International Journal of Research in Engineering, Science and Management
Volume-3, Issue-6, June-2020
www.ijresm.com | ISSN (Online): 2581-5792

Blockchain Technology for Secure Electronic Health Record Systems

T. Ambikadevi Amma[1], Silja Varghese[2], V. Baby[3], Laya Rose Joseph[4*]
[1]*Principal & Professor, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Pampady, India*
[2,3]*Assistant Professor, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Pampady, India*
[4]*PG Scholar, Department of Computer Science and Engineering, Nehru College of Engineering and Research Centre, Pampady, India*
*Corresponding author: layarose.joseph@gmail.com

***Abstract*: Blockchain have been a fascinating examination zone for quite a while and the advantages it gives have been utilized by various different businesses. So also, the human services division stands to profit tremendously from the blockchain innovation because of security, protection, secrecy and decentralization. By and by, the Electronic Health Record (EHR) frameworks face issues with respect to information security, respectability and the executives. The sharing of individual health records can assist with improving the exactness of the specialist's analysis and to advance the advancement of clinical research. At present, to lessen the upkeep cost of information, individual health records are generally re-appropriated to an outsider, for example, the cloud specialist organization. For this situation, patients may lose direct power over their own Health records and the semi-believed cloud specialist co-op may mess with or uncover individual Health records. Thusly, guaranteeing the protection and uprightness of individual Health records and understanding the fine-grained get to control are urgent issues when individual Health records are shared. As a conveyed design with decentralized and sealed highlights, blockchain gives another approach to ensure the individual Health records sharing framework.**

In this paper, we examine how the blockchain innovation can be utilized to change the EHR frameworks and could be an answer of these issues. We present a structure that could be utilized for the usage of blockchain innovation in human services division for EHR. The point of our proposed system is right off the bat to actualize blockchain innovation for EHR and also to give secure capacity of electronic records by characterizing granular access rules for the clients of the proposed structure. This structure gives the EHR framework the advantages of having an adaptable, secure and basic blockchain-based arrangement.

***Keywords*: Blockchain, Health record, Smart contract.**

1. Introduction

To comprehend the complexities of the rising electronic Health record framework, it is useful to realize what the Health data framework has been, is currently, and necessities to turn into. The clinical record, either paper-based or electronic, is a specialized apparatus that bolsters clinical dynamic, coordination of administrations, assessment of the quality and viability of care, look into, lawful insurance, instruction, and accreditation and administrative procedures. It is the business record of the medicinal services framework, reported in the typical course of its exercises. The documentation must be verified and, in the event that it is manually written, the sections must be neat.

Before, the clinical record was a paper storehouse of data that was looked into or utilized for clinical, inquire about, regulatory, and money related purposes. It was seriously restricted as far as openness, accessible to just a single client at once. The paper-based record was refreshed physically, bringing about postponements for record consummation that kept going somewhere in the range of 1 to a half year or more. Most clinical record divisions were housed in establishments' storm cellars in light of the fact that the heaviness of the paper blocked different areas. The doctor was in charge of the consideration and documentation forms and approved the arrival of data. Patients once in a while saw their clinical records.

A second confinement of the paper-based clinical record was the absence of security. Access was constrained by entryways, locks, ID cards, and repetitive sign-out methods for approved clients. Unapproved access to tolerant data set off no cautions, nor was it comprehended what data had been seen.

Today, the main role of the documentation continues as before—backing of patient consideration. Clinical documentation is frequently examined into an electronic framework quickly and is regularly finished when the patient is released. Record culmination times must meet authorizing and administrative prerequisites. The electronic Health record is intelligent, and there are numerous partners, analysts, and clients of the documentation. Since the administration is progressively engaged with subsidizing social insurance, offices effectively survey documentation of care.

Big changes in information technology and networking have affected the way of people live today. Technology advances in all areas of human existence, meaning that what we use differs

greatly from what we used to be. New improvement in health care has been invented as changes in technology affected human life. With the emergence of EHR patients are now able to store and share their data accurately. The personal health records have valuable data, which we share with the research institution, pharamacy, and healthcare systems. Due to growth of technology, there are a lot of advantages that users get in the field of security and in other areas. Although there are many benefits of technology in the security sector, there are few issues in EHR, such as ownership of the data and integrity. Blockchain is what makes us a novel technology to use as a solution for this security issues. Prior to the approach of current innovation, human services segment utilized paper based framework to store the clinical records, i.e., utilizing written by hand system. This paper-based clinical record framework was wasteful, shaky, disorderly and was not temper-confirmation. It likewise confronted the issue of information duplication and repetition as all the organizations that patient visited had different duplicates of patient's clinical records.

The social insurance area confronted a pattern move towards EHR frameworks that were intended to join paper-based and electronic clinical records (EMR). These frameworks were utilized to store clinical notes and research facility brings about its different parts. They were proposed to upgrade the security part of the patients by forestalling mistakes and expanding data get to. The objective of EHR frameworks was to take care of the issues looked by the paper-based medicinal services records and to give a productive framework that would change the condition of social insurance part. The EHR frameworks have been executed in various medical clinics around the globe due the advantages it gives, for the most part the improvement in security and its cost-adequacy. They are viewed as a crucial piece of social insurance part as it gives a lot of usefulness to the medicinal services. These functionalities are electronic capacity of clinical records, patients‟ arrangement the board, charging and records, and lab tests. They are accessible in a significant number of the EHR framework being utilized in the human services division. The fundamental center is to give secure, temper-confirmation, and shareable clinical records across various stages. In spite of the way that thought behind use of EHR frameworks in the medical clinics or social insurance was to improve the nature of human services, these frameworks confronted certain issues and didn't meet the desires related with them. In the individual medical records sharing framework, patient's very own medical records are frequently redistributed to the outsider, for example, the cloud specialist co-op so as to accomplish asset sharing and decrease the upkeep expenses of server farm. In light of the current situation, one of the most questionable issues is the means by which to guarantee the security, protection and accessibility of individual medical records while accomplishing fine-grained get to control. A viable arrangement is to join distributed storage, accessible symmetric encryption, and characteristic based encryption together. Yet, this methodology additionally presents another arrangement of difficulties. In the first place, when different encryption systems are utilized to secure individual medical records redistributed to the cloud server, unified key administration will prompt a solitary purpose of disappointment. Also, practically all quality based encryption plans require a confided in power to set up the framework and convey the private keys for framework members. In any case, it is exceptionally hard to track down a totally trustworthy expert in actuality. Moreover, the framework members normally escrow their credit private keys to the confided in expert in the trait based encryption conspire. This alleged key escrow issue can bargain the classification of individual medical records redistributed by patients to the cloud server, particularly when the approval place is compromised. At long last, the cloud stage may not be dependable because of issues, for example, representative debasement. During the sharing of the individual medical records, the cloud server may return altered or somewhat qualified scrambled individual medical records to clients for its advantage. These mistaken or inadequate individual medical records can delude clients, (for example, specialists, inquire about organizations or different patients) into making bogus decisions that imperil the lives of patients or others.

Luckily, the rise of blockchain innovation gives another approach to take care of the above issues. The utilization of blockchain for key administration and dispersion makes key administration and conveyance simpler and increasingly secure. What's more, the blockchain has the qualities of unforgeable and sealed. Each occasion or exchange on the blockchain is timestamped and can't be altered once it is recorded on the blockchain. Along these lines, putting away the hash estimations of encoded individual medical records onto the blockchain not exclusively can successfully maintain a strategic distance from the terrible results brought about by wrong or mostly fulfilled scrambled individual medical records returned by the noxious cloud server. In the interim, the cloud server can likewise be encouraged to genuinely play out the activity as indicated by the necessities of clients.

2. Related Work

The EHR framework additionally faces some different issues which are as per the following:

Interoperability: It is the route for various data frameworks to trade data between them. The data ought to be interchangeable and must be usable for additional reasons. A significant part of EHR frameworks is its Health Information Exchange (HIE) or by and large information sharing angle. With various EHR frameworks being sent in different clinics they have a fluctuating degree of phrasings, specialized and utilitarian capacities which makes it to have no generally characterized standard [1]. In addition, at specialized level the clinical records being traded ought to be interpretable, and that deciphered snippet of data could be additionally utilized [2].

Information Breaches: Data breaks in human services part moreover requires the need of a superior stage. An investigation [2] was finished for investigating the information penetrates in EHR frameworks and it delineated that 173 million information passages have been bargained in these frameworks since October 2009. Another study directed by Argaw et al. [3], clarifies that emergency clinics have become an objective of digital assaults and an expanding pattern has been seen by the specialists while directing this investigation that a great deal of research work has been done in this space [3][5] [6]. Additionally, numerous EHR frameworks are not intended to satisfy the necessities and prerequisites of the patients and face the issues identified with wastefulness and poor adjustment of these frameworks [7]. The writing additionally proposes that utilization of EHRs have acquainted negative results with data handling [8]. These issues make it sensible to discover a stage that would be useful in changing social insurance division to show restraint focused, i.e., Blockchain. A stage which is secure, straightforward and it likewise gives information trustworthiness to the clinical records of the patients. This paper proposes a system that makes such a decentralized stage that would store patient's clinical records and give access of those records to suppliers or concerned people, i.e., tolerant. We additionally mean to tackle the versatility issue of blockchain, as it isn't in the structure of blockchain to store gigantic volumes of information on it. In this way, we would use off-chain scaling technique that makes use of the fundamental medium to take care of the versatility issue by putting away the information on that medium. Additionally, our proposed work is meaning to fathom the previously mentioned data asymmetry and information breaks issue looked by the EHR framework.

As the basic innovation of Bitcoin, the blockchain first showed up in Bitcoin: a shared money framework distributed by Satoshi Nakamoto in 2008, which depicts in detail how to set up another arrangement of decentralized point-to-point exchanging framework without trust establishment, and its feasibility has been demonstrated by the steady activity of bitcoin since 2009 [11]–[13]. As of late, motivated by the extraordinary achievement of blockchain in the monetary field, numerous scientists have started to effectively investigate the utilization of blockchain innovation in different fields. For instance, decentralized web of things, decentralized information sharing [14]–[18].

By investigating the current plans, it very well may be seen that the current individual medical records sharing plans dependent on distributed storage and blockchain can't accomplish fine-grained get to control of information well. Furthermore, there is the danger of protection spillage in these incorporated administration frameworks. Specifically, when a client needs to check the rightness and the respectability of scrambled individual health records returned by the cloud server, it is important to much of the time connect with the cloud server, which makes the plan wasteful by and by. Focusing on these issues in the current plans, in this paper, we propose another individual health records offering plan to information uprightness evident dependent on blockchain.

3. Design of the Scheme

Contemplations about information availability, protection, moral issues, and transparency significance, we present a design of EHR, related in blockchain and smart contracts, that could make Health records interoperability conceivable and safe on a worldwide scale.

Our System, showed in fig. 1, has the accompanying parts:

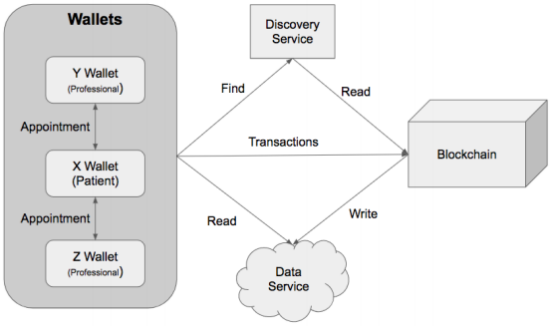

Fig. 1. Proposed architecture

Blockchain. A distributed ledger, fit for to execute brilliant agreements. This segment is dependable to record references to Health exchanges, for example, Health arrangements, clinical tests, endorsed drug, and so forth. digital money framework, a block contains money exchanges. In a protection layer for electronic Health records, a block can contain pointers to Health data. For instance, when a persistent X is seen by a specialist in the emergency clinic Y, an exchange is attached to the record saying that Y approach that data of X.

- Data Service. An information stockpiling administration important to keep the Health records. In this proposition, it is a cloud document framework, where each record is claimed by X and can be perused by Y. This arrangement can be executed, for instance, by utilizing mainstream cloud benefits in the market, for example, Google Drive, Megadrive, and Dropbox. To be utilized in our engineering, the information administration must give: cloud get to, record get to control and interfaces to add and evacuate perusing access to the documents.
- Wallets. An electronic wallet is capable to store the clients private and open cryptographic keys. The open key is the client recognizable proof in the arrangement. The mail and secret phrase used to get to the information administration are likewise kept by the wallet. The wallet is the fundamental interface and technique for access to the framework.
- Discovery Service. This non mandatory and assistant framework is utilized to quicken data search. It is a record to the data put away in the blockchain. For model, given a patient X, recognized by his open key X+, the disclosure

administration offers a rundown of exchanges in the blockchain possessed by X. It should likewise offer an interface to discover X and Y given a pointer to an information document. This administration could be actualized utilizing a NoSQL base that keeps a view (with inevitable consistency) of the blockchain. There is no security issue identified with this part since it just read the blockchain and the inquiries results can be handily checked by the neighborhood duplicates of the blockchain. Furthermore, the Discovery Service can develop to offer essential administrations of a quest for experts.

The design isolates the exchange control (made utilizing the blockchain record) from the information stockpiling (Data Service). We could envision an answer where all information is put away in the record, at the same time, for execution reasons, it isn't practical. One trait of this engineering is to assign the information the board to the clients. The patient claims the information and can erase or limit access to it at whatever point the person needs. The center of the engineering is the arrangement of savvy contracts. They are put away in the records and are liable for:

- Store another exchange in the record.
- Receive and procedure get to asks for.
- Register all information get to allowed.

4. Blockchain Technology

Blockchain innovation is grounded on the idea of an appropriated record, which acts like a database containing information about the authentic setting of trades including those specialists. It is continually evaluated by gatherings of operators (chose by various arrangements, contingent upon the application space). The consequence of each examining is put away in a square and communicate to the system. Squares are consecutively affixed to the record, framing a cryptographically-connected chain. Endeavors to alter the squares or to change their request can be effectively distinguished. The entire network may acknowledge or dismiss the unwavering quality of any square, agreeing to a predefined set of rules. In the event that an operator gets a few legitimate increments to their neighborhood duplicate of the record, they generally pick the longest chain of legitimate squares (or the soonest one, in the event that they have a similar length), disregarding other clashing and less pertinent chains. This thoughtfully basic methodology guarantees that agreement is in the long run reached, even in situations where engendering is delayed because of high system inertness.

So also, sick intentioned hubs may attempt to embed vindictive passages in the record, in any case, the network will just reject their squares and disregard their chain, viably constraining them to maintain the standards.

On the off chance that reviewing is affirmed by the network, at that point the record – perhaps containing later, beforehand unsubstantiated exchanges – is reproduced over the operators. Something else, the biggest acknowledged bit of the record is imitated with data about discords and relating moves to be made – whose impacts are then enrolled as new exchanges to be examined in future rounds of confirmations.

A blockchain based arrangement can, in this way, be conceived to guarantee availability of data in any huge scope framework. It tends to be generally suitable for the dispersion of wellbeing records over a system of social insurance specialists, given that arrangements are given for inertness and capacity prerequisites identified with it, given that (1) peers are required to store duplicates of the record of associations and (2) exchanges and blockchains essentially should be scattered over the system of companions.

Ethereum [Wood 2014] is a blockchain-based stage for completely decentralized applications. It depends on the idea of brilliant agreements, which are techniques that decide successions of activities with the goal for companions to connect with one another. Savvy contracts can be utilized to actualize operators that are applicable to oversee data. For instance, brilliant agreements can contain rules to train access to the substance of scrambled wellbeing data. Along these lines, savvy agreements could permit actualizing a protection layer in a conveyed data framework.

As clarified before blockchain are shaped together by a number of blocks associated together in a distributed organize in this way making decentralized application. The header of these blocks contains hashes of past blocks in them. A block contains three things in it which are information, hash of current block and hash of past block. The information could be anything as it relies upon the sort of blockchain. As if there should be an occurrence of bitcoin, the information comprises of coins that areas a matter of fact electronic money [13]. The hash that is put away in these blocks contains a SHA-256 cryptographic calculation which is utilized for one of a kind ID of a block on the chain.

5. Merits of Blockchain Innovation

Blockchain innovation utilizes a disseminated arrange, containing information in alter safe structures. Blockchain exchanges are just refreshed or included through the formation of new hash esteems and, in this manner, existing exchanges can't be adjusted. To get this, the potential utilization of blockchain innovation should be portrayed against all highlights which make the blockchain remarkable from others:

Distributed ledger: Transactions are annexed in a conveyed framework on the system, which makes framework recuperation by wiping out a solitary purpose of disappointment or brought together substance;

Consensus mechanism: Transactions are possibly refreshed when every single checked client in the system consent to the state of the exchange;

Provenance: The total information or resource's history is accessible on the blockchain organize;

Immutability: Records on the system can't be altered or

messed with; in this manner, all data is secure and trusted;

Certainty: When an exchange is submitted on a blockchain, it can't be altered or turned around; and

Smart contract: The codes are made on a blockchain organize, and the PC and hubs execute on an activated occasion. Thus, the codes are auto-executed inside the time period. To this end, Blockchain can possibly decrease straightforwardness and security issues, for example, trust of outsiders at any phase of an exchange; this implies all middle people or outsiders are disposed of with the coming of blockchain innovation.

6. The Scheme Entities

Patient: The proprietor of individual health records. So as to accomplish asset sharing and diminish the expense of information upkeep, the patient for the most part encodes individual health records and transfers them to the cloud server. In our plan, the patient is for the most part liable for sending the shrewd agreement, producing and dispersing characteristic private key for the client.

Client: Individuals or associations that get to patient's very own health records for inquire about or other helpful purposes.

Cloud server: It stores encoded individual health records and catchphrase files of scrambled individual health records transferred by the patient, and gives the hunt administration to clients with get to rights in the individual health records sharing stage.

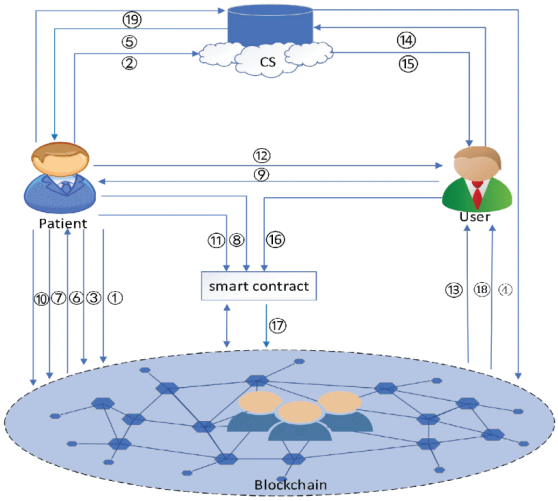

Fig. 2. Scheme model

7. The Workflow of the Scheme

Our plan incorporates four phases: initial stage, individual health records storage, individual health records sharing and individual health records the executives.

A. Initialization Stage

In this stage, the patient instates a few parameters for some time in the future, and conveys the assembled information trustworthiness confirmation agreement to blockchain and records the agreement address and ABI. As appeared in 1 of figure 2.

B. Personal health records storage stage

This stage incorporates three techniques: redistributing arrangement, stockpiling authorization and capacity affirmation. Among them, redistributing arrangement compares to the means step 2, 3 in Figure 2, stockpiling requirement relates to the means 4, 5 in Figure 2, and capacity affirmation relates to the means 6, 7, 8 in Figure 2. Each progression is portrayed as follows:

Step-2: The patient encodes individual wellbeing record set to be re-appropriated to the cloud server with an accessible symmetric encryption conspire and sends the created ciphertext set and the watchword file set to the cloud server.

Step-3: The patient scrambles the key of accessible symmetric encryption conspire with a trait based encryption plan, and spares the ciphertext of the way in to the blockchain through an exchange and records the exchange id.

Step-4: The cloud server stores individual wellbeing record ciphertext set and the watchword list set sent by the patient and constructs a mark dependent on the put away close to home wellbeing record ciphertext set. At that point the mark is spared to the blockchain through an exchange, and the exchange id is recorded.

Step-5: The cloud server sends the exchange id recorded in the progression Step 4 to the patient.

Step-6: The patient peruses the mark of the cloud server from blockchain as indicated by the exchange id sent by the cloud server. When the mark is approved, the patient accepts that the individual wellbeing record ciphertext set put away by the cloud server is right.

Step-7: The patient spares the hash estimations of all encoded individual wellbeing records to the blockchain as exchanges and records all exchange ids.

Step-8: The patient produces watchword files for the hash estimations of all scrambled individual wellbeing records and stores these lists into the information respectability confirmation contract. From that point onward, the patient erases the nearby close to home wellbeing record set and the relating ciphertext set.

C. Personal Health Records Sharing Stage

This stage incorporates four strategies: demand get to, get to approval, individual wellbeing records recovery, and individual wellbeing records check. Solicitation get to compares to steps 9, 10, 11, 12 of figure 2. Access approval relates to step 13 of Figure 2. Individual wellbeing records recovery relating to steps 14, 15 of figure 2. Individual wellbeing records check relating to steps 16, 17, 18 of figure 2. Each progression is demonstrated as follows:

Step-9: The client sends an entrance demand containing his/her character data and Ethereum account address to the patient.

Step-10: The patient chooses a suitable quality set for the client and produces the comparing characteristic private key, and the property private key is encoded with a symmetric key

created through the Diffie-Hellman key trade convention and put away to the blockchain through an exchange, and the exchange id is recorded.

Step-11: The patient includes the client's Ethereum account address to the information honesty check contract.

Step-12: The patient sends the agreement address and ABI recorded in step 1, the exchange ids recorded in steps 3, 10, and the quality set chose in step 10 to the client.

Step-13: The client first peruses the ciphertext of the characteristic private key and the ciphertext of the accessible symmetric encryption plot key from blockchain as indicated by the exchange ids in the message sent by the patient. At that point, the client successively executes the unscrambling calculation of the symmetric encryption plot and the decoding calculation of the credit based encryption plan to reestablish the characteristic private key and the accessible symmetric encryption conspire key.

Step-14: The client creates a token utilizing the key of the accessible symmetric encryption plot got in step Step13 and the catchphrase he/she is keen on, and afterward sends the token to the cloud server.

Step-15: The cloud server plays out a pursuit as indicated by the token got from the client and returns indexed lists to the client.

Step-16: The client calls the information uprightness confirmation contract with the token that is created in step 14.

Step-17: The information uprightness confirmation contract reacts to the client's solicitation, plays out the pursuit and recoveries the looked through exchange id set to the blockchain as occasions.

Step-18: The client gets the exchange id set returned by the information honesty confirmation contract through observing the blockchain, and peruses the hash estimations of the objective documents from the blockchain as per the exchange id set. Afterward, the client confirms the trustworthiness and rightness of the indexed lists returned by the cloud server dependent on the hash esteems read from the blockchain.

D. Personal Health Records Management Stage

In the stage, the patient transfers the recently created individual wellbeing records to the cloud server or erases some encoded individual wellbeing records put away in the cloud server, which relates to step 19 of figure 2.

8. Design Objectives

Accessible encryption instruments and property based encryption systems can viably address the issues of protection release, constrained catchphrase search capacity, and access control when sharing individual wellbeing records in the distributed storage. In any case, it will likewise present another arrangement of difficulties. Right off the bat, there are countless individual wellbeing records, despite the fact that security assurance and fine-grained get to control can be accomplished by legitimately scrambling them with a quality based encryption plot, the plan is wasteful. The blend of symmetric encryption and trait based encryption is a successful method to take care of this issue. Be that as it may, the issue of the key security in the encryption conspire should be settled earnestly. To take care of this issue, our plan utilizes blockchain to acknowledge key administration and dissemination. Specifically, considering the expense of putting away information on the blockchain, our plan receives the property based encryption plot with steady ciphertext length, and security evidence of the plan is explained in literature [10].

Furthermore, in the characteristic based plan, the trait authority creates and deals with the quality private keys for the framework members may prompt issues, for example, key maltreatment and security spillage. To take care of this issue, our plan makes the patient go about as the ascribe position to create and circulate the quality private key for the client.

What's more, furnishing approved clients with the capacity to rapidly recover information is an interesting point when sharing individual health records. To accomplish this objective, we develop a file building calculation dependent on literature [9], and store the watchword list set of scrambled individual health records created by the calculation to the cloud server.

At long last, accomplishing effective information honesty confirmation is additionally a critical issue to be tackled when sharing individual wellbeing records. In our plan, the hash estimations of encoded individual health records are put away in the blockchain, and the significant file set is put away in the keen agreement, which gives another plan to take care of this issue. In addition, so as to assist patients with dealing with their own health records redistributed to the cloud server, file update and list cancellation calculations are built in our plan.

9. Conclusion

In this paper we examined how blockchain innovation can be valuable for medicinal services division and how might it be utilized for electronic health records. Regardless of the headway in medicinal services area and mechanical development in EHR frameworks they despite everything confronted a few issues that were tended to by this novel innovation, i.e., blockchain. Our proposed system is a mix of secure record stockpiling along with the granular access rules for those records. It makes such a framework, that is simpler for the clients to utilize and comprehend.

Individual medical records sharing plan is proposed. In the new plan, the patient produces and conveys the trait private key for the client, empowering the plan to accomplish fine-grained get to control without depending on any outsider. Likewise, in view of the blockchain has the qualities of decentralization and sealed, the utilization of the blockchain to keep up keys in the plan makes the administration and dissemination of keys progressively secure. Besides, the hash estimations of encoded individual medical records are put away on the blockchain, and the related list set is put away in the shrewd agreement, so the individual medical records beneficiary can helpfully and

rapidly confirm the honesty of scrambled individual medical records got from the cloud server. Despite the fact that our plan takes care of a portion of the issues in the current individual medical records sharing plans. In any case, how to check whether the cloud server performs document update and record erase activities as indicated by the patient's necessities during the individual medical record the executives stage despite everything needs further research. What's more, the job based access additionally benefits the framework as the clinical records are just accessible to the trusted and related people. This additionally takes care of the issue of data asymmetry of EHR framework.

References

[1] M. Reisman, “EHRs: The Challenge of Making Electronic Data Usable and Interoperable.,” *P T*, vol. 42, no. 9, pp. 572–575, 2017.

[2] W. W. Koczkodaj, M. Mazurek, D. Strzałka, 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.

[3] 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.

[4] A. McLeod and D. Dolezel, “Cyber-analytics: Modeling factors associated with healthcare data breaches,” *Decis. Support Syst.*, vol. 108, pp. 57– 68, 2018.

[5] L. Coventry and D. Branley, “Cybersecurity in healthcare: A narrative review of trends, threats and ways forward,” *Maturitas*, vol. 113, pp. 48–52, 2018.

[6] “The Future of Health Care Cybersecurity,” *J. Nurs. Regul.*, vol. 8, no. 4, Supplement, pp. S29–S31, 2018.

[7] D. Spatar, O. Kok, N. Basoglu, and T. Daim, “Adoption factors of electronic health record systems,” *Technol. Soc.*, vol. 58, no. February, p. 101144, 2019.

[8] 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.

[9] R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions", *Proc. ACM Conf. Comput. Commun. Secur.*, pp. 79-88, 2006.

[10] N. Attrapadung, J. Herranz, F. Laguillaumie, B. Libert, E. de Panafieu and C. Ràfols, "Attribute-based encryption schemes with constant-size ciphertexts", *Theor. Comput. Sci.*, vol. 422, pp. 15-38, Mar. 2012.

[11] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson and T. Hayajneh, "Healthcare blockchain system using smart contracts for secure automated remote patient monitoring", *J. Med. Syst.*, vol. 42, no. 7, pp. 130-138, 2018.

[12] C. Lin, D. He, X. Huang, K. K. R. Choo and A. V. Vasilakos, "BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0", *J. Netw. Comput. Appl.*, vol. 116, pp. 42-52, Aug. 2018.

[13] C. Lin, D. He, X. Huang, M. K. Khan and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems", *IEEE Access*, vol. 6, pp. 28203-28212, 2018.

[14] S. Wang, Y. Zhang and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems", *IEEE Access*, vol. 6, pp. 38437-38450, Jun. 2018.

[15] Y. Zhu, Y. Qin, Z. Zhou, X. Song, G. Liu and W. C.-C. Chu, "Digital asset management with distributed permission over blockchain and attribute-based access control", *Proc. IEEE Int. Conf. Services Comput. (SCC)*, pp. 193-200, Jul. 2018.

[16] Y. Zhu, Y. Qin, G. Gan, Y. Shuai and W. C.-C. Chu, "TBAC: Transaction-based access control on blockchain for resource sharing with cryptographically decentralized authorization", *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, pp. 535-544, Jul. 2018.

[17] M. Baza, M. Nabil, N. Lasla, K. Fidan, M. Mahmoud and M. Abdallah, "Blockchain-based firmware update scheme tailored for autonomous vehicles", Nov. 2018,

[18] K. Fan, Y. Ren, Y. Wang, H. Li and Y. Yang, "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G", *IET Commun.*, vol. 12, no. 5, pp. 527-532, Mar. 2018.