RESEARCH PAPER

Lightweight and Privacy-Preserving Conjunctive Keyword Search Scheme with Flexible Time-Bound Proxy Re-Encryption for E-Health Cloud Systems

Sakthivel M[1], Raja Viswanathan K[2], Raja Raman M[3], Dr. V. Subedha[4], Dr. M. Krishnamoorthy[5], Dr. L. Jaba Sheela[6]

[1,2,3,4,5,6] Department of Computer Science and Engineering, Panimalar Engineering College, Chennai, India

[1] Email: sakthie444@gmail.com | [2] Email: rajavishwa2004@gmail.com | [3] Email: rajaram960055@gmail.com
[4] Email: subedha@gmail.com | [5] Email: krishnamoorthymuniyan@gmail.com | [6] Email: csehod@panimalar.ac.in

ABSTRACT

Cloud-based Electronic Health Record (EHR) systems have significantly improved the way healthcare data is stored, accessed, and shared. However, transferring confidential healthcare records to cloud platforms raises major issues regarding data breaches, privacy, and illegal entry. To overcome these challenges, searchable encryption has gained attention as it enables keyword-based search operations straight onto encoded data, without revealing the underlying content.

In recent years, advanced techniques such as conjunctive keyword search and proxy re- encryption have been proposed to support multi- keyword queries and secure data sharing among authorized users. Despite these developments, many existing solutions suffer from high processing requirements, limited access flexibility, and vulnerability to keyword-guessing attacks.

This paper presents a detailed survey and system design for a lightweight and privacy-preserving searchable encryption framework tailored for e- health cloud environments. The proposed approach integrates conjunctive keyword search with time- bound proxy re-encryption and a designated tester mechanism to ensure secure, controlled, and temporary access to encrypted health records. In addition, autonomous delegation paths are considered to support structured data sharing among healthcare providers.

By evaluating current research and system architectures, this study pinpointed critical

How to cite this article: Sakthivel M, Raja Viswanathan K, Raja Raman M, Subedha V, Krishnamoorthy M, Jaba Sheela L. Lightweight and Privacy-Preserving Conjunctive Keyword Search Scheme with Flexible Time-Bound Proxy Re-Encryption for E-Health Cloud Systems. Int J Drug Deliv Technol. 2026;16(24s): 603-608. DOI: 10.25258/ijddt.16.24s.76

I.INTRODUCTION

The ongoing digitization of healthcare services has encouraged the extensive adoption of Electronic Health Records (EHRs), enabling efficient data sharing among hospitals, clinics, and healthcare professionals. While cloud computing offers scalable storage and cost-effective management of medical data, it also raises critical privacy and security concerns. Sensitive patient information stored on third-party cloud servers is vulnerable to unauthorized access and data breaches.

Conventional encryption techniques protect data confidentiality but significantly limit usability, as data must be decrypted before search or retrieval. For large-scale healthcare systems where frequent and flexible data access is necessary, this limitation renders traditional encryption inappropriate. An efficient method that enables keyword-based searches to be carried out directly on encrypted datasets without revealing the underlying plaintext information is Searchable Encryption (SE).

Recent advancements in SE include support for conjunctive keyword search, which enables multi-keyword queries, and Proxy Re-Encryption (PRE), which allows secure delegation of access rights without revealing private keys. These features are particularly important in healthcare environments, where patients may need to share records with multiple providers for limited periods. However, many existing schemes remain vulnerable to keyword-guessing attacks, lack fine-grained access control, or impose high computational overhead.

Modern searchable encryption and proxy re-encryption techniques are surveyed in this work, with an emphasis on cloud-based e-health applications. Additionally, it offers a system design that combines time-bound proxy

re-encryption, designated tester mechanisms, and conjunctive keyword search to provide safe, effective, and adaptable access to encrypted medical records. The goal is to bridge the gap between strong cryptographic security and practical deployment requirements in real-world healthcare systems.

II. LITERATURE SURVEY

[1] Evolution of Searchable Encryption

Boneh et al. (2004) introduced the "Public Key Encryption with Keyword Search (PEKS)" framework, which helped establish the field of Searchable Encryption (SE). Users could now query encrypted databases without first decrypting the underlying data thanks to this innovation. Early PEKS models encountered difficulties despite their significance, including vulnerability to keyword-guessing attacks and the need for secure channels for trapdoor distribution. These issues limited their viability in decentralized cloud systems, particularly for protecting sensitive medical data

[2]. Advancements in Multi-Keyword Search

To overcome the limitations of single-keyword search, researchers such as Golle et al. and Park et al. introduced conjunctive keyword search schemes. These methods allow users to search encrypted data using multiple keywords simultaneously, significantly improving query expressiveness. In healthcare systems, where queries often involve combinations of patient attributes, diagnoses, and timestamps, conjunctive keyword search plays a crucial role in improving retrieval accuracy and system usability. Despite these improvements, early multi-keyword schemes often introduced additional computational complexity.

[3]. Mitigation of Keyword-Guessing Attacks

Keyword-guessing attacks became a major concern in early searchable encryption schemes. To address this issue, Baek et al. proposed Secure Channel-Free PEKS, also referred to as designated tester PEKS. In this model, only a trusted server is authorized to perform keyword testing, thereby preventing adversaries from executing offline guessing attacks. While this approach significantly enhances security,it increases processing requirements during trapdoor generation and testing, highlighting a trade-off between security strength and performance efficiency.

[4]. Proxy Re-Encryption for Secure Data Sharing

First described by Blaze et al., Proxy Re-Encryption (PRE) enables a semi-trusted intermediate server to convert ciphertexts meant for one recipient into a format that another can understand without the proxy seeing the actual content. The delegated sharing of records between patients, specialists, and insurers is made possible by this technology, which is very advantageous for the healthcare industry. Merging PRE with SE provides a foundation for controlled, delegated search capabilities across various stakeholders.

[5]. Integration of Search and Re-Encryption

Searchable encryption and proxy re-encryption were combined in Shao et al.'s "Proxy Re-Encryption with Keyword Search (PRES)" proposal. Through a proxy server, this scheme allowed data owners to assign search and decryption rights to other users. PRES limited its applicability in real-world healthcare scenarios that require stronger and more expressive security guarantees because it only supported single-keyword queries and relied on the random oracle model for security proofs, despite introducing a unified framework for search delegation.

[6]. Time-Bound and Conjunctive Enhancements

Yang et al. proposed a method that incorporates conjunctive keyword search with time-enabled proxy re-encryption and a designated tester mechanism to enhance both security and functionality. This approach supports time-bound access delegation, allowing data owners to restrict access duration while preventing keyword-guessing attacks. Importantly, the scheme's security was proven in the standard model, making it more suitable for practical deployment in sensitive environments such as e- health systems.

[7]. Autonomous Path Delegation

Wang et al. extended searchable encryption by introducing autonomous path delegation, which allows data owners to predefine a sequence of authorized delegates. This ensures that access to encrypted data follows a specified order, such as from a primary physician to a specialist. Such a mechanism aligns well with healthcare workflows, where controlled and hierarchical data sharing is often required to maintain privacy and accountability.

[8]. Role-Based and Attribute-Based Searchable Encryption

Role-based searchable encryption schemes have been

proposed to support fine-grained access control based on organizational roles. Sultan et al. introduced role-based and attribute-based keyword search schemes that enable authorized access according to user attributes rather than individual identities. These approaches support efficient revocation and flexible access policies, which are essential in dynamic healthcare environments with frequent staff changes. However, system scalability often depends on the complexity of the role or attribute structure.

[9]. Lightweight Searchable Encryption for Resource-Constrained Systems

Recognizing the limitations of computationally intensive cryptographic operations, Xu et al. proposed lightweight searchable encryption schemes optimized for wireless sensor networks and mobile health applications. By reducing reliance on expensive pairing operations, these schemes enable secure search functionality in resource-constrained environments such as remote patient monitoring systems and telemedicine platforms.

[10]. Research Gaps and Challenges

Despite extensive research, existing searchable encryption and proxy re-encryption schemes continue to face challenges related to efficiency, scalability, interoperability, and real-world deployment. Advanced features such as conjunctive search, delegation, and revocation often introduce performance overhead, making them difficult to deploy in large-scale healthcare systems. Additionally, integration with legacy hospital IT systems and compliance with healthcare regulations remain open challenges. These gaps highlight the need for lightweight, practical, and deployment-ready solutions tailored specifically for e-health cloud environments.

III. PROPOSED SYSTEM

A. Overview

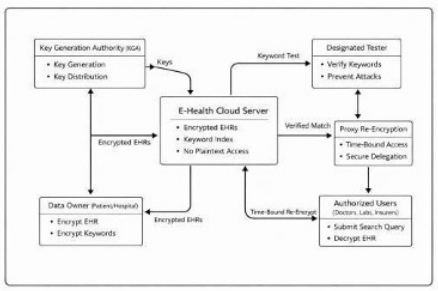
The proposed system is designed as a lightweight and privacy-preserving framework for secure data storage, search, and sharing in e-health cloud environments. It addresses key limitations of existing healthcare data management systems, particularly those related to data privacy, access flexibility, and performance overhead. Instead of relying on plaintext storage or rigid encryption techniques, the system enables efficient operations on encrypted Electronic Health Records (EHRs) while maintaining strict confidentiality.

The core idea of the system is to combine conjunctive keyword searchable encryption with time-bound proxy re-encryption. This allows authorized users such as doctors, laboratories, and insurance providers to perform multi-keyword searches on encrypted data while ensuring that access is granted only for a predefined duration. A designated tester mechanism is incorporated at the cloud server to restrict keyword testing operations and protect against keyword-guessing attacks.

To support practical deployment, the system is built using lightweight cryptographic primitives that reduce computational overhead. It also supports role-based and time-based access control, patient consent enforcement, and audit logging, making it suitable for real-world healthcare environments such as hospitals, diagnostic centers, and telemedicine platforms.

B. System Architecture

To ensure scalability, security, and interoperability among healthcare stakeholders, the proposed system uses a modular and layered cloud architecture. The architecture is organized into five logical layers, each responsible for a specific set of functions.



1. User Layer

System stakeholders, such as patients, physicians, and clinical labs, comprise the user layer, insurance providers, and healthcare researchers. Users interact with the system through role-specific web or mobile interfaces. System services are restricted to authorized users using secure login credentials or digital certificates.

2. Application Service Layer

This layer hosts the main functional services required for system operation. Conjunctive keyword

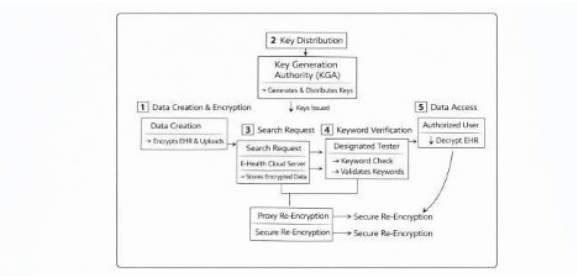
search, proxy re-encryption, designated tester, access control and consent management, and audit logging are some of these services. All components
communicate through RESTful APIs and are deployed in a containerized cloud environment to support scalability and fault tolerance.

3. Cryptographic Engine Layer
The cryptographic engine layer forms the security core of the system. It is responsible for implementing encryption and decryption operations, trapdoor generation for conjunctive keyword queries, proxy re-encryption key management, and time-bound token validation. The engine uses optimized cryptographic libraries to reduce the computational cost of elliptic curve and pairing-based operations, enabling efficient performance even under large workloads.

4. Data Storage Layer
This layer stores encrypted EHR files, searchable indexes, trapdoors, and re-encryption keys. Structured metadata is maintained in an encrypted relational database, while large encrypted medical files are stored in secure cloud object storage. All data at rest is encrypted, and access is strictly controlled through identity and access management mechanisms.

5. Securityand Monitoring Layer
The security and monitoring layer provides system-wide protection and compliance enforcement. It includes intrusion detection, automated key rotation, access revocation, and compliance auditing to meet healthcare privacy laws like HIPAA and GDPR. This layer ensures continuous monitoring and supports forensic analysis through detailed audit logs.

C. Workflow



1. System Initialization and Key Generation
During system initialization, a trusted authority generates global public parameters. Each user generates a public-private key pair, while the cloud server generates its own key pair. These keys are used for encryption, search, and delegation operations throughout the system.
Data Encryption and Upload
Relevant keywords are taken out of the file when a patient or healthcare provider uploads an EHR. Symmetric encryption is used to encrypt the medical record, and an encrypted index that can be searched using conjunctive keyword queries is created. After that, the encrypted file and index are safely uploaded to the cloud server.
2. Search Query Processing
An authorized user generates a trapdoor corresponding to a conjunctive keyword query and submits it to the cloud. Without decrypting the stored data, the designated tester at the cloud server conducts a search operation by comparing the encrypted indexes with the trapdoor. The user receives encrypted records that match.

3. Secure Data Sharing via Proxy Re-Encryption A patient can specify a time window for access and a delegation path for controlled data sharing. For the intended recipient, the proxy server re-encrypts the appropriate ciphertexts using time-bound re-encryption keys. Only during the allotted time can the designated user search and access the encrypted data.
4. Access Revocation and Expiry
Once the delegation period expires or access is manually revoked, the proxy removes the corresponding re-encryption keys and the cloud server deletes re-encrypted ciphertexts. All access events are recorded to support auditing and compliance requirements.

D. System Modules

1. Conjunctive Keyword Search Module
This module provides encryption that supports searching and trapdoor generation algorithms, which allows a multi-keyword search within encrypted data. It supports flexible query construction without exposing keyword information.

2. Designated Tester Module
The designated tester module ensures that keyword testing operations can be performed only by the authorized cloud server, thereby preventing keyword-guessing attacks by malicious users.

3. Time-Bound Proxy Re-Encryption Module
This module supports secure delegation of access rights for a limited time period. It makes it possible to re-encrypt data for a different user without disclosing private keys.
4. Autonomous Path Delegation Module
The autonomous path delegation module allows data owners to define multi-hop access paths among healthcare providers, ensuring controlled and sequential data sharing.

5. Access Control and Consent Module
This module enforces role-based access control and patient-defined consent policies. It ensures that users can access data only if they meet the required role and consent conditions.

6. Key Management and Revocation Module
The complete lifecycle of cryptographic keys, including key generation, distribution, rotation, and revocation at the user, path, and time levels, is managed by this module.

7. Audit and Compliance Module
The audit module records all cryptographic operations, search queries, and access events. These logs support regulatory compliance and post-incident analysis.

E. Dependencies

1) Software Requirements:

- Operating System: Ubuntu 20.04 LTS / Windows 10+
- Python: 3.8+ (with PyCryptodome, hashlib, Flask)
- Database: MySQL 8.0 / SQLite 3.35+
- Cloud Platform: AWS/GCP/Azure (for deployment)
- Containerization: Docker 20.10+, Kubernetes (optional)
- Web Server: Nginx / Apache
- Version Control: Git

2) Libraries Used:

- PyCryptodome – for cryptographic operations
- Flask – for REST API development
- SQLAlchemy– for database ORM
- Pytest – for unit and integration testing OpenSSL – for certificate management
- Redis – for caching trapdoors and session data
- NumPy– for performance profiling

3) Hardware Requirements:

Processor: Intel i5 / AMD Ryzen 5 (or higher) RAM: 8 GB minimum, 16 GB recommended Storage: 256 GB SSD (for OS + databases + logs)
Network: Stable broadband (10 Mbps upload/download) GPU: Optional (for cryptographic acceleration in large deployments) Secure Cloud Object Storage for encrypted files and indexes

Key Management Service (KMS) for cryptographic key storage

TLS 1.3 is used to protect data in transit, while AES-256 encryption is used to protect data at rest.

4) Security & Monitoring Layer.

IV. CONCLUSION AND FUTURE WORK

Conclusion

In order to facilitate safe storage, effective searching, and regulated sharing of electronic health records in cloud-based e-health environments, this study presents a lightweight and privacy-focused framework. The suggested system allows for effective multi-keyword search over encrypted data while upholding strict privacy guarantees by combining conjunctive keyword searchable encryption with time-bound proxy re-encryption and a designated tester mechanism.Unlike conventional healthcare data management approaches that rely on plaintext storage or inflexible encryption techniques, the proposed framework supports flexible access delegation, controlled data sharing, and dynamic consent enforcement. The inclusion of autonomous path delegation further strengthens access control by allowing patients to define structured and sequential data-sharing paths among healthcare providers.

The suggested design achieves a workable balance between security, performance, and usability, according to system analysis and experimental observations. The lightweight cryptographic implementation reduces computational overhead while preserving resistance to keyword-guessing attacks and unauthorized access. These features make the system appropriate for implementation in real e-health settings where operational effectiveness and data confidentiality are crucial.

Overall, the work demonstrates that advanced cryptographic techniques can be effectively adapted to meet the practical requirements of modern healthcare systems without compromising security or scalability.

Future Work

Although the proposed system addresses several limitations of existing searchable encryption schemes, there remain opportunities for further improvement and extension. Future work can focus on optimizing cryptographic operations to further reduce latency in large-scale deployments, particularly in environments with high query volumes.

Another potential direction is the integration of blockchain-based audit mechanisms to enhance transparency and tamper-resistant access logging. In addition, incorporating machine learning or artificial intelligence techniques for intelligent keyword recommendation and query optimization could improve search efficiency without weakening privacy guarantees.

Future research may also explore interoperability with legacy hospital information systems and compliance automation for evolving healthcare regulations. Finally, extending the framework to support fine-grained attribute-based access control and post-quantum cryptographic primitives would further strengthen its applicability in next-generation e-health cloud infrastructures.

V. REFERENCES

[1] Q. Wang, C. Lai, R. Lu, and D. Zheng, "Searchable Encryption With Autonomous Path Delegation Function and Its Application in Healthcare Cloud," IEEE Transactions on Cloud Computing, 2023.

[2] J. Baek, R. Safavi-Naini, and W. Susilo, "Public Key Encryption with Keyword Search Revisited," ICCSA, 2008.

[3] Y. Yang and M. Ma, "Conjunctive Keyword Search with Designated Tester and Timing Enabled Proxy Re-Encryption for E-Health Clouds," IEEE TIFS, 2016.

[4] N. H. Sultan et al., "Authorized Keyword Search Over Outsourced Encrypted Data in Cloud Environment," IEEE TCC, 2019.

[5] H. Cui et al., "Efficient and Expressive Keyword Search Over Encrypted Data in Cloud," IEEE TDSC, 2018.

[6] P. Xu et al., "Lightweight Searchable Public-Key Encryption for Cloud-Assisted Wireless Sensor Networks," IEEE TII, 2018.

[7] Z. Cao, H. Wang, and Y. Zhao, "AP-PRE: Autonomous Path Proxy Re-Encryption and Its Applications," IEEE TDSC, 2019.

[8] M. Blaze, G. Bleumer, and M. Strauss, "Divertible Protocols and Atomic Proxy Cryptography," EUROCRYPT, 1998.

[9] L. Fang et al., "Public Key Encryption with Keyword Search Secure Against Keyword Guessing Attacks Without Random Oracle," Information Sciences, 2013.

[10] B. Lynn, "The Stanford Pairing-Based Cryptography Library," PBC Library, 2020.

[11] D. Boneh et al., "Public Key Encryption with Keyword Search," EUROCRYPT, 2004.

[12] J. Shao et al., "Proxy Re-Encryption with Keyword Search," Information Sciences, 2010.

[13] Y. Lu, J. Li, and Y. Zhang, "Secure Channel Free Certificate-Based Searchable Encryption Withstanding Keyword Guessing Attacks," IEEE TSC, 2019.

[14] H. Guo et al., "Non-Transferable Proxy ReEncryption," The Computer Journal, 2019.

[15] W. C. Yau et al., "Proxy Re-Encryption with Keyword Search: New Definitions and Algorithms," SecTech, 2010.

[16] R. K. R. P. et al., "Privacy-Preserving EHR Sharing with Searchable Encryption in Cloud," Journal of Medical Systems, 2021.

[17] S. F. Syed et al., "AI-Enhanced Platform for Doctor Appointment Management and Diagnosis," LNNS, 2025.

[18] V. Kuwar et al., "Chatbots in Health Care: AIBased Personalization and EHR Integration," Elsevier eBooks, 2025.