Secure and Encrypted Personal Health Record in Cloud

Abarna S
Final year M.E, Department of Computer Science
Priyadarshini Engineering College, Anna University
Vaniyambadi, Vellore District, Tamilnadu, India, Email: s.abarna4u@gmail.com
Dr.A.S.Kumaresan M.E., Ph.D., FIE.,
Head Of Department
Department of Computer Science
Priyadarshini Engineering College
Anna University, Vaniyambadi, Vellore District, Tamilnadu, India

----------**ABSTRACT**----------

Personal health record (PHR) service is an emerging model for health information exchange. In PHR systems, patient's health records and information are maintained by the patient himself through the Web. In reality, PHRs are often outsourced to be stored at the third parties like cloud service providers. However, there have been serious privacy concerns about cloud service as it may expose user's sensitive data like PHRs to those cloud service providers or unauthorized users. Using attribute-based encryption (ABE) to encrypt patient's PHRs in cloud environment, secure and flexible access control can be achieved. Yet, problems like scalability in key management, fine-grained access control, and efficient user revocation remain to be addressed. In this paper, we propose a privacy-preserving PHR, which supports fine-grained access control and efficient revocation.

Keywords**- Health, environment, scalability, revocation, third parties.**

I. INTRODUCTION

Cloud-Based Personal Health Record systems (CBPHR) such as Microsoft Health Vault and Zebra Health are rising. A typical CB-PHR system consists of three entities: data owners, data providers and a cloud server. In CBPHR system, data owners and data providers are defined as patients themselves and hospitals, respectively. Data owners can directly authorize data providers to upload their PHRs to the cloud. The CB-PHR system allows data owners to access their PHRs anytime and anywhere, be better prepared for medical appointments and unexpected emergencies, maintain a more complete picture about personal health, and even achieve fitness goals. Data providers can explore. Privacy concerns are among the main obstacles for the wide adoption of CB-PHR systems. In particular, many people have deep concerns that there can be unauthorized access to their sensitive PHRs. For example, the cloud may have business interest in analyzing the PHRs, and it may also have malicious employees or even be hacked. A natural way to alleviate the privacy concerns is to let data owners and providers upload encrypted PHRs to the cloud which does not possess the decryption keys.

II. SYSTEM STUDY

2.1. Feasibilty Study

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company.

Economic Feasibility:This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified. Thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased. Please do not revise any of the current designations.

Technical Feasibility:This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility:The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

III. MODEL AND PROBLEM STATEMENT

To enable efficient and privacy-preserving search in a

multi-source cloud-based PHR environment, MEIM should satisfy the following privacy and performance guarantees.

- Index/Query privacy: In MEIM, each index is constructed as an MDB-tree. To achieve index/query privacy, indexes/queries will be encrypted under MOPSE before outsourcing. Then, the cloud will process the encrypted queries on the encrypted indexes without decrypting any information.
- Authorized search: MEIM should ensure that data providers can query only data files within their permission. That is, data providers are hard to generate the fake queries.
- Efficiency: The efficiency is defined as the user's overhead of query requests. To keep efficiency, the cloud will merge encrypted indexes without knowing indexes information, and the user just needs to encrypt query once to efficiently retrieve PHRs of her interests.

IV. MULTI-SOURCE ENCRYPTED INDEXES MERGING MECHANISM

4.1. Architecture Diagram

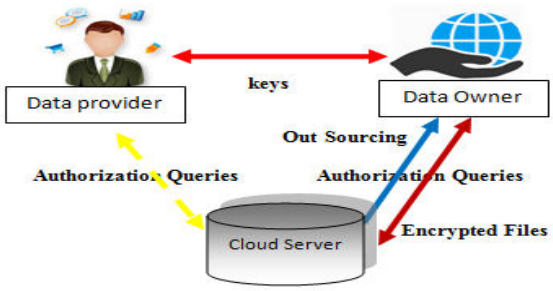

Fig. 1. Overall Architecture

4.2. Overview

In order to satisfy multiple design goals, we propose a novel MEIM mechanism. Fig.1 shows the working processes of MEIM.

Data user: Preprocessing generates a group-shared parameter KG and a shared security key K for data providers, and generates a shared security key KC for the cloud. QueryGenU generates query requests of data user; FilesDecU decrypts encrypted data files.

Data providers: FilesEnc runs the existed symmetrical encryption for encrypting data files and encrypts the symmetric key under the data user's public key. IndexEnc creates the index as an MDB-tree and encrypts the index with MOPSE. QueryGenP generates query requests of data providers. FilesDecP decrypts encrypted data files.

The Cloud: IndexesTrans merges multiple encrypted indexes and segments this merged index to two indexes:BS Index and H Index. PrivacyQuery performs query on BS Index for data provider's query and performs query on H Index for data user's query. The cloud then returns matched encrypted data files to data user or data providers.

4.3. Transforming Encrypted Indexes

Upon receiving these encrypted indexes, the cloud merges two indexes by an recursive merging procedure from the root to leafnodes, in which MEIM just only compares the suffix of the ciphertext. Then, the cloud segments the merged index to two separated indexes: BS Index and H Index. It satisfies and is shared among the cloud and data user.

V. PERFORMANCE ANALYSIS

Index Encryption. Assume that the attribute and record numbers for each index are fixed at σ and γ, respectively. The upper bound μ and lower bound ν are appropriate for all attribute values ($\tau=\mu-\nu+1$). The complexity of inserting a record to an index is $O(\sigma*\tau)$ due to the height of the tree is σ. Thus, when an index contains γ records, the time complexity of building an index is $O(\sigma * \gamma * \tau)$. For index encryption, the encryption time relies on the symmetric encryption method, thus the time complexity thereof is not listed.

Indexes Transforming. For simplify, we mainly consider the time complexity of merging two indexes (i.e., MDBtrees). Since the suffix of a plaintext for various providers are distinguish, merging two indexes is equivalent to that of merging their roots. It can takes $O(\tau\ 2)$ to merging two encrypted indexes, where τ denotes the maximum number elements on the root. While, for segmenting merged index, it can be viewed as traversing an MDB-tree, so the time complexity of segmenting index is $O(n*\sigma * \gamma * \tau)$. **Query.** In MEIM scheme, the query is divided into two categories: the query for data providers and the query for data user. For data providers' query, the time complexity of prefix query on an MDB-tree is $O(\sigma*\tau*(128+1))$, where 128 denotes the bits of a hash key. Thus, the query time complexity for data providers without MOPSE is $O(\sigma * \tau*(128+1))$.

VI. SECURITY ANALYSIS

Index/Query Privacy. We claim that MEIM achieves both index privacy and query privacy under out threat model. The ciphertext indexes for attribute values consist of two parts: BS Index for data providers' query and H Index for data users' query. The cloud obtains the parameter hc where hc is an OPMPH function shared by the cloud and data user. On one hand, the cloud will guess the index/query contents of data providers Thus, the cloud is hard to get the contents of the indexes/queries of data providers. On the other hand, the cloud will guess the index/query contents of data user, i.e., H Index.

VII. RELATED WORK

One fundamental and common form of data utilization is the keyword search operation, i.e., to quickly sort out matching information from the huge amount of datasets according to specific search keywords. Many existing Keyword-based search techniques,

which are widely adopted on the plaintext data, cannot be directly used on the cipher text data. In order to solve this problem, some general purpose solutions are proposed based on fully homomorphic encryption or oblivious RAMs. However, these methods are impractical because of their high computational overhead. On the contrary, more practical solutions, such as Searchable Encryption (SE), have made specific contributions to addressing the need for secure search over outsourced data. SE is a cryptographic primitive that supports keywords search over encrypted data, which not only saves huge network bandwidth and computation resources for users but also migrates the burdensome search operation to the cloud server to utilize its strong computational capacity. So far, researchers have developed abundant SE schemes to achieve various search functionality, such as single keyword search, multikeyword conjunctive search, ranked search, similarity search, etc.

The proposed efficient multi-keyword ranked search schemes, which supported the deletion and insertion of documents flexibly. Due to the adoption of a tree based index structure, this scheme can achieve sub linear search time. However, schemes were only suitable for multi-keyword text search, in which the index was constructed based on term frequency. Moreover, their schemes were unable to deal with multi-attribute subset conjunction and range conjunction search over record collection (e.g. EMRs), which has multiple attributes. Therefore, on the premise of ensuring data security and patients' privacy, developing efficient multi attribute conjunctive keyword search schemes over encrypted EMRs, which support update operation, becomes an especially requested issue.

VIII. CONCLUSION

In this project, we explore the problem of privacy-preserving query for multi-source in the cloud-based PHR environment. Different from prior works, our proposed MEIM mechanism enables authenticated data owner to achieve secure, convenient, and efficient query over multiple data providers' data.

To implement the efficient query, we introduce MDBT as the data structure. To reduce the overhead of query generation of data owner, and allow the cloud server to securely query, we propose a novel multiple order-preserving symmetric encryption (MOPSE) schemes. To make our model more practical,

we propose an enhanced multiple order-preserving symmetric encryption (MOPSE+) scheme to satisfy the hierarchical authenticated query. Moreover, we leverage rigorous security proof to prove that our schemes are security. Finally, we demonstrate that the MEIM mechanism is computationally.

IX. ACKNOWLEDGMENT

At the very outset, I wish to express my sincere thanks to all those who were involved in the completion of this project. My most sincere salutations go to **Anna University** that gave me an opportunity to have sound base of Computer Science and Engineering. I thank **Dr. P. NATARAJAN. M.E.,Ph.D.,FIE,** Principal of Priyadarshini Engineering College for permitting me to accomplish this project.

I offer my sincere thanks to **Dr. A.S. KUMARESAN. M.E.,Ph.D.,FIE.,** Head of the Department of Computer Science and Engineering and my Internal guide for giving this opportunity and his full encouragement. I am grateful to **DR.S. VIJAYARANGAN, M.E,Ph.D.,** Associate Professor**,** our Coordinator, for her valuable guidance in carrying out the project work and her full encouragement.

REFERENCES

[1] Xue K, Hong J, Xue Y, Wei D, Yu N, Hong P, (2017) "CABE: A New Comparable Attribute-based Encryption Construction with 0-Encoding and 1-Encoding," IEEE Trans Comput., vol. 66, no. 9, pp. 1491 – 1503.

[2] 2. Ma X, Zhu Y, Li X, (2017) "An efficient and secure ridge regression outsourcing scheme in wearable devices," Computers & Electrical Engineering, DOI: 10.1016/j.compeleceng.2017.07.019

[3] Li M, Yu S, Cao N, Lou W, (2011). "Authorized private keyword search over encrypted data in cloud computing," in ICDCS'11, Minneapolis, Minnesota.

[4] Benaloh J, Chase M, Horvitz E, Lauter K, (2009) "Patient controlled encryption: ensuring privacy of electronic medical records," in: ACM workshop on CCS'09, New York, NY

[5] Li M, Yu S, Zheng Y, Ren K, W. Lou,(2013) "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption," IEEE T Parall Distr., vol. 24, no. 1, pp. 131 – 143.

[6] Li M, Yu S, Ren K, W. Lou, (2010) "Securing personal health records in cloud computing: Patient-centric and fine-grained data access control in multiowner settings," in SecureComm'10, Singapore.

[7] Sun J, Zhu X, Zhang C, Fang Y, (2011) " HCPP: Cryptography based secure system for patient privacy and emergency healthcare" in ICDCS'11, Minneapolis, Minnesota.

[8] Liu J, Huang X, Liu J, (2015) "Secure sharing of personal health records in cloud computing: ciphertext-policy attribute-based signcryption," Future Gener Comp Sy., vol. 52, pp. 67 – 76.

[9] Scheuermann P, Ouksel M, (1982) "Multidimensional B-trees for associative searching in database systems," Inform Syst., vol. 7, no. 2, pp. 123 – 137.

[10] Wang C, Zhang B, Ren K, Roveda J , Chen C, Xu Z, (2014) " A Privacy-aware cloud-assisted healthcare monitoring system via compressive sensing" in INFOCOM'14, Tornto, Canada.