Enabling Secure and Efficient Search Operations on Medical Cloud Data using Dynamic Searchable Symmetric Encryption

Thippesh D
4th semester MCA AMCEC
MCA, AMC
thippeshd1999@gmail.com

Dr. M S Shashidhar
Professor and HOD,
hodmca@amceducation.in

Abstract

The paper discusses the challenges of securely outsourcing medical data to cloud servers while maintaining privacy and usability

To enable dynamic searching over encrypted data, the first solution combines safe k-Nearest Neighbor and attribute-based encryption algorithms. With this method, the forward privacy and backward privacy that are necessary for dynamic searchable symmetric encryption are achieved. Backward privacy prohibits unauthorized users from deducing previously encrypted terms, while forward privacy assures that additions to the data in the future cannot expose information about earlier searches.

The second method fixes the issue with key sharing that kNN-based searchable encryption systems have. It proposes an enhanced solution to facilitate secure and efficient sharing of encryption keys among authorized doctors. By solving this key sharing problem, the usability of the outsourced medical data is improved.

The SEDSSE projects that are being developed have a number of benefits over current plans. They exhibit better storage efficiency, search complexity, and updating complexity

INTRODUCTION

The content offered introduces a research study that focuses on secure and efficient dynamic searchable symmetric encryption (SEDSSE) algorithms for medical online data It emphasizes the significance of enhancing healthcare systems' scalability and medical services, which may be done using cloud computing. Patients can keep their data on cloud servers by utilizing cloud resources. and share it with doctors for remote access and analysis.

Before transferring data to the cloud, encryption is required to safeguard sensitive medical information. Encrypted data, however, presents difficulties for effective searching. The idea of Searchable Symmetric Encryption (SSE) is covered in the article as a means of enabling keyword searches across encrypted cloud data. Multiple search features, including fuzzy keyword search and multi-keyword search, are supported by existing SSE systems.

The paper focuses on k-Nearest Neighbor (kNN) based SSE schemes for searching encrypted data. However, existing approaches using shared secret keys among users may lead to privacy breaches. Additionally, achieving dynamic SSE (DSSE) for supporting encrypted keyword searches even with data insertions and deletions poses difficulties.

To ease these concerns, the research offers a (SEDSSE) technique created exclusively for medical cloud data. SEPSSE I and SEPSSE II, There are displayed two schemes. By integrating kNN, SEPSSE I achieves forward privacy, backward privacy, and collusion resistance. The key sharing issue in kNN-based searchable encryption algorithms is better addressed by SEPSSE II.

The study highlights the benefits of the proposed techniques, including decreased storage costs, increased search effectiveness, and streamlined update procedures. Tests have been done on the storage overhead, index generation, trapdoor creation, and query performance..

LITERATURE SURVEY

1. Attribute-based encryption enabling secure and scalable sharing of personal health records in cloud computing

The goal is to address the privacy concerns associated with outsourcing personal health records (PHRs) to third-party servers, such as cloud providers. The system offers safe and regulated access to the data by encrypting each patient's PHR file using attribute-based encryption (ABE) methods.

Here are the key points outlined:

Patient-Centric Framework: The proposed structure strongly emphasizes patients' discretion over who has access to their personal health records. By encrypting the PHRs before outsourcing, patients can maintain ownership and retain control over their sensitive health information.

Attribute-Based Encryption (ABE): Fine-grained and scalable data access control is accomplished using ABE approaches. ABE allows encryption and decryption of data based on specific attributes or policies, enabling flexible and controlled access to PHRs.

Multiple Data Owner Scenario: The framework takes into account a situation in which the PHR system has several data owners (patients). By making key management less complicated for both owners and users, this multi-owner arrangement improves scalability.

Security and Privacy: To provide a high level of patient privacy, the recommended solution makes advantage of multiauthority ABE. This guarantees that the PHR data may only be accessed and decrypted by authorized organizations that possess the necessary characteristics.

Dynamic Access Policies and Attribute Modification: Access policies and file properties may be dynamically changed thanks to the framework. This allows for flexible updates to access control rules and ensures that changes in permissions can be efficiently managed.

User and Attribute Revocation: The scheme enables efficient revocation of users and attributes on demandThe framework allows for the dynamic adjustment of file properties and access controls.The system provides effective attribute and user revocation on demand. This implies that when necessary, such as when a user's access rights need to be terminated, access privileges can be promptly canceled.

The proposed scheme's security, scalability, and efficiency are supported by extensive analytical and experimental results, demonstrating its effectiveness in addressing the challenges of privacy exposure, key management, flexible access control, and user revocation in PHR systems stored in semitrusted servers.

2. Facilitating efficient and secure ranked keyword search on cloud-stored data

The project's main goal is to develop a system that allows users to securely rank keywords over Encoded Cloud-based data to find relevant results and accurately restore files. Here are the key points outlined:

Data Privacy in Cloud Computing: Sensitive cloud data must be encrypted before being sent to commercial public clouds in order to safeguard data privacy. However, this encryption poses challenges for effective data utilization services.

Limitations of Traditional Searchable Encryption: Traditional searchable encryption methods allow for keyword searches over encrypted data but only enable Boolean searches. This restriction is insufficient to fulfill the demands of a sizable user base and an enormous volume of cloud-based data.

The challenge of safe ranked keyword search over encrypted cloud data is discussed in this work..By presenting search results with a ranking of relevance and increasing the precision of file retrieval, ranked search improves usability.

One-to-Many Order-Preserving Mapping: The answer uses a one-to-many order-preserving mapping mechanism to adequately safeguard the private score data.. This technique ensures that the privacy of keywords is maintained while enabling accurate ranking.

Security and Usability: The suggested approach accomplishes ranked keyword search while offering a robust security assurance that is equivalent to earlier searchable encryption techniques. This means that data privacy is preserved, and relevant search results can be obtained.

Experimental Results: Extensive testing has revealed that the recommended strategy is effective. These tests confirm the solution's ability to safely conduct ranked keyword searches over encrypted cloud data.

SYSTEN ANALYSIS

EXISTING SYSTEM: Concerning k-Nearest Neighbor (kNN) searches over encrypted data, in particular, the issues with dynamic searchable symmetric encryption (DSSE) methods and the remedies already in place. DSSE aims to support encrypted keyword search even when data is dynamically inserted or deleted from a collection while preserving privacy.

Here are the key points outlined:

kNN-based SSE Schemes: Several DSSE schemes based on the kNN approach have been proposed. However, these schemes often share the same secret key among users, which can lead to privacy disclosure.

Existing Approaches: Stefanov et al. proposed an efficient DSSE scheme that achieves forward privacy but lacks backward privacy. Some researchers have used the Oblivious Random Access Memory (ORAM) technique to address both forward and backward privacy. However, these approaches introduce complexities in storage, search, and updating processes.

Trade-Off between Privacy and Complexity: The passage highlights the trade-off between achieving forward and backward privacy in DSSE schemes and the increased complexity associated with using techniques like ORAM.

PROPOSED SYSTEM: The authors' prior study is built upon in this work, which also tackles two additional issues: Users of search are distributed secret keys differently, and the cloud server and users work together. The suggested plan was created expressly for the healthcare system with the goal of enhancing performance and security.

Here are the key points outlined:

SEDSSE Scheme: The paper introduces the SEDSSE scheme, which extends and improves upon the authors' previous research In the context of medical cloud data, the objective is to create a reliable and effective solution for dynamic searchable symmetric encryption.

Collusion and Key Distribution: The suggested plan tackles the issue of cloud server and search user collusion. It also tackles the problem of different secret key distribution among search users, which is a challenge in kNN-based searchable encryption schemes.

Attribute-Based Encryption (ABE): The paper leverages (ABE) techniques in the proposed SEDSSE scheme, referred to as SEPSSE I. ABE enables attribute-based, fine-grained access control, which boosts the system's security and effectiveness.

Enhanced Scheme: The authors further suggest an improved system dubbed SEPSSE II, building on SEPSSE I. The key sharing issue that frequently arises in kNN-based searchable encryption methods is the focus of this improved approach..

IMPLEMENTATION

1.Trusted authority: Is a trusted third party that plays a crucial role in attribute-based encryption (ABE) systems, particularly when it comes to encrypting sensitive medical documents. An ABE system bases data

Cryptography and decryption on the access regulations attached to the data as well as the individual qualities given to users.

The trusted authority would be in charge of creating the encryption keys necessary to encrypt the documents in the case of medical records. The doctors who are permitted to see the records would need to meet particular access restrictions or qualities, which would be incorporated into the encryption process.

For example suppose that a patient's medical records include private information about a particular medical condition.. The access policy might require that only doctors with specialized knowledge or expertise in that particular condition are allowed to decrypt and view the documents. The associated encryption key with this access policy would be created by the trusted authority.

When a doctor wants to access the encrypted medical documents, they would need to present their credentials or attributes to the trusted authority to obtain the decryption key. The trusted authority would give the doctor the proper decryption key to access and decrypt the papers if their characteristics fit the access policy linked to the encrypted documents.

2.Patient : By implementing attribute-based encryption and creating searchable keywords for the papers, the patient is taking precautions to preserve the privacy of their data. The Server in the cloud receives the Encoded documents and indexes, and the secure kNN algorithm is used to build the indexes that match the keywords. The patient also provides the search physicians with the secret key so they may decrypt the information.

This approach combines encryption and indexing techniques to achieve both data privacy and efficient search capabilities. By encrypting the documents, the patient ensures that the data remains secure even if it's stored on a remote server. The access policy associated with attribute-based encryption allows only authorized individuals to decrypt and access the documents.

Each document is given a set of keywords to help in effective searching and information retrieval. The pages that match certain search queries may be quickly and precisely retrieved using the indexes built using these keywords. By using a secure kNN approach, the patient ensures that the search process is secure and that the privacy of the data is preserved.

3.Cloud server : The patients' submitted encrypted papers and their accompanying indexes are kept on the cloud server, which serves as an intermediate entityThe server's responsibility is to grant authorized search doctors access to information and search services.

A search doctor can send a message to the virtual server to obtain certain documents.. A cryptographic token or query known as a trapdoor is one that is created depending on the search parameters, such as certain keywords or properties. The trapdoor is made to be impenetrable, concealing neither the real search criteria nor the substance of the papers.

The virtual server utilizes the encrypted files and indexes it has saved to perform certain actions after obtaining the trapdoor. The server can identify the matched documents using these processes without having to decode the full dataset, depending on the encryption and indexing methods employed. This procedure keeps the papers' privacy intact while yet allowing for effective search capabilities.

The virtual server provides the search doctor with a list of articles that meet their requirements when the procedures are complete.

4. Doctor : he patient can provide the authorized doctor the secret code. This secret key allows the doctor to generate trapdoors, which are digital tokens that are used to look for documents that have been outsourced and kept on a cloud server.

When a doctor needs to find certain information, she develops a set of search terms based on the necessary criteria. Using the patient's secret key and the collection of search phrases, the doctor builds a trapdoor that is specifically tailored to them. This trapdoor is then delivered to the cloud server.

After receiving the trapdoor, the cloud server performs the necessary operations on the encrypted documents and indexes stored in its database. It fetches the relevant publications based on the search words you typed in the trapdoor. The cloud server then gives the doctor the group of matching documents.To to The doctor must use the attribute-based encryption (ABE) key he or she obtained from a reliable source to decode the matching

papers' content before they can be accessed and read. The physician's ability to decode papers encrypted using attribute-based encryption is made possible by the ABE key..

SYSTEM ARCHITECTURE :

- User Interface:

This component provides an interface for users to interact with the system. Users can submit search queries, upload and retrieve medical data, and manage their access privileges.

Depending on the needs, the user interface may be a web-based application or a mobile app..

- Client-Side Encryption:

The client-side encryption component encrypts the data using a symmetric encryption method, such as AES (Advanced Encryption Standard), prior to uploading the medical data to the cloud.On the client side, the encryption keys are securely maintained and kept..

- Searchable Symmetric Encryption (SSE) Module:

This module allows users to search for specific medical records while the data remains encrypted in the cloud.The SSE module implements a DSSE scheme that enables efficient keyword-based searches over encrypted data.

The module creates encrypted data structures or indexes that allow search operations to be performed without exposing the underlying plaintext data.

- Cloud Storage:

The cloud is used to store the encrypted medical data as well as any encrypted indexes or data structures.

Data redundancy should be offered by the cloud storage system., availability, and security measures, such as access controls and encryption at rest.

- Access Control:

This component manages user access privileges and authentication.

Before using the system or carrying out any actions, users must be authenticated.

Certain medical records can only be accessed by people who are authorized owing to access control techniques.

- Query Processing and Evaluation:

When a search query is submitted by a user, the query processing component processes the query and evaluates it against the encrypted indexes or data structures.

The evaluation process should be efficient and enable fast retrieval of relevant encrypted medical records.

- Security and Privacy:

To safeguard the confidentiality and integrity of the medical data, the system design should incorporate a number of security features, including secure key management, secure communication routes, and access control mechanisms.Sensitive patient data can be further protected by using privacy-preserving methods like differential privacy or data anonymization.

CONCLUSION :

The authors of the aforementioned research provide two very secure dynamic searchable encryption technique. Let's explore the key features and advantages of each scheme:

The first scheme**:** This plan enables both forward privacy and backward privacy, as well as collusion resistance between the virtual server and search consumers. Collusion resistance makes sure that even if the virtual server and search users work together maliciously, they will be unable to access important information without authorization. Backward privacy ensures that older versions of the ciphered information are secure when new updates are produced, while forward privacy ensures that modifications to ciphered information in the future won't expose information about earlier versions.

The second scheme: Building upon the first scheme, the second scheme addresses the key sharing problem that is often encountered in kNN-based searchable encryption schemes. The key sharing problem refers to the challenge of securely distributing and managing the secret keys required for encryption and decryption in a multi-user setting.

When contrasting the recommended systems' storage, search, and update complexity with those of past research, they show better efficiency. Performance assessments that take into account storage overhead, index construction, trapdoor generation, and query execution reveal how effective the suggested solutions are. The authors confirm that their methods offer superior performance in a number of areas of the searchable encryption system through comprehensive testing.

REFERENCES :

[1] D. Cash, A. Kupc¸ ¨ u, and D. Wichs, “Dynamic proofs of retrievability via ¨oblivious ram,” in Advances in Cryptology–EUROCRYPT. Springer, 2013, pp. 279–295.
[2] S. Luo, J. Hu, and Z. Chen, “Ciphertext policy attribute-based proxy reencryption,” in Information and Communications Security. Springer, 2010, pp. 401–415.
[3] R. Brinkman, Searching in encrypted data. University of Twente, 2007.
[4] X. Yuan, X. Wang, C. Wang, A. Squicciarini, and K. Ren, “Enabling privacy-preserving image-centric social discovery,” in Proceedings of IEEE ICDCS, 2014, pp. 198–207