IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

Decryptable Attribute-Based Keyword Search on E-Health Cloud

Krishna Sham P[1], Sushant Rao J[2], Nisarga B S[3], Harshit Ganesh H R[4], Umme Hani[5]
Students, Department of Information Science and Engineering[1,2,3,4]
Assistant Professor, Department of Information Science and Engineering[5]
Vidya Vikas Institute of Engineering and Technology, Mysuru, Karnataka, India

Abstract: *Cloud computing provides lot of benefits to enterprises to offload their data and software services to cloud saving them lot of money that has to be spent on infrastructure setup cost. Enterprises wanted to offload their data to cloud and save on their infrastructure cost. But when offloading the data security and privacy is a important concern. In this work, we focus on the search on encrypted data and provide a effective solution for the search. Searchable symmetric encryption (SSE) allows retrieval of the encrypted data over cloud. We formulate the privacy issue from the aspect of similarity relevance and scheme robustness. We observe that serve-side ranking based on order-preserving encryption (OPE) inevitably leaks data privacy. To eliminate the leakage, we propose a secure-channel free ciphertext-policy decryptable attribute-based keyword search (CP-DABKS) scheme on eHealth cloud in the Internet of Things (IoT) platform. Additionally in CP-DABKS, we employ a vector space model and homomorphic encryption. The vector space model helps to provide sufficient search accuracy, and the homomorphic encryption enables users to involve in the ranking while the majority of computing work is done on the server side by operations only on ciphertext.*

Keywords: Medical, eHealth, Attribute-based Keyword search, Cloud computing

I. INTRODUCTION

Cloud computing, a critical pattern for advanced data service, has became a necessary feasibility for data users to outsource data. The idea of cloud computing is based on a very fundamental principal of „reusability of IT capabilities'. The difference that cloud computing brings compared to traditional concepts of "grid computing", "distributed computing", "utility computing", or "autonomic computing" is to broaden horizons across organizational boundaries. Controversies on privacy, however, have been incessantly presented as outsourcing of sensitive information including e-mails, health history and personal photos is explosively expanding. Reports of data loss and privacy breaches in cloud computing systems appear from time to time. The main threat on data privacy roots in the cloud itself. When users outsource their private data onto the cloud, the cloud service providers are able to control and monitor the data and the communication between users and the cloud at will, lawfully or unlawfully. Instances such as the secret NSA program, working with AT&T and Verizon, which recorded over 10 million phone calls between American citizens, cause uncertainty among privacy advocates, and the greater powers it gives to telecommunication companies to monitor user activity. To ensure privacy, users usually encrypt the data before outsourcing it onto cloud, which brings great challenges to effective data utilization. However, even if the encrypted data utilization is possible, users still need to communicate with the cloud and allow the cloud operates on the encrypted data, which potentially causes leakage of sensitive information. Furthermore, in cloud computing, data owners may share their outsourced data with a number of users, who might want to only retrieve the data files they are interested in. One of the most popular ways to do so is through keyword-based retrieval. Keyword-based retrieval is a typical data service and widely applied in plaintext scenarios, in which users retrieve relevant files in a file set based on keywords. However, it turns out to be a difficult task in ciphertext scenario due to limited operations on encrypted data. Besides, to improve feasibility and save on the expense in the cloud paradigm, it is preferred to get the retrieval result with the most relevant files that match users' interest instead of all the files, which indicates that the files should be ranked in the order of relevance by users' interest and only the files with the highest relevances are sent back to users. A series of searchable symmetric encryption (SSE) schemes have been proposed to enable search on ciphertext. Traditional SSE schemes enable users to securely retrieve the ciphertext, but these schemes support only Boolean keyword search, i.e., whether a keyword exists in a file or not, without considering the difference

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

of relevance with the queried keyword of these files in the result. To improve security without sacrificing efficiency, schemes presented in show that they support top-k single keyword retrieval under various scenarios. The attempts to solve the problem of top-k multikey word over encrypted cloud data. These schemes, however, suffer from two problems—Boolean representation and how to strike a balance between security and efficiency. In the former, files are ranked only by the number of retrieved keywords, which impairs search accuracy. In the latter, security is implicitly compromised to tradeoff for efficiency, which is particularly undesirable in security-oriented applications. Preventing the cloud from involving in ranking and entrusting all the work to the user is a natural way to avoid information leakage. However, the limited computational power on the user side and the high computational overhead precludes information security. The issue of secure multi-keyword top-k retrieval over encrypted cloud data thus is: how to make the cloud do more work during the process of retrieval without information leakage. In an ABE system, encrypted data can be shared by multiple users with certain set of attributes (i.e., enabling one-to-many encryption). Specifically, a sender can control the access of encrypted documents based on the attributes of the receivers. Only users who satisfy all the attributes can decrypt the encrypted documents. Considering the flexibility of searching on fine grained sharing of encrypted data, many variants of attribute based keyword search (ABKS) schemes that combine PEKS with ABE have been proposed. To solve the security issues and limitations of the existing ABKS schemes, we propose a secure-channel free ciphertext-policy decryptable attribute-based keyword search (CP-DABKS) scheme. Our scheme resists KGAs and does not require a secure channel to transmit the trapdoor generated by a user. The proposed scheme can be applied to a telemedicine system as shown in Fig. 1. Telemedicine is the delivery of health care services through information and communication technology in two or more separate locations. Medical practitioners use the underlying technology platform to exchange medical and clinical information for the benefits of individual patients and communities. Long distance diagnosis, treatment and counseling are provided to the injured and sick in rural or suburban areas that lack of health care services.A large number of electronic health records are stored in the telemedicine cloud server. Our proposed CP-DABKS scheme is applied to enable the cloud server for protecting the confidentiality of the EHRs as well as providing finegrained access control. Consider a patient who lives in a rural area A of Province B. When he/she is admitted to a local hospital with limited medical resources, he/she may wants to receive better medical treatment via telemedicine. For this example, the patient or the local hospital is the data sender. If he/she has a knee problem, the keyword associated to the plaintext message to be sent is ‘‘orthopaedic disorder’’. The plaintext message may include the patient’s age, sex, health history, as well as readings obtained from the patient’s wearable devices or body sensors. The access structure can be set up based on which medical centers or physicians should access the patient’s health records. For example, only large telemedicine hospitals satisfying three conditions can access them, which are >5 years of telemedicine experience, orthopaedic department, province B. The patient or the local hospital uploads the encrypted keywords and access structure as well as ciphertext of health records to the telemedicine cloud platform.

II. PROBLEM

The main problem is data leakage and privacy in clouds. When users outsource their private data onto the cloud, the cloud service providers are able to control and monitor the data and the communication between users and the cloud at will, lawfully or unlawfully.

III. EXISTING SYSTEM

The concept of similarity relevance and scheme robustness to formulate the privacy issue in searchable encryption schemes and then solve the insecurity problem by proposing a Two-Round Searchable Encryption (TRSE) scheme. Novel technologies in the cryptography community and information retrieval (IR) community are employed including homomorphic encryption and vector space model. Considering the large number of data users and documents in the cloud, it is necessary to allow multiple keywords in the search request and return documents in the order of their relevance to these keywords. Related works on searchable encryption focus on single keyword search or Boolean keyword search, and rarely sort the search results. Also Existing works with ABKS schemes which provides more powerful and flexible search operations which allow encrypted data to be retrieved by multiple users satisfy set of attributes. However, there are still some limitations and security issues on the existing ABKS schemes.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

3.1 Disadvantages

Many of the existing ABKS schemes only support for the encryption of keyword and require a separate cryptographic primitive to encrypt the message. Also, most of the schemes cannot resist offline keyword guessing attacks by inside attackers (i.e., the honest-but-curious servers). A secure-channel is needed for most of the ABKS schemes to transmit the trapdoors between the server and receiver.

3.2 Proposed System

In the proposed scheme, the majority of computing work is done on the cloud while the user takes part in ranking, which guarantees top-k multi keyword retrieval over encrypted cloud data with high security and practical efficiency. Our contributions can be summarized. We propose the concepts of similarity relevance and scheme robustness. We, thus, perform the first attempt to formulate the privacy issue in searchable encryption, and we show server side ranking based on order-preserving encryption (OPE).We propose a scheme, which uthoriz the secure multi keyword top-k retrieval over encrypted cloud data. Specifically, we employ relevance score to support multi keyword top-k retrieval.We explore the problem of multikeyword ranked search over encrypted cloud data (MRSE), and establish a set of strict privacy requirements for such a secure cloud data utilization system.A secure-channel is needed for most of the ABKS schemes to transmit the trapdoors between the server and receivers. To solve these problems, we propose a secure-channel free ciphertext-policy decryptable attribute-based keyword search (CP-DABKS) scheme.

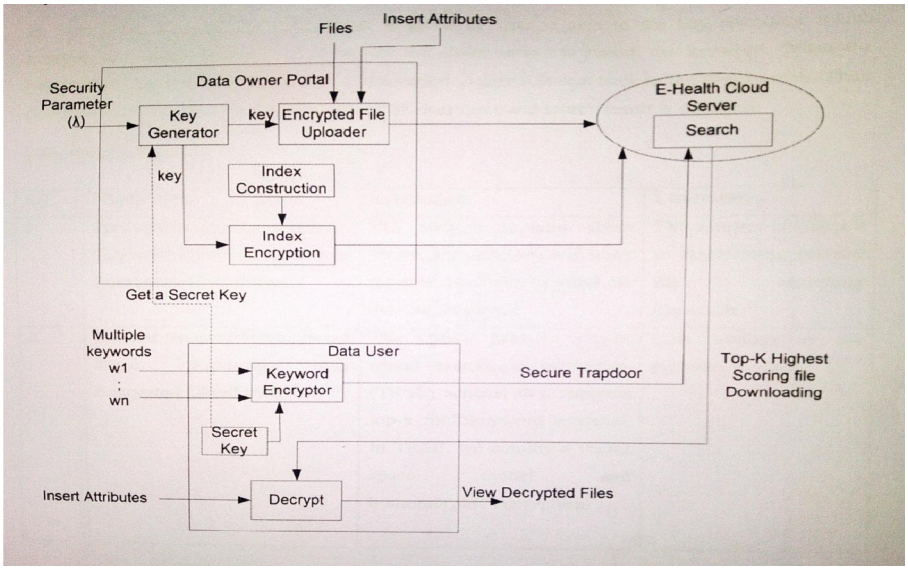
A. Advantages

The proposed scheme allows the authorised user who satisfy the access structure to decrypt the ciphertext. Our scheme not only resists the insider keyword guessing attack, but also eliminates the secure channel for trapdoor transmission. We formally define and prove the security of the proposed CP-DABKS scheme.We also demonstrate its application on an eHealth cloud platform.

3.3 Objectives

- Main objective is to maintain security and privacy for the data in Cloud.
- To avoid data leakage is another objective in this project.
- To compute Trapdoor Technique to achieve privacy between the patients and doctors.
- Policy based Attribute matching technique to maintain the data privacy

IV. SYSTEM REQUIREMENTS



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

4.1 Modules Used

- **Data Owner:** In the data owner portal, the key is generated using key generator. That is given to the file uploader to upload it in the cloud. The same key is also given to the index encryption after the construction of index and it is also sent to the cloud.
- **Data User:** The E- Health cloud server stores the data and it encrypts the data and gives back the result to the user.
- **E-Health Cloud Server:** In Data User, a search keyword which is given by user is sent to the key encryptor which encrypts the search keyword. It is sent to the cloud server to search the keyword. When the keyword is found, it is decrypted and downloaded. Again it is sent back to the cloud server. Then it sends the encrypted top-k score to the result decryptor and search result is obtained.

4.2 Softwares Used

- **Java:** One of the most widely used programming languages, Java is used as the server-side language for most back-end development projects, including those involving big data and Android development. Java is also commonly used for desktop computing, other mobile computing, games, and numerical computing. Java offers higher cross- functionality and portability as programs written in one platform can run across desktops, mobiles, embedded systems.
- Java is free, simple, object-oriented, distributed, supports multithreading and offers multimedia and network support.
- **HTML** It's the fundamental technology behind everything you see in a web browser, and it's used to build everything from simple web pages to complex web applications and services. HTML elements form the building blocks of all websites. HTML allows images and objects to be embedded and can be used to create interactive forms.HTML is needed to create user interface elements like buttons, images, text fields, etc., for the web, so beginners navigate through a webpage.
- **Netbeans:** NetBeans IDE is a free and open source tool, integrated development environment for application development on Windows, Mac, Linux, and Solaris operating systems. NetBeans IDE is more well known as the popular web development tool that streamlines the building and deployment of applications. With support for programming languages, like Java, PHP, and HTML.
- **Amazon S3:** Amazon Simple Storage Service (Amazon S3) is an object storage service that offers industry-leading scalability, data availability, security, and performance. Customers of all sizes and industries can use Amazon S3 to store and protect any amount of data for a range of use cases, such as data lakes, websites, mobile applications, backup and restore, archive, enterprise applications, IoT devices, and big data analytics. Amazon S3 provides management features so that you can optimize, organize, and configure access to your data to meet your specific business, organizational, and compliance requirements.
- **Java Development Kit:** The JDK is a development environment for building applications, applets, and components using the Java programming language. The JDK includes tools useful for developing and testing programs written in the Java programming language and running on the Java platform.

V. CONCLUSION AND FUTURE SCOPE

In this project, we propose a new data access control scheme for multi-authority cloud storage systems. The proposed scheme provides two-factor protection mechanism to enhance the confidentiality of outsourced data. If a user wants to recover the outsourced data, this user is required to hold sufficient attribute secret keys with respect to the access policy and authorization key with regard to the outsourced data. In our proposed scheme, both the size of ciphertext and the number of pairing operations in decryption are constant, which reduce the communication overhead and computation cost of the system. In addition, the proposed scheme provides the user-level revocation for data owner in attribute-based data access control systems. And Keyword based file search is processed at the user side for faster search. In future, as most of the update works are implemented by the CSP, it is assumed that the CSP will not collude with the revoked users. To demonstrate the security of our scheme, we design two security games: indistinguishability against selective ciphertext-policy and chosen plaintext attack (IND-sCP-CPA) game and indistinguishability against chosen keyword attack (IND-CKA) game.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 9, June 2022
Impact Factor: 6.252

REFERENCES

[1]. Ning Cao; Cong Wang; Ming Li; Kui Ren; Wenjing Lou, "Privacy-Preserving Multi-Keyword Ranked Search over Encrypted Cloud Data", IEEE Transactions on Parallel and Distributed Systems (Volume: 25, Issue: 1, Jan. 2014).

[2]. Jiadi Yu; Peng Lu; Yanmin Zhu; Guangtao Xue; Minglu Li, "Toward Secure Multikeyword Top-k Retrieval over Encrypted Cloud Data", IEEE Transactions on Dependable and Secure Computing (Volume: 10, Issue: 4, July-Aug. 2013).

[3]. AnuradhaMeharwad, G.A.Patil, "Efficient Keyword Search over Encrypted Cloud Data", International Conference on Information Security & Privacy (ICISP2015), 11-12 December 2015.

[4]. Ziq ing Guo, Hua Zhang, Caijun Su,n Qiaoyan Wen, Wenmin Li, "Secure multi-keyword ranked search over encrypted cloud data for multiple data owners", Journal of Systems and Software Volume 137, March 2018, Pages 380-395.

[5]. Larry A. Dunning; Ray Kresman, "Privacy Preserving Data Sharing With Anonymous ID Assignment", IEEE Transactions on Information Forensics and Security (Volume: 8, Issue: 2, Feb. 2013).

[6]. Jian Wang; Yan Zhao; Shuo Jiang; Jiajin Le , "Providing Privacy Preserving in Cloud Computing", 3rd International Conference on Human System Interaction, IEEE, 2010.

[7]. Yan-Cheng Chang, Michael Mitzenmacher, "Privacy Preserving Keyword Searches on Remote Encrypted Data", International Conference on Applied Cryptography and Network Security, Springer, 2015.

[8]. Jin Li , Qian Wang, Cong Wang , Ning Cao , Kui Ren , and Wenjing Lou, "Enabling Efficient Fuzzy Keyword Search over Encrypted Data in Cloud Computing".