Role-Based Secure Access and Searchable Encryption Model for Medical Records

K .Srinivas[1], P.Akanksha[2*] , T.Sainadh[3], Ch.Bhavya[4], M.Hemacharan[5],

Vignan Institute of Technology and Science, JNTUH, India

srinivas.kmt@gmail.com, akankshareddy1125@gmail.com, t.sainadhreddy7777@gmail.com, 506bhavyachirgurupati@gmail.com, charanreddy34793@gmail.com

*Corresponding author: Name: K Srinivas (srinivas.kmt@gmail.com)

ABSTRACT

The rapid adoption of cloud computing in healthcare systems has enabled efficient storage and sharing of electronic medical records. However, medical data contains highly sensitive information, making security, privacy, and access control critical challenges. Traditional encryption techniques ensure confidentiality but do not support searching over encrypted data. Moreover, healthcare systems involve multiple users such as doctors, nurses, patients, and insurance agents, each requiring different access privileges. This paper proposes RB-SEMR, a Role-Based Secure Access and Searchable Encryption Model for Medical Records. The proposed system integrates role-based access control with searchable encryption to enable secure storage, fine-grained access control, and efficient keyword search over encrypted medical records. The RB-SEMR model improves data confidentiality, access accuracy, and system efficiency, making it suitable for cloud-based healthcare environments.

Keywords*: Role-based access control, Medical Records, Cloud Security, Data Privacy*

1. Introduction

Nowadays, with the rapid growth of cloud computing technologies and the widespread digitisation of healthcare services, electronic medical record systems have reached a level of maturity suitable for large-scale adoption and deployment. Cloud-based healthcare platforms significantly benefit patients and medical institutions by enabling efficient storage, sharing, and management of personal health records (PHRs). Through these systems, hospitals collect large volumes of medical data, such as diagnosis reports, prescriptions, laboratory results, and treatment histories, which enable doctors to provide timely and accurate medical care. In addition, these medical records can be utilised by researchers and analysts to study disease patterns and improve treatment strategies.

However, in most practical scenarios, medical records are stored on third-party cloud servers, which raises serious security and privacy concerns. Once the data is outsourced to the cloud, neither patients nor healthcare providers have direct control over their sensitive information. This lack of control increases the risk of data leakage, unauthorised access, and misuse of confidential medical records. Therefore, protecting the privacy and confidentiality of outsourced medical data has become a critical challenge in cloud-based healthcare environments.

In real-world healthcare systems, medical records are often shared among multiple entities such as hospitals, diagnostic centres, insurance companies, and government health agencies. For instance, healthcare institutions may authorise insurance agencies to access billing-related information or allow research organisations to analyse anonymised medical records for public health studies. Although such data sharing improves healthcare services, traditional data management and retrieval techniques may unintentionally expose sensitive patient information. Hence, securely storing, managing, and retrieving medical records while preserving privacy is a major challenge. To prevent information leakage from cloud-stored medical records, all personal health records should be encrypted before being outsourced. Encryption ensures data confidentiality and protects against attacks from malicious users and curious cloud servers.

Proceedings of ICICCS-2026 (Poster Papers), DMPedia Lecture Notes in Computer Science & Engineering.
ISBN: 978-81-993813-1-5

Nevertheless, encryption also introduces significant usability challenges. In particular, conventional encryption techniques make it difficult to perform efficient searches over encrypted data, as traditional information retrieval methods rely on plaintext content. Due to this limitation, many existing systems fail to meet the practical requirements of healthcare applications, which often require keyword-based searches.

To address this issue, searchable encryption techniques have been widely adopted in recent research. With searchable encryption, medical records are encrypted along with encrypted keyword indexes before being uploaded to the cloud. Authorised users, such as doctors or healthcare administrators, can generate a search token corresponding to a specific keyword and submit it to the cloud server. The cloud server can then perform keyword searches over the encrypted index and return the matching encrypted records without learning the actual keywords or plaintext data. This allows efficient data retrieval while preserving data privacy.

Although searchable encryption enables secure searching, healthcare systems also require fine-grained access control due to multiple users with different responsibilities. For example, doctors require access to complete medical records, while nurses may only need access to patient vitals, and insurance agents should only access billing information. Without proper role-based access control mechanisms, searchable encryption alone cannot prevent unauthorised access to data. Therefore, integrating role-based access control with searchable encryption is essential for secure management of medical data as per Fig. 1.

In summary, existing approaches face challenges in fine-grained access control and efficient retrieval of encrypted medical records. This paper proposes *RB-SEMR,* an integration of role-based access control with searchable encryption to ensure secure, efficient access in cloud-based healthcare systems.

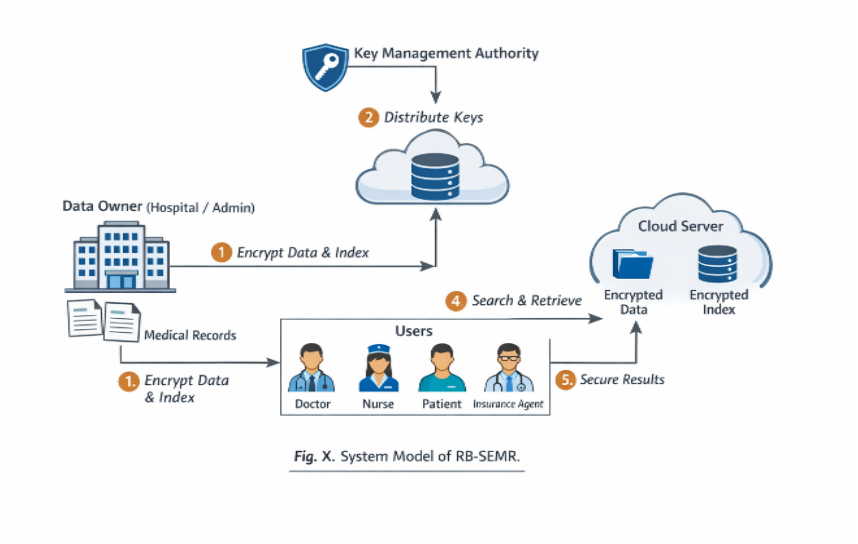

Fig1. System Model Diagram of RB-SEMR

2. Research Methodology

To obtain the desired output from the given input, the proposed system follows a systematic methodology comprising multiple stages. These stages ensure secure processing, controlled access, and efficient retrieval of medical records in a cloud-based environment.

A. Dataset Description:

Medical records are organised into balanced, structured datasets by access category. The dataset is randomly split into 80% for system configuration and validation and 20% for testing, ensuring reliable evaluation of the proposed RB-SEMR model.

B. Data preprocessing:

Data preprocessing ensures accurate and secure handling of medical records by removing redundant and inconsistent data. The records are normalised, structured, and prepared for encryption and keyword indexing, enabling efficient and error-free storage and retrieval.

C. Data Augmentation

Data augmentation enhances the system's robustness and reliability. The primary objective of this step is to increase data diversity and reduce bias in access patterns. By generating variations of existing records, the system minimises the risk of overfitting access rules to a limited dataset. Augmentation also helps maintain balance among different access roles, ensuring that the access control mechanism performs consistently across all user categories. The augmented dataset is then prepared for encryption and secure storage.

D. Proposed paradigm*:*

The proposed RB-SEMR (Role-Based Secure Access and Searchable Encryption Model for Medical Records) addresses the critical challenges of data confidentiality, fine-grained access control, and efficient retrieval in cloud-based healthcare systems. The paradigm integrates Role-Based Access Control (RBAC) with Searchable Encryption (SE) to ensure that sensitive medical records remain protected while still being accessible to authorised users.

In the RB-SEMR framework, medical records are generated and managed by healthcare providers such as hospitals or clinics, which act as data owners. Before outsourcing medical records to the cloud, all records are encrypted to prevent unauthorised access. At the same time, important keywords related to the medical records, such as patient identifiers, disease names, or test types, are extracted and used to create a secure, encrypted index. Both the encrypted records and the encrypted index are stored on the cloud server, ensuring that no plaintext information is exposed to third-party service providers.

Role-Based Access Control assigns predefined roles to users such as doctors, nurses, patients, and insurance agents, with access privileges strictly defined according to responsibilities. Role-based cryptographic keys ensure that users can access only authorised medical data, enforcing the principle of least privilege. To enable efficient retrieval, searchable encryption is used, in which authorised users generate secure search tokens to perform keyword searches over encrypted indexes without revealing data or keywords to the cloud. Retrieved records are decrypted locally only by authorised users, ensuring secure, fine-grained access and efficient retrieval in cloud-based healthcare systems.

E..Application

The proposed RB-SEMR model is primarily applicable to modern cloud-based healthcare systems where secure storage, controlled access, and efficient retrieval of medical records are essential. As healthcare institutions increasingly adopt digital platforms, managing sensitive patient data while maintaining privacy and compliance has become a major concern. RB-SEMR directly addresses these challenges by combining role-based access control with searchable encryption.

In real-world hospital environments, multiple stakeholders such as doctors, nurses, patients, laboratory staff, insurance agents, and healthcare administrators interact with medical records daily. Each of these users requires access to different portions of the data based on their responsibilities. RB-SEMR ensures that users can access only information relevant to their assigned roles, preventing unauthorised exposure of sensitive medical details. For example, doctors can securely search and access complete medical histories, nurses can retrieve patient

vitals, and insurance agents can access only billing-related information—without compromising patient privacy. The model is also highly suitable for telemedicine platforms and multi-hospital networks, where medical records are shared across institutions through cloud infrastructure. By encrypting records before outsourcing them to the cloud and enabling keyword-based search over encrypted data, RB-SEMR allows healthcare professionals to retrieve required records quickly without revealing sensitive information to third-party cloud providers. Additionally, RB-SEMR supports medical research and public health analysis by enabling controlled access to encrypted datasets. Researchers can securely search for and retrieve authorised data, ensuring compliance with data protection regulations while enabling large-scale medical studies. This makes the model valuable to government health agencies, research organisations, and insurance systems that rely on accurate, secure access to medical data.

Overall, RB-SEMR enhances trust, privacy, and efficiency in digital healthcare ecosystems. Its ability to provide fine-grained access control along with secure and efficient data retrieval makes it a practical and scalable solution for real-world cloud-based medical record management systems as per Fig.2.

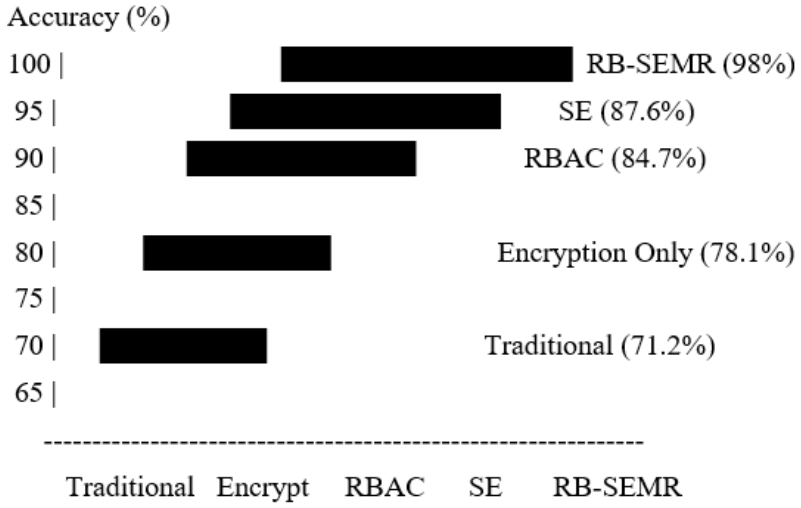

Fig2. Accuracy Comparison of Existing Systems and Proposed RB-SEMR Model

3. Conclusions

In this paper, we presented RB-SEMR, a Role-Based Secure Access and Searchable Encryption Model designed for secure management of medical records in cloud-based healthcare systems. The proposed approach addresses critical challenges, including data confidentiality, privacy preservation, fine-grained access control, and the efficient retrieval of encrypted medical records. By integrating role-based access control with searchable encryption, the system ensures that sensitive healthcare data remains protected while remaining accessible to authorised users based on their roles and responsibilities. RB-SEMR effectively prevents unauthorized access by enforcing strict role-based permissions and ensures that cloud service providers cannot learn any sensitive information from stored data or search queries. At the same time, the searchable encryption mechanism enables efficient keyword-based retrieval without decrypting data in the cloud, thereby maintaining both usability and security. This balance between strong security and practical functionality makes the proposed model well-suited for real-world healthcare environments involving multiple stakeholders. Overall, RB-SEMR enhances trust in cloud-based medical record systems by ensuring secure storage, controlled access, and privacy-preserving data retrieval. The model can be effectively adopted in hospitals, telemedicine platforms, insurance systems, and healthcare research environments. Future work can focus on

improving system scalability, reducing computational overhead, and integrating advanced authentication or audit mechanisms to strengthen security and performance further.

4. Future Scope

The proposed RB-SEMR model can be further enhanced to support large-scale healthcare environments involving multiple hospitals and cloud platforms. Future work may focus on improving system scalability and reducing computational overhead to efficiently handle growing volumes of medical data. Advanced access control mechanisms, such as attribute-based encryption, can be integrated to enable more flexible and dynamic permission management. Additionally, incorporating audit and monitoring mechanisms would improve accountability and ensure compliance with healthcare security regulations. RB-SEMR can also be extended by integrating emerging technologies such as blockchain for secure access logging and artificial intelligence for privacy-preserving medical data analysis. These enhancements would make the system more robust, scalable, and suitable for next-generation cloud-based healthcare applications.

References

[1] S. Yu, C. Wang, K. Ren, and W. Lou, *"Authorized private keyword search over encrypted personal health records in cloud computing,"* in *Proc. IEEE Intl. Conf. Distributed Computing Systems (ICDCS)*, Jun. 2011, pp. 1–10.

[2] S. Yu, C. Wang, K. Ren, and W. Lou, *"Achieving secure, scalable and fine-grained data access control in cloud computing,"* in *Proc. IEEE INFOCOM*, Mar. 2010, pp. 1–9.

[3] D. C. Kaelber et al., "A research agenda for personal health records (PHRs)," *Journal of the American Medical Informatics Association*, vol. 15, no. 6, pp. 729–736, 2008

[4] A. Zhao and H. Tian, *"Secure sharing of electronic medical records based on blockchain and searchable encryption," Electronics*, vol. 14, no. 13, article 2679, 2025

[5] N. H. Sultan, M. Laurent, and V. Varadharajan, *"Securing organization's data: A role-based authorized keyword search scheme with efficient decryption,"* arXiv:2004.10952, 2020.

[6] M. A. de Carvalho Junior and P. Bandiera-Paiva, *"Health information system role-based access control: Implementation characteristics, concerns, and limitations," J. Med. Syst.*, 2018.

[7] Gascoyne, Peter, Jutamaad Satayavivad, and Mathuros Ruchirawat. "Microfluidic approaches to malaria detection." *Acta Tropica* 89.3 (2004): 357-369.

[8] D. C. Garrison III et al., "On the practicality of cryptographically enforcing dynamic access control policies in the cloud," *arXiv:1602.09069*, 2016.

[9] R. Imam, *"A systematic literature review of attribute based encryption for e-health," J. King Saud Univ. – Computer and Info. Sciences*, 2022

[10] Wikipedia, "Searchable symmetric encryption," accessed 2025, available: https://en.wikipedia.org/wiki/Searchable_symmetric_encryption (for basic definition/background).