Secure Searchable Encryption and Proxy Re-Encryption Framework for Privacy-Preserving E-Healthcare Systems

Ms.K.BabyRamya, Mrs.K.Pavani, K.Vasudevarao

Assistant Professor in the Department of MCA ,s SRK Institute of Technology, Vijayawada

Assistant Professor&Head of Department of MCA, SRK Institute of Technology, Vijayawada.

Student in the Department of MCA, SRK Institute of Technology, Vijayawada

Abstract: E-healthcare systems generate and store large volumes of sensitive patient data, which raises significant concerns regarding privacy, security, and efficient data access. Traditional encryption techniques ensure confidentiality but limit the ability to search over encrypted data and restrict flexible access control. To address these challenges, this paper proposes DSAS, a secure and privacy-preserving data sharing framework that integrates searchable encryption with conditional proxy re-encryption. In the proposed system, patient healthcare records (PHRs) are encrypted before being stored in the cloud, ensuring data confidentiality. Authorized users can perform keyword-based searches on encrypted data without revealing sensitive information. Furthermore, the system enables secure delegation of access rights from one doctor to another when needed, without exposing the underlying data or conditions. The framework achieves key security properties such as proxy invisibility, condition hiding, and collusion resistance. Experimental analysis demonstrates that the proposed system provides efficient, secure, and scalable data sharing suitable for real-world e-healthcare environments.

Index terms - E-Healthcare, Data Security, Searchable Encryption, Proxy Re-Encryption, Conditional Access Control, Privacy Preservation, Cloud Computing, Personal Health Records (PHR), Secure Data Sharing

1. INTRODUCTION

The rapid advancement of wearable devices, sensors, and cloud computing technologies has significantly transformed modern e-healthcare systems. These systems continuously collect large volumes of Personal Health Records (PHRs), enabling

doctors to monitor patients effectively and provide timely medical services. However, storing such sensitive healthcare data on cloud servers introduces serious challenges related to data privacy, security, and unauthorized access.

To protect confidentiality, encryption techniques are widely used before uploading data to the cloud. Although encryption ensures data security, it makes data retrieval difficult because traditional methods cannot perform searches over encrypted data. To address this issue, searchable encryption techniques have been introduced, allowing authorized users to search encrypted data using keywords without revealing sensitive information. Despite this advantage, these systems require the data owner or doctor to remain online for access control, which is not always practical in real-world scenarios.

Proxy Re-Encryption (PRE) is a promising solution that enables secure delegation of access rights from one user to another. For example, a doctor can delegate access to another doctor during unavailability. However, conventional PRE schemes suffer from several limitations, such as excessive power of the proxy, lack of fine-grained control, and vulnerability to collusion attacks. These limitations can compromise the overall security of the e-healthcare system.

To overcome these challenges, this paper proposes a secure framework called DSAS (Data Sharing and Authorized Searchable) system, which integrates searchable encryption with conditional proxy re-encryption. The proposed system ensures that healthcare data remains encrypted, searchable, and securely accessible only to authorized users. It also supports conditional delegation while preserving privacy through properties such as proxy invisibility, condition hiding, and collusion resistance. The framework improves both security and efficiency, making it suitable for real-world e-healthcare applications.

2. LITERATURE SURVEY

2.1 Searchable encryption revisited: Consistency properties, relation to anonymous IBE, and extensions:

In terms of consistency (the degree to which false positives are generated) for public-key encryption with keyword search (PEKS), we find and close several gaps. We define statistical and computational relaxations of the current concept of perfect consistency, demonstrate the computational consistency of the Boneh et al. scheme (Advances in

Cryptology—EUROCRYPT 2004, ed. by C. Cachin, J. Camenisch, pp. 506–522, 2004), and offer a new statistically consistent scheme. Additionally, we offer a transformation from an anonymous identity-based encryption (IBE) scheme to a safe PEKS method that ensures consistency in contrast to the former. Lastly, we propose three extensions of the fundamental concepts discussed here: identity-based encryption with keyword search, public-key encryption with temporary keyword search, and anonymous hierarchical identity-based encryption.

2.2 Improved proxy reencryption schemes with applications to secure distributed storage:

An application known as atomic proxy re-encryption was introduced by Blaze, Bleumer, and Strauss (BBS) in 1998. In this application, a semitrusted proxy transforms a ciphertext for Alice into a ciphertext for Bob without revealing the underlying plaintext. As a technique for handling encrypted file systems, we anticipate that quick and safe re-encryption will grow in popularity. Significant security problems have prevented BBS re-encryption from being widely used, despite its speedy computation. We show the value of proxy re-encryption as a way to add access control to a secure file system and provide novel re-encryption methods that achieve a stronger sense of security, in line with recent work by Dodis and Ivan. Our experimental file system's performance metrics show that proxy re-encryption can function well in real-world scenarios.

2.3 Public key encryption with keyword search revisited:

Boneh, Di Crescenzo, Ostrovsky, and Persiano presented the public key encryption with keyword search (PEKS) technique, which allows one to search for encrypted keywords without jeopardizing the security of the original material. In this article, we address two crucial PEKS scheme difficulties that Boneh et al.'s study did not address:"removing secure channel"and"refreshing keywords."We highlight the original PEKS scheme's inefficiency as a result of using the secure channel. By creating an effective PEKS scheme that eliminates a secure channel, we are able to fix this issue. Then, we contend that when keywords are employed often in the PEKS scheme, caution should be exercised because this might compromise PEKS security.

2.4 Towards a secure incremental proxy re-encryption for e-healthcare data sharing in mobile cloud computing:

Many players and stockholders in the e-healthcare sector have universal access to a pool of shared resources thanks to cloud computing. Cloud computing's rapid popularity has unavoidably sparked worries about the security of the data that is outsourced. Mobile devices have limited resources, thus in order to be implemented, security solutions must discharge the computing comprehensive operations on the cloud. Traditionally, the mobile client would have to encrypt and calculate the hash value from scratch whenever any changes were made to the uploaded data. In order to enhance file modification chores, we want to offer in this work a pairing-free incremental proxy re-encryption system without certificates that would run proportionately to the amount of updates in time rather than the document length. In terms of energy usage and turnaround time, the suggested plan significantly improves the file modification system. The Z3 solver has been used in a formal way to verify the suggested system.

2.5 Secure sharing of mobile personal healthcare records using certificateless proxy re-encryption in cloud:

Physicians can make crucial judgments and save lives because to the prompt and widespread availability of personal health information. Cloud computing has the ability to give all parties involved in the electronic healthcare sector, including patients, medical professionals, insurance companies, and others, ubiquitous and instantaneous access to a shared pool of resources and services. Cloud computing's rapid development and use in electronic healthcare systems has unavoidably sparked worries about the protection of outsourced data. This study performs a cryptanalysis of Qin's system, which violates the scheme's secrecy. Additionally, we suggested a single-hop unidirectional certificateless proxy re-encryption strategy based on elliptic curves that is lightweight, pairing free, and suitable for low-power mobile devices in order to securely share mobile personal health information with the public cloud. In certificateless proxy re-encryption, patients encrypt their data using their public keys before it is outsourced to the cloud. A cloud-resident semitrusted proxy then re-encrypts the data into ciphertext using the public key of the intended receiver without disclosing any information about the encrypted message. Through formal analysis against selected ciphertext attacks in the

random oracle paradigm, we demonstrate its security. Compared to current systems, our suggested technique is more effective and appropriate for low-power mobile devices.

3. METHODOLOGY

i) Proposed Work: The proposed system introduces DSAS (Data Sharing and Authorized Searchable), a secure framework for e-healthcare data sharing that combines searchable encryption with conditional proxy re-encryption. The main objective is to ensure that sensitive Personal Health Records (PHRs) are securely stored in the cloud while still allowing efficient and authorized access.

In this system, patient data collected from wearable devices is encrypted before being uploaded to the cloud server, ensuring confidentiality and preventing unauthorized access. To enable efficient retrieval, a searchable encryption mechanism is employed, allowing authorized users such as doctors to perform keyword-based searches over encrypted data without revealing the actual content or keywords.

Additionally, the system incorporates conditional proxy re-encryption to support secure delegation of access rights. When the primary doctor (Alice) is unavailable, access permissions can be delegated to another doctor (Bob) through the cloud server without decrypting the data. The delegation is controlled by specific conditions, ensuring fine-grained access control and minimizing unnecessary data exposure.

The proposed framework also achieves important security properties such as proxy invisibility, which prevents distinguishing between original and re-encrypted data; condition hiding, which protects sensitive conditions from the proxy; and collusion resistance, which ensures that even if the proxy and delegate collude, the original user's private key remains secure. Overall, the DSAS system provides a secure, efficient, and scalable solution for real-time e-healthcare data sharing.

ii) System Architecture: The proposed DSAS system architecture consists of three main entities: Cloud Server, Alice (data owner/doctor), and Bob (authorized user/delegate). Alice registers into the system, encrypts patient healthcare records, and uploads them to the cloud server. The cloud server acts as a semi-trusted entity that stores encrypted datasets, manages user authorization, and processes all user queries. It enables searchable encryption by allowing keyword-based search over encrypted data

without revealing sensitive information. Bob, as an authorized user, can register, log in, and request access to patient data by submitting encrypted search queries (trapdoors), ensuring secure and privacy-preserving retrieval.

Furthermore, the system supports secure delegation using conditional proxy re-encryption. When Alice is unavailable, she can delegate access rights to Bob through the cloud server without decrypting the data. The cloud performs re-encryption on ciphertexts so that Bob can decrypt only the authorized information. This process ensures key security properties such as proxy invisibility, condition hiding, and collusion resistance, preventing unauthorized access and leakage of sensitive data. Overall, the architecture ensures secure storage, efficient retrieval, and controlled sharing of healthcare data in a scalable cloud environment.

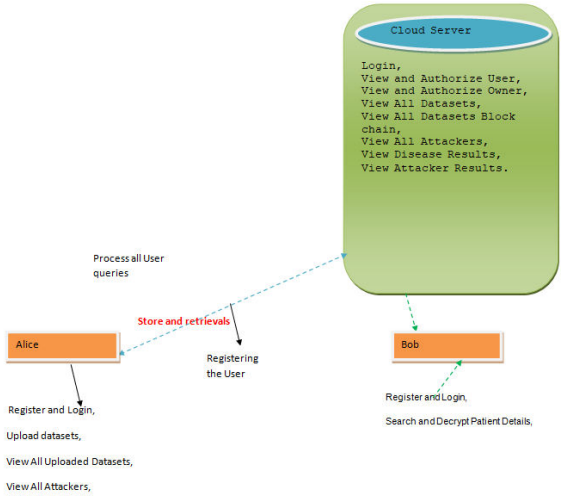

Fig.1. Proposed Architecture

iii) MODULES:

1. Cloud Server

The Cloud Server acts as a central entity responsible for storing encrypted healthcare data and managing system operations. It handles user authentication, dataset storage, and access control mechanisms. The server performs searchable encryption operations, processes user queries, and applies proxy re-encryption for secure data delegation. It also monitors system activities such as attackers and data access results to ensure system security.

2. Alice (Data Owner/Doctor)

Alice is the primary data owner who collects patient healthcare records and uploads them to the cloud. Before uploading, all datasets are encrypted to ensure confidentiality and privacy. Alice manages access permissions and can delegate access rights to another authorized user when required. She can also view uploaded datasets and monitor unauthorized access attempts.

3. Bob (Authorized User/Delegate)

Bob represents the authorized user or delegate who can access patient data based on permissions granted by Alice. After registration and authorization, Bob can perform keyword-based searches on encrypted data using trapdoors. The system allows Bob to decrypt only the permitted data, ensuring secure and controlled access without exposing sensitive information.

iv) ALGORITHMS:

1. Searchable Encryption (SE)

Searchable Encryption enables users to perform keyword-based searches over encrypted healthcare data without decrypting it. In this approach, the data owner generates encrypted indexes for keywords and uploads them along with encrypted PHRs to the cloud. When a user wants to search, a secure trapdoor is generated using the keyword, which is sent to the cloud server. The server matches the trapdoor with encrypted indexes and retrieves relevant data without learning the actual content or keyword, thus preserving privacy.

2. Proxy Re-Encryption (PRE)

Proxy Re-Encryption allows secure delegation of access rights from one user (Alice) to another (Bob) through the cloud server. Alice generates a re-encryption key using her private key and Bob's public key. The cloud server uses this key to transform ciphertexts encrypted under Alice's key into ciphertexts that Bob can decrypt. This process ensures that the cloud does not learn the original data while enabling secure and flexible access control.

3. Conditional Proxy Re-Encryption (CPRE)

Conditional Proxy Re-Encryption enhances PRE by adding access conditions to the re-encryption process. The data owner specifies certain conditions (e.g., specific keywords or attributes), and only the data satisfying these conditions can be re-encrypted for the delegate. This provides fine-grained access control and prevents unauthorized data sharing. Additionally, the system ensures condition-hiding so that sensitive conditions are not exposed to the cloud server.

4. Hashing Technique

Hashing is used to ensure data integrity and secure verification of datasets. Each dataset is processed through a hashing function to generate a unique hash value before storage. During retrieval, the hash value is recalculated and compared to detect any data modification or tampering. This enhances

the security and reliability of healthcare data transactions within the system.

4. EXPERIMENTAL RESULTS

The proposed DSAS framework was implemented using Java/J2EE with MySQL as the backend to evaluate its performance in a cloud-based e-healthcare environment. The system was tested with multiple users, including data owners (Alice) and authorized users (Bob), to analyze secure data storage, retrieval efficiency, and access delegation. Experimental evaluation shows that all patient healthcare records (PHRs) are successfully encrypted before being uploaded to the cloud, ensuring complete data confidentiality. The searchable encryption mechanism enables efficient keyword-based retrieval over encrypted datasets without exposing sensitive information.

Furthermore, the proxy re-encryption mechanism demonstrates effective and secure delegation of access rights. When the primary doctor is unavailable, the system allows controlled access transfer to another authorized user without decrypting the data. The results confirm that the system achieves important security properties such as proxy invisibility, condition hiding, and collusion resistance. In addition, the system shows low computational overhead and fast response time during search and retrieval operations, making it scalable and suitable for real-time healthcare applications. Overall, the experimental results validate that the proposed DSAS system is efficient, secure, and practical for modern e-healthcare systems.

Accuracy: The ability of a test to differentiate between healthy and sick instances is a measure of its accuracy. Find the proportion of analysed cases with true positives and true negatives to get a sense of the test's accuracy. Based on the calculations:

Accuracy = TP + TN /(TP + TN + FP + FN)

$$Accuracy = \frac{(TN + TP)}{T}$$

Test Accuracy: 0.9895

Precision: The accuracy rate of a classification or number of positive cases is known as precision. Accuracy is determined by applying the following formula:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Pr}\,e\,cision = \frac{TP}{(TP + FP)}$$

Recall: The recall of a model is a measure of its capacity to identify all occurrences of a relevant machine learning class. A model's ability to detect class instances is shown by the ratio of correctly predicted positive observations to the total number of positives.

$$Recall = \frac{TP}{(FN + TP)}$$

mAP: One ranking quality statistic is Mean Average Precision (MAP). It takes into account the quantity of pertinent suggestions and where they are on the list. The arithmetic mean of the Average Precision (AP) at K for each user or query is used to compute MAP at K.

$$\boldsymbol{mAP = \frac{1}{n}\sum_{k=1}^{k=n} AP_k}$$

$$\boldsymbol{AP_k = \text{ the AP of class } k}$$

$$\boldsymbol{n = \text{ the number of classes}}$$

F1-Score: A high F1 score indicates that a machine learning model is accurate. Improving model accuracy by integrating recall and precision. How often a model gets a dataset prediction right is measured by the accuracy statistic..

$$F1 = 2 \cdot \frac{(Recall \cdot \text{Pr}\,e\,cision)}{(Recall + \text{Pr}\,e\,cision)}$$

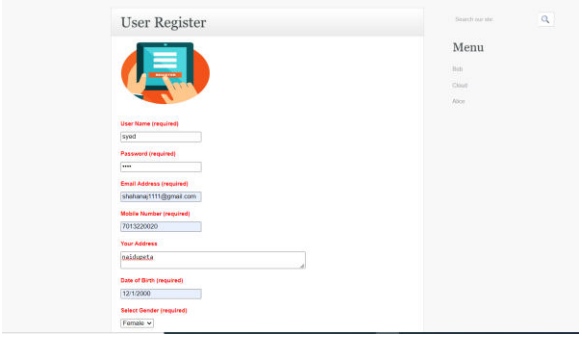

Fig2 user register

Fig3 cloud login

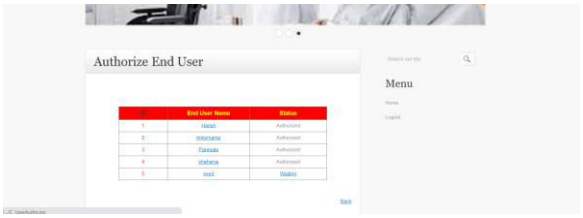

Fig4 authorize end user

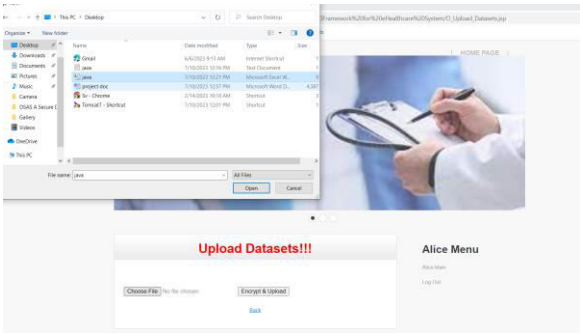

Fig.8. input upload

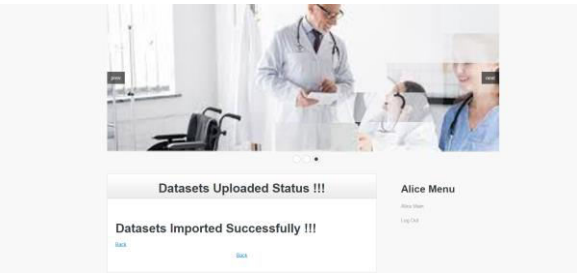

Fig.9. output

5. CONCLUSION

This paper presented DSAS, a secure and efficient data sharing framework for e-healthcare systems using searchable encryption and conditional proxy re-encryption. The proposed system ensures that personal healthcare records (PHRs) are encrypted before being stored in the cloud, thereby preserving data privacy and confidentiality. It enables authorized users to perform keyword-based searches over encrypted data without revealing sensitive information, improving both security and usability.

Furthermore, the system supports secure delegation of access rights through proxy re-encryption, allowing continuous healthcare services even when the primary doctor is unavailable. The framework achieves key security features such as proxy invisibility, condition hiding, and collusion resistance, ensuring robust protection against unauthorized access and attacks. Experimental results demonstrate that the proposed system is efficient, scalable, and practical for real-world e-healthcare applications.

6. FUTURE SCOPE

The proposed DSAS framework can be further enhanced by integrating advanced technologies to improve security, scalability, and intelligence in e-healthcare systems. One possible extension is the integration of blockchain technology to provide decentralized and tamper-proof storage of healthcare records, ensuring higher data integrity and trust. Additionally, incorporating artificial intelligence and machine learning models can enable predictive analysis for early disease detection and personalized treatment recommendations based on patient data.

Furthermore, the system can be optimized for IoT-based wearable devices by implementing lightweight cryptographic techniques to reduce computational overhead. Future work can also focus on

supporting multi-cloud environments for improved reliability and data availability. Enhancing real-time data processing, strengthening access control policies, and improving user authentication mechanisms will make the system more robust and adaptable to large-scale healthcare applications.

REFERENCES

[1] M. Abdalla, M. Bellare, D. Catalano, E. Kiltz, T. Kohno, T. Lange,

J. Malone-Lee, G. Neven, P. Paillier, and H. Shi, ``Searchableencryption

revisited: Consistency properties, relation to anonymous IBE, and exten-sions,"in Proc. Annu. Int. Cryptol. Conf. Berlin, Germany: Springer, 2005,pp. 205_222.

[2] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, ``Improved proxy re-encryption schemes with applications to secure distributed storage,"ACMTrans. Inf. Syst. Secur., vol. 9, no. 1, pp. 1_30, 2006.

[3] J. Baek, R. Safavi-Naini, and W. Susilo, ``Public key encryption withkeyword search revisited,"in Proc. Int. Conf. Comput. Sci. Appl. (ICCSA),2008, pp. 1249_1259.

[4] T. Bhatia, A. K. Verma, and G. Sharma, ``Towards a secure incrementalproxy re-encryption for e-healthcare data sharing in mobile cloud com-puting,"Concurrency Comput., Pract. Exper., vol. 32, no. 5, p. e5520,Mar. 2020.

[5] T. Bhatia, A. K.Verma, and G. Sharma, ``Secure sharing of mobile personalhealthcare records using certi_cateless proxy re-encryption in cloud,"Trans. Emerg. Telecommun. Technol., vol. 29, no. 6, p. e3309, Jun. 2018.

[6] I. F. Blake, G. Seroussi, and N. Smart, ``Advances in Elliptic CurveCryptography (London Mathematical Society Lecture Note Series (317)),vol. 19. Cambridge, U.K.: Cambridge Univ. Press, no. 20, 2005, p. 666.

[7] M. Blaze, G. Bleumer, and M. Strauss, ``Divertible protocols and atomicproxy cryptography,"in Advances in Cryptology-EUROCRYPT. Berlin,Germany: Springer, 1998, pp. 127_144.

[8] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, ``Publickey encryption with keyword search,"in Proc. Int. Conf. Theory Appl.Cryptograph. Techn. Berlin, Germany: Springer, 2004, pp. 506_522.

[9] D. Boneh and B. Waters, ``Conjunctive, subset, and range queries onencrypted data,"in Proc. Theory Cryptogr. Conf. Berlin, Germany:Springer, 2007, pp. 535_554.

[10] H. Fang, X. Wang, and L. Hanzo, ``Learning-aided physical layer authen-tication as an intelligent process,"IEEE Trans. Commun., vol. 67, no. 3,pp. 2260_2273, Mar. 2019.

[11] H. Fang, L. Xu, and X. Wang, ``Coordinated multiple-relays basedphysical-layer security improvement: A single-leader multiple-

followersStackelberg game scheme,"IEEE Trans. Inf. Forensics Security, vol. 13,

no. 1, pp. 197_209, Jan. 2018. [12] L. Fang, W. Susilo, C. Ge, and J. Wang, ``Chosen-ciphertext secureanonymous conditional proxy re-encryption with keyword search,"Theor.Comput. Sci., vol. 462, pp. 39_58, Nov. 2012.

[13] L. Fang, J. Wang, C. Ge, and Y. Ren, ``Fuzzy conditional proxy re-encryption,"Sci. China Inf. Sci., vol. 56, no. 5, pp. 1_13, May 2013.

[14] J. Feng, L. T. Yang, R. Zhang, W. Qiang, and J. Chen, ``Privacy preserv-ing high-order bi-Lanczos in cloud-fog computing for industrial appli-cations,"IEEE Trans. Ind. Informat., early access, May 28, 2020, doi:10.1109/TII.2020.2998086.

[15] J. Feng, L. T.Yang, Q. Zhu, and K.-K.-R. Choo, ``Privacy-preserving tensordecomposition over encrypted data in a federated cloud environment,"IEEE Trans. Dependable Secure Comput., vol. 17, no. 4, pp. 857_868,Jul. 2020.

Author Profiles

Ms. K. Baby Ramya is working as an Assistant Professor in the Department of MCA at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. She completed her MCA from Krishna University. She has around 3 years of teaching experience at SRK Institute of Technology. Her areas of interest include Machine Learning, Data Science, and Computer Applications.

Mrs.K.Pavani is working as Assistant&Head of Department of MCA ,in SRK Institute of technology in Vijayawada. She done with MCA ,M. Tech in Computer Science .She has 10 years of Teaching experience in SRK Institute of technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes AI ML, etc.

Mr.K.Vasudevarao is an MCA Student in the Department of Computer Application at SRK Institute Of Technology, Enikepadu, Vijayawada, NTR District. He has Completed Degree in B.Sc.(computers) from Andhra Loyola College, Vijayawada. His area of interest are DBMS and Java.