IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303049 |

Privacy Preserving Secured Data Distribution between Multiple Hospitals and Medical Institutes

Mrs.Tejaswini Vinayak Patil

HOD, Department of Computer Engineering, K.P.Patil Institute of Technology (Polytechnic), Mudal, Maharashtra, India

ABSTRACT: Electronic medical data have significant advantages over paper-based patient records when it comes to storage and retrieval. However, most existing medical data sharing schemes have security risks, such as being prone to data tampering and forgery, and do not support the ability to verify the authenticity of the data source. Medical Internet of Things are generating a big volume of data to enable smart medicine that tries to offer computer- aided medical and healthcare services with artificial intelligence techniques like deep learning and clustering.

KEYWORDS: Blockchain, encryption, medical data, privacy, and security.

I. INTRODUCTION

Nowadays we have huge data of patient health records and details generated at different medical organizations that provide health services to patients. This data is crucial and important to medical organizations. All the medical organizations now store their data in electronic manner in an efficient way onto cloud storages. But when such technology is introduced there is a chance of data leak or hacking which can cause great impact on the system if in any way the information is forged or manipulated or stolen. Medical fields extensively incorporate data mining and encryption technologies for such purposes. Also it is challenging issue for hospitals to analyse large medical data from different hospitals. It is also important to share the data with different medical institutes in secure manner.

II. RELATED WORK

The system that we will be emphasizing on implementing will consist of storing of huge medical data related to patients on a cloud system that can be accessed by multiple medical organizations at a single time basically a client server application where the client will be the hospitals, medical institues and the server will be the cloud storage.. All they will need is their verification through a third party authenticator and the hospital authority. It will consist of modules like signature and access control policy generation, Data encryption with ABS-OD, data clustering and user verification and retrieval.

III. METHODOLOGY

Module 1: Segregation of data item and access control policy:

Access policy will be generated by hospital for users who need data. Hospital and medical institutions first register to the hospital authority servers. The data of all the patient related medical history is collected and segregated onto the proposed system. By applying to the encryption and decryption keys the data access is being provided. Hospitals first prepare access control policy for patient's data. And then transfer it to hospital authority server. Hospital authority servers prepare the private and signature key on that access policy and transfer it to hospital and medical institutes.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303049 |

Module 2: Data encryption with ABE-OD:

Medical data related to all patients from various hospitals will be uploaded onto a hospital authority server. This data need to be encrypted to safeguard its integrity from hackers as it is personal information and confidential. After receiving signature key hospital encryption of the medical record is done using ABE-OD. Hospital authority server use cyclic group with bilinear map. ABE-OD is nothing but a encryption technique that resolves its encryption mechanism by outsourcing the encrypted keys for decryption.

Module 3: Data Clustering with HOPCM on CSP:

Data uploading takes place in the form of tensors. Tensors are nothing but the encrypted details of any hospital repository. This tensors needs to be uploaded on third party cloud service providers. For this clustering needs to be performed and that is where we introduce HOPCM. The high-request possibility c-implies calculation (HOPCM) will be performed on the cloud framework for clinical information grouping on transferred tensors. After receiving the encrypted data from hospital authority server, cloud service provider will apply HOPCM. It assigns each object into one group. Then membership matrix is generated. Cluster centres are prepared. Further dataset is partitioned into subsets. Distance values are calculated and stored on server. If the clustering size increases and we face enormous data further we can use the Block chain mechanism as well.

Module 4: User verification and data retrieval:
In this module the private key obtained from the cloud authority server will be used to decrypt the data downloaded at user side. Here user can be a medical institute authority person. Medical institute authority person will send request to CSP using search key. CSP returns matching clustered data with transformed encryption along with access key id. Then institute requests decryption of data to hospital authority server. For this purpose user first needs to get himself verified along with the data downloaded. ABS is used in this process of verification and retrieval. After verifying the signature, hospital authority server sends the key to medical institute user. And data user can obtain the clustered data in decrypted form.

IV. EXPERIMENTAL RESULTS

We have existing systems that have encryption of data related to patients in an hospital done through block chain mechanism. These systems can be easily broken through and data privacy can be an issue faced in those. So to overcome these issues We plan hospital data sharing System, which will allow to store the patient data to the cloud in secured manner and also will allow to share it between multiple hospitals and institutions. This can guarantee secure storage and sharing of clinical information. The proposed work accomplishes the classification and protection of hospital patent's records which was not available in the systems that already exists . In our work, the hospital authority figures explicit access strategies and approves medical institute researchers to encode clinical information by utilizing ABE, which can guarantee adaptable access control to cloud clinical information and empower the hospitals to completely take an interest in the sharing of clinical information.

V. CONCLUSION

This article suggests a novel approach to medical data exchange that blends blockchain technology with cloud storage benefits. Our plan makes advantage of the blockchain system to store encrypted medical data on a cloud server and maintain the address of the corresponding medical data, including medical-related information and ciphertext. Consequently, the proposed method meets the immutability criterion. as well as unforgeability. The attribute-based cryptosystem can be used to ensure the privacy of medical data stored in cloud guaranteed, and the reliability of the source of the medical data can be confirmed. Furthermore, the OD-ABE technique can help reduce the computational strain on users of medical data. The analysis's findings indicate that the suggested scheme performs well in terms of security and computation overhead.

The suggested algorithm significantly improves in relation to clustering effectiveness of the conventional possibilistic C-means algorithm, particularly when a lot of data is gathered. In addition, we created a cloud-edge system to

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Referred Journal |

|| Volume 13, Issue 3, March 2024 ||

| DOI:10.15680/IJIRSET.2024.1303049 |

accomplish data co-clustering across many hospitals. One significant benefit the created solution makes use of cloud computing to increase clustering efficiency while keeping the original data private. Subsequent research endeavours will centre on validating the proposed framework in practical scenarios. To be more precise, we will implement the created system in an actual hospital setting in order to verify the suggested approach.

REFERENCES

[1] 1. Fanyu. Bu, C. Hu, Q. Zhang, C. Bai, L. T. Yang and T. Baker, "A Cloud-Edge-Aided Incremental High-Order Possibilistic c-Means Algorithm for Medical Data Clustering," IEEE Transactions on Fuzzy Systems, vol. 29, no. 1, pp. 148-155, Jan. 2021, doi: 10.1109/TFUZZ.2020.3022080.

[2] 2. Xiaodong. Yang, T. Li, X. Pei, L. Wen and C. Wang, "Medical Data Sharing Scheme Based on Attribute Cryptosystem and Block chain Technology," IEEE Access, vol. 8, pp. 45468-45476, 2020, doi: 10.1109/ACCESS.2020.2976894.

[3] 3. A. Ekblaw, ‘‘A case study for blockchain in healthcare: MedRec prototype for electronic health records and medical research data,’’ Proceeding of IEEE Open Big Data Conference, 2016, p. 13.

[4] 4. M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, ‘‘Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,’’ IEEE Transaction on Parallel Distribution System, vol. 24, no. 1, pp. 131–143, Jan. 2013.

[5] 5. H. Wang and Y. Song, ‘‘Secure cloud-based EHR system using attribute-based cryptosystem and Blockchain,’’ Journal of Medical System, vol. 42, no. 8, pp. 152–161, Jul. 2018.

[6] 6. L. Cheung and C. Newport, ‘‘Provably secure ciphertext policy ABE,’’ Proceeding of 14th ACM Computer and Communication Security Conference (CCS), 2007, pp. 456–465.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details