IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 09, Issue 10, October. 2019, Series -IV, PP 38-43

Evading Intrusion and Protection for Patient Information in Electronic Health Records System

Panchareddy Gayathri[1], Dr. A.Mary Sowjanya[2]
[1]*M.Tech Scholar (IT), Dept. of Computer Science and Systems Engineering,*
[2]*Assistant Professor, Dept. of Computer Science and Systems Engineering, Andhra University College of Engineering (A), Visakhapatnam, Andhra Pradesh, India.*
Received 16 October 2019; Accepted 31 October 2019

Abstract: Cloud computing is a rising as additional processing worldview in the medical part other than different business. Storing the medical information in cloud makes the treatment effective by recovering patient's medical history from the database. This framework gives a situation where patient's records are stored and it will be referenced by the specialists to improve the efficiency of the treatment. This handles the medical history of every person of the nation and gives access to every single enlisted hospital to peruse or refresh the information. The hospital which accesses the database must be enlisted and more likely than not got a permit. Also, even any hospital staff can peruse paper documents which shouldn't be seen, as long as they have physical access to the record. So in this work, an endeavor is made to give top of the line security to the patient's delicate information. At whatever point the patient go for a treatment, their medical information will be stored into the database utilizing their recognizable proof number. We propose a plan to help undertakings to effectively share secret information on cloud servers utilizing Hierarchical attribute based encryption algorithm.

Keywords: Block chain, Data Privacy, Electronic Health Records, Patient-Centric.

I. INTRODUCTION

The social period of human services, for example, Patients-Like Me, can procure information from other tantamount patients through information about the customer's specific discoveries. Albeit sharing medical information about relational association is helpful for the two patients and authorities, delicate information can be spilled or taken, which causes security and security issues without delivering profitable information. This medical information in the interpersonal organization is valuable for the two patients and specialists, private information can be spilled or taken, which causes security and security issues without compelling insurance of shared information. Notwithstanding the way that this procedure can prompt a situating, wherein people are fascinated, the estimation of the gauge could be substantial. A healthbased information accumulation based plan was displayed to ensure and include various kinds of health care information. The article looks at security and insurance issues in flexible human help frameworks, including security affirmation for the government managed savings information aggregate, security for information arrangement and unfortunate behavior [2]. It is an exhibit of versatile security, especially for information driven applications, in a circumstance based on dispersed processing to guarantee information protection, information unwavering quality and access control to application information. Gives a careful examination of security affirmation in human services with the assistance of the cloud. Advanced medical information and pictures are likewise much of the time been traded all through the world consistently through Internet. These information can be seen or controlled during their transmission by means of a non-controlled channel. Anyway the current arrangements can secure the patient information during transmission, yet can't stop within assault where the director of the patient database uncovers the delicate patient information. Step by step, private medical records are progressively being stored at server farms by hospitals or firms. Many advanced algorithms are produced for prescient investigation of medical information so truth be told, an ever increasing number of activities will be done over private patient information. So there's need of worries about the security for touchy information since medical information are stored remotely, off-premise server farms. Specifically in any of the health area, a delicate patient record must be kept private. Security of such touchy information must be ensured, in the event that it is scrambled by the information proprietor before it is being stored in server farms. Accordingly, just the verified information proprietor will have the option to access the information by unscrambling it utilizing given private decoding key. Encryption procedure limits the likelihood to re-appropriate algorithm over the remotely stored information, particularly if the server farm have no access to the unscrambling key, since the key is especially basic, for any standard encryption plans, to decode the information by playing out certain algorithm upon it. This framework approves the doctor and medical specialist.

II. RELATED WORK

Different health related fields in which we have seen a coordinated effort with blockchain are portrayed underneath. Electronic Health Records are a safe and helpful method for dealing with the patient's assets and information. In current framework just specialists approach patient's information but since of EHRs patients can approach their own information and they can choose which information they need to share by utilizing different attribute signature scheme.[1] Designing an effective key administration conspire for securing mental information as in health blockchain there is an issue of imposing business model of mental information and there is a tremendous need to improve the strength of information. [2]. Coordinated effort of EHRs and doctors has prompted a powerful healthcare framework that is progressively secure, safe to use by patients and has practically every one of the answers for patient related issues. [3]. Healthcare design that incorporates BSN cell phones (sensor information supplier) and has a patient driven methodology, understanding driven and has blockchain and healthcare given interface that persistently screens the state of patients and sends updates to the concerned hospital or specialist so that incase of any crisis medical aid would be given by specialists by changing the working of machines by hospital itself. Square chain gives that the message passed is sealed, accessible consistently and keeps away from single purpose of disappointment [4]. We realize that blockchains are open and the information in them is open, so the security of the information lies in the key, we have to choose a key administration plot for improving the security of our information and making it alter safe. For this we are planning a lightweight reinforcement framework and a key recuperation framework utilizing a BSN for structuring the necessary plan. [5] Metric information is produced for computing dyslexia in kids. With portable mixed media, IoT and auto evaluating algorithms consolidated together we plan a framework which tells us about the level of dyslexia in a patient and can be shared over the globe by versatile medical experts. [6] Using shrewd agreements and access control system to think about the information and abrogate the access to information if there should arise an occurrence of any infringement of information. A model is planned so as to share information by utilizing blockchain between cloud administration providers.[7] By accessing the electronic health records specialists, doctors and attendants spare a ton of time that was generally lost in documentation and experiencing all the past medical history of the patient. It additionally prompted cost decrease, less desk work and age of a powerful electronic health record framework [8] Blockchain is utilized in building keen agreements, to build up a procedures that permits to communicate in a trust less and auditable way. The contacts made are cryptographically certain and can't be changed subsequently guarantee that both the gatherings comply with the standards of the agreement. [9] In a beekeeper framework, Homomorphic algorithms should be possible on an information without taking in anything from them. Its issue tolerant as its convention works successfully until limit quantities of servers are straightforward and dynamic [10]. Blockchain is utilized to give a more extensive stage to the understudies, as they can access every one of the stages in regards to their concentrated based on their credits. It gives a decentralized just as all inclusive confided in stage for understudies [11].

III. HOW BLOCKCHAIN WORKS

The term “Blockchain” refers to the way BC stores transaction data – in “blocks” that are linked together to form a “chain.” The chain grows as the number of transactions increases. Since every entry is stored as a block on a chain, the care you receive is added to your personal ledger. At its core, blockchain is a distributed system recording and storing transaction records. In a blockchain system, there is no central authority. Instead, transaction records are stored and distributed across all network participants. Rather than having a centrally located database that manages records, the database is distributed to the networks and transactions are kept secure via cryptography. BC eliminates the need for a middleman that traditionally may facilitate such transactions. The Blockchain was designed so transactions are immutable, i.e. they cannot be deleted. Thus, Blockchains are secure and meddle-free by design. Data can be distributed, but not copied. When it comes to digital assets and transactions, you can put almost anything on a Blockchain. Different scenarios call for different Blockchains. The BC technology currently has the following features [2,3]:

1. Peer-to-Peer (P2P) Network: The first requirement of BC is a network, an infrastructure shared by multiple parties. This can be a LAN at a small scale or the Internet at a large scale. All nodes participating in a BC are connected in a decentralized P2P network. Transactions are broadcast to the P2P network. Due to some limitations of P2P networks, some vendors have provided cloud-based BCs.

2. Cascaded Encryption: A BC uses encryption to protect transaction data. Blocks are encrypted in a cascaded manner, i.e. the encryption result of the previous block is used in encrypting the current block. The BC is secured by public key cryptography, with each peer generating its own public-private key pairs.

3. Distributed Database: A BC is digitally distributed across a number of computers. Each party on a BC has access to the entire database and no single party controls the data or the information. Since BC is decentralized, there is no need for central authorizes such as banks.

4. Transparency with Pseudonymity: Each node or participant on a blockchain has a unique 30-plus-character alphanumeric address that identifies it. Users can choose to remain anonymous or provide proof of their identity to others.

5. Irreversibility of Records: Once a transaction is entered in the database and the accounts are updated, the records cannot be altered. Records on the database is permanent, chronologically ordered, and available to all others on the network.

IV. DATA ACCESS CONTROL MODELS AND TECHNIQUES

Data Access Control is one of the most important technologies to ensure adequate security of cloud computing. There was some traditional access control model which originated in the year of 1970s with the aim to prevent malicious users from accessing resources and avert them to use the potential resources illegally.

Access control mechanisms are a necessary and crucial design element to an application's security. In general, a web application should protect front-end and back-end data and system resources by implementing access control restrictions on what users can do, which resources they have access to, and what functions they are allowed to perform on the data. Ideally, an access control scheme should protect against the unauthorized viewing, modification, or copying of data. Additionally, access control mechanisms can also help to limit malicious code execution, or unauthorized actions through an attacker exploiting infrastructure dependencies (DNS server, ACE server, etc.).

Before selecting the data access control mechanisms, there are several fundamental steps that lend a hand speed up and elucidate the design process;

1. Try to quantify the relative value of information to be protected in terms of Confidentiality, Sensitivity, Classification, Privacy, and Integrity related to the organization as well as the individual users. Designing complicated and inconvenient data access controls around uncategorized or non-sensitive data can be counterproductive to the eventual goal or principle of the web application.
2. Determine the relative interaction that data owners and creators have within the web application. Some applications may restrict any and all creations or ownership of data to anyone but not the administrative or built-in system users.
3. Specify the process for granting and revoking user access control rights on the system, whether it is a manual process, automatic upon registration or account creation, or through an administrative front-end tool.
4. Clearly, delineate the types of role driven functions of application support. Try to determine which specific user functions should be built into the web application (logging in, viewing their information, modifying their information, sending a help request, etc.) as well as administrative functions (changing passwords, viewing any users data, performing maintenance on the application, viewing transaction logs, etc.).
5. Try to align access control mechanisms as close as possible to the organization's security policy. Much of information from the policy can map very well over the carrying out of access control (acceptable time period of certain data access, types of users allowed in seeing certain data or performing certain tasks, etc.). These types of mappings usually work in the most excellent way with Role Based Access Control.

There are a plethora of accepted data access control models in the information security territory. Cloud computing is dynamic in nature and it supports the following traditional Access Control Models, such as Discretionary Access Control (DAC), Mandatory Access Control (MAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC). Data Access Control actually refers to the control over access to the various system resources after a user's account testimonials and distinctiveness have been legitimated and access to the system approved. For example, a specific user, or group of users, might only be given access to certain files after logging into a system, while simultaneously being deprived of access to all other resources.

A. Discretionary Access Control

Discretionary Access Control (DAC) is used to limit access to information based on the distinctiveness of consumers and/or membership in certain clusters. Access decisions are typically based on the authorizations granted to a user based on the credentials that the owner presented at the time of authentication (username, password, hardware/software token, etc.). Typically in DAC models, the owner of information or any resource is able to change its permissions. The downside of this method is overseer not been able to administer these authorizations on files/information loaded on the web server.

B. Mandatory Access Control

Mandatory Access Control (MAC) is the strictest among all levels of control and is primarily used by the government. MAC takes a hierarchical approach in controlling access to the resources. In this environment, the system administrator has sole responsibility for defining access control to all resource objects such as data files. In this model, security labels are assigned to all resource objects. These security labels contain two kinds of

information - a classification (top secret, confidential etc.) and a category (management level, department or project to which the object is available).

When a user requests to access a resource, the operating system checks the user's classification and categories and compares them to the properties of the object's security label. If the user's testament matches the MAC security tag properties, the access is permitted. It is important to note, does both the classification and categories match. A user with top-secret classification, for example, cannot access a resource if they are not only a member in one of the required categories of that object. MAC requires a careful planning to implement. Once it is put into operation, it enforces a high system administration overhead due to necessitate evenly updating of object and accounting labels to have a room for new data, new users and modifications in the categorization and classification of existing users.

C. Role Based Access Control

Another name of this is called as Non-discretionary Access Control and uses real-world approach in structuring access control. Access under RBAC is based on user's profession function within the organization to which the computer system fits in.

Essentially, RBAC assigns special permissions to particular cadres in an organization. For instance, an accountant in a business will be allocated to the Accountant role, achieving access to all the resources legalized for all accountants on the system. Similarly, the developer role can be assigned to software engineer. A user under RBAC may only be assigned a single role in an organization. The accountant illustrated above obtains the same authorizations as all other accountants, nothing more and nothing less.

D. Rule-Based Access Control:

Rules-Based Access Control, access is allowed or denied to resource objects based on a set of rules defined by a system administrator. In this model, access properties are stored in Access Control Lists (ACL) associated with each resource object. When a meticulous account or group endeavors to access a resource, the operating system verifies the rules contained in the ACL for that resource.

Rules-Based Access Control includes conditions such as allowing access to an account or a group to a network connection in certain hours of the day or days of the week. As all access permissions are controlled solely by the system administrator, the user cannot change anything.

V. Blockchain Applications

Blockchain has the potential for addressing significant healthcare issues. Here are the most likely applications [6]:

- ***Medical Data Management:***The healthcare industry is drowning in data— patient medical records, complex billing, clinical trials, medical research, etc. Some of the record pieces are with the primary doctor, some with specialists, and some on devices that track one's health. This way care providers can have the complete medical history of the patient. For health care to reap the benefits of a blockchain-based medical record, it must grant access to everyone that might need patient's information [7].
- ***Drug Development:*** Blockchains can facilitate new drug development by making patient results more widely accessible. It can help reduce the counterfeit drug implications. Blockchain technology is an excellent counter to threats that are rapidly approaching (integrity-based attacks) and it is a good forward-looking tool we might deploy to address them. BC will also enable drug developers to run clinical trials and share medical samples more securely [8].
- ***Clinical trials:*** Using blockchain can make clinical trials reliable at each step by keeping track and time-stamping at each phase of the trial. This could reduce waste. Another blockchain use-case would be the adoption of electronic informed consent in clinical trials. BC improves accountability and transparency in the clinical trial reporting process.
- ***Data Security:***Blockchain technology has the potential to be the infrastructure that is needed to keep health data private and secure. Other applications include counterfeit drug prevention and detection, validation and payment of claims, clinical trial results, outcome-based payments, reimbursement of healthcare services, exchange of health data, and supply chains [9].

VI. PROPOSED METHOD

The main architecture consists of mainly three nodes, patient node, service provider node and Physician node. Let us see what happens at each phase of the system.

a. Patient node: The patient will have all the health records issued by the provider. Now in the ethereum client, with the help of the smart contract he will edit the access permissions for the records to prevent the file from scattering across different nodes. Nucypher key management system is used with umbral to provide double encryption for the records.

b. Service provider node: The service provider especially the health organisation maintains the individual reports. These reports are sent to the end user safely. They also participate in the Blockchain network to initiate a transaction bounty is requested.

c. Physician node: The Physician request the end customer that is the patients to send the reports to check his health status. The patient would provide the view permission to doctor to view the patient record. The medical blockchain will transparently offer data on a while, wherein and for what motive the healthcare records modified into used. Access to all medical facts on the scientific blockchain is managed by way of the person, which prevents malicious get entry to medical information from the resource.

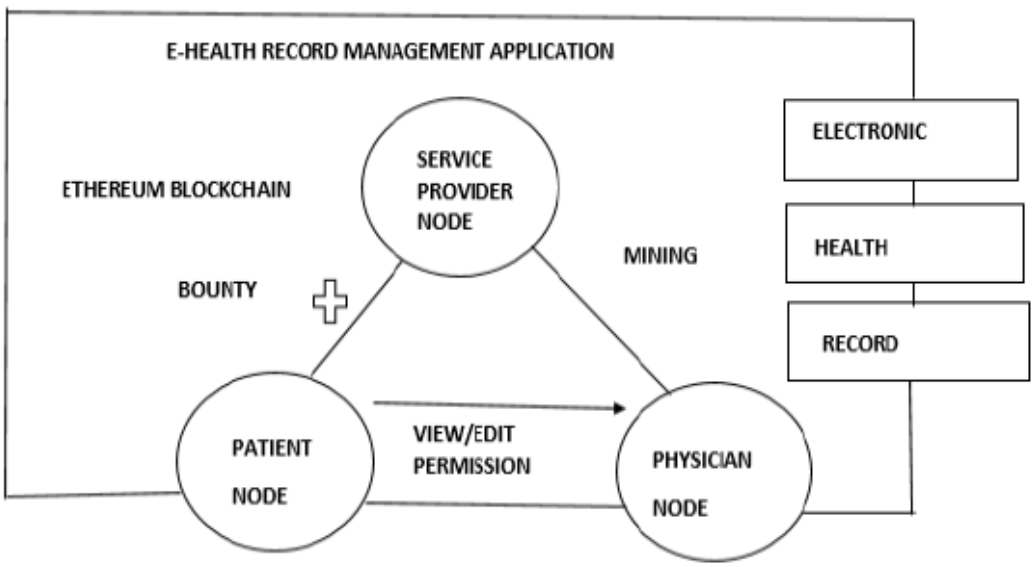

Figure.1. Proposed Architecture of E-Health Record System using Blockchain Technology

VII. CONCLUSION

The blockchain revolution has made its way to the healthcare industry, and leaders are now wondering what is possible and how blockchain can solve many issues that plague the industry. BC is the technology that will possibly have the greatest impact on the next few decades; not social media or big data or robotics. Although BC is not fully mature, the healthcare system can take advantage of a beneficial disruptive innovation that will stand the test of time like blockchain. Blockchain has great potential for the future and will cause disruptive changes in the healthcare industry.EHR'S in collaboration with blockchain provides following features: accurate, up-to-date, and complete information about patients at the point of care , Enabling quick access to patient records for more coordinated, efficient care, Securely sharing electronic information with patients and other clinicians, Helping providers more effectively diagnose patients, reduce medical errors, and provide safer care, Improving patient and provider interaction and communication, as well as health care convenience

REFERENCES

[1]. Multiple Authorities for Blockchain inElectronic Health Records SystemsRUI GUO, HUIXIAN SHI, QINGLAN ZHAO, and DONG ZHENG
[2]. IlyaSukhodolskiy, Sergey Zapechnikov, "A blockchain-based access control system for cloud storage", 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow, 2018, pp. 1575-1578.
[3]. Maithilee Joshi, Karuna P. Joshi, and Tim Finin, "Attribute-Based Encryption for Secure Access to Cloud-Based EHR Systems", 2018 IEEE International Conference on Cloud Computing.
[4]. Javier Herranz, Fabien Laguillaumie, Benoˆıt Libert, and Carla Ra`fols, "Short Attribute-Based Signatures for Threshold Predicates"
[5]. A. English and J. Lewis. "POLICY FORUM: Privacy Protection in Billing and Health Insurance Communications," American Medical Association Journal of Ethics, Vol 18, No 3, 2016, pp. 279-287
[6]. L. Zhuo-Rong, C. En-Chi, H. Kuo-Hsuan, and L. Feipei. "A secure electronic medical record sharing mechanism in the cloud computing platform." 2011 IEEE 15th International Symposium on Consumer Electronics (ISCE), IEEE Conferences, 2011, pp. 98-103
[7]. K. KissiMireku, F. Zhang, and K. Gbongli. "Patient knowledge and data privacy in healthcare records system." 2nd International Conference on Communication Systems, Computing and IT Applications (CSCITA), IEEE Conferences, 2017, pp. 154-159
[8]. R. Pankomera and D. Van Greunen, "Privacy and Security Issues for a Patient-centric Approach in Public Healthcare in a Resource-Constrained Setting," Conf. Proc., 2016, pp. 978–1

[9]. R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure AttributeBased Signature Scheme with Multiple Authorities for Blockchain in Electronic Health Records Systems," IEEE Access, 2018, vol. 3536, pp. 1–1.
[10]. S. Sharma, K. Chen, and A. Sheth, "Towards Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems," 2018.

Authors

PANCHAREDDY GAYATHRI Holds a B.Tech Degree in Computer Science & Engineering from Dr.L.Bullayya College of Engineering for Women Affiliated to Andhra University, Visakhapatnam. She presently Pursuing M.Tech (IT) in Department of Computer Science and Systems Engineering from Andhra University College of Engineering,Visakhapatnam. Area of interest include Compiler Design,Cryptography,FLAT,Web Technologies,Web Programming and Blockchain Technologies.

Dr. A.MarySowjanya Working as Asst. Professor, Department Of Computer Science and Systems Engineering In Andhra University, Visakhapatnam. Her Area of interests include Machine Learning, Classification Data Mining and Knowledge Discovery, Sentiment Analysis.

Panchareddy Gayathri." Evading Intrusion and Protection for Patient Information in Electronic Health Records System." IOSR Journal of Engineering (IOSRJEN), vol. 09, no. 10, 2019, pp. 38-43