Block-Chain based Personal Health Record (PHR) Sharing Scheme

Mohamed Farook A[1]
B.E. CSE Student,
HKBKCE, Bengaluru

Nagashree S K[2]
B.E. CSE Student,
HKBKCE, Bengaluru

Mounika Yalla[3]
B.E. CSE Student,
HKBKCE, Bengaluru

Neha Mittal[4]
B.E. CSE Student,
HKBKCE, Bengaluru

***Abstract*—In this paper, we propose a new secure EHR sharing scheme with data integrity verifiable based on blockchain and cloud computing. Aiming at the problems of privacy disclosure, loss of control rights in the process of personal health record sharing; to achieve privacy protection, the new scheme uses symmetric encryption and attribute-based encryption techniques to achieve privacy protection and fine- grained access control. Comparing with the existing schemes, the new scheme allows patients to distribute attribute private key for users, hence many security problems can be avoided.**

Further, the new scheme uses blockchain to manage keys in the scheme. The new scheme stores the hash values of encrypted personal health records in blockchain, and the related index set is stored in smart contract, which can further improve the efficiency of data integrity verification.

Keywords—Data security, data integrity, blockchain, cloud computing.

I. INTRODUCTION

It is very important to share the personal health records, as it can improve accuracy of the doctor’s diagnosis and to help in progress of medical research. Generally, to lower the maintenance cost of data, the personal health records are usually outsourced to a third party such as cloud service provider. But in this case, the cloud service provider may tamper with or reveal the personal health records. Therefore, ensuring the privacy of personalhealth records and realizing the fine-grained access control are the major issues when the personal health records are shared. Blockchain as a distributed architecture with decentralized and tamper-proof features, it provides a new way to protect the personal health records sharing system. Usually data is most likely to be stored on data storage servers such as mail servers and file servers in crypted formto reduce security and privacy risks.[1]

In recent years, the development of network information technology and cloud technology has brought a huge change in people’s lifestyle. The emergence of personal health records sharing system based on electronic information and cloud technology enables patients to store, manage and share their health information conveniently, efficiently and accurately. As the healthcare information can be recorded and managed by the patient, personal health records provide a complete and accurate personal medical history that can be obtained online and shared easily. These personal health records are valuable resources, and can be used conveniently. The personal health records are usually outsourced to a third party such as cloud service provider. Under the circumstances, one of the major issues is how to ensure the security, privacy of personal health records while achieving fine-grained access control. The best suitable solution is to combine cloud storage, symmetric encryption, and attribute-based encryption together.

II. LITERATURE SURVEY

[1] U. Premarathne et al., "Hybrid Cryptographic Access Control for Cloud-Based EHR Systems," in IEEE Cloud Computing, vol. 3, no. 4, pp. 58-64, July-Aug. 2016, doi: 10.1109/MCC.2016.76.

A cryptographic role-based access control model for electronic health record (EHR) systems uses location- and biometrics-based user authentication and a steganography-based technique to embed EHR data in electrocardiography (ECG) host signals.

To manage EHRs efficiently and securely, it proposes a design based on steganography, which hides confidential EHR data inside the ECG host data. Steganography offers more efficient and secureinformation concealment than traditional cryptography. Only authorized users can extract data based on their security parameters. Steganography- based approach therefore improves the security of storage and retrieval of EHRs by hiding them inside ECG signals, and enhances performance through flexible feature adoption.

In Role-based access control model, the access requests are mapped to generate the session keys. Keberos protocol is used to securely communicate the session keys to the CSP and the user. The authentication server and the ticket granting server (TGS) are the two main parts of Kerberos protocol, uses role-based access control to manage user’s roles and distributes session keys to users to performdifferent tasks.

In future work, a robust key exchange management between various parties can be involved. Key revocations and risk mitigation strategies can also beconsidered.

[2] Thwin, Thein & Vasupongayya, Sangsuree. (2019). Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Security and Communication Networks. 2019. 1-15. 10.1155/2019/8315614.

This work aims to handle these blockchain drawbacks and propose a blockchain-based PHR model. The proposed model is built using the blockchain technology to support a tamper resistance feature. Proxy re-encryption and other cryptographic techniques are employed to preserve privacy. Features of the proposed model include fine-grained and flexible access control, revocability of consent, auditability, and tamper resistance.

In this model, to ensure confidentiality, the PHR data will be encrypted using the public key (master key) of the PHR owner and stored on a cloud storage. The PHR will be shared through a proxy re- encryption process. Therefore, the re-encryption keys and other information needed for an authentication process will be stored on a proxy which is called the gateway server. The metadata of the PHR will be stored on the private blockchain to support search and features that can resist tampering. The PHR will be accessed by the PHR owner or others such as healthcare providers, e.g., doctors, nurses.

In future it is possible to provide a revocable access control mechanism on blockchain. Also, there are other issues such as limited storage and privacy of on chain data for using blockchain in PHR development which can be handled.

[3] Hylock RH, Zeng X. A Blockchain Framework for Patient-Centered Health Records and Exchange (Health Chain): Evaluation and Proof-of-Concept Study. J Med Internet Res. 2019 Aug 31;21(8):e13592. doi: 10.2196/13592. PMID: 31471959; PMCID: PMC6743266.

This work presents Health Chain, a novel patient-centered blockchain framework. The intent is to bolster patient engagement, data curation, and regulated dissemination of accumulated information in a secure, interoperable environment.

A mixed-block blockchain was proposed to support immutable logging and redactable patient blocks. Patient data is generated and exchanged easily. Patients receive cryptographic identities in the form of public and private key pairs. Public keys are stored in the blockchain and helps for securing and verifying transactions. Further, the system uses proxy re-encryption (PRE) to share information through revocable, smart contracts, ensuring the preservation of privacy and confidentiality. Finally, several PRE improvements are offered to enhance performance and security.

Proxy re-encrypted data with dynamic keys, incremental server storage, and additional server- side encryption are the best performing of the strongest configurations which can be worked upon.

[4] Roehrs, Alex & André da Costa, Cristiano & Righi, Rodrigo & Silva, Valter & Goldim, Jose & Schmidt, Douglas. (2019). Analyzing the Performance of a Blockchain-based Personal Health Record Implementation. Journal of Biomedical Informatics. 92. 103140. 10.1016/j.jbi.2019.103140.

This article presents the implementation and evaluation of a PHR model that integrates distributed health records using blockchain technology and the open EHR interoperability standard. It thus follows Omni PHR architecture model, which describes an infrastructure that supports the implementation of a distributed and interoperable PHR.

This method involves implementing a prototype and then evaluating the integration and performance of the records from different production databases. Also adding upon the unified view of records, their evaluation criteria also focused on non-functional performance requirements, such as response time, CPU usage, memory occupation, disk, and network usage. The Chord algorithm for directing and limiting data replication is a more scalable alternative than conventional cryptocurrency platform replication models, where all nodes receive all data. Chord's scalability is a critical factor to effectively support health data. Particularly it enables data replication with restricted access, providing control and management by patients and healthcare professionals.

This Omni PHR prototype can be evolved to incorporate additional databases and conduct additional tests to evaluate its performance in even more scalable and realistic production environments.

[5] D. Song, A. Perrig, and D. Wagner, "Practical techniques for searches on encrypted data," Proceeding 2000 IEEE Symposium on Security and Privacy. IEEE, 2000, pp. 44–55.

Usually data is most likely to be stored on data storage servers such as mail servers and file servers in crypted form to reduce security and privacy risks. But to gain security certain functionalities had to be left behind. For example, if a client wishes to retrieve only documents containing particular words, it was not known how to let the data storage server perform the search and answer the querywithout loss of data confidentiality.

In this paper, they describe cryptographic schemes for the problem of searching on encrypted data and provide proofs of security for the resulting crypto systems. The techniques have a number of crucial advantages. They are provably secure: they provide provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext; they provide query isolation for searches, meaning that the untrusted server cannot learn anything more about the plaintext than the search result; they provide controlled searching, so that the untrusted server cannot search for an arbitrary word without the user's authorization; they also support hidden queries, so that the user may ask the untrusted server to search for a secret word without revealing the word to the server. The algorithms presented are simple, fast (for a document of length, the encryption and search algorithms only need stream cipher and block cipher operations), and introduce almost no space and communication overhead, and hence are practical to use.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based encryption for fine-grained access control of encrypted data,” Proceedings of the 13th ACM Conference on Computer and Communications Security. ACM, 2006, pp. 89–98

Sensitive data is stored and shared by third party sites on Internet, therefore there will be a need to encrypt data stored at these sites. One of the drawbacks of encrypting data is that it can be selectively shared only at a coarse-grained level (i.e., giving another party your private key). Here they develop a new cryptosystem for fine-grained sharing of encrypted data that is called as Key-Policy Attribute-Based Encryption (KP-ABE). In this cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. It demonstrates the applicability of their construction to sharing of audit-log information and broadcast encryption. Their construction supports delegation of private keys which subsumes Hierarchical Identity-Based Encryption (HIBE).

[7] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, “Searchable symmetric encryption: improved definitions and efficient constructions,” ACM Conference on Computer and Communications Security 2006. ACM, 2006, pp. 79–88,

Searchable symmetric encryption (SSE) allows a party to outsource the storage of the data to another party in a private manner, while maintaining the ability to selectively search over it. This problem hasbeen the focus of active research and several security definitions and constructions have been proposed. In this paper they began by reviewing existing notions of security and propose new and stronger security definitions. They then presented two constructions that shows secure under their new definitions. Interestingly, in addition to satisfying stronger security guarantees, their constructions are more efficient than all previous constructions. Further, prior work on SSE is only considered the setting where only the owner of the data is capable of submitting search queries. Here they consider the natural extension where an arbitrary group of partiesother than the owner can submit search queries. They formallydefined SSE in this multi-user setting, and presented an efficient construction.

[8] A. Bahga and V. K. Madisetti, "A Cloud- based Approach for Interoperable Electronic Health Records (EHRs)," in IEEE Journal of Biomedical and Health Informatics, vol. 17, no. 5, pp. 894-906, Sept. 2013, doi: 10.1109/JBHI.2013.2257818.

The cloud can provide several benefits to all the stakeholders in the healthcare ecosystem through systems such as Health Information Management Systems (HIMS), Laboratory information system (LIS), Radiology Information System (RIS), Pharmacy Information System (PIS) etc. With public cloud based HER systems, hospitals don’t need to spend a significant portion of their budget onIT Infrastructure.

[9] A. Ge, J. Zhang, R. Zhang, C. Ma and Z. Zhang, "Security Analysis of a Privacy- Preserving Decentralized Key-Policy Attribute- Based Encryption Scheme," in IEEE Transactions on Parallel and Distributed Systems, vol. 24, no. 11, pp. 2319-2321, Nov. 2013,doi: 10.1109/TPDS.2012.328.

As attribute-based encryption (ABE) can simultaneously provide flexible access control and data confidentiality functionalities, it has become a promising technique for building secure access in practical distributed systems. They had first made some observations on Han et al’s scheme. Then, they gave a generic attack on the scheme. Their attack employs the observations, and breaks the weak ties between authorities. Their idea was to remove such connections by changing the identifier associated with particular secret keys. Their main aim was to improve security.

[10] K. Yang, X. Jia and K. Ren, "Secure and Verifiable Policy Update Outsourcing for Big Data Access Control in the Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 12, pp. 3461-3470, 1 Dec. 2015, doi: 10.1109/TPDS.2014.2380373.

Attribute-Based Encryption (ABE) has emerged as a promising technique to ensure the end-to-end data security in cloud storage system. It allows data owners to define access policies and encrypt the data under the policies, such that only users whose attributes satisfying these access policies can decrypt the data.

III. METHODOLOGY

Cryptographic technique

Cryptographic techniques are used to ensure secrecy and integrity of data in the presence of an adversary. Based on the security needs and the threats involved, various cryptographic methods such as symmetric key cryptography can be used during transportationand storage of the data.

FTP Protocol

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections. FTP is a client-server protocol where a client will ask for a file, and a local or remote server will provide it.

MVC Architecture

Model View Controller or MVC is a software design pattern for developing web applications. The MVC pattern is made up of the following threeparts:

- **Model** – Model objects store data retrieved from the database.
- **View** – View is a user interface. It displaysmodel data to the user and also enables them to modify them.

- **Controller** – The Controller handles the user request. It processes the request and returns the appropriate view as response.

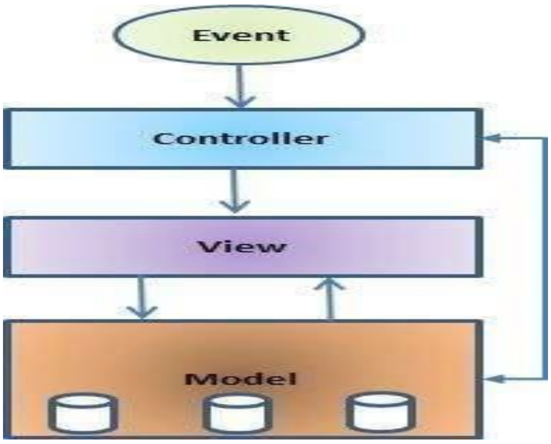

Fig. 1. MVC Architecture

Cloud Technology

Cloud computing is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centres available to many users overthe Internet.

Block chain Technology

Block chain technology is a structure that stores transactional records, also known as the block, of the public in several databases, known as the "chain", in a network connected through peer-to-peer nodes. Typically, this storage is referred to as a digital ledger.

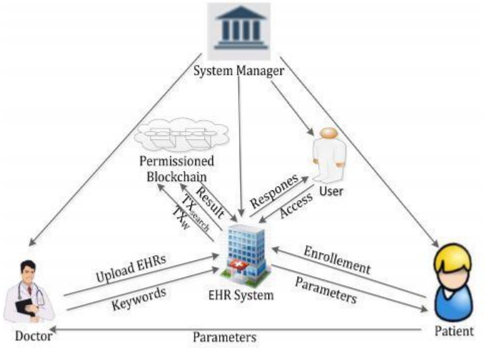

Fig. 2. System Architecture

IV. CONCLUSION ANDFUTUREWORK

Aiming at preserving patient privacy in an EHRs system on block chain, multiple authorities are introduced into ABS and put forward a MA-ABS scheme, which meets the requirement of the structure of blockchain, as well as guarantees the anonymity and immutability of the information. andthe patient private keys need to be constructed, N - 1 corrupted authorities cannot succeed in collusion attacks. Hence, protects the data from several attacks.

In existing system, single attribute is used. We can add multiple attributes. In Enhancement work, we are going to create hybrid cloud setup. Meaning that softwares are running in private servers and data willbe stored in public server in block chain. In present system, Diffie-Hellman encryption technique is used. In our work, we are using RSA cryptosystem.

REFERENCES

[1] D. Song, A. Perrig, and D. Wagner, ''Practical techniques for searches on encrypted data,'' in Proc. IEEE Symp. Secur.Privacy, May 2000, pp. 44–55.

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, ''Searchable symmetric encryption: Improved definitions and efficient constructions,'' in Proc. ACM Conf. Comput. Commun. Secur., 2006, pp. 79–88.

[3] [3] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, ''Secure ranked keyword search over encrypted cloud data,'' in Proc. IEEE 30th Int. Conf. Distrib. Comput. Syst., Jun. 2010, pp. 253–262.

[4] N. Premasathian and S. Choto, ''Searchable encryption schemes: With multiplication and simultaneous congruences,'' in Proc. 9th IEEE Int. ISC Conf. Inf. Secur. Cryptol., Tabriz, Iran, Sep. 2012, pp. 147–150.

[5] H. Li, F. Zhang, J. He, and H. Tian, ''A searchable symmetric encryption scheme using blockchain,'' Nov. 2017, arXiv:1711.01030. [Online]. Available: https://arxiv.org/abs/1711.01030

[6] Y. Zhang, R. H. Deng, J. Shu, K. Yang, and D. Zheng, ''TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain,'' IEEE Access, vol. 6, pp. 31077–31087, 2018.

[7] A. Sahai and B. Waters, ''Fuzzy identity-based encryption,'' in Advances in Cryptology— EUROCRYPT (Lecture Notes in Computer Science), vol. 3494, R. Cramer, Ed. Berlin, Germany: Springer-Verlag, 2005, pp.457– 473.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, ''Attribute- based encryption for fine-grained access control of encrypted data,'' in Proc. 13th ACM Conf. Comput. Commun. Secur., 2006, pp. 89–98.

[9] J. Bethencourt, A. Sahai, and B. Waters, ''Ciphertext-policy attribute-based encryption,'' in Proc. IEEE Symp. Secur. Privacy, May 2007, pp. 321–334.

[10] M. Chase and S. S. Chow, ''Improving privacy and security in multiauthority attribute-based encryption,'' in Proc. 16th ACM Conf. Comput. Commun. Secur., 2009, pp. 121–130.

[11] N. Attrapadung and H. Imai, ''Dual-policy attribute based encryption,'' in Proc. Int. Conf. Appl. Cryptogr. Netw. Secur., vol. 5536. Springer, 2009, pp. 168–185.

[12] M. Green, S. Hohenberger, and B. Waters, ''Outsourcing the decryption of ABE ciphertexts,'' in Proc. USENIX Secur. Symp., 2011, no. 3, p. 34.

[13] J. Hur and D. K. Noh, ''Attribute-based access control with efficient revocation in data outsourcing systems,'' IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 7, pp. 1214–1221, Jul. 2011.

[14] P. Zhang, Z. Chen, K. Liang, S. Wang, and T. Wang, ''A cloud-based access control scheme with user revocation and attribute update,'' in Proc. Australas. Conf. Inf. Secur. Privacy. Springer, 2016, pp. 525–540.

[15] J. Li, X. Lin, Y. Zhang, and J. Han, ''KSF-OABE: Outsourced attributebased encryption with keyword search function for cloud storage,'' IEEE Trans. Services Comput., vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.

[16] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, ''Flexible and fine-grained attribute-based data storage in cloud computing,'' IEEE Trans. Services Comput., vol. 10, no. 5, pp. 785–796, Jan. 2016.

[17] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, ''User collusion avoidance CPABE with efficient attribute revocation for cloud storage,'' IEEE Syst. J., vol. 12, no. 2, pp. 1767–1777, Jun. 2018.

[18] J. Li, Q. Yu, and Y. Zhang, ''Key-policy attribute-based encryption against continual auxiliary input leakage,'' Inf. Sci., vol. 470, pp. 175–188, Jan. 2019.

[19] J. Li, Q. Yu, and Y. Zhang, ''Hierarchical attribute based encryption with continuous leakage-resilience,'' Inf. Sci., vol. 484, pp. 113–134, May 2019.

[20] K. Emura, A. Miyaji, A. Nomura, and K. Omote, ''A ciphertext-policy attribute-based encryption scheme with constant ciphertext length,'' in Proc. Int. Conf. Inf. Secur. Pract. Exper. Berlin, Germany: Springer 2009, pp. 13–23.