ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

To Implement a Secure Design for Health Records and Permission Management Using Block Chain

S Tanooja Rani [1]

M.Tech Student, Department of Computer Science and System Engineering, Andhra University College of Engineering (A), Visakhapatnam, AP, India [1]

ABSTRACT: Electronic health record (EHR) sharing enables to improve the quality and reduce the cost of healthcare, but it is still challenging because of technique issues even though patients and healthcare organizations are willing to share. These technical barriers include confidentiality, privacy, interoperability, integrity and so on. Maintaining these records securely and providing accessibility to only authenticated users is the major task at concern. This system has to be implemented in a decentralized and more secure way in order to prevent leakage of information, tampering of records, and all other kinds of attacks possible on the centralized server. Blockchain is a decentralised, peer-to-peer network system which stores files very efficiently with the help of cryptographic hashes. In this paper, we propose a blockchain and health records based approach by implementing attribute-based authentication to enable the secure sharing of healthcare data. By implementing this approach: 1) all patient's fragmented EHR pieces can be viewed as a whole record and stored secure against tampering; 2) the authenticity of patients' EHRs can be verified; 3) flexible and re-grained access control can be provided and 4) maintaining a clear audit trail is possible.

KEYWORDS: Electronic Health Record(EHR), Blockchain, Crypographic hash

I. INTRODUCTION

During medical care service, large amount of data are created and need to be stored safely for a long period, often a life time. One major difference between healthcare data and other big data sharing is that electronic health records (EHRs) are normally highly sensitive, which may make patients and medical organizations reluctant to share. On the other hand, however, EHR sharing [17, 19] can benefit both patients and medical organizations in a few ways. First of all, data sharing can facilitate medical research, for example, pooling multiple medical trials together for better understandings and scientific discoveries. Secondly, collaboration between different healthcare organizations (even cross-boarder cases) will be easier, such as doctors accessing patient's medical records, the reimbursement of medical treatment in a foreign country and so on. Thirdly, regulations and standards to facilitate secure EHR sharing will be developed and strengthened, which will in turn bring more trust among different medical organizations and thus can offer patients better service and further improve medical research as well. However, there still exist some technical barriers that hinder EHR sharing and make it challenging in many ways. According to a literature survey [13] on research papers about main security issues related to EHRs sharing from the year 2004 to 2014, the main eight security issues (from the most concerned to the least) are confidentiality, privacy, access control, integrity, data authenticity, user authentication, audibility and transparency. It is urgent to solve these issues to enable secure EHR sharing.

II. RELATED WORK

During recent years, blockchain [5, 21] has been brought in the area of medical healthcare to solve security issues such as integrity and data authenticity. A blockchain is a distributed ledger to record transactions between parties. One of its most promising features is its decentralized structure. Storing EHRs on a centralized server may attract attacks from

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

malicious parties, and the failure of an important site will probably cause service failure or interruption. However, a decentralized blockchain-based system has high probability to avoid this issue and thus makes it easier and more possible to provide continuous service. Another advantage of blockchain is that, due to the security of hash functions [14] and the proof-of-work (PoW) [15], it is hard to tamper transactions stored in the blocks.

As far as we know, there are not so many research results in blockchain-based EHR sharing. In [12], an approach for health information exchange network is proposed. There are two main contributions. First of all, it suggests solving the issue of interoperability by EHR semantic and format checking to ensure that all EHRs in the blockchain network have the same format. Secondly, it has proposed an algorithm to randomly choose the next miner to save computation power and system resources. In addition, [12] suggests using blockchain encryption, privacy preserving keyword searches and smart contracts to provide privacy and anonymity, but no detailed approaches included. The medical system MedRec proposed in [3] is built on contracts for easier management of EHRs. Users' identification strings are mapped to their Ethereum addresses in registrar contracts (RCs) to keep users anonymous. Patient-provider relationship contracts (PPRs) de ne how data are managed and accessed; PPRs are referenced by links contained in summary contracts (SCs) so that all medical records of a patient can be united as a whole piece. However, [3] does not provide any detailed approaches to solve issues such as how patients' EHRs are encrypted and accessed by authorized users, how users are authenticated and how to maintain an audit log about EHRs' accessing. In [20], a blockchain based App HGD (Healthcare Data Gateway) is developed to provide patients an easy way to control and manage their medical data. All data are stored in the blockchain cloud and managed through the data management layer. Only the authorized can access patients' data, the replica of which may be enforced to be destroyed when the authorized period is over. [7] focusses on discussing about the main aspects of medical records, and the advantages and disadvantages of using blockchain on the storage and retrieval of medical records.

III. EXISTING SYSTEM

The existing system is theMedRec: a novel, decentralized record management system to handle EMRs, using blockchain technology. It gives patients acomprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, MedRec manages authentication, confidentiality, accountability and data sharingcrucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. We incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain "miners". This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata.

IV. PROPOSED SYSTEM

The proposed system is the Electronic health recordssystem which is decentralized and more secured in order to prevent leakage of information, tampering of records, and all other kinds of attacks possible on the centralized server. In this system patients, doctors and management of the hospital management were the included. The patients have the login and registrations there by they can register and consult the doctor by entering their problem. The doctor can view the appointments of the patients and can give the access for the consulting by accepting the appointment. The management can view the details of the patient and doctors. The details which are entered by the patient and doctors are be encrypted by using SHA algorithm. The encrypted data can not be tempered and a better security for the patient records is provided.

MedRec-based Approach

To better understand the proposed blockchain-based approach for EHR secure sharing, a big picture will be presented in this section, including main entities and the main structure.

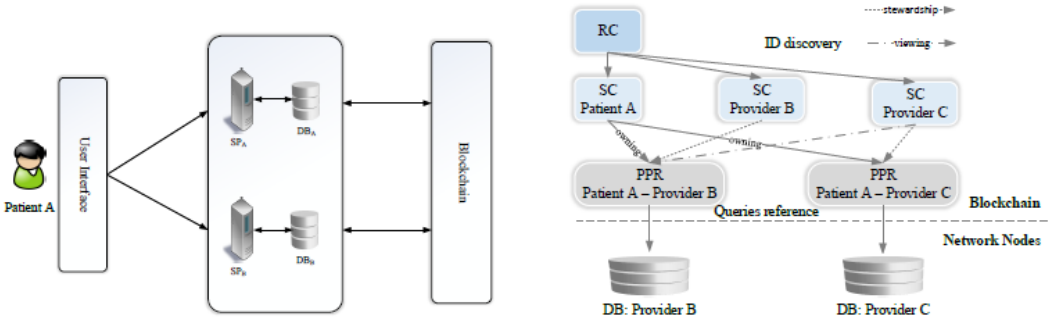
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019



(a) Big view of the main structure (b) MedRec contracts

Figure 1: Main structure of Our Approach

Main entities

Before introducing the system, we first describe main entities and their roles so as to have a big view of the system construction. Patient A patient is a person who seeks for healthcare services from medical, health and welfare organizations. Patients' privacy and the security of their EHRs are the main concerns in this paper. Service provider There are two types of service providers, i.e., those that provide health and welfare services (denoted by SPI) and those that only provide storage services (denoted by SPII). Users Patients are only one type of users. To avoid mixing patients with those who access patients' EHRs, when we say users, it refers to the latter. Thus, a patient can also become a user when he accesses another patient's EHRs. An attribute issuer is an entity that issues attribute keys to users and patients. Instead of one trusted attribute issuer, multiple and parallel attribute issuers are used. The main reason is that we want to avoid any centralized entity that may become the bottleneck or attack target of malicious parties.

V. THEMAINSTRUCTURE

One main goal of our approach is to provide patients with better and easier management for their fragmented EHR pieces, which can be implemented based on MedRec proposed in [3]. As shown in Fig. 1(a), the patient is using services from service providers A and B (denoted by SPA and SPB respectively), and the data generated by each service provider are stored in their own databases denoted by DBA and DBB. Considering the sizes of EHRs, only contracts (such as PPRs) but not data will be stored on the blockchain, where contracts are data structures by following which a patient can access his data stored on service providers' database.

The process how a patient store and access his data is as follows. When a patient (i.e., patient A) first joins the block chain-based healthcare network, he first registers himself through RC. To provide services, providers A and B also need to register themselves in RC. From the entries in RC, patients can link to their own SCs, the summaries with references to PPRs, which de ne the way how a provider manages patients' EHRs and how EHRs can be accessed. Since PPRs are an assortment of data pointers that consist of query strings, the patient can execute the query strings and then get related records. Therefore, when patient A uses the service provided by SPA, the generated data can be stored in either DBA or on the cloud. For the latter case, we still consider it as a special service (i.e., cloud storage), so we will only discuss the first situation here. To store data in DBA and related contracts on the block chain, SPA first generates related PPRs and send them as part of the transactions in the next block that will be added in the blockchain. Once a new block is mined and verified, patient A's PPRs will be added as transactions in the newly mined block, and the links to the new PPRs will also be added in SCs. Meanwhile, the service provider will enforce EHR changes in its database. In this way, all EHR changes will be updated and recorded in the blockchain. For instance, data deletion, data stored in

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

the database will be deleted, but the action of deleting and the agreement to deletion from the patient's side will also be considered as contracts, which will also be uploaded to the blockchain. Data pieces stored separately can be referenced by different PPR entries with links in SCs. As a result, even though patient A is using services from different service providers and EHRs stored separately, all these fragmented data pieces can still be connected and be viewed a whole piece (Refer to [3] for more details). To keep patients' data secure, all blocks uploaded to the blockchain should be encrypted and later can be searched by privacy preserving keyword searches [10, 11, 16].

EHR sharing and accessing

As described in Subsection 2, EHRs are not stored on blockchain but Internet nodes owned by service providers or cloud servers. If these service providers are not fully trusted, EHRs should be encrypted before being uploaded to the servers. In addition, to ensure data authenticity, the encrypted data should also be signed by the owner. The private key the owner uses to sign is generated based on its Ethereum address. Since a user can have as many addresses as he wants to, the signature will not reveal his identity or hinder his privacy. To achieve both privacy and data authenticity, signcryption [1] will be applied in our approach.

The main idea of Signcryption used in our approach can be illustrated in Fig. 2. Suppose there is a patient who wants to share his EHRs with other users (e.g., doctors, nurses and his family members). In order to control those who can access his EHRs, the patient needs to de ne the access policies, which are presented by attribute predicate. Public parameter obtaining: before uploading encrypted EHRs to a server, a patient first needs to retrieve public parameters such as public attribute keys from attribute issuers (one or multiple) that he trusts. Data encryption, signing and uploading: there are three main parts in this step, i.e., EHRs encryption, data key encryption and cipher text signing.
One thing to notice is that the signcryption we use here is a simple combination of encryption and signature. However, one needs to carefully choose the ABE and the signature schemes to achieve better security and efficiency. A detailed example of cloud-based signcryption can be found in [9].

Data accessing: this step includes three parts: i.e., signature verification, data key and EHRs decryption. After downloading fC1; C2; g, the user first validates to check data authenticity. If is valid and the user possesses the attributes required in predicate, he decrypts C2 to get the data key K. Finally, decrypt C1 using K to recover the plaintext EHRs. The patient uploads the signed cipher text to the server; (3) the server sends the PPRs generated for the new EHRs to the blockchain as part of the transactions of the next block; (4) once a new block is mined and verified, the server changes the links to the new PPRs in SCs; (5) the server adds the signed cipher text of EHRs in its database; (6) the server sends a notification to the patient whether his EHRs are successfully added.

EHR deleting To delete old EHRs stored on a server, the following needs to be done: (1) the owner (patient) of the EHRs needs to send a delete request to the server; (2) the server sends the EHR deleting information as part of the transactions of the next block; (3) once a new block is mined and verified, the server changes SCs to unlink the PPRs which reference to the EHRs to be deleted; (4) the server deletes patient's EHRs; (5) the server sends a notification to the patient whether his EHRs are successfully deleted.

EHR modification includes the following steps: (1) the patient encrypts the new data with the same data key and then signs it; (2) the patient uploads the signed cipher text to the sever; (3) the server sends the modification and new PPRs to the blockchain; (4) once the changes are updated in the blockchain, the server unlinks the old PPRs and links the new PPRs if necessary; (5) the server deletes the old EHRs and adds the new; (6) the service sends a notification to the patients whether his EHRs are successfully modified.

Access policy change refers to the situation that the data owner (the patient) has changed the rules how his EHRs can be accessed. Since the access policies are represented by attribute predicates, based on which the data key is encrypted. Therefore, the main changes that happen on the patient side is to re-encrypt the data key, while the EHRs does not need to be re-encrypted. The procedure goes as follows: (1) the patient downloads the encrypted EHRs first; (2) the patient encrypts the data key and signs the encrypted EHRs and the encrypted data key; (3) the patients uploads the signed

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

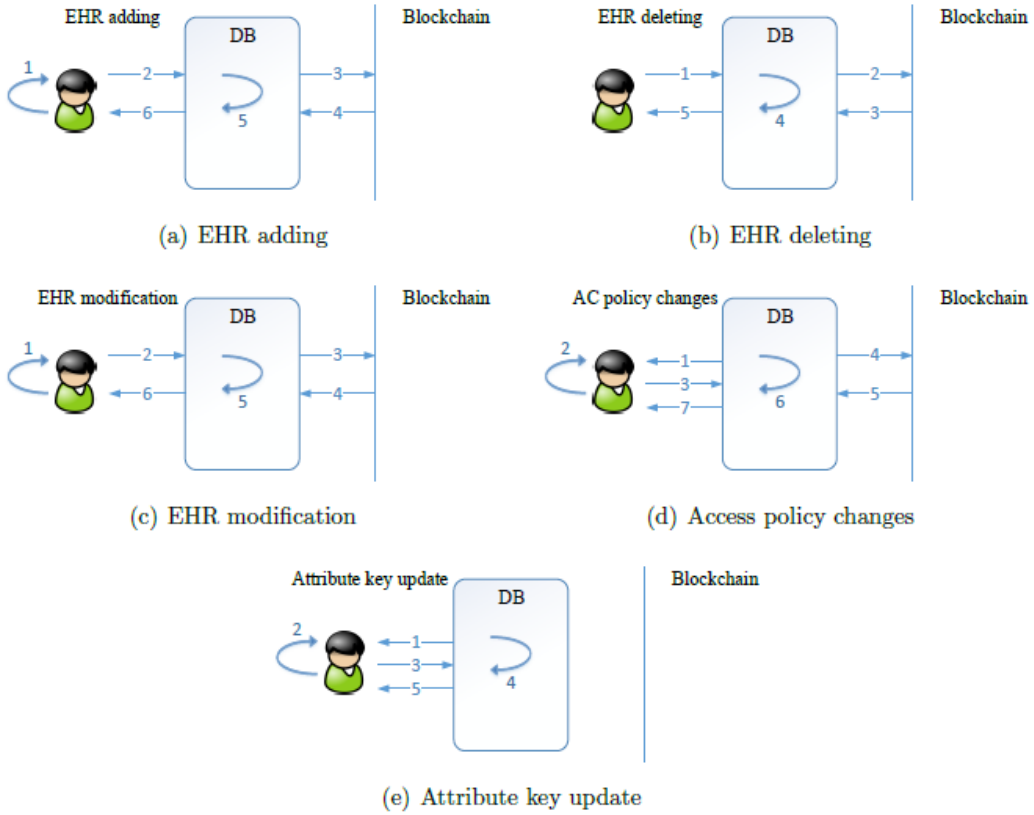
(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

cipher text to the server; (4) the server sends new PPRs as part of the transactions of the next block; (5) once the new block is mined and verified, the server unlinks the old PPRs and links the new PPRs; (6) the server replaces the old encrypted data key together with the signature with the new ones; (7) the server sends a notification to the patients whether the access policies are successfully modified.

Attribute key update Different from access policy changes, attribute key update will not cause any changes on the blockchain, because the attribute key update will not affect the way how patients' EHRs are accessed. The whole process goes as follows: (1) the patient downloads the encrypted EHRs from the server; (2) the patient encrypts the data key with new attribute keys, sign the encrypted EHRs and the encrypted data key; (3) the patient uploads the signed cipher text to the server; (4) the server replaces the old encrypted data key together with the signature with the new ones; (5) the server sends a notification to the patients whether the update is successful.



(a) EHR adding (b) EHR deleting

(c) EHR modification (d) Access policy changes

(e) Attribute key update

User authentication

Before accessing a patient's EHRs, a user needs to be authenticated first. PKI-based authentication is one of the mostly used authentication approach. Since the public and private key pair of a user on blockchain is based on one of its many addresses, it will be hard to trace his identity when necessary. In this paper, we suggest using an authentication approach based on attributes (i.e., ABA). There are several different reasons. First of all, it provides anonymous authentication, which means that the user's identity is still unknown to the verifier except for that the user satisfies the authentication requirement. Secondly, the signature generated for the authentication can serve as an evidence or be used to trace the user who has requested to access the EHRs. According to [6, 18], a signature generated by the user during authentication can be opened to reveal the user's identity and thus serve as an evidence or for audit information. Thirdly, in order to access encrypted EHRs, users have to obtain attribute keys and maintain them. Therefore, these

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

keys can also be used for authentication without any extra storage cost. If the authentication and data decryption happen successively, we can furthermore design more efficient protocols that can fulfill the requirements of both authentication and data decryption, to avoid part of the overlapped computations.

Miners and incentive measures

Service providers can act as miners to mine new blocks to hold record changes (contracts changes more specifically) of their users or to pay for the service from attribute issuers if they need to use their services. One interesting but still possible reason for attribute issuers to be miners is that to be a certified attribute issuer, one of the criteria can be that they need to have enough proven contribution to the system, and the contribution is measured by how many blocks they have mined. Except for service providers and attribute issuers, entities such as researchers or other medical organizations can also act as miners to pay for the use of shared data. For the patients, on the one hand, they may need to pay for the service from their service providers or attribute issuers. However, on the other hand, they may get paid by sharing their data. If what a patient earns by sharing his data is not enough to pay for the service, he can also choose to act as a miner if he wishes to.

Security discussion

In this section, we discuss the security issues related to the approach we proposed in Section 3. The main goal of the proposed approach is to provide a solution for the main security issues discussed in Section 1, including confidentiality, privacy, access control, integrity, data authenticity, audibility, transparency and interoperability. Based on the approach proposed in Section 2, we discuss each of these security issues in the following:

Confidentiality means not revealing contents to those who are not supposed to know. In this paper, it includes two aspects, the confidentiality of patients' EHRs and contracts (PPRs) stored on the blockchain. On the one hand, patients' EHRs are encrypted and can only be accessed by those allowed to, where the details can be found in EHR sharing in Subsection 3. On the other hand, PPRs stored on the blockchain are encrypted and then can be searched by privacy preserving keyword searches.

Privacy provides user anonymity, which is mainly anonymous authentication in this paper and is achieved by pseudo address based public and private key pair, ABE and ABA. Users can create multiple addresses, based on which public and private key pairs are generated to sign, for example, PPRs, EHRs changes and so on. In PKI-based infrastructure, public and private key pairs can normally be considered as users' identifying information. However, since the public and private key pair is based on one of a user's many addresses, it is generally hard to identify a user by his key pairs or his traces left on the blockchain. In addition, since PPRs and EHRs are encrypted, sensitive information will also be protected.

Access control there are mainly two aspects related to the access of EHRs, i.e., a patient accessing his own EHRs and a user accesses other patients' EHRs. A patient accessing his own data is through the interface (as described in Subsection 2 and Fig. 1), by which all his data crumbs are united together as a whole one from the patient's point of view. However, the process is quite different from a user accessing a patient's EHRs. First of all, the user searches what he is interested by keywords and the results (usually encrypted PPRs) will be sent to the user. If the user is allowed to access the data, he can execute the PPRs and will be returned with the requested EHRs that are encrypted by ABE (Refer to Subsection 3 for more details).

Integrity Considering the security of hash functions, it is computationally di cult to tamper the content of one block without changing the hash value stored in the next block. Furthermore, every node (or service nodes for better efficiency in practice) has a copy of the blockchain data, the change of a certain block will be easily detected if a node communicates with other nodes. Besides, even though patients' EHRs are not stored on the blockchain, their merkle roots [4] are included in the block. As a result, if the EHRs are tampered, the merkle root value will change, which will then cause the content change of the block. Therefore, by using blockchain, EHRs can be stored secure and correct without being tampered.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

Data authenticity Patients need to sign their EHRs before related contracts are added to the blockchain. Given these signatures as well as the integrity provided by the blockchain, data authenticity can be provided.

Audibility and Transparency Since all changes of patients' data will be recorded and then added to the blockchain, it is possible to keep a integrate, clear and transparent trail audit of EHR changes, and patients can have access to these trails as long as he has access to the blockchain network. In addition, each user who wants to access EHRs should be authenticated first by ABA and the signature will be stored and can be used later to trace the user's identity.

Interoperability Unlike a centralized network where different healthcare organizations have their own systems, the decentralization of blockchain is designed to be convenient for each entity to communicate with each other. However, it doesn't mean that a healthcare system built on blockchain will have no difficulty concerning to interoperability. [12] Has proposed that except for validity check, semantic and format check of EHRs should also be required and only those blocks that have passed both checks can be added to the blockchain, which means that all entities of the blockchain should agree on the same standard how EHRs should be expressed. This can also be adopted in our approach to provide interoperability without any extra e ort in modifying the main structure.

VI. CONCLUSION

We have proposed a blockchain-based approach to build a decentralized healthcare network for secure EHRs sharing. Our main concern is to solve the security issues of confidentiality, access control, privacy, audibility and so on. The recording of any EHR changes on the blockchain keeps patientdata safe from being tampered and enables an easily accessible, integrate and transparent audit information for the patients. Furthermore, the application of encryption provides data authenticity and a flexible way to access the shared data. The patients can view their data as well as the doctors and can view their files whenever needed. The records which were kept in the blockchain is secured and cannot be tampered which gives authenticity to the patients and doctors in the hospital management.

VII. FUTUREWORK

We have proposed a framework for secure personalized web search. Here we build the user profile by using domain knowledge. We also proposed a method to maintain the privacy and confidentiality by encrypting the user profile at the server side. Security is also provided to transportation of the data. Our system also able to detect the which session is typical is which is not. We performed some experiments that shows better search result when we use advanced user profile as compared with simple user profile on same queries. In the future we would try to enhance the search quality based on user search preference and also aim to provide more security from the adversaries.

REFERENCES

[1] Asaph Azaria, Ariel Ekblaw, Thiago Vieira and Andrew LippmanMedRec: Using Blockchain for Medical Data Access and Permission Management, *Media LabMassachusetts Institute of Technology Cambridge, MA, 02139, USA Email: {azaria, aekblaw, tvieira, lip}@mit.edu*
[2] K. D. Mandl *et al.*, "Public standards and patients' control: how to keep electronic medical records accessible but private," *BMJ*, vol. 322, no. 7281, pp. 283–287, 2001.
[3] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and G. Das, "Everything you wanted to Know about the Blockchain", *IEEE Consumer Electronics Magazine*, Volume 7, Issue 4, July 2018, pp. 06–14.
[4] D. Puthal, N. Malik, S. Mohanty, E. Kougianos, and C. Yang, "The Blockchain A Decentralized Security Framework", *IEEE Consumer Electronics Magazine*, Vol. 7, No. 2, pp. 18--21, 2018.
[5] Z.Dou, R. Song, and J.-R. Wen, "A Large-Scale Evaluation and Analysis of Personalized Search Strategies," Proc. Int'l Conf. World Wide Web (WWW), pp. 581-590, 2007.
[6] J. Teevan, S.T. Dumais, and E. Horvitz, "Personalizing Search via Automated Analysis of Interests and Activities," Proc. 28th Ann. Int'l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR), pp. 449-456, 2005.
[7] M.Spertta and S. Gach, "Personalizing Search Based on User Search Histories," Proc. IEEE/WIC/ACM Int'l Conf. Web Intelligence (WI), 2005.
[8] B. Tan, X. Shen, and C. Zhai, "Mining Long-Term Search History to Improve Search Accuracy," Proc. ACM SIGKDD Int'l Conf. Knowledge Discovery and Data Mining (KDD), 2006.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 10, October 2019

[9] K. Sugiyama, K. Hatano, and M. Yoshikawa, "Adaptive Web Search Based on User Profile Constructed without any Effort from Users," Proc. 13th Int'l Conf. World Wide Web (WWW),2004.
[10] X.Shen, B. Tan, and C. Zhai, "Implicit User Modeling for Personalized Search," Proc. 14th ACM Int'l Conf. Information and Knowledge Management (CIKM), 2005.
[11] X.Shen, B. Tan, and C. Zhai, "Context-Sensitive Information Retrieval Using Implicit Feedback," Proc. 28th Ann. Int'l ACM SIGIR Conf. Research and Development Information Retrieval (SIGIR), 2005.
[12] F.Qiu and J. Cho, "Automatic Identification of User Interest for Personalized Search," Proc. 15th Int'l Conf. World Wide Web (WWW), pp. 727-736, 2006.
[13] J. Pitkow, H. Schu¨ tze, T. Cass, R. Cooley, D. Turnbull, A. Edmonds, E. Adar, and T. Breuel, "Personalized Search," Comm. ACM, vol. 45, no. 9, pp. 50-55, 2002.
[14] Y. Xu, K. Wang, B. Zhang, and Z. Chen, "Privacy-Enhancing Personalized Web Search," Proc. 16th Int'l Conf. World Wide Web (WWW), pp. 591-600, 2007.
[15] K. Hafner, Researchers Yearn to Use AOL Logs, but They Hesitate, New York Times, Aug. 2006.
[16] A.Krause and E. Horvitz, "A Utility-Theoretic Approach to Privacy in Online Services," J. Artificial Intelligence Research, vol. 39, pp. 633-662, 2010.
[17] J.S.Breese, D. Heckerman, and C.M. Kadie, "Empirical Analysis of Predictive Algorithms for Collaborative Filtering," Proc. 14th Conf. Uncertainty in Artificial Intelligence (UAI), pp. 43-52, 1998.
[18] P.A. Chirita, W. Nejdl, R. Paiu, and C. Kohlschu¨ tter, "Using ODP Metadata to Personalize Search," Proc. 28th Ann. Int'l ACM SIGIR Conf. Research and Development Information Retrieval (SIGIR), 2005.
[19] A. Pretschner and S. Gauch, "Ontology-Based Personalized Search and Browsing," Proc. IEEE 11th Int'l Conf. Tools with Artificial Intelligence (ICTAI '99), 1999.
[20] E. Gabrilovich and S. Markovich, "Overcoming the Brittleness Bottleneck Using Wikipedia: Enhancing Text Categorization with Encyclopedic Knowledge," Proc. 21st Nat'l Conf. Artificial Intelligence (AAAI), 2006.