# E-Healthcare Cloud Secure Fine-Grained Encrypted Keyword Search

GHAININATH S, Prof Rajesh N

*Student, Department of MCA, AMC Engineering College(VTU), Bengaluru, India Professor, Department of MCA, AMC Engineering College(VTU), Bengaluru, India*

**Abstract**

*E-healthcare systems are gaining popularity as wearable medical devices and sensors continue to evolve. Personal health records (PHRs) are collected by these devices and kept on a remote cloud. These records shouldn't be accessible to anybody who isn't authorized, and the cloud service providers shouldn't be able to extract any information from the saved records. One practical solution to the problems outlined above is to use attribute-based encryption (ABE) for accurate access control and searchable encryption for keyword searches on encrypted data.*

*On the other hand, the method ought to enable users to search PHRs on devices with modest processing and bandwidth capabilities. Most works that are currently accessible on ABE do not support as wearable medical devices and sensors have developed.*

**KEYWORDS:** *Cyber security, HIDS NIDS Machine Learning, GCR-MN, CNN,*

## 1. INTRODUCTION

In recent years, the usefulness of electronic medicine has increased, and it has advanced swiftly due to the expansion of the Internet of Things and the popularity of mobile communication devices. Patients' heart rate, blood pressure, respiration, ECG, and other data may be captured thoroughly by using wireless sensor technology. Utilizing the M2M technologies and the current communication infrastructure**.** Sensitive information about the distant patient might be sent to different medical facilities, doctors, or other medical services. With these advantages, more and more patients are outsourcing their data to a cloud server where they may subsequently access it from anywhere using mobile devices. Data privacy is a big issue, especially when it comes to highly sensitive information like personal health records (PHRs) collected by resource-constrained wearable medical devices and sensors.

These documents contain patient privacy information such as case report, inspection report, and basic identifying information. If this privacy information are stored in plaintext, they are vulnerable to attack by malicious parties that have simple access to the private information of other users. In this setting, a cloud server or malignant patients can be inspired to access and obtain sensitive data. To preserve privacy, the PHRs should be stored in an encrypted manner on the cloud. However, because of encryption, it can be difficult for patients or doctors to access particular data. A simple option is for patients or clinicians to download and locally decode the complete encrypted record set before searching the plaintext data for the desired outcomes. It has been argued that a better strategy than this unsuccessful one is searchable encryption (SE). Before putting the encrypted private data in the cloud server in a searchable encryption system, the user prepares a search query and sends it to the server. The search trapdoor allows the server to browse the encrypted data. The search trapdoor is made possible by the user's private key and a few words. Additionally, only those having search access and the search private key are permitted to construct.

### 2. Literature Survey:

Title: Title: Secure Fine-Grained Encrypted Keyword Search for Literature Review on E-Healthcare Cloud. By enabling effective electronic health record (EHR) storage, sharing, and retrieval, e-Healthcare Cloud solutions have transformed the healthcare sector. Concerns about patient data security and privacy are brought up by the

sensitive nature of EHRs. Researchers have focused on developing effective and secure search operations on encrypted EHRs to address these problems. One such answer is granular encrypted keyword search.This study suggests a safe and effective method for finding keywords with fine granularity in cloud computing settings. A searchable symmetric encryption (SSE) method is used in the system to enable safe keyword search operations while maintaining data.As of right now, the data collection is too tiny to train with bigrams or trigrams efficiently, but we want to keep gathering data with systems based on methods such as searchable symmetric encryption and attribute-based encryption. These articles provide practical advice and techniques for protecting the confidentiality, privacy, and speedy retrieval of electronic health data in cloud settings for healthcare. To meet the evolving needs of healthcare organizations for the safety of patient information, it is essential to do more research in this area to enhance the security and performance of fine-grained encrypted keyword search for E-Healthcare Cloud.

## 3.SYSTEM ARCHITECTURE

A secure fine-grained encrypted keyword search system architecture for E-Healthcare Cloud often comprises a variety of components and technologies to protect the security and integrity of sensitive medical data.

Here is a brief explanation of the key components involved; particular designs may differ depending on the requirements of the system and design choices.

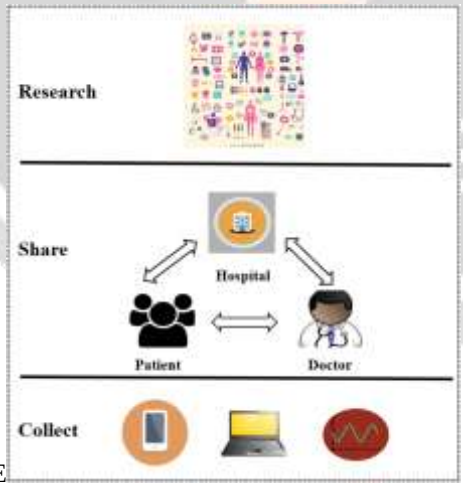
Infrastructure for the cloud The system architecture is dependent on the cloud infrastructure to store and process the encrypted medical data. Typically, this infrastructure comprises of virtualization software, storage devices, and cloud servers.

Data Encryption: Using a variety of encryption techniques, the confidential medical information is encrypted before being saved in the cloud.

Using encryption methods like symmetric key encryption or public-key encryption, the data may be secured. It is possible to set access restriction based on certain attributes.

Using fine-grained encryption solutions, such as attribute-based encryption, access control may be provided based on certain data-related features.

Users may do keyword searches on encrypted content using the Searchable Encryption Module without revealing the content itself.




SYSTEM ARCHITECTURE

**Fig[1] System Architecture**

## 4. Existing System:

Literal offered a framework for permitted private keyword search with proxy re-encryption.

The authors employed hierarchical predicate encryption to set up a system for authorized private keywords. The proposed system places the responsibility of determining a doctor's search qualifications on a number of regional, reliable agencies.To create a system for allowed private terms, the authors used hierarchical predicate encryption. The suggested approach entrusts a number of regional, reputable organizations with the duty of evaluating a doctor's search qualifications.

`

## 5. Proposed System:

The policy leakage and computationally expensive search issues are the main obstacles to adopting attribute-based encryption in our e-healthcare scenario.
The Fast Keyword Search-Hidden Policy ABE (FKS-HPABE) system, a cutting-edge secure fine-grained encrypted keyword search technology, is used in this work to overcome these problems.
In the cloud computing system for e-healthcare, we offer a permitted keyword search mechanism over the encrypted PHRs.

Thanks to our system's support for fine-grained search authorization, only doctors who fulfill the patient-enforced policy requirements may create legitimate trapdoors and access the associated PHRs.

## 6.INOVATION

In order to address the challenges of privacy, security, and efficient information retrieval as they occur in healthcare systems, a growing corpus of research is being conducted in the area of secure, fine-grained, encrypted keyword search for the E-Healthcare Cloud.

## 7.METHODOLOGY

When creating a secure, fine-grained, encrypted keyword search for E-Healthcare Cloud systems, there are often three crucial stages. While specific strategies could alter depending on the choices taken during system design and system requirements. Understanding the precise needs and goals of the E-Healthcare Cloud system is the first stage. The needs for security and privacy, data access rules, performance restrictions, and regulatory compliance issues are all included in this. The sensitive medical data needs to be encrypted before being stored in the cloud. The data can be protected using a variety of encryption methods, including symmetric key encryption, public-key encryption, and hybrid encryption. Using fine-grained encryption solutions, such as attribute-based encryption, access control may be provided based on certain data-related features.

Access control may be provided based on certain data-related attributes using fine-grained encryption techniques, such as attribute-based encryption.

## 8.OBJECTIVES

1. The main objectives of implementing secure fine-grained encrypted keyword search in E-Healthcare Cloud systems are to improve privacy, security, and data retrieval efficacy while conforming to regulatory norms.
2. The main goal is to protect the privacy of private medical information kept in the E-Healthcare Cloud.
3. By encrypting the data, unauthorized parties cannot access or understand the content, thus preserving patient privacy and protecting sensitive healthcare information from unauthorized disclosure.

## ADVANTAGES

1.Enhanced Data Privacy.

2. Confidentiality of data.

## DISADVANTAGES

1.Increased Computational Overhead
2. Complexity and Development Effort

## RESULTS

Get the most recent information and search results on safe, fine-grained, encrypted keyword searches in the E-Healthcare Cloud domain by using the following steps: To get the most recent information and search results for a safe, fine-grained encrypted keyword search in the E-Healthcare Cloud domain.

Based on the application, the outcome could contain different types of information. For instance, the return can include the recognized letter, word, or phrase that corresponds to the detected hand motion if the device is

intended for sign language recognition. The detected Indian sign connected to the recorded motion may be the outcome in the case of Indian sign recognition.

## FUTURE WORK

Future work can focus on improving the scalability and performance of fine-grained encrypted keyword search systems in the E-Healthcare Cloud This includes developing efficient indexing techniques, query processing algorithms, and resource management strategies to handle large-scale healthcare datasets and accommodate increasing user demands. Extending the search capabilities of encrypted keyword search systems can be a focus of future work. This includes supporting more complex search operations, such as fuzzy search, similarity search, or advanced ranking algorithms, while maintaining data privacy and security.

## V1. CONCLUSION

Enhanced data privacy and confidentiality by encrypting sensitive medical data.

Fine-grained access control mechanisms enable precise control over data access.

Secure keyword search operations allow authorized users to retrieve specific medical data while preserving data privacy.

Adherence to legal regulations like GDPR or HIPAA.

Improved data integrity and authentication through encryption and access control.

Efficient search capabilities while maintaining data confidentiality.

Interoperability and collaboration facilitated by secure data sharing mechanisms.

## REFERENCES

Curtmola, R.Searchable symmetric encryption: Improved definitions and effective implementations, in Proc. 13th ACM Conf. Comput. Commun. Secure, 2006, pp. 7988. J. Garay, S. Kamara, and R. Ostrovsky.

[2]. B. Lynn, 2006, PBC library. [Online]. http://crypto.stanford.edu/pbc is a resource.

[3] Fuzzy identity-based encryption by A. Sahai and B. Waters was published in Proc.Annu. Int. Conf. Theory Appl. Cryptographic Techn. 2005, pp. 457–473.

[4] Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data, IEEE Trans. Inf. Forensics Secur., vol. 12, no. 8, pp. 1874-1884, August 2017. Z. Fu, F. Huang, K. Ren, W. Jian, and W. Cong.

[5]. In Proc. IEEE Symp. Secur. Privacy, 2000, pp. 44–55, D. X. Song, D. Wagner, and A. Perrig published Practical algorithms for searches on encrypted data.