A Novel Technique To Access Sensitive Medical Data With Access Policies

Dega Sunil Kumar
Computer Science and Engineering
Kalasalingam Academy of Research and Education
9920004540@klu.ac.in

Madala Teja
Computer Science and Engineering
Kalasalingam Academy of Research and Education
9920004544@klu.ac.in

Bestha Aruna Sai
Computer Science and Engineering
Kalasalingam Academy of Research and Education
9920004553@klu.ac.in

Pamidi Venkata Sreekanth Reddy
Computer Science and Engineering
Kalasalingam Academy of Research and Education
9920004548@klu.ac.in

Dr. Suresh Kumar
HOD
Computer Science and Engineering
Kalasalingam Academy of Research and Education
hodcse@klu.ac.in

Abstract: Ensuring the efficient and secure access of sensitive health records is one of the main issues challenging healthcare systems. This work offers a novel method that combines the Harmony Search Algorithm (HSA) with Attribute-Based Encryption (ABE) to provide strict data security, patient privacy, and robust access controls. Inspired by the evolution of musical harmony, the Harmony Search Algorithm successfully integrates ABE fundamentals to create and enhance controls on access that manage the retrieval of personal medical records. A dynamic framework is managed through this association, whereby HSA optimizes the development and growth of access controls and ABE presents a fine-grained, attribute-based method to encrypting and decrypting sensitive data.

This creative approach makes use of the HSA's ability to adapt access rules continuously to meet changing legal requirements and healthcare needs. The ABE algorithm offers local management of data access through making sure that only allowed entities with the necessary features can decode specific medical information, which enhances data security. With a primary focus on ensuring legal compliance, the framework's development was influenced by tight healthcare data laws, patient confidentiality, and ethical values. The recommended methodology offers an optimal combination of data security concepts and efficiency methods, representing an important progress in the domain of medical data management. This method integrates HSA and ABE to provide a framework that is safe, flexible and responsible for obtaining private medical information. This will maintain the security of patients and safety while expanding data useful for specified organizations.

Keywords:* *privacy; healthcare data; security; Flexible; optimisation

I. INTRODUCTION:

An innovative way to access sensitive health records with well-constructed controls for access has been implemented, indicating an important move further in healthcare technology. This strategy maintains a careful balance between patient privacy and data security and provides necessary access to vital data. In a scenario where strong legal regulations and moral standards collide with medical innovations, looking for effective, secure, and ethical data access ways is crucial. The execution of this unique technique reflects the union of advanced technological innovation with an unbroken dedication to protecting the confidentiality of private medical data.

In simple terms, this creative strategy aims to remake regulations for data availability in the medical field by using modern facilities encryption, safe access methods, and secure privacy technologies—all while handling a complex structure of ethical and legal requirements. By doing this, it attempts to equally transform the availability of health-related data and set the standard for moral administration of data within the health care industry. With the release of this arrival, the next phase in healthcare taking decisions begins, a time during which technology and ethics converge to allow informed choices while upholding a constant dedication to patient privacy and data security.

II. LITERATURE SURVEY:

Specified keywords search scheme for EHR sharing

Shufen Niu1 · Fei Yu1 · Mi Song1 · Song Han1 · Caifen Wang

The work presents a focused search for keywords method for Electronic Health Record (EHR) sharing, resolving privacy concerns with searchable encryption. Doctor-specified keywords may be used to conduct secure EHR searches thanks to a combination of searchable encryption and proxy re-encryption. Sensitive patient data should not be misused or accessed without authorization, according to the suggested plan. We discuss the perks as well as cons of the many existing methods for EHR sharing including proxy re-encryption and searchable encryption. The paper's conclusion highlights Although the importance of more research to increase performance as it preserves data security. Through the use of the program, doctors may allocate keywords for data users to authorize for managed and excluded access to electronic health records (EHR). The practical use ensures patient privacy by offering EHR without indicating vital data as well as securely searching for established keywords. Experts must supply exact keyword specifications in order for the program to work; otherwise, the availability of data may be denied. The identify method of verification added by the medical cloud may result in a delay in the data recovery process.

III. ALGORITHM:

Searchable Encryption and Proxy re-encryption.

A Secure Framework for Health Record Management Using Blockchain in Cloud Environment

G Verma et al 2021 J. Phys.: Conf. Ser.1998

The challenges of securely maintaining health records in electronic health systems are investigated in the research review, with special particular focus on security, privacy, and limited usage control. It presents how medical institutions employ electronic systems and how a lot of medical data is created on every single day. Examined are the drawbacks of centrally situated information handling, such as the difficulty in exchanging records throughout medical establishments. In addition to introducing the concept of Electronic Health Data (EHD), the study further highlights the drawbacks of the relevant, institution-specific deployments.

To address all of these issues, the inquiry recommends a secure infrastructure for delivered health record management that integrates the concept of blockchain. It underlines various benefits of blockchain science and technology, such as secure entry control, privacy protection, and multi-user data sharing. Attribute-based encryption (ABE) with searchable keys should be utilized for controlled access at a fine level. The scientific survey's summary, which also emphasizes the design's potential for greater acceptance in the years to come, involving validation on open records and relevance to multiple kinds of medical structures, uses simulated outcomes to illustrate the recommended framework's utility and security.

A Secure Searchable Encryption Framework for Data Security using Personal Data Storage (PDS) Module

Kottu satya naga divya #1, a. Durga devi #2,2021

In the existing research on personal data storage (PDS), there has been a significant change from service-centric to focused on users types, encouraging users to take control over their data by conducting separate logical storage facilities. Cloud computing has played an essential part in supporting this transformation through the delivery of infinite resources via the Internet. However, because remaining cloud servers feature encryption, key creation, and data managing functionality, there are reservations about private medical data. Responding to this gap, A strategy known as Establish Personal Data keeping (PDS) has been constructed to ensure the protection of health information from patients while overcoming authorisation and encryption difficulties. The study of literature discloses that cloud services do not now have any privacy protections in place. This emphasizes the necessity for new technologies, such as the PDS, which will improve data safety and access control over the exchange of medical material.

Deep Learning Based Homomorphic Secure Search-Able Encryption for Keyword Search in Blockchain Healthcare System: A Novel Approach to Cryptography

Aitizaz Ali 1, Muhammad Fermi Pasha 1 , Jehad Ali 2,3,* , Ong Huey Fang 1 , Mehedi Masud 4 , Anca Delia Jurcut 5 and Mohammed A. Alzain 6,2022

This work explores the combination of deep learning with the use of blockchain technology in the medical field to enhance security and privacy in patient health records (PHR). Existing blockchain-based health insurance platforms are being attacked for relying solely on the storage of information, which leaves them insecure. The proposed technology introduces an innovative and reliable searchable blockchain founded on deep learning. The shortcomings of traditional authentication systems are stressed in the study, and attribute-based signatures (ABS) are proposed as a way to improve PHR security. It also emphasizes how attribute-based secure communication and blockchain technology must work together. Additionally, the study represents a trust-based technique that promotes transparency, reliability, and performance by utilizing algorithmic trust.

Towards privacy-preserving content-based image retrieval in cloud computing, IEEE Trans. Cloud computing, vol. 6, no. 1, pp. 276–286, 2019.

Thang Hoang , Attila A. Yavuz , Member, IEEE, and Jorge Guajardo.

Providing an effective NDD interface that can be utilized with encrypted in-network preservation is the aim of this project. First, we apply locality-sensitive encryption and biometric methodologies for converting the NDD challenge into a keyword search in order enhance performance. Next, put into operation a rewarding multi-key searchable encryption system that, even in instances in which the data are encrypted using multiple keys and originated from numerous resources, requires a single encrypted user queries. While bringing together the previously characterized methods doesn't appear to yield predictable outcomes, devise a secure method of filtering conclusions applying Yao's jumbled networks to avoid user-side after processing.

Additionally, we have improved our architecture to address any malicious activity by in-network servers. Numerous studies on real-world image datasets reveal that our method will achieve the same precision to the text with minimal security expense.

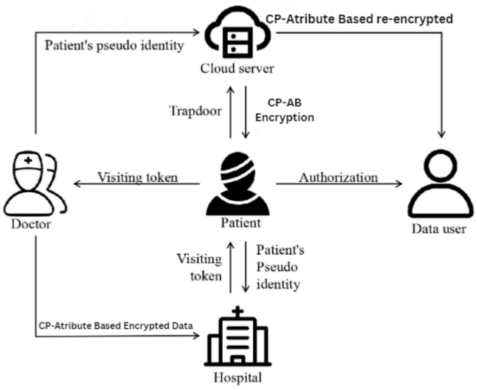
CP-Atribute Based re-encrypted
Patient's pseudo identity
Cloud server
Trapdoor
CP-AB Encryption
Visiting token
Authorization
Doctor
Patient
Data user
Visiting token
Patient's Pseudo identity
CP-Atribute Based Encrypted Data
Hospital

Fig. 1.

IV. METHODOLOGY:

A. Attribute Based Encryption

Attribute-Based Access Control: Data can be encrypted using ABE employing a list of buildings or only a few of them. These features could be any aspect that describes someone else or the data itself, like section, age, role, or any other attribute.

Extremely fine Control: Unlike typical encryption systems which allow permission based on set parameters user keys, ABE permits access based on matching specific attribute-based limitations. Content may, for illustration, be encrypted in order to limit accessibility to only those who meet the policy's criteria and contain a specific set of characteristics. Two ABE Types: ABE mostly comes in two forms:

Important Guidelines ABE, or KP-ABE, assigns keys to users based upon the characteristics they have and encrypts data in compliance with a predetermined policy. Users are able to decode the data if its features match the standards specified at the time of encryption. Applying an attribute-based regulations, the Ciphertext Policy ABE (CP-ABE) encrypts data and delivers keys to consumers based upon the attributes provided. Someone else can decrypt the contents if its properties match with the rules connected to the encrypted data.

Flexibility and Scalability: ABE provides flexibility by allowing access control settings to be modified without requiring re-encrypting data. It is quite flexible in situations where access permissions must be changed often.

Difficulties: The processing cost and complexity of ABE can be problematic, particularly in large-scale systems. In order to prevent ambiguities or conflicts in access control, maintaining characteristics and policies also needs careful thought.

Significant promise exists for ABE in maintaining data security while enabling effective and adaptable access control in delicate industries including cloud computing, healthcare, and finance. It has established itself as a crucial component of contemporary cryptography systems thanks to its capacity to apply intricate access controls while concealing critical data..

B. Harmony Search Algorithm

An optimisation method that draws inspiration from nature to discover the best answer to problems with optimisation is called the harmonic search algorithm. It is predicated on the idea of mimicking the way players improvise in a jazz group, altering their tones to produce harmony..

Geem et al. (2001) created the well-known metaheuristic algorithm known as the harmony search algorithm (HSA). Musicians' improvisational techniques serve as an inspiration for HSA. To create the ideal harmony, a musician looks for the right notes. This idea served as the foundation for the development of HSA, which finds a good answer to optimisation problems.

To confirm HSA's performance, its developers conducted a great deal of experimentation. The following are the primary features of HSA:

Three things are not necessary: (1) decision variables do not need to be initially defined; (2) derivate information is not needed; and (3) just a small number of control parameters are needed for fine tuning [6]. Owing to these features, HSA is favoured above the other metaheuristic approaches currently in use. Many other types of problems, including scheduling, global optimisation, power engineering, computer vision, social economic, and clustering issues, may be resolved with HSA. The HSA is regarded as a straightforward algorithm that is effective. Additionally, other academics looked at the applicability of HSA in many fields.

Harmony Memory: It keeps track of prior effective fixes, or harmonies, for the issue.

Improvisation: By taking into account the current ones and their characteristics, new solutions (harmonies) are created.

Evaluation: Based on a fitness function, the created solutions are assessed.

Updating Memory: The least suitable answer is replaced in the memory by a new one if it outperforms the current ones.

The phases of the algorithm entail striking a balance between exploitation (using the best answers currently available) and exploration (creating new solutions).

When the objective function is smooth and the search space is continuous, it is especially helpful for optimisation issues. However, depending on the parameters and features of the problem, its performance may differ.

It is used in many different domains, including as biology, economics, and engineering, to solve issues with scheduling, function optimisation, and parameter estimation.

Optimising parameters like harmony memory size, pitch adjustment rate, bandwidth, etc. is essential for improving convergence and accuracy for certain issue categories.

C. Working Flowchart

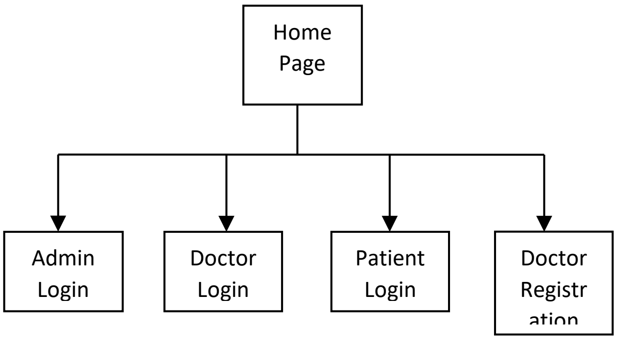

Fig. 2. Working Flowchart

V. CONCLUSION

Harmony Search Algorithm (HSA) and Attribute-Based Encryption (ABE) together create a novel framework for sensitive medical data access. The optimisation powers of HSA and the attribute-based access control of ABE are used in this fusion to improve access procedures and guarantee granular control for increased secrecy. Through iterative refining, access rules are brought into accordance with changing regulatory requirements and healthcare environments, as well as ethical and legal frameworks. Because only approved entities with pertinent characteristics are able to access certain medical information, ABE's granular control offers a strong defence against breaches. The ethical, legal, and practical ramifications of implementation must be carefully considered, necessitating cooperation between regulatory agencies, healthcare providers, and technologists.

This innovative strategy strengthens patient privacy protections while improving data accessibility, marking a step towards a more ethical, secure, and flexible healthcare data ecosystem.

REFERENCES

[1] [1] M. Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multi-owner settings," in Security and Privacy in Communication Networks. Springer, pp. 89–106, (2016).

[2] [2] A. M.-H. Kuo, "Opportunities and challenges of cloud computing to improve health care services," Journal of medical Internet research, vol. 13, no. 3, (2017).

[3] [3] 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 Transactions on Parallel and Distributed Systems, vol. 24, no. 1, pp. 131–143, (2018).

[4] [4] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, (2019).

[5] [5] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An smdpbased service model for interdomain resource allocation in mobile cloud networks," IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 2222–2232, (2019).

[6] [6] M. M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1805–1818, (2019).

[7] [7] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geodistributed clouds for e-health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and Health Informatics, vol. 18, no. 2, pp. 430–439, (2020).

[8] [8] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 8, pp. 1467–1479, (2021).

[9] [9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 11, pp. 3025–3035, (2021).

[10] [10] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multikeyword top-k retrieval over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing, vol. 10, no. 4, pp. 239–250, (2022).

[11] [11] Le, D.-N., Parvathy, V.S., Gupta, D., Khanna, A., Rodrigues, J.J.P.C., Shankar, K." IoT enabled depthwise separable convolution neural network with deep support vector machine for COVID-19 diagnosis and classification" International Journal of Machine Learning and Cybernetics, vol. 12, no. 11, pp. 3235-3248, (2021).

[12] [12]Elhoseny, M., Bian, G.-B., Lakshmanaprabu, S.K., Shankar, K., Singh, A.K., Wu, W." Effective features to classify ovarian cancer data in internet of medical things" Computer Networks, vol. 159, pp. 147-156, (2019).