ISSN 2278-3091
Volume 9 No.2, March -April 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse110922020.pdf
https://doi.org/10.30534/ijatcse/2020/110922020

An Effective Method to Secure Electronic Health Record Based on Block Chain Technology

Ch. Himaja, Y. Sriram Chowdary, Dr Amarendra K , Dr S Ananthakumaran

Department of Computer Science and Engineering,
Koneru Lakshmaiah Education Foundation,
Vaddeswaram, Guntur, Andhra Pradesh, India
amarendra@kluniversity.in

ABSTRACT

Personal Health Records (PHR) is an rise of patient-eccentric model for health condition exchange information, which is unremarkable source for maintenance at the third party, similar to the Cloud Supplier. Still, their is broad privatizes considerations as a Personal Health Data may be open to the third party server or the unauthorized party. To assure the patient's records management, is made easily accessed to their own PHR by the code, It is similar to the methodology of the cipher PHR before outsourcing the data.As yet, issue like probability of privacy exposure is complex, measurable in the key management,the flexible access and the efficient user revocation, has to be remained as the complex challenges towards achieving the fine-grained, cryptography to enforce the data access control. In this report, We have an tendency to propose the completely unique patient-eccentric theoretical account and a set of mechanism for the knowledge access the management to PHR, kept in trusted server. For the achievement of fine-grained & ascend-able knowledge access the management to PHR, So we have the tendency to leveraging attribute based mostly encoding (ABE) technique to cipher every patient's records. Differ from the preceding work to protect the knowledge outsource, their is an possibility for concentrating on the multiple knowledge owner state of transaction & split the user in the scheme to multiple due to security region,which will decrease the key management quality to proprietor and the users.The state of patient's privacy is to be secure in the same time period by exploiting the multiple number of authorities. The theme collectively permits the dynamical modified to access policy (or) the file attribute, to support the economically the on-demand users (or) attribute to there vocation and the break-glass method to access the underneath emergency brake situations.

Key words : Electronic Health Record(EHR), Blockchain Technology, URL, Data Storing.

1. INTRODUCTION

Now a days, people are more concern about the health related issues. People are very conscious about the health and want to take care by themselves like storing all the health information with them and also of maintaining a lots of files which leads to confuse. Not only the common people but also the celebrities, public servants, elite business group persons want to keep their health related information in secret by storing the data in their individual servers without leaking to public. For example, if the famous person is suffering with any secret disease like AIDS, HIV or any dangerous cancer then the persons may be humiliated by public. Also by knowing their health information by themselves can make them more conscious about their health and no need to depend on any other person about their health related data. So that we are using some techniques to provide security to the patients data from the hacking. Block chain helps us to provide the security to the data by using the previous key to the server and the data is confidentially protected.

2. LITERATURE SURVEY

In e-Health, patient information data from the Electronic Health Records (EHR) could be collected from the aggregate resources, such as the wearable device, smart sensor & medical used equipment[6]. It has been reported to the quantity of patient information data is growing at them rate of 48 percent per annual for reaching 2,314 ZB by 2020. According to the United States, there are more than 2,181 cases based on health care violation data between 2009 to 2017, resultant to the revelation of 17,67,09,305medical data of the patient records in the health and human services department[5]. As the outcomes, the protecting for the patient's medical data has to be transformed into an important content in the Health records. Though the encryption addresses the some of the underlying safety and legal issue to the EHR, is accessed by the controllers, in particular this is very challenging for implementing the effectiveness due to the highly distributed and disintegrate the nature of EHR

data, the colonial state between the data owners and the users. Consequently, supplying the flexible & the pulverized accessible control solvent for the storing data is a overriding involvement. Lately, Block chain have recommended to show the similar result for the PHR data management. The inbuilt is secured by using the blueprint of the characteristic of the Block chain-based infrastructure should have the latent to furnish the Tamper-proof log to the approachable/accessible events of the EHR. In this peculiar state, the approachable events are substantiated and the transcribed through the consensus performance is addition to the earlier state of Block chain. However, the expected from the EHR management, is the traditional Block chain-based methods to sustain from two residential drawbacks. First, though the Block chain can guarantee data integrity, it miss the right access control mechanism to include the dealings performed by the assorted associates. Next, the storing size of blocks in the Block chain is constricted to provide EHR data hold in X-rays and videos (like, ultrasonically visible images). The report proposes the complex architecture by using the Block chain and the Edge nodes to assist the attribute-based accession for the control of EHR data[9]. Generally, the hyper ledger composer fabric Block chain executed by the smart contracts which is programmed along with the Access Control Lists (ACL) for implementing the identity-based approach to the standard of the EHR data and the log legal access to the physical phenomenon of the Block chain for penetrability and accountability[7]. In the cooperation with the edge nodes accumulated with the PHR data will promote the enforced data to the Attribute Based Access Controlled (ABAC) to the EHR data with the policies nominal in the abbreviated language or the authorization (ALFA). The abbreviated language maps the forthwith to the Extensible access control Mark up Language (XACML), it also gives the compendious cognitive content. An constituent, Hash digest, it is utilized to defend the unity of stored data in the EHR data accumulated in the Edge nodes, that assist in detecting the modification in EHR. Moreover, the one-time used self-destroying URL, Incorporated with the IP addresses of the EHR data in the edge nodes, that are documented with the Smart contracts, which will being returned with health care furnish after the eminent executing of the ACL way to the policy. The health care provider then uses URL to the accession of the PHR data for the edge nodes. Hence, the desirable users for the patient health record who passes the ABAC obligatory from the edge nodes, that could be accessible by requesting the PHR data. For authorizing the design, using the hybrid architecture is by the Hyper ledger Composer Fabric program. To step-up, we have to conduct many experiments to confirm the Smart contracts and access to the control policy, shows the planned method is maintained by a traceable access and the dealing data records from the EHR managements. The report evaluates the system operations through many experiments of the transaction processed in required time and intermediate outcome time is against the illegitimate PHR data is requested below the various settings.

2.1 Block Chain

Block chain is an secured ledger. It manage increasing lists of transaction data in an hierarchically extending blocks of chains with the every block is restrained by the using some techniques to obligate fortified unity of the transaction data. The new blocks are only bound up to the central Block chain based on the flourishing competition of an decentralized agreement of the procedure[11]. Abstractly, the gain to the data about transaction recorded in a block, which also hold over the hash value in the whole block by itself, can be seen its crypto-graphical image and the hash worthy of foregoing blocks, that functioned has an crypto-graphical link to previous block in Block chain[4].

An decentralized agreement of process implemented by the system, that controls the -

1. Acknowledgment of new block to the block chain method.
2. Read protocols to assure the confirmation of the block chain.
3. Consistence info of content in the dealing of records encapsulated in copy of the every block chain retained on every node.

As the result, the block chain assure that after the dealing record is additive to a block and also a block have been with the achievement created and engaged to the block chain, the dealing records may not be edited or declared retrospectively [2], the unity of information complacent in the each and every block of the block chain are warranted, and the block, which is bound up to the block chain, that cannot be manipulated by any means. Therefore, Block chain functions as a secured and the distributed ledger, that collects all the proceedings between an open-sourced network system effectively, continual, and an verifiable mode. While considering the Bit coin system, block chain is engaged with secured, private and responsible public depository for all kind of transactions that crafts the bit coin on the Bit coin networking system[1]. This guarantee that all the bit coin proceedings are recorded, configured and stored in the crypto-graphical bonded block, that are chained in an verifiable and relentless mode[10]. Block chain is importantly shielded in the securing bit coin proceedings for some illustrious and strong security, more privacy and trust problems, as more spending, unofficial revealing of secluded proceedings, dependence in the entrust authority, and entrust goodness in an decentralized computing's[8].Bit coin ways to the distribute block chain had being the idea for some other

applications as health care, logistics, education certificates, cloud sourcing, secured storage[3].

3. PROPOSED MODEL

It elaborate the complex design to facilitate access to the management of EHR knowledge by the pattern of each block chain and the edge node.The following entities are played an major role in this method.

Patient: It is an entity which possess the PHR information to be accessible and also specify the policy of the PHR data accessing in one's own.

Health care Provider: An health care provider is entity which necessarily accessed the PHR data by patients by themselves and desire the accessibility to authorities to the patient.

Smart sensor(imaging equipment): An device that collects the PHR information from patients and sent to end users. It can also consider X- rays and so on, that yields the PHR data from the patient.

EHR data: It is a small part info that is closely-held by the patient and accessible only to the approved health care providers like hospital authorities.

Edge node: An computation with depository device that stock the PHR information and attaches to the ABAC policy.

Block chain: Block chain is used as an back end provider and stores all the information that is provided by the health care providers.

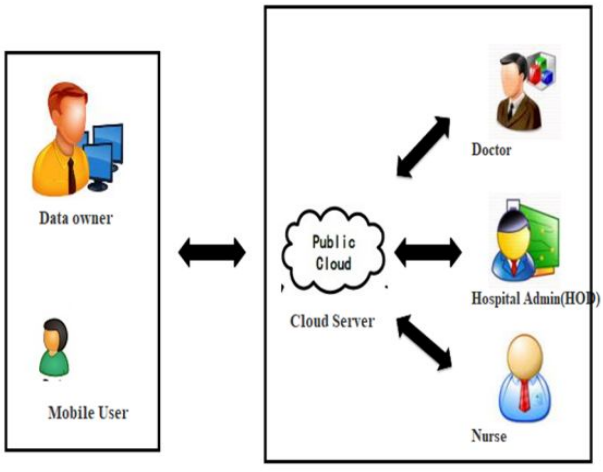

Figure 1. : System Architecture

As shown in Fig. 1. of the proposed system, the e-Health records of a patients' personal records have been stored with the nurse, who is handling all the patient details. The medical details like symptoms, the disease and tests related to diagnosis of the disease are stored with the doctors. The data stored with the doctor and nurse of a particular patients' information can be identified by a unique patients id-number. The patients personal information are given to the nurse server by the data owner. The complete personal and medical details are stored in the server and the Hospital administrator. Here the block chain server will take the information from the data owner and provide some security steps and transfer the data based on it type to the other modules like doctor,nurse and hospital admins. The security is provided to the information by the secret key which is only visible to the administrator. If any detection of using the secret key in wrong purpose then the user and the user using IP address will be Blocked. By login with user-id, can get only details related to the patient's medical information, But login with admin-id, can the information related to the patients personal and medical information.

4. OUTCOME

As shown in Fig. 2.The patient can login to the hospital website and the admin can also login by using his password which is created while programming, which is different to the user, he has to create his account in the website by providing the following information along with the Ip address which we are using.

As shown in Fig. 3.The data owner who will forward the information of patient to the other modules like nurse, doctor and hospital administrator can be done. The data owner will get all the information of the patient while login to website and send the data to that particular module based on the information type.

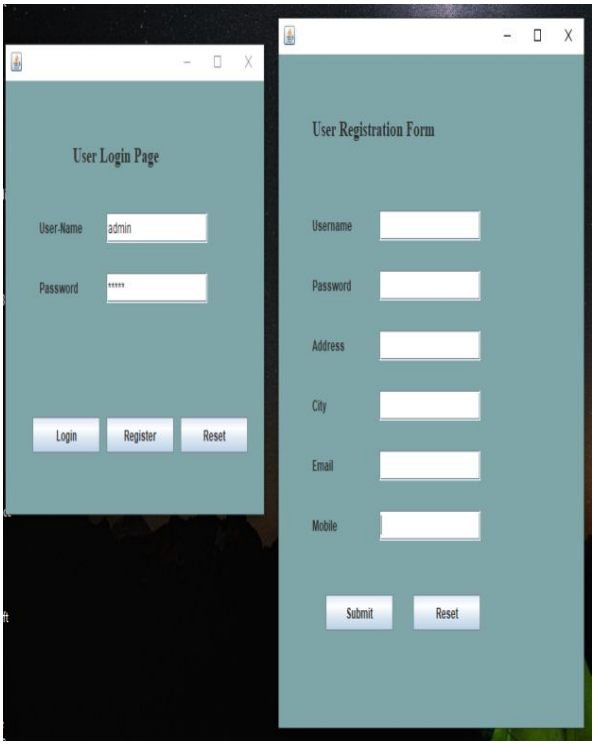

Figure 2: Login page

As shown in Fig. 4, the patient personal details is stored by filling the required information by the hospital staff at the reception and submitting it by providing the ip address. The medical report can be filled by the doctor based on the patients medical test reports which done only by the doctors and access is given to all the doctors in the hospital by entering the unique patients id-number.

The medical summary, which contains all the personal and medical information related to every patient by their id number. In this, we browse the patients details and also can be modified only by the authorized users like admins.

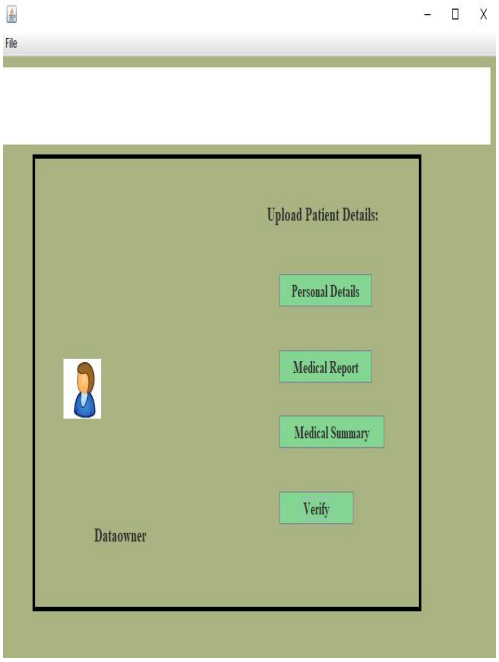

Figure 3: Uploading the data

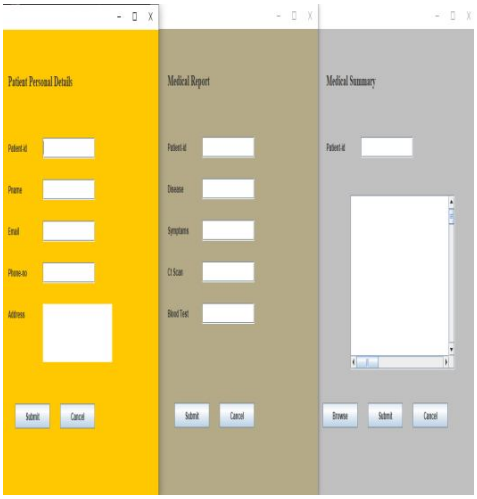

Figure 4: Detailed reports

5. MAINTAINENCE

It covers to the wide extent of the activities including the changing code and the program blunder. To decrease the obligation for help in time goes on, and also have the even more accuracy described in the client's necessities during the system structure headway. Depending upon the necessities, the structure that has been made to fulfill the essential requires to the great possible degree. While the progress is in development, it might have chance to incorporate with the many features based on the necessities in future. The programming code and organizing the fundamentals and direct it, which will make fixture less complex.

6. CONCLUSION

The Transparency of block chain enables the auditing and understanding the storing of the health records and security for EHR to transform into more opened, lucid and independent to the audit-able and the potential solution would be based on block chain technology. This report look into the outlook of block chain technology in preserving the information and its utility in EHR system. Block chain will be public verifiable and distributed in a way that no one can corrupt it in any forms. Block chain has provided the storage for the confidential data by the hospitals to tamper it.

REFERENCES

1. Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "**An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends**," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564. https://doi.org/10.1109/BigDataCongress.2017.85
2. Yli-Huumo J, Ko D, Choi S, Park S, Smolander K (2016) **Where Is Current Research on Blockchain Technology?—A Systematic Review.** PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journal.pone.0163477
3. Miraz, Mahdi H., and Maaruf Ali. "**Applications of Blockchain Technology Beyond Cryptocurrency**." Annals of Emerging Technologies in Computing 2.1 (2018): 1–6. Crossref. Web. https://doi.org/10.33166/AETiC.2018.01.001
4. Michael Crosby, Nachiappan, Pradan Pattanayak, Sanjeev Verma and Vignesh Kalyanaraman , **Blockchain Technology Beyond Bitcoin,** ,Applied Innovation Review, Issue No. 2m,June 2016 https://doi.org/10.1007/s10916-018-0994-6
5. S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California (2016).
6. H.Li,Y.Dai,andX.Lin,''**Efficiente-health data release with consistency guarantee under differential privacy**,'' in Proc. 17th Int. Conf. E-Health Netw., Appl. Services (HealthCom), 2016, pp. 602–608.
7. H. Wang and Y. Song, ''**Secure cloud-based EHR system using attributebased cryptosystem and blockchain**,'' J. Med. Syst., vol. 42, no. 8, p. 152, 2018.
8. W.Xu,L. Wu,and Y.Yan,''**Privacy preserving scheme of electronic health records based on blockchain and**

homomorphic encryption,'' J. Comput. Res. Develop., vol. 55, no. 10, pp. 2233–2243, 2018.

9. Rachapudi, V., Krishna Sai, T., Hari Priya, S., Pushpahas, K., **An effective approach to classify retina images for diabetic retinopathy**, International Journal of Advanced Trends in Computer Science and Engineering, 8(6),pp. 3345-3350,2019. https://doi.org/10.30534/ijatcse/2019/106862019
10. Sang Young Lee, **PHR System using Blockchain Technology**, International Journal of Advanced Trends in Computer Science and Engineering Volume 8 No. 6 pp. 3188 -3193,2019 https://doi.org/10.30534/ijatcse/2019/84862019
11. Norliza Katuk, The application of blockchain for halal product assurance: **A systematic review of the current developments and future directions**, International Journal of Advanced Trends in Computer Science and Engineering Volume 8 No. 5 1893 - 1902 ,2019. https://doi.org/10.30534/ijatcse/2019/13852019