ISSN No:-2456-2165

A Survey on Efficient Block Chain Authentication Scheme Based on Electronic Health Records

Swati Laxmeshwar
Department of Computer Science and Engineering
City Engineering College, Bangalore, India

Deepak N.R
Department of Computer Science and Engineering
City Engineering College, Bangalore, India

Abstract:- With the quick selection of the Cloud-based Electronic Health Record (EHR) frameworks, health providers are particularly concerned about overseeing cloud-based information protection. Current methodologies either have a flexibility bottleneck requiring patients to accept each sharing of their clinical details or a confidence bottleneck by providing a sole power control of each entry, thus increasing the issue of a single intention of attack. The exchange of electronic health records (EHRs) has a very good centrality for infection studies and the commitment of specialists Lately, a cloud-based electronic health record sharing program has offered a range of conveniences, but cloud centralization unfailingly opens up risks to information security and safety. Blockchain innovation can be seen as a positive solution to addressing these issues by virtue of its one kind of decentralization, namelessness, unforgeability, and unquestionable status. In this paper , we propose a secure and protection-based blockchain saving EHR sharing convention. Information requesters will look through the ideal catchphrase from the information provider to the relevant EHRs on the EHR Consortium blockchain and get the re-encryption ciphertext from the cloud server following the approval of the information owner. The plan mostly uses accessible encryption and restrictive intermediary reencryption to recognize information security, protect and control.

Keywords:- *Electronic Health Records, Data Sharing, Blockchain, Data Security, Privacy Preservation.*

I. INTRODUCTION

In distributed computing, customers need to surrender their data to the cloud for capacity and business activities, while the cloud specialist organization is normally a business endeavor that can't be trusted[3]. In appropriated registering, clients need to give up their information to the cloud for limit and business exercises, while the cloud master association is regularly a business try that can't be trusted[3]. Human administrations records are one of the most sensitive domains for confirmation, yet 66% of social protection affiliations experienced a security event in 2014 [9,11]. Patients who have had their records lost or taken are in danger for clinical and cash related deception. With the quick headway of information development and Internet advancement, Electronic Health Records (EHRs), as a replacement of standard unique duplicate patient's wellbeing records on paper, deal with the issues of paper that easy to lose, hard to set something aside for along time and hard to pass on. One such adaptable human administrations application is progressed in this paper, which lets patients interface with the authorities by sharing his/her wellbeing records, which are mixed at the customer end using IBBE plan and a while later set aside on the cloud, which can be furthermore decoded by the experts who are endorsed. Arrangements singular organizations and open organizations, close by instructing and research works out. Singular human administrations, for instance, benefits in clinical centers, patient's homes, and different sections. Open restorative administrations organizations incorporate medications given for patients, food, and wellbeing measures to keep up a neighborly circumstance around individuals. So also, medications of spreading diseases are done by using educating and ask about workplaces.

With the development of imaginative advancements, including Mobile Cloud Computing (MCC) and the Internet of Medical Things (IoMT),the social insurance industry has seen critical changes in e-health tasks [7], [8]. Patients presently can gather their own health data at locally situated on cell phones, (for example, cell phones and wearable sensors) and offer on cloud conditions where medicinal services suppliers can get to right away to break down clinical records and give opportune clinical backings. This snappy e-health administration permits medicinal services suppliers to remotely screen patients and offer walking care at home, which encourages social insurance conveyance as well as brings financial advantages.

II. RELATED WORK

A. Attribute-based encryption

Attribute Based Encryption (ABE) is a variation of topsy-turvy encryption in relies on characteristics utilized. [4].The fundamental objective for this encryption is to give security, get to control with adaptability, versatility, and fine-grained get to control. Furthermore, Secure sharing of data is of the on-request client. To take care of these issues, variations of Attribute-Based Encryption can be utilized.

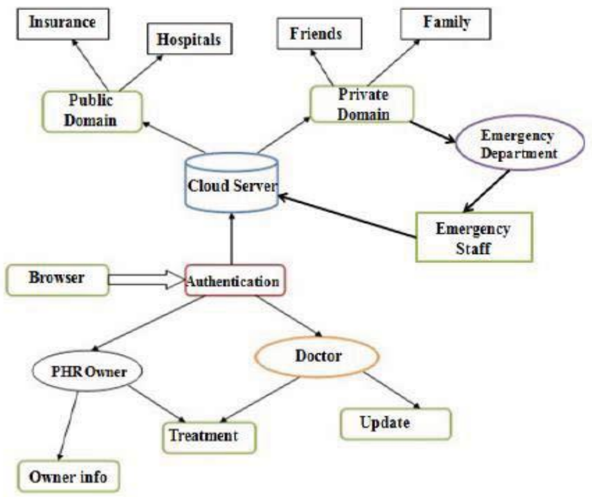

Fig 1:- Cloud-Based Health Record System

B. Profile matching

Profile coordinating is a strategy for looking at changed client's profiles.The client's profile additionally contains delicate data, so guarantee that private data isn't spilled to the outsider [1]. Two standard ways were proposed. 1) The client's profile will be taken as a lot of traits that utilizes a private set crossing point to accomplish property coordinating based sharing and encryption. For trading the negligible private data of taking an interest clients, 2)The client profile as a vector is taken to gauge social vicinity [1].Schemes for coordinating measurements. This depends on symmetric encryption.

C. Identity based encryption

IBE instrument can decrease the expense of surveying time for quiet records by utilizing extraordinary id [1]. Character based mark methods to ensure social insurance information in cloud computing.A Lightweight Identity-based encryption conspire is a lot of valuable for medicinal services observing. Rizwana et al. propose Attribute-Based Encryption (ABE) to scramble every patient's clinical record document [11]. ABE methods, for example, key approach characteristic based encryption, job based encryption are utilized. A methodology that safely empowers stockpiling with controlled sharing. Understanding protection is kept up profoundly secure utilizing different cryptographic calculations utilized on the different kinds of information. The fundamental objective of proposing a framework for keeping up an electronic wellbeing record is to make sure about them before sharing among social insurance suppliers. The proposed framework depends on an online framework with secure login and enlistment for the client. Cloud capacity is utilized for adaptable recovery and furthermore for information order and information encryption.

Dr.M.Umashankar proposed another calculation [12] for which incorporates the distinctive security methods to accomplish protection for individual wellbeing records. To improve the information to be gotten to from anyplace whenever, and furthermore, it will protect the security of wellbeing information. It permits the clients to recover information rapidly from the database. Procedure of recover the information effectively with the assistance of equal computational inquiries. Consistent observing of the patients over web by utilizing cloud condition, the enrollment is the procedure which is utilized for confirmation of client as legitimate or invalid client, and the register client can send and recover the data. In their proposed work to be adjusted the heap and increment the exhibition with extra room and processor load by utilizing numerous cloud servers.

D. EHR Sharing with Cloud

So on accomplish information security during the procedure of EHR sharing, some entrance control plans enthusiastic about cloud were presented in [3][5]. Another technique for fine-grained get to regulate called ciphertext strategy property based sign-cryption and secure sharing of individual wellbeing records in distributed computing was proposed in [3]; In [4], a proficient and secure fine-grained get to regulate plot was introduced which might understand approved clients **to** urge to EHRs in distributed storage. It underpins some particular doctors to compose on EHRs; [5] proposed a various leveled examination based encryption conspire and built up a novel approach refreshing plan by utilizing the intermediary re encryption strategy to accomplish dynamic access control in cloud-based EHR frameworks.

For improving the inquiry capacity and interoperability of EHR sharing, [6] proposed another cloud-based EHR framework supporting fluffy watchword scan for secure information sharing and successful usage of the EHRs; [7] used conjunctive catchphrase search with intermediary re-encryption to manufacture a safe EHR looking plan for information sharing between various clinical institutions.Moreover,[8] proposed a general structure for secure sharing of EHRs that patients are permitted to safely store and offer their EHR in the cloud server and specialists can get to the EHRs in cloud.

E. EHR Sharing With Blockchain

With the advancement of blockchain innovation, its decentralized, recognizability and mysterious attributes have been generally worried in utilizations of clinical industry issues. At present, numerous researchers are concentrating on the protection and security in EHR sharing dependent on blockchain innovation. So as to assist patients with utilizing and offer their own wellbeing information helpfully and securely, Amofa et al.[10] introduced a blockchain design to understand the security control of individual information in wellbeing data trade by coordinating shrewd agreements with client created worthy policies.The engineering limited information security chances by planning a component to control the mutual information. X. Zheng et al.[11]proposed a theoretical structure for individual nonstop unique wellbeing information sharing dependent on blockchain innovation. It is enhanced by distributed storage, share data identified with individual wellbeing in a protected and straightforward manner. In [12], a character and access the executives framework utilizing blockchain innovation to help the confirmation and approval of substances in computerized frameworks was proposed. This framework portrayed the use of blockchain in Hyperledger Fabric system for personality verification and access the board. In addition, Guo et al. [14] proposed a property based mark plot with different specialists to guarantee the adequacy of typified EHRs in the blockchain. In this plan, the patient embraced the message as per the qualities and just gave the proof that he had bore witness to it.

A few plans join cloud innovation with blockchain innovation to improve the security of EHR sharing. Cao et al. [13] proposed a cloud-helped secure eHealth framework, utilizing blockchain innovation to shield redistributed EHRs in cloud from illicit alteration. The key thought of this framework was that EHRs must be re-appropriated by confirmed members. Every procedure on the redistributed EHRs was coordinated into open blockchain as an exchange. Liu et al. [18] proposed a blockchain-based protection safeguarding information sharing plan, to be specific, BPDS. In BPDS, the cloud was utilized to store the first EMRs safely and a sealed consortium blockchain was intended to share the EMR files. The plan utilized along these lines to diminish the danger of clinical information spillage. The utilization of consortium blockchain guarantees that the EMRs can't be adjusted discretionarily.In[19],a stockpiling plan and administration system were proposed for putting away, sharing, and utilizing clinical information dependent on blockchain and cloud. In this scheme,blockchain-based individual clinical information applications can give a patient clinical data administration without abusing security concerns.

A different profession concentrated on taking care of the security and access control of EHR sharing on the blockchain.Reference [15] proposed a secret information sharing model to help an individual wellbeing record framework dependent on blockchain innovation and intermediary re-encryption strategy. The model tackled three significant issues: protection of on-chain information, constrained capacity for enormous clinical information, and assent renouncement. Reference [16] introduced blockchain-based framework engineering to accomplish auditable clinical information sharing and human services information get to authorization taking care of. In different perspectives, Chen et al. [17] proposed a blockchain-based accessible encryption conspire for electronic clinical record sharing to improve information accessibility. In this situation, the development of EHR lists put away in the blockchain was mind boggling consistent articulations so information clients can utilize those sensible articulations to look the files. Exploiting the decentralized property of blockchain, information proprietors had unlimited oversight over who can see their EHRs. Blockchain innovation ensures information trustworthiness, hostile to obstruction, and discernibility. Not the same as the above works, Zhang and Lin et al. [29] proposed a multi-composed blockchain-based secure and protection saving PHI sharing (BSPP) for conclusion upgrades. In BSPP, the private blockchain was utilized to store PHI for clinic and the consortium blockchain was liable for recording the protected lists of the PHI. The plan utilized open key encryption with watchword look for acknowledging information security and protection conservation of information sharing on consortium blockchain.

III. PRELIMINARIES

A. Blockchain Technology

In disseminated processing, clients need to give up their information to the cloud for limit and business exercises, while the cloud pro association is typically a business attempt that can't be trusted[3]. Human administrations records are one of the most unstable domains for confirmation, yet 66% of social protection affiliations experienced a security event in 2014 [9,11]. Patients who have had their records lost or taken are in danger for clinical and cash related distortion. With the quick progression of information development and Internet advancement, Electronic Health Records (EHRs), as a replacement of standard unique duplicate patient's wellbeing records on paper, deal with the issues of paper that easy to lose, hard to put Blockchain is an orchestrated summary of records associated together through a chain on blocks[22]. It is fundamentally a decentralized database, which is another application strategy for scattered data storing, feature point transmission, accord framework, encryption figuring, and other PC propels. It is moreover a scattered record that can't be adjusted or formed by using the cryptography procedure. Current blockchain systems can be organized into three sorts: Public blockchain, private blockchain, and consortium blockchain[24].Public blockchain is approval less blockchain where all records are clear to individuals when all is said in done and anyone can participate in the structure and access information, for example, Bitcoin, Ethereum. A private blockchain is seen as a concentrated framework since an affiliation totally controls the structure. Consortium blockchain is a for the most part decentralized system since it is administered by a couple of affiliations. In consortium blockchain, simply those center points that begin from endorsed affiliations can get to data in blockchain. In our work, we direct EHR data sharing on consortium blockchain. A couple of clinical centers contain an association and make a consortium blockchain, which tracks secure records for patient's EHR. In blockchain, the best way to deal with show up at accord among Untrustworthy center points in spread condition is called understanding framework. The agreement instrument is the focal point of blockchain advancement. Check of work, proof of stake, sensible by zantine adjustment to non-basic disappointment and some extraordinary accord instrument have been proposed for blockchain.

IV. SURVEY RESULTS

Sl.No	Author	Published Method	Security Strength
1	Praneeta K.Maganti	Identity and Attribute based cryptosystems	Includes both Identity-Based Encryption (IBE) and Attribute-Based Encryption (ABE) together to perform encryption and decryption on secure plain text.
2	Seung Geol Choi	Multi Authority Access Attribute Based Encryption (MA-ABE)	In the ciphertext, the access mechanism is secret, and malicious users are unable to acquire sensitive information through the access structure, which effectively preserves user privacy.
3	Selvam L and Arokia Renjit J	Fine-Grained Enhanced Attribute Based Encryption(ABE)	Bilinear map and Access trees
4	Dr.S.Pariselvam	Identity Based Encryption (IDE),DES Scheme	HIBE and WIBE
5	Yong Wang	Blockchain-Sharing Mobile E-Health systems	A trustworthy Access Control Mechanism Using Smart Contracts To Achieve Secure Ehrs Sharing Among Different Patients And Medical Providers

Table 1:- Survey Results

V. CONCLUSION

A blockchain based EHR sharing is more secure than some other plan. So as to understand the validation plan of EHRs framework dependent on blockchain. We first officially characterize the EHRs framework model in the setting of consortium blockchain. At that point we structure a character based mark plot with different experts for the blockchain based EHRs framework. The plan has productive marking and check algorithms.With conjunctive watchword accessible encryption and contingent intermediary re encryption to acknowledge information security and protection conservation of information sharing between various clinical foundations.

REFERENCES

[1]. H.K.Patil and R.Seshadri,“Big data security and privacy issues in healthcare,” in *Proc. IEEE Int. Congr. Big Data*, Anchorage,AK,USA,Jun./Jul. 2014, pp. 762_765.

[2]. J.Li and X.Li, “Privacy preserving data analysis in mental health researc,” in *Proc. IEEE Int. Congr. Big Data*, New York, NY, USA, Jun./Jul. 2015,pp. 95_101.

[3]. J. Liu, X. Huang, and J. K. Liu, “Secure sharing of Personal Health Records in cloud computing: Ciphertext-policy attribute-based signcryption,”*Future Gener. Comput. Syst.*, vol. 52, pp. 67_76, Nov. 2015.

[4]. X. Liu, Y. Xia, W. Yang, and F. L. Yang, ``Secure and ef_cient querying over personal health records in cloud computing," *Neuro Comput.*,vol. 274, pp. 99_105, Jan. 2018.

[5].] X. Liu, Q. Liu, T. Peng, and J. Wu, ``Dynamic access policy in cloudbased personal health record (PHR) systems," *Inf. Sci.*, vol. 379, pp. 62_81,Feb. 2017.

[6]. Z. Liu, J.Weng, J. Li, J. Yang, C. Fu, and C. F. Jia, ``Cloud-based electronic health record system supporting fuzzy keyword search," *Soft Comput.*,vol. 20, pp. 3243_3255, Aug. 2016.

[7]. X. Wang, A. Zhang, X. Ye, and X. Xie, ``Secure-aware and privacy preserving electronic health record searching in cloud environment," *Int.J. Commun. Syst.*, vol. 32, p. e3925, May 2019. doi: 10.1002/dac.3925.

[8]. M.H.Au, T.H.Yuen,J.K. Liu, W. Susilo, X. Huang, Y. Xiang, and Z. L.Jiang, "A general framework for secure sharing of personal health records in cloud system," *J. Comput. Syst. Sci.*, vol. 90, pp. 46_62, Dec. 2017.

[9]. G. Zyskind, O. Nathan, and A. S. Pentland, ``Decentralizing privacy:Using blockchain to protect personal data," in *Proc. IEEE Secur. Privacy Workshops*, vol. 90, May 2015, pp. 180_184.

[10]. S. Amofa, E. B. Sifah, K. O.-B. Agyekum, S. Abla, Q. Xia, J. C. Gee, and J. B. Gao, ``A blockchain-based architecture framework for secure sharing of personal health data,'' in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Healthcom)*. Ostrava, Czech Republic, 2018, pp. 1_6.

[11]. X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, ``Blockchain-based personal health data sharing system using cloud stor- age,'' in *Proc. IEEE 20th Int. Conf. e-Health Netw., Appl. Services (Health-com)*. Ostrava, Czech Republic, Sep. 2018, pp. 1_6.

[12]. T. Mikula and R. H. Jacobsen, ``Identity and access management with blockchain in electronic healthcare records,'' in *Proc. 21st Euromicro Conf.Digit. Syst. Design (DSD)*, Prague, Czech Republic, 2018, pp. 699_706.

[13]. S. Cao, G. Zhang, P. Liu, X. Zhang, and F. Neri, ``Cloud-assisted secure eHealth systems for tamper-proo_ng EHR via blockchain,'' *Inf. Sci.*, vol. 485, pp. 427_440, Jun. 2019.

[14]. R.Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,"*IEEE Access*, vol. 6, pp. 11676_11686, 2018.

[15]. T.T.Thwin and S. Vasupongayya,"Blockchain based secret-data sharing model for personal health record system,'' in *Proc. 5th Int. Conf.Adv. Inform., Concept Theory Appl. (ICAICTA)*, Krabi, Thailand, 2018, pp. 196_201.

[16]. A. Theodouli, S. Arakliotis, K. Moschou, K. Votis, and D. Tzovaras,``On the design of a blockchain-based system to facilitate healthcare data sharing,'' in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun., 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, New York, NY, USA, Aug. 2018, pp. 1374_1379.

[17]. L. X. Chen, W.-K. Lee, C.-C. Chang, K.-K. R. Choo, and N. Zhang, ``Blockchain based searchable encryption for electronic health record sharing,'' *Future Gener. Comput. Syst.*, vol. 95, pp. 420_429, Jun. 2019.

[18]. Z. Ying, L.Wei, Q. Li, X. Liu, and J. Cui, ``A lightweight policy preserving EHR sharing scheme in the cloud,'' *IEEE Access*,vol.6, pp. 53698_53708,2018.

[19]. V. Ramani, T.Kumar, A. Bracken, M. Liyanage, and M. Ylianttila, ``Secure and efficient data accessibility in blockchain based healthcare systems,'' in *Proc. GLOBECOM*, Dec. 2018, pp. 206_212.

[20]. N. Ri_, E. Rachkidi, N. Agoulmine, and N. C. Taher, ``Towards using blockchain technology for eHealth data access management,'' in *Proc. IEEE 4th Int. Conf. Adv. Biomed. Eng.*, Oct. 2017, pp. 1_4.

[21]. Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, ``MeDShare: Trust-less medical data sharing among cloud service providers via blockchain,'' *IEEE Access*, vol. 5, pp. 14757_14767, 2017.

[22]. X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, ``Integrating blockchain for data sharing and collaboration in mobile healthcare applications,'' in *Proc. IEEE 28th Annu. Int. Symp. Pers., Indoor, Mobile Radio Commu. (PIMRC)*, Oct. 2017, pp. 1_5.

[23]. S.Wang,Y. Zhang, andY. Zhang, ``Ablockchain-based framework for data sharing with fine-grained access control in decentralized storage systems,''*IEEE Access*, vol. 6, pp. 38437_38450, Jun. 2018.

[24]. M. Steichen, R. Norvill, B. F. Pontiveros, and W. Shbair, ``Blockchainbased, decentralized access control for IPFS,'' in *Proc. IEEE Blockchain*, Jul. 2018, pp. 1499_1506.

[25]. M. S. Ali, K. Dolui, and F. Antonelli, ``IoT data privacy via blockchains and IPFS,'' in *Proc. 7th Int. Conf. Internet Things*, Oct. 2017, p. 14

[26]. Y. Chen, H. Li, K. Li, and J. Zhang, ``An improved P2P file system scheme based on IPFS and blockchain,'' in *Proc. IEEE Big Data (Big Data),*Dec. 2017, pp. 2652_2657.

[27]. R. Ausanka-Crues. *Methods for Access Control: Advances and Limitations*. [Online]. Available:http://citeseerx.ist.psu.edu/ ?doi=10.1.1.596.2814

[28]. R. Xu, Y. Chen, E. Blasch, and G. Chen, ``BlendCAC: A smart contract enabled decentralized capability-based access control mechanism for the IoT,'' *Computers*, vol. 7, no. 3, p. 39,2018.

[29]. O. Novo, ``Blockchain meets IoT: An architecture for scalable access management in IoT,'' *IEEE Internet Things J.*,vol. 5, no. 2, pp. 1184_1195, Apr. 2018.

[30]. J.Kang *et al.*,``Blockchain for secure and efficient data sharing in vehicular edge computing and networks,''*IEEE Internet Things J.*,to be published.

[31]. *Ethereum Blockchain App Platform*. Accessed: Mar.25,2018.[Online].Available:https://www.ethereum.org