MANTECH Publications

Recent Trends in Computer Science and Software Technology
Volume 7, Issue 3, September-December 2022

Personal Health Record Management with Blockchain Sharing Technique

Dr. Saroj Kaler[1], Neerja Rani[2], Monica Baxla[3]

Professor[1], Student[2,3]

Department of CSE

Abhinav Institute of Technology and Management

Corresponding Author's Email: -*neerjarani845@gmail.com*

Abstract

In this article, we describe a brand-new, secure EHR sharing system built on cloud computing and blockchain technology, with verified data integrity. With the aim of addressing data security and the loss of control rights during personal health record exchange, the new system uses symmetric encryption and attribute-based encryption approaches to enable privacy protection and fine-grained access restrictions. Comparatively to existing systems, the new strategy enables patients to give private key attributes to users, eliminating a number of security issues. Additionally, the new scheme manages scheme keys via the blockchain. The original method further enhances the efficacy of information reliability confirmation by storing the linked file set in a clever agreement together with the hash benefits of encoded individual health data on the blockchain.

Keywords: -*blockchain, cloud computing, data integrity, Data security.*

INTRODUCTION

Personal health records must be shared because they can enhance the accuracy of a doctor's assessment and advance clinical research. To reduce costs associated with information support fees, individual health records are frequently moved to alternative organizations, such as the cloud-based specialist co-op. However, in this case, the cloud service provider might falsify or divulge private medical information. Thus, crucial challenges in the sharing of personal health records include maintaining data privacy and

implementing granular access controls. Blockchain offers fresh ideas for securing the system for exchanging sensitive health data because it has a distributed architecture with decentralised and manipulable properties. The most likely candidates for reducing security and privacy issues are data storage servers, such as mail servers and encrypted file servers [1].

The development of networking, informatics, and cloud computing in recent years has significantly changed how people live. Patients can now save, manage, and communicate their health information in an easy, efficient, and accurate way thanks to the development of a system for sharing personal health data based on electronic data and cloud computing. Personal health records offer a consistent and objective medical record that is simple to access online and share because the patient can enter and update their own health information.

These individual health records are precious and practical resources. The sharing of personal health information with outside parties, such as cloud service providers, is commonplace. How to secure the security, privacy, and management of personal health data is one of the key challenges in these circumstances. The optimum strategy combines attribute-based coding, symmetric coding, and cloud storage.

Related Works

Electrocardiography (ECG) signals are combined with EHR data using a location-based authentication system, biometric authentication, and steganography techniques in an EHR cryptographic role-based access control model [1]. For the effective and secure management of EHRs, a steganography-based architecture [1] is presented that hides sensitive EHR data inside the ECG host data. Information can be hidden more effectively and securely with steganography than with conventional encryption. Depending on their security settings, only authorised users are able to retrieve data.

By offering a PHR-based blockchain architecture, this study [2] seeks to alleviate these blockchain disadvantages. Blockchain technology is used to allow manipulator resistance in the suggested method. Multi- and other diversified surroundings are suggested for privacy. The proposal model has a twin of authorization, auditability, auditability, and tamper resistance, all of which are rather good and dynamic. The PHR data is

encrypted using the PHR owner's public key (master key) and stored in a cloud storage system in this architecture to maintain secrecy [2]. The PHR is transported through a proxy re-encoding procedure. As a result, the gateway server, a proxy, is where the re-encryption keys and other authentication data are kept.

To enable a search and features that can withstand manipulation, the PHR data is kept on a private blockchain. The PHR owner and others, such as doctors, nurses, and others, will have access to the PHR. This study [3] introduces The Health Chain, a cutting-edge blockchain architecture focused on patients. In a secure, interoperable setting, the objective is to promote patient involvement, data curation, and controlled distribution of gathered information. A mixed block blockchain was suggested [3] to include immutable logging and redactable patient blocks. Patient data is produced and distributed readily. Public and private key pairs for a patient's digital identification are provided. Public keys are kept on the blockchain and are used to secure and validate transactions. The system also employs proxy encryption (PRE) to transmit data, and revocable intelligent contracts are used to ensure privacy and secrecy. Finally, a number of PRE upgrades are offered to enhance performance and security. The proxy re-encrypted data with dynamic keys, incremental server storage, and extra server-side encryption enable the fastest instals. The PHR paradigm, which combines distributed health records with blockchain technology and the open standard for EHR interoperability, is discussed in this article [4] along with its deployment and assessment. It follows the "Omni PHR" architectural principle, which outlines the design of a distributed and interoperable PHR.

It requires [4] the creation of a prototype, followed by an assessment of the performance of the integration of data from several production databases. Additionally, their assessment criteria paid attention to how the records worked as a whole, taking into account things like response time, CPU utilisation, memory occupancy, and disc and network usage. As opposed to normal Bitcoin replication systems in which all nodes receive all data, the chord approach is more scalable. To manage health data successfully, chord scalability is essential. It allows for data replication with controlled access and provides patients and healthcare professionals with monitoring and management.

SYSTEM ARCHITECTURE

Cryptographic Technique

In the presence of an adversary, cryptographic procedures are used to ensure data confidentiality and integrity. Depending on the security needs and dangers, several cryptographic approaches, such as symmetric key cryptography, may be used during data transit and storage.

FTP Protocol

Using TCP/IP connections, the File Move Protocol (FTP), an internet protocol, may be used to transfer data between computers connected to the internet. A protocol between a client and a server is called FTP. A client requests a file, which is subsequently delivered by a nearby or distant server.

MVC Architecture

The Model View Controller or MVC is a web-based software design paradigm. The MVC pattern consists of three parts:

- **Model –** Model objects store data retrievedfrom the database.
- **View –** View is a user interface. It displays model 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.

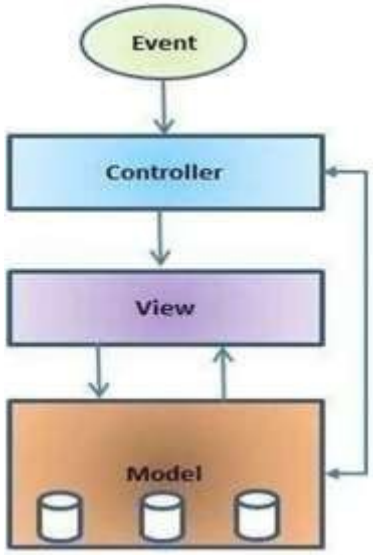

Fig.1:-MVC Architecture

Cloud Technology

Without needing direct user administration, cloud computing offers on-demand access to computer system resources, principally data storage and processing power. The phrase is frequently used to describe data centres that cater to a sizable Internet user base.

Block Chain Technology

In a network connected by pair-to-pear nodes, commonly known as the "block," Block Chain Technology is a technology that maintains public transactional records in many databases called the "chain" in a network. The term "digital ledger" is widely used to describe this kind of storage.

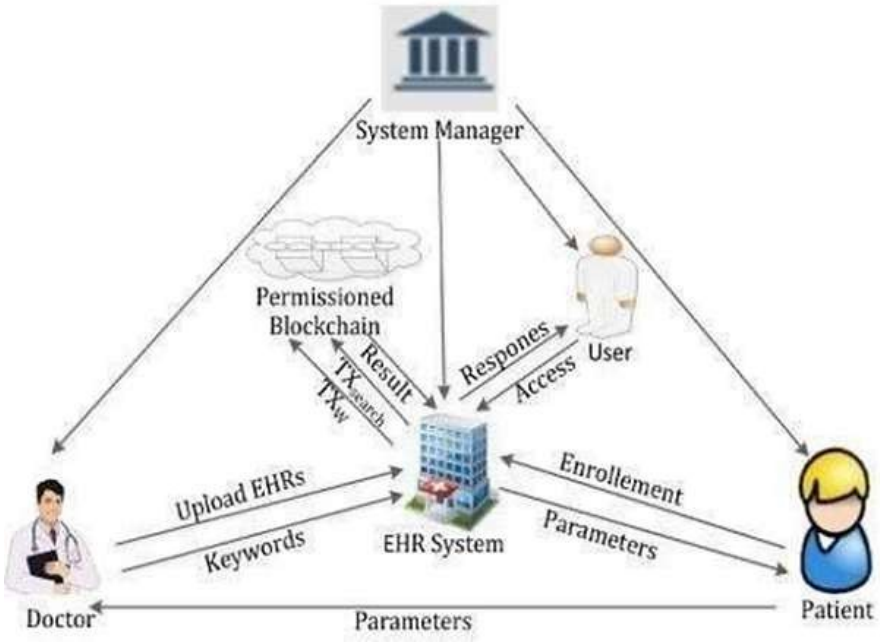

Fig.2:-System Architecture

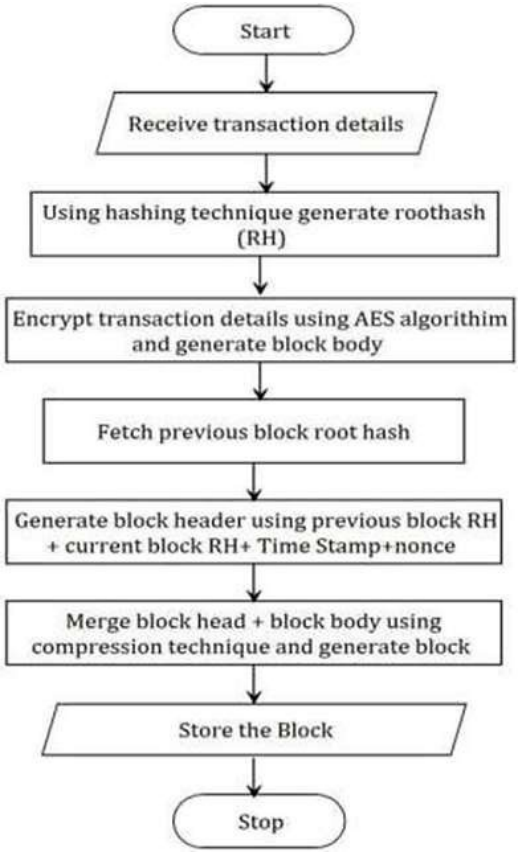

Fig.3:-File upload flowchart

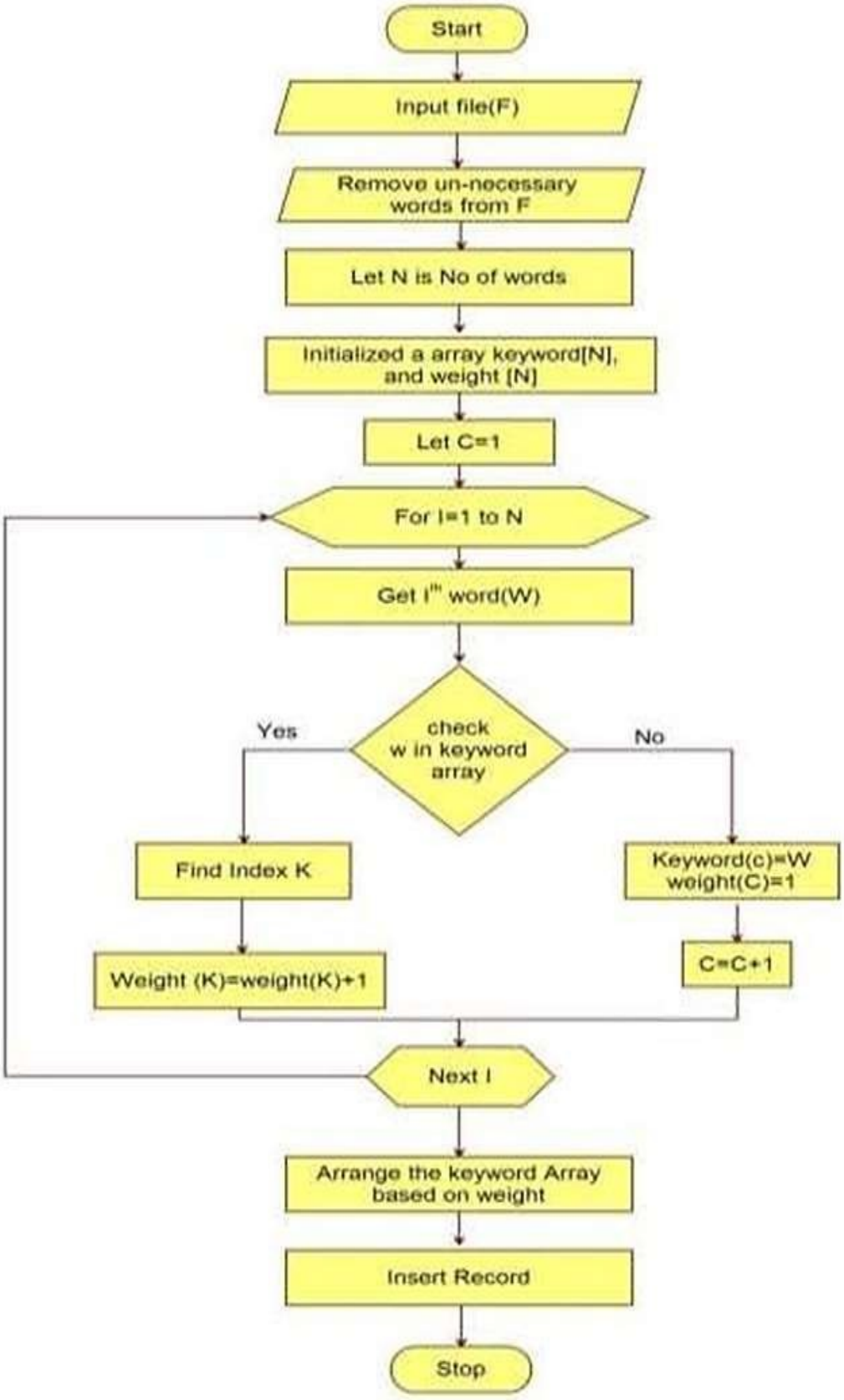

Fig.4:-Flowchart for processing of file

EXPERIMENTAL SETUP

- **Key Generation**

  The administrator will produce the keys for encryption and decryption. The administrator can create a secret key using the symmetric AES method.

- **Access Control and Upload file usingFTP protocol**

  Computers utilise FTP (File Transfer Protocol) as a set of guidelines and instructions to move files from one system to another across the internet. The uploaded files will be accessible to the administrator, who will use the FTP protocol to store them in the cloud after encrypting them with a master secret key for security reasons. Grades dictate any access restrictions. For instance, only grade A users will be able to access a file if an administrator selects grade A when uploading it.

- **Keyword Indexing Module**

  Look for keywords and remove any extraneous file terms. Use the MD5 algorithm to transform the keywords into a hash code, and then store the hash code in an index array to determine the content's keyword weight. A 128-bit hash result is produced using the faulty but widely used MD5 (Message Digest Algorithm).

Send Aggregate Key

Look for keywords and remove any extraneous file terms. Use the MD5 algorithm to transform the keywords into a hash code, and then store the hash code in an index array to determine the content's keyword weight. A hash value of 128 bits is produced using the flawed but commonly used MD5 (Message Digest Algorithm).

Search with Keyword

The user must choose the aggregate key after typing "indentsearch." Your word should be converted to a hash. obtain public and hash keys, decode, and separate them.

Hash codes are produced using a hash key and keyword. The recipient must verify the keyword index and display all file names for the user if any matching files are present after sending the hashcodes to the server. View the server's shortlisted files and decrypt the file.

IMPLEMENTATION

Requirement Analysis

The required software product's needs are extracted. This stage involves developing a

business scenario using the SRS (Software Requirement Specification) document.

Design

Physical structure, hardware, operating systems, programming, communications, and software security are all being planned for. Making sure the software system complies with the required product standards is the focus of the design phase.

Testing

Testing evaluates the user needs for the application. Here, the programme is assessed to look for issues. Examples of unit tests Dynamic testing's initial step, initialization testing, is mostly the domain of developers, then test engineers. When expected test results are obtained or discrepancies can be adequately explained and accepted, unit tests are run.

System Testing

The entire system is examined for both functioning and lack thereof. The complete system is first configured in a controlled environment, and the test team performs "black box" testing.

CONCLUSION

Multiple specialists joined ABS and produced an MA-ABS plot that complies with blockchain structure criteria while also assuring unknown data and permanence in order to give patient security in a square chain framework for EHRs. Additionally, since corrupted N-1 authorities are unable to defend against collusion attempts, patient private keys must be produced. Various threats to data are mitigated.

REFERENCES

1. Bahga, A., &Madisetti, V. K. (2013). A cloud-based approach for interoperable electronic health records (EHRs). IEEE Journal of Biomedical and Health Informatics, 17(5), 894- 906.
2. Li, J., Yu, Q., Zhang, Y., &Shen, J. (2019). Key-policy attribute-based encryption against continual auxiliary input leakage. Information Sciences, 470, 175-188.
3. Yang, K., Jia, X., &Ren, K. (2014).Secure and verifiable policy update outsourcing for big data access control in the cloud. IEEE Transactions on ParallelandDistributed Systems, 26(12), 3461-3470.
4. Sahai, A., & Waters, B. (2005, May). Fuzzy identity-based encryption. In Annual international conference on the theory and

applications of cryptographic techniques (pp. 457- 473). Springer, Berlin, Heidelberg.

5. Li, J., Lin, X., Zhang, Y., & Han, J. (2016). KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage. IEEE Transactions on Services Computing, 10(5), 715-725.
6. Premarathne, U., Abuadbba, A., Alabdulatif, A., Khalil, I., Tari, Z., Zomaya, A., &Buyya, R. (2016). Hybrid cryptographic access control for cloud-based EHR systems. IEEE Cloud Computing, 3(4), 58-64.
7. Zhang, P., Chen, Z., Liang, K., Wang, S., & Wang, T. (2016, July). A cloud- based access control scheme with user revocation and attribute update. In Australasian Conference on Information Security and Privacy (pp. 525-540). Springer, Cham.
8. Li, J., Yu, Q., & Zhang, Y. (2019). Hierarchical attribute based encryption with continuousleakage- resilience. Information Sciences, 484, 113-134.
9. Zhang, Y., Deng, R. H., Shu, J., Yang, K., &Zheng, D. (2018). TKSE: Trustworthy keyword search over encrypted data with two-side verifiability via blockchain. IEEE Access, 6, 31077-31087.
10. Li, H., Zhang, F., He, J., &Tian, H. (2017). A searchable symmetric encryption scheme using blockchain. ArXiv preprint arXiv:1711.01030.
11. Ge, A., Zhang, J., Zhang, R., Ma, C., & Zhang, Z. (2012). Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme. IEEE Transactions on Parallel and Distributed Systems, 24(11), 2319-2321.
12. Deepak, N. R., &Balaji, S. (2015). A Review of Techniques used in EPS and 4G-LTE in Mobility Schemes. International Journal of Computer Applications, 109(9).
13. Li, J., Yao, W., Zhang, Y., Qian, H., & Han, J. (2016). Flexible and fine- grained attribute-based data storage in cloud computing. IEEE Transactions on Services Computing, 10(5), 785- 796.
14. Deepak, N. R., &Balaji, S. (2015, December). Performance analysis of MIMO-based transmission techniques for image quality in 4G

wireless network. In 2015 IEEE International Conference on Computational Intelligence and Computing Research (ICCIC) (pp. 1-5). IEEE.

15. Thanuja, N., & Deepak, N. R. (2021, April). A Convenient Machine Learning Model for Cyber Security. In 2021 5th International Conference on Computing Methodologies and Communication (ICCMC) (pp. 284- 290). IEEE.