Privacy-Focused Dynamic Searchable Symmetric Encryption for Medical Cloud Environments

[1]J. Dhaneswari, [2]R. Durga Praveen, [3]B. Vamsi Krishna, [4]R. Dhanalakshmi, [5]A. Radhika

Department of CSE, SRK Institute of Technology, Vijayawada, A.P, India.

Abstract: **In medical cloud computing, patients can outsource their encrypted medical data to cloud servers, granting access only to authorized doctors. While encryption ensures data confidentiality, it complicates search operations over the encrypted data. To address this, we propose two Secure and Efficient Dynamic Searchable Symmetric Encryption (SEDSSE) schemes tailored for medical cloud environments. The first scheme combines secure k-Nearest Neighbour (kNN) and Attribute-Based Encryption (ABE) to support dynamic search while ensuring forward and backward privacy. To overcome key-sharing challenges inherent in kNN-based schemes, we further introduce an enhanced scheme. Compared to existing approaches, our solutions offer improved storage efficiency, lower search and update complexity, and strong privacy guarantees. Experimental results validate the effectiveness of our schemes in terms of storage overhead, index construction, trapdoor generation, and query performance.**

INTRODUCTION

The digital transformation of healthcare has increased reliance on cloud computing for medical data storage and management, enhancing accessibility and coordination among healthcare professionals. However, this shift raises critical concerns about data security, patient privacy, and access control. Traditional encryption methods, while effective in securing data, hinder efficient search and retrieval operations. To address these challenges, we propose a Privacy-Focused Dynamic Searchable Symmetric Encryption (DSSE) framework that balances security, search efficiency, and accessibility.

Our approach integrates Advanced Encryption Standard (AES) for encrypting individual medical records, ensuring fast and secure data confidentiality. To support efficient search over encrypted data, we employ the k-Nearest Neighbor (kNN) algorithm, enabling dynamic and privacy-preserving queries without exposing sensitive information. Additionally, Attribute-Based Encryption (ABE) is utilized to enforce fine-grained access control, allowing only authorized users to decrypt specific data based on their roles.

This combination of AES, kNN, and ABE provides a scalable, secure, and efficient system for cloud-based medical data management. The system supports dynamic updates and complies with regulations such as HIPAA and GDPR. By enabling secure storage, controlled access, and efficient encrypted search, the proposed DSSE-based solution addresses key privacy and usability challenges in medical cloud environments.

LITERATURE SURVEY

Recent research in A Survey on Searchable Symmetric Encryption Feng Li et al., May 2024

This survey reviews various SSE schemes, highlighting their strengths, limitations, and security concerns such as forward and backward privacy. It emphasizes the trade-offs between performance and privacy, providing a foundation for future SSE advancements in cloud applications.

Differential Privacy Enhanced Dynamic SSE for Cloud Environments Peigi Tu, Xingjian Wang, Feb 2024

This paper proposes a DSSE scheme integrated with differential privacy to protect search and access patterns. It improves privacy without compromising performance, supporting secure dynamic updates and efficient encrypted search.

EXISTING SYSTEM

Existing medical data storage solutions often lack privacy-preserving searchable encryption, requiring data decryption or exposing sensitive information during search operations. This compromises patient confidentiality and hampers efficient data retrieval. Furthermore, many traditional systems fail to meet regulatory standards such as HIPAA and GDPR, risking legal penalties and undermining trust in cloud-based healthcare solutions. These limitations underscore the need for an advanced encryption framework that ensures strong security, efficient searchability, and strict access control while supporting the scalability of medical cloud storage.

LIABILITIES OF EXISTING SYSTEM

1. Inefficient Search Over Encrypted Data
   Traditional encryption methods do not support efficient search operations, requiring full decryption to retrieve specific records, which leads to high computational overhead and delays.
2. Lack of Dynamic Encryption Support
   Most systems are static and require complex re-encryption for updates, making it difficult to add, modify, or delete records securely and efficiently.
3. Weak Access Control Mechanisms
   Basic role-based access controls lack fine-grained enforcement, increasing the risk of unauthorized access and insider threats.
4. Privacy Risks During Search Operations
   Search functionalities often expose metadata or require partial decryption, compromising patient confidentiality and enabling potential data leakage.
5. Vulnerability to Cyberattacks Existing systems are not robust against modern cyber threats like ransomware, unauthorized access, or side-channel attacks, making sensitive data vulnerable.

PROPOSED SYSTEM METHODOLOGY

Cloud-based medical record systems offer scalability and remote accessibility but face significant security and privacy challenges. Traditional encryption methods, including symmetric and asymmetric cryptography, hinder efficient data retrieval, as searching typically requires full decryption, leading to delays and computational overhead. Moreover, these systems often lack dynamic encryption support, making updates cumbersome and inefficient.

Weak access control mechanisms further compromise security, with basic role-based controls failing to enforce fine-grained or encryption-based policies. Privacy risks also arise from potential data exposure to cloud providers, especially during search operations that may reveal metadata or require partial decryption. Additionally, existing systems are vulnerable to cyberattacks and lack resilience against evolving threats such as ransomware and side-channel attacks.

Traditional models also do not support attribute-based access control, limiting policy flexibility based on roles, locations, or authority levels. Inefficient key management and distribution remain critical flaws, as compromised keys can expose sensitive data or render it inaccessible. These limitations highlight the urgent need for a secure, dynamic, and privacy-preserving medical data encryption framework for cloud environments.

PROPOSED SYSTEM ARCHITECTURE

Patients encrypt their medical records using Advanced Encryption Standard (AES) before outsourcing them to the cloud. They also define access policies and generate secure indexes for searchable encryption.

Healthcare professionals are granted access based on specific attributes using Attribute-Based Encryption (ABE). ABE enforces fine-grained access control, allowing users to decrypt data only if their attributes match the defined policy. The cloud server stores encrypted medical records and searchable indexes. It performs search operations over encrypted data using a secure k-Nearest Neighbour (kNN) algorithm without learning the content of the records or queries.

Searchable Index and Secure Query Processor:
A searchable index is maintained to enable efficient retrieval of encrypted data. The secure query processor on the cloud performs ranked search using the kNN algorithm, ensuring relevance-based results without compromising privacy.

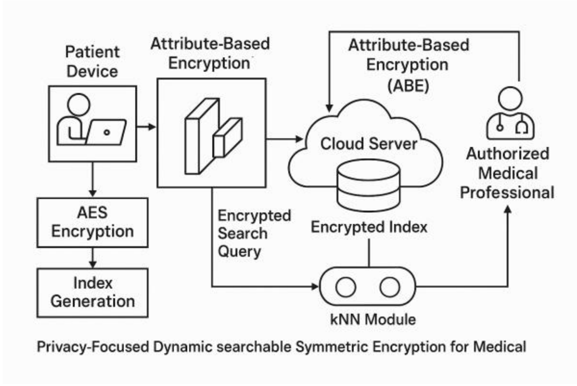

Patient Device
Attribute-Based Encryption
Attribute-Based Encryption (ABE)
Cloud Server
Authorized Medical Professional
AES Encryption
Index Generation
Encrypted Search Query
Encrypted Index
kNN Module
Privacy-Focused Dynamic searchable Symmetric Encryption for Medical

Fig: System Architecture

BENEFITS OF THE PROPOSED SYSTEM

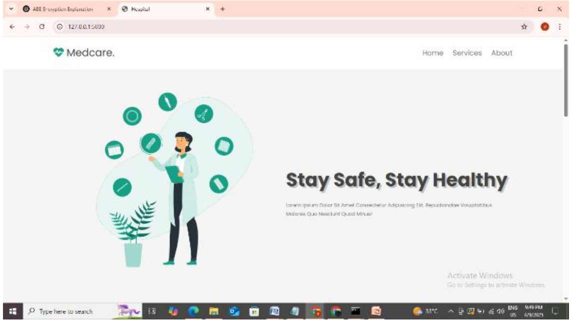
There are four advantages regarding abstract when compared to other solutions available. Enables fast and privacy-preserving searches over encrypted data using the secure kNN algorithm, eliminating the need for full decryption. Supports real-time updates (add, delete, modify) on encrypted medical records without compromising security or performance. Uses Attribute-Based Encryption (ABE) to ensure only authorized users with matching attributes can access specific data. Provides forward and backward privacy, protects against metadata leakage, and resists cyber threats like ransomware and unauthorized access.

RESULTS

The proposed system demonstrates efficient and scalable performance across varying dataset sizes. For 100 records, encryption, decryption, search, and access control operations complete rapidly, with AES encryption taking only 15 ms and kNN search 20 ms, indicating fast processing times for small datasets.

As the dataset increases to 500 and 1000 records, processing times grow moderately, showing the system's ability to scale effectively without significant performance degradation. For 1000 records, AES encryption and kNN search take 85 ms and 110 ms, respectively, reflecting consistent efficiency for medium datasets.

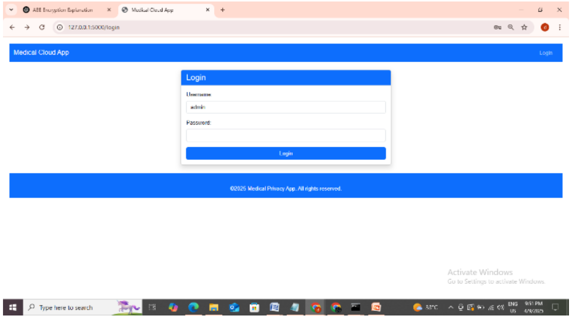
Even with 5000 records, the system maintains reasonable performance: AES encryption and kNN search complete in 400 ms and 550 ms, respectively, while ABE-based access control takes 600 ms. This illustrates that the system remains scalable and practical for large-scale medical databases, making it suitable for real-world healthcare applications



Stay Safe, Stay Healthy

Lorem Ipsum Dolor Sit Amet Consectetur Adipisicing Elit. Repudiandae Voluptatibus Molores Quo Nesciunt Quod Minus!

Fig: Home Page

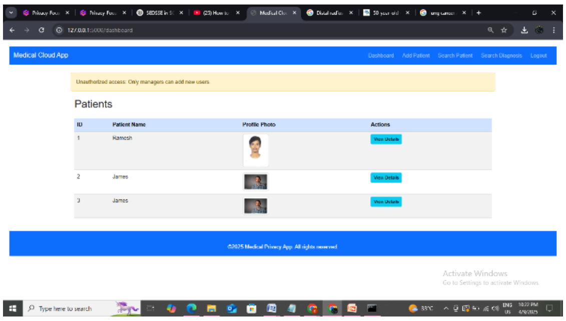


Username: admin

Password:

©2025 Medical Privacy App. All rights reserved.

Fig: Login Page



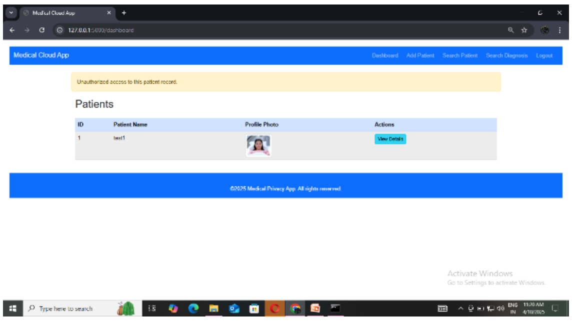
Unauthorized access: Only managers can add new users.

Patients

ID	Patient Name	Profile Photo	Actions
1	Ramesh		View Details
2	James		View Details
3	James		View Details

©2025 Medical Privacy App. All rights reserved.

Fig: Dashboard



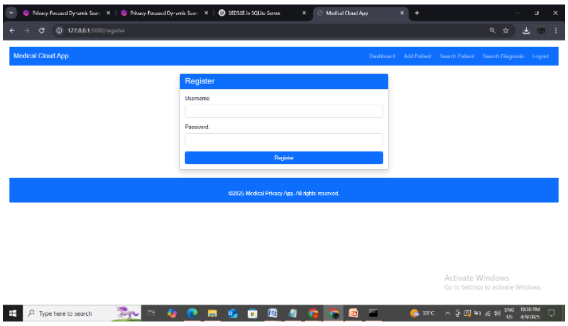
Unauthorized access to this patient record.

Patients

ID	Patient Name	Profile Photo	Actions
1	test1		View Details

©2025 Medical Privacy App. All rights reserved.

Fig: Access Control

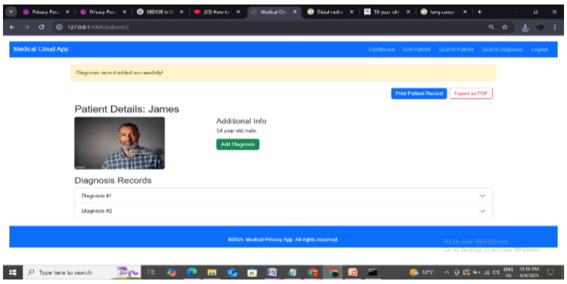


Username:

Password:

©2025 Medical Privacy App. All rights reserved.

Fig: Registration Page



Diagnosis record added successfully!

Patient Details: James

Additional Info

54-year-old male.

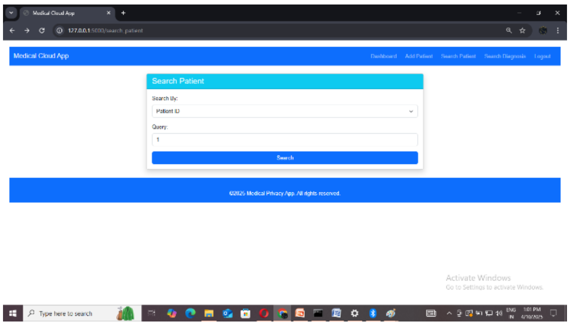
Diagnosis Records

Diagnosis #1

Diagnosis #2

©2025 Medical Privacy App. All rights reserved.

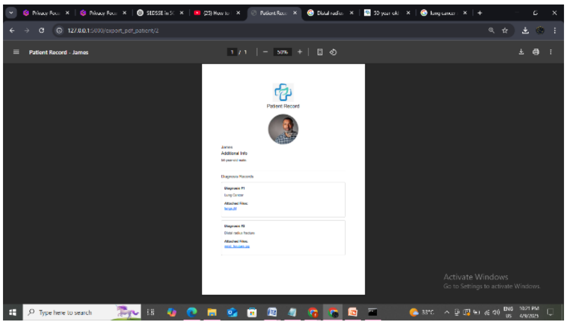
Fig: Patient Record



Search By: Patient ID

Query: 1

Fig: Search Patient



Diagnosis #1
Lung Cancer
Attached Files:

Diagnosis #2
Distal radius fracture
Attached Files:

Fig: Export Patient Record

CONCLUSION

The proposed Privacy-Focused Dynamic Searchable Symmetric Encryption (DSSE) system provides a secure and efficient framework for storing and managing medical records in cloud environments. By combining AES for data encryption, kNN for privacy-preserving search, and ABE for fine-grained access control, the system ensures data confidentiality, searchable encryption, and restricted access to authorized users. It supports dynamic updates, allowing records to be added, modified, or deleted without re-encrypting the entire dataset. Experimental results demonstrate that the system offers strong security while maintaining practical performance, making it well-suited for large-scale healthcare applications.

FUTURE SCOPE

Future enhancements of the system can include the integration of homomorphic encryption to perform computations directly on encrypted data, enhancing usability without compromising privacy. Machine learning algorithms could be incorporated to improve search accuracy and efficiency. Expanding the system to support multi-user environments with hierarchical access control would allow differentiated access for healthcare professionals. Additionally, adopting blockchain technology could further strengthen data integrity and auditability. Continued optimization efforts can focus on reducing processing times and scaling the system for even larger medical datasets.

REFERENCES

[1] D. X. Song, D. Wagner and A. Perrig, "Practical techniques for searches on encrypted data", Proc. IEEE Symp. Secur. Privacy, pp. 44-55, 2000.

[2] C. Bösch, P. Hartel, W. Jonker and A. Peter, "A survey of provably secure searchable encryption", ACM Comput. Surv., vol. 47, no. 2, pp. 18:1-18:51, Aug. 2014.

[3] D. Boneh, G. Crescenzo, R. Ostrovsky and G. Persiano, "Public key encryption with keyword search", Proc. Adv. Cryptology-EUROCRYPT, pp. 506-522, 2004.

[4] E.-J. Goh, "Secure indexes", 2003, [online] Available: http://eprint.iacr.org/2003/216/.

[5] E. Shen, E. Shi and B. Waters, "Predicate privacy in encryption systems", Proc. 6th Theory Cryptography Conf. Theory Cryptography, pp. 457-473, 2009.

[6] R. Curtmola, J. Garay, S. Kamara and R. Ostrovsky, "Searchable symmetric encryption: Improved definitions and efficient constructions", Proc. 13th ACM Conf. Comput. Commun. Secur., pp. 79-88, 2006.

[7] E. Stefanov, C. Papamanthou and E. Shi, "Practical dynamic searchable encryption with small leakage", Proc. NDSS Symp., 2014.

[8] S. Kamara and C. Papamanthou, "Parallel and dynamic searchable symmetric encryption", Proc. Int. Conf. Financial Cryptography Data Secur., vol. 7859, pp. 258-274, 2013.

[9] S. Kamara, C. Papamanthou and T. Roeder, "Dynamic searchable symmetric encryption", Proc. ACM Conf. Comput. Commun. Secur., pp. 965-976, 2012.

[10] Feng Li, Jianfeng Ma, Yinbin Miao, Ximeng Liu, Jianting Ning, Robert H. Deng," A Survey on Searchable Symmetric Encryption", May 2024.

[11] M. S. Islam, M. Kuzu and M. Kantarcioglu, "Access pattern disclosure on searchable encryption: Ramification attack and mitigation", Proc. NDSS Symp., 2012.

[12] A. Sahai and B. Waters, "Fuzzy identity-based encryption", Proc. 24th Annu. Int. Conf.

Theory Appl. Cryptographic Techn., pp. 457-473, 2005.

[13] V. Goyal, O. Pandey, A. Sahai and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data", Proc. ACM Conf. Comput. Commun. Secur., pp. 89-98, 2006.

[14] J. Bethencourt, A. Sahai and B. Waters, "Ciphertext-policy attribute-based encryption", Proc. IEEE Symp. Secur. Privacy, pp. 321-334, 2007.

[15] J. Katz, A. Sahai and B. Waters, "Predicate encryption supporting disjunctions polynomial equations and inner products", Proc. Theory Appl. Cryptographic Techn. 27th Annu. Int. Conf. Adv. Cryptology, pp. 146-162, 2008.

[16] J. Lai, R. H. Deng and Y. Li, "Expressive CP-ABE with partially hidden access structures", Proc. 7th ACM Symp. Inf. Comput. Commun. Secur., pp. 18-19, 2012.

[17] K. Kurosawa and Y. Ohtaki, "UC-secure searchable symmetric encryption", Proc. Int. Conf. Financial Cryptography Data Secur., vol. 7397, pp. 285-298, 2012.

[18] E. Shi and B. Waters, "Delegating capabilities in predicate encryption systems", Proc. Int. Colloquium Automata Languages Program., pp. 560-578, 2008.

[19] Peiyi Tu, Xingjun Wang, Differential Privacy Enhanced Dynamic Searchable Symmetric Encryption for Cloud Environments, Feb-2024