct command over their own wellbeing records and the semi-believed cloud specialist co-op may mess with or uncover individual wellbeing records. Subsequently, guaranteeing the protection and uprightness of individual wellbeing records and understanding the fine-grained admittance control are pivotal issues when individual wellbeing records are shared [7]. In a distributed architecture [8], with decentralized and carefully designed highlights, blockchain gives another approach to secure the individual wellbeing records sharing framework. In this paper, we propose another individual wellbeing records offering plan to information respectability undeniable dependent on blockchain. Focusing on the issues of security divulgence, restricted keyword and loss of control rights in the task of individual wellbeing record sharing, the new plan utilizes accessible symmetric encryption and quality-based encryption strategies to accomplish security assurance.

III. Existing system

Many healthcare providers use cloud technology with caution due to the risks involved such as unauthorized use or access to private and sensitive health data. To mitigate security and privacy concerns, some guidelines and recommendations must be addressed by cloud service providers.The recent growth of digital health initiatives- like telehealth doctor visits – is a major contributor to the severe increase in breached patient records. As more healthcare functions continue to move online over the next year, it’s extremely important to ensure these processes

are protected from outside threats. This trend will continue as many healthcare providers are still slow in responding to threats while the decentralized systems make them more vulnerable to attacks.When a breach occurs, not only are you compromising confidential patient information, but you also face a hefty penalty if you're found to have violated the many compliant standards regulating the industry.Many medical providers are investing in proper safeguards to better protect sensitive patient data.Vendors holding this certification are significantly less susceptible to facing ransomware attacks or data breaches.

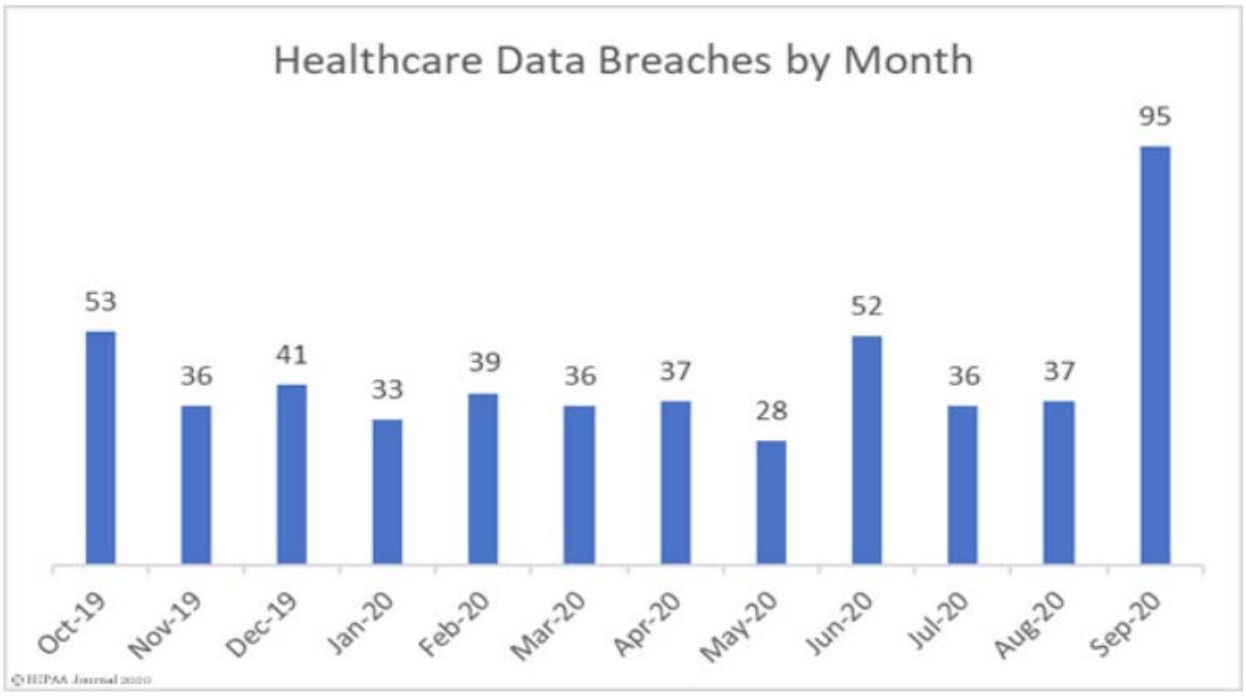


Figure 1. Healthcare Data Breaches by Month Wise

IV. Proposed work

The aim of this system is to create it affordable to seek out a platform that may be useful in remodeling aid sector to be patient-centered. A platform that is secure, clear and it conjointly provides knowledge integrity to the medical records of the patients. To proposes a multilevel blockchain mechanism that makes such a suburbanized platform thatstore patient's health medical records. These advantages create it an affordable option for medical records on that, as a result of the innovation of technology within the aid trade has created thesafety medical knowledge a high priority. once a medical history is generated and signed. It will be created into the blocks that provides unauthorized person cannot be modified or altered.

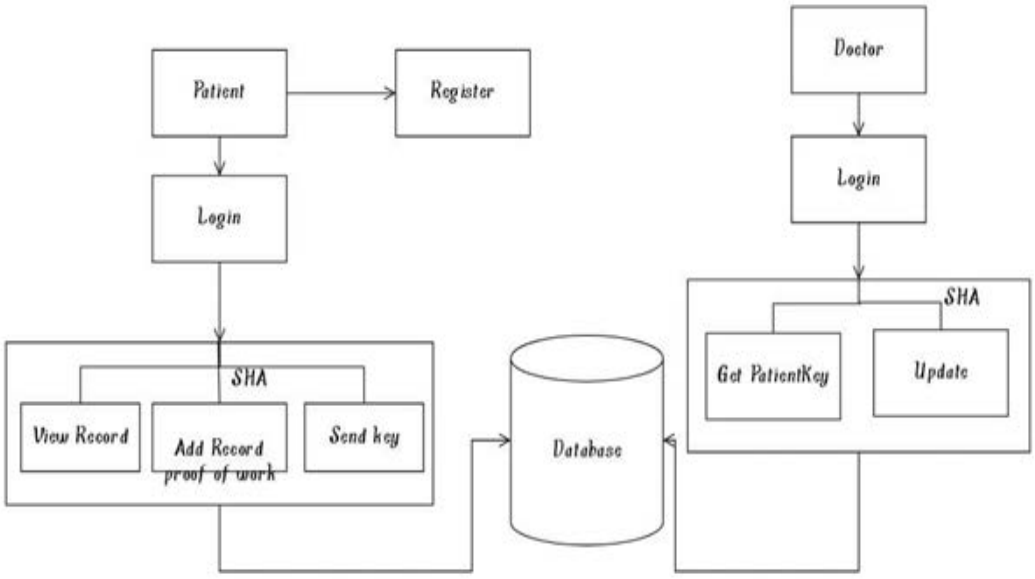


Figure 2. Overall Architecture Process

In existing system, Personal Health System (PHS) uses artificial care systems to model and represent patient's conditions, diagnosis, and treatment method, then applies process experiments to investigate and valuate numerous therapeutic regimens, and implements parallel execution for care processes. SHA-256 could be a unidirectional work that changes over a content of any length into a line of 256 pieces.It's a changed variant of SHA1, that progressively could be a changed SHA0.

Proposed SHA 256 Algorithm:

Step 1: All variables square measure thirty-two-bit unsigned integers andcalculated by modulo 232.

Step 2: For every square, there's one spherical constant k[i] and one entry within the message schedule array w[i], $0 \leq i \leq 63$.

Step 3: The compression operate uses eight operating variables, a through h.

Step 4: Big-endian convention is employed once expressing the constants during this pseudocode, and once parsing message block information from bytes to words.

V. Modules

User Module:

In this user module, the personregisters the general details like name, age, gender, address and health sensitive information. They use the customers call and mystery for login to visualize opportunity info.

Get Patient Details:

The blockchain became created in keeping with the affected person details. Each block connected with the consumer document their required information. Hence those are maintained with the aid of using the block. Whenever the consumer requirement is needed, the document can be retrieved from everywhere at any time.

Update Block:

In this module, the person needs to change or update their records with the knowledge of doctor, the report can be modified with the aid of using the SMTP (simple mail transfer protocol) in order that the medical doctor can update patient's clinical description.

Medical Records:

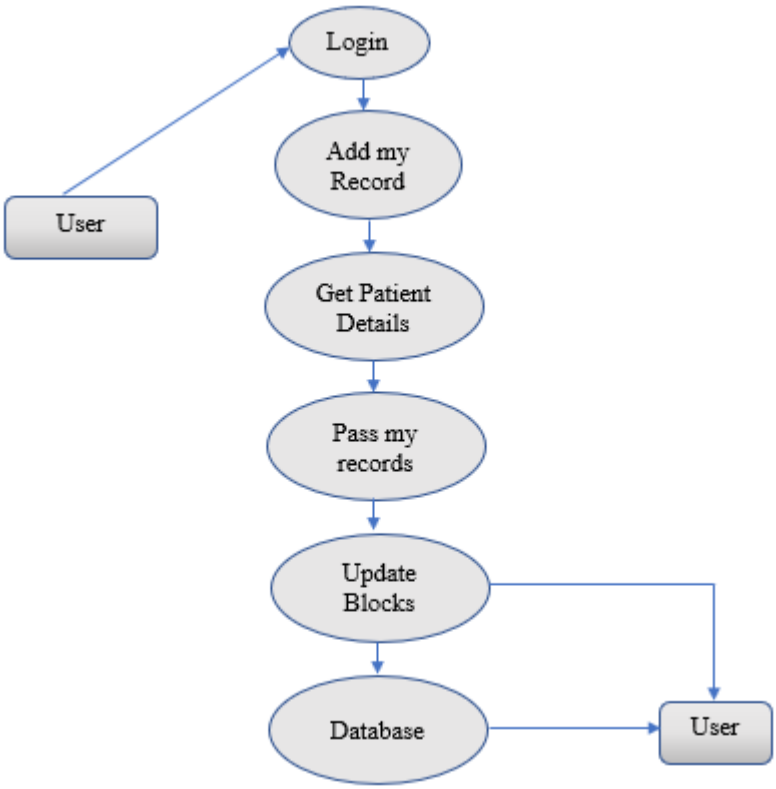
The module defines that the person document and additionally the scientific information vicinity unit maintained through storing the statistics into the block chain.

Verifying the Data:

Data validation manner checking the accuracy and excellent of supply facts earlier than the usage of, uploading or in any other case processing factsthrough the usage of POW (Proof of Work) set of rules the file that have been up to date through health practitioner is confirmed whether or not it's far correct.

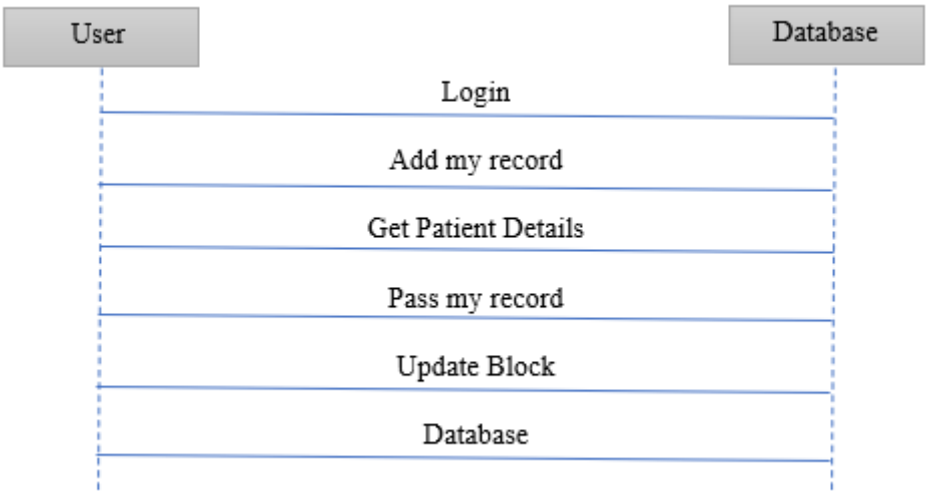
Use Case Diagram

A use case diagram shows the connection amongst actors and use cases. The fundamental additives a person or any other machine as a way to engage with the machine modeled. A use case is an outside view of the machine that represents a few movements the person would possibly carry out so as to finish a task.



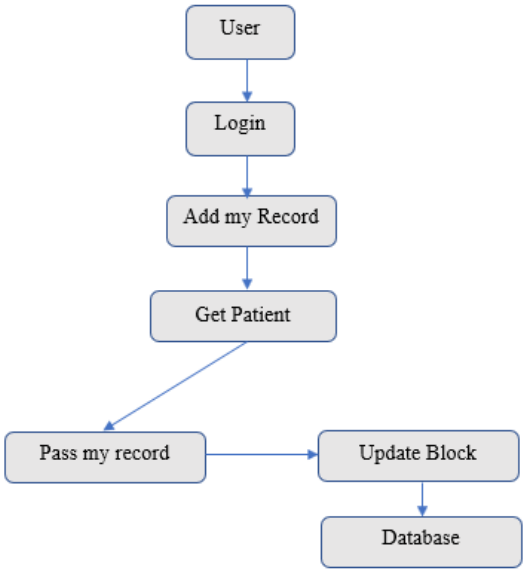
Sequence Diagram

A sequence diagram in Unified Modeling Language (UML) is a type of interplay diagram that suggests how strategies function with each other and in what order. It is a assemble of a Message Sequence Chart. Sequence diagrams are now and again known as occasion diagrams, occasion scenarios, and timing diagrams.



Activity Diagram

Activity diagrams are graphical representations of workflowsand movements with assist for choice, generation and concurrency. In the Unified Modeling Language, activity diagrams may be used to explain the enterprise and operational step by step workflows of additives in a system. Aactivity diagram indicates the general glide of control.



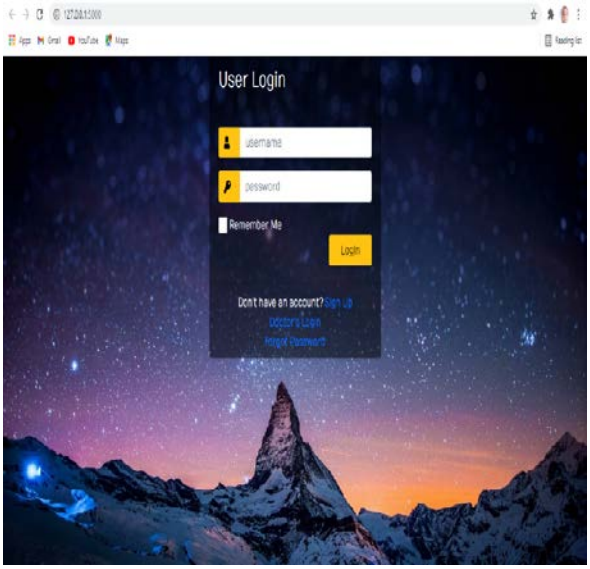


Figure 3. User's Registration Page

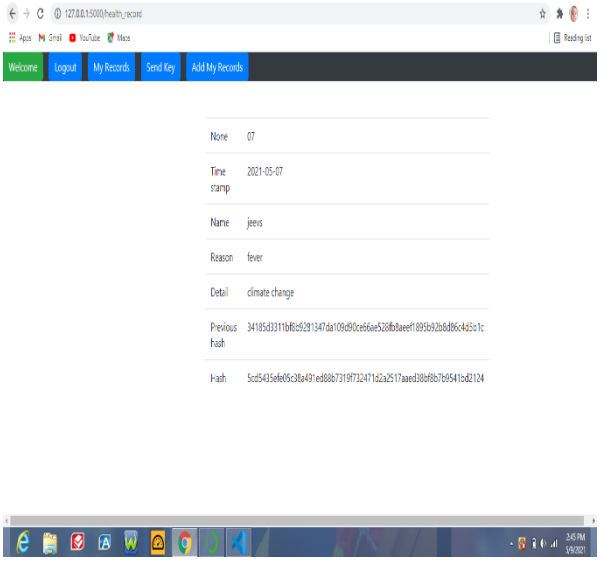


Figure 4. Encrypted Data Page

VI. Conclusion

Blockchain permits the association of check, portrayal and data sharing while inside thegiving information related with confirmation, valuable asset saving and enabling for the patient and making parts social security extra insightful. Contrasted with the current EHR frameworks, that utilization customer worker plan, the arranged framework utilizes blockchain for rising strength and security. Blockchain technology tends to capacity challenges and is predicated on open guidelines, provides a shared distributed read of the health information and can conjointly widespread acceptance and preparation throughout all industries. Utilization of the planned health blockchain that's delineated during this paper has the potential to interact countless people, health care suppliers, health care entities and medical researchers to share the huge quantity of genetic, diet, lifestyle, environmental and health information with a warranted security and privacy protection.

References

[1] G.Jetley and H. Zhang, “Electronic health records in IS research: Quality issues, essential thresholdcs and remedial actions,” Decis. Support Syst., pp. 113–137, 2019.

[2] K. Wisner, A. Lyndon, and C. A. Chesla, “The electronic health record’s impact on nurses’ cognitive work: An integrative review,” Int. J. Nurs. Stud., vol. 94, pp. 74–84, 2019.

[3] M.Hochman, “Electronic Health Records: a ``Quadruple Win,'' a ``Quadruple Failure,'' or Simply Time for a Reboot?” J. Gen. Intern. Med., vol. 33, no. 4, pp. 397–399, Apr. 2018.

[4] Q. Gan, “Adoption of Electronic Health Record System: Multiple Theoretical Perspectives,” 2014 47th Hawaii Int. Conf. Syst. Sci., pp. 2716–2724, 2014.

[5] T.Vehko et al., “Experienced time pressure and stress: electronic health records usability and information technology competence play a role,” BMC Med. Inform. Decis. Mak., vol. 19, no. 1, p. 160, Aug. 2019.

[6] W.Koczkodaj, M. Mazurek, D. Strzalka, A. Wolny-Dominiak, and M. Woodbury-Smith, “Electronic Health Record Breaches as Social Indicators,” Soc. Indic. Res., vol. 141, no. 2, pp. 861–871, 2019.

[7] S. T. Argaw, N. E. Bempong, B. Eshaya-Chauvin, and A. Flahault, “The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review,” BMC Med. Inform. Decis. Mak., vol. 19, no. 1, pp. 1–11, 2019.

[8] A.Sonya, G.Kavitha, “Securing the Healthcare Data with BlockchainTechnology” International Journal of Advanced Science and Technology,Vol. 29, No.4, (2020), pp.9474 –9481.

[9] A.Sonya, G.Kavitha “Encrypting Healthcare Data in Cloud Using Cryptographic Algorithms” Test Engineering and Management, Volume 83, Page No. 26722 – 26731, August 2020.

[10] A.Sonya “Distributed Application (DApp) for Securing User: Interaction Logs forTask Using Ethereum block chain and Smart Contracts in Solidity” International

[11] Journal of Multidisciplinary Research and Growth Evaluation, ISSN:2582-7138,Vol 2,pg no – 152-159, 2021.

[12] A.Sonya, G.Kavitha "A Comprehensive Review on Prediction of Heart ConditionUsing Machine Learning Algorithm" Journal of Critical Views, Volume 7, Issue 19,July 2020.

[13] A.Sonya, G.Kavitha "Security and Privacy Preserving for Patient's E-Health Care Applications", Test Engineering and Management, Volume 82, Page No.1781-1786, February 2020.

[14] A.Sonya, G.Kavitha"Preserving Human Health Care Records Based On Hybrid Learning Methods In Cloud Computing" International Journal of Control and Automation, Vol. 12, No. 6, (2019), pp. 465-476.

[15] A.Sonya, G.Kavitha"Transmission of Secure Sensitive Health Care InformationUsing Hybrid Encryption in Cloud Computing", International Journal of Advanced Science and Technology Vol. 28, No. 15, (2019), pp. 344-354.

[16] McLeod and D. Dolezel, "Cyber-analytics: Modeling factors associated with healthcare data breaches," Deci's. Support Syst., vol. 108, pp. 57–68, 2018.