Public-Key Searchable Encryption Scheme with Charm Prototyping

I.Umamaheswara rao[1], V.V.S Nataraj[2], V.Vikranth Reddy[3], N.Raghu Vamshi[4]
[1] *Associative Professor, Computer Science Engineering, St.Martins Engineering College.*
[2,3,4] *B.Tech, Computer Science Engineering, St.Martins Engineering College.*

ABSTRACT

With the drastic change of computer technology, most of the data owners are conducting a keyword search process for an encrypted data which is stored in cloud server on behalf of the user without learning about the under lying plain texts. However, there are various schemes for an encrypted data which supports either a single (or) conjuctive keyword search remaining are able to perform an expressive search format by using a keyword in an efficient manner. In this project, we are going to describe about the searching process of a encrypted data which is present in the cloud by using a keyword in an expressive way, by allowing different search policies and how it is working. When comes to security we are providing a high end security model which reaches to our standard. Finally the implementation of this scheme is carried out by using a rapid prototyping tool called charm.

INTRODUCTION

Consider a cloud-based healthcare information system that hosts outsourced personal health records (PHRs) from various healthcare providers. The PHRs are encrypted in order to comply with privacy regulations like HIPAA. In order to facilitate data use and sharing, it is highly desirable To have a searchable encryption (SE) scheme which allows the cloud service provider to search over encrypted PHRs on behalf of the authorized users (such as medical researchers or doctors) without learning information about the underlying plaintext. Note that the context we are considering

Supports private data sharing among multiple data providers and multiple data users. Therefore, SE schemes in the private-key setting [1], [2], [3], which assume that a

Single user who searches and retrieves his/her own data, are not suitable. On the other hand, private information retrieval (PIR) protocols [4], [5], [6], which allow users to retrieve a certain data-item from a database which publicly stores data without revealing the data-item to the database administrator, are also not suitable, since they require the data to be publicly available. In order to tackle the keyword search problem in the cloud-based healthcare information system scenario, we resort to public-key encryption with keyword search (PEKS) schemes, which is firstly proposed in [7]. In a PEKS scheme, a ciphertext of the keywords called "PEKS ciphertext" is appended to an encrypted

PHR. To retrieve all the encrypted PHRs containing a keyword, say "Diabetes", a user sends a "trapdoor" associated with a search query on the keyword "Diabetes" to the cloud service provider, which selects all the encrypted PHRs containing the keyword "Diabetes" and returns them to the user while without learning the underlying PHRs. However, the solution in [7] as well as other existing PEKS schemes which improve on [7] only supports equality queries [8].

Set intersection and Meta keywords1 [9], [10] can be used for conjunctive keyword search. However, the approach based on set intersection leaks extra information to the cloud server beyond the results of the conjunctive query, whilst the approach using Meta keywords require 2m Meta keywords

To accommodate all the possible conjunctive queries for m keywords. In order to address the above deficiencies in conjunctive keyword search, schemes such as the ones in were put forward in the public-key setting.

EXISTING SYSTEM

In a private-key SE setting, a user uploads its private data to a remote database and keeps the data private from the remote database administrator. Private-key SE allows the user to retrieve all the records containing a particular keyword from the remote database. However, as the name suggests, private-key SE solutions only apply to scenarios where data owners and data users totally trusted each other.

- **Private Information Retrieval.** With respect to public database such as stock quotes, where the user is unaware of it and wishes to search for some data-item without revealing to the database administrator which item it is, private information retrieval (PIR) protocols were introduced, which allow a user to retrieve data from a public database with far smaller communication then just downloading the entire database. Nevertheless, in our context, the database is not publicly available, the data is not public, and so the PIR solutions cannot be applied.

DISADVANTAGES OF EXISTING SYSTEM:

- Private-key SE solutions only apply to scenarios where data owners and data users totally trusted each other.
- Nevertheless, in our context, the database is not publicly available, the data is not public, and so the PIR solutions cannot be applied.

PROPOSED SYSTEM:

- we propose a public-key based expressive SE scheme in prime-order groups, which is especially suitable for keyword search over encrypted data in scenarios of multiple data owners and multiple data users such as the cloud-based healthcare information system that hosts outsourced PHRs from various healthcare providers.
- Our expressive SE scheme consists of a trusted trapdoor generation center which publishes a public system parameter and keeps a master key

in secret, a cloud server which stores and searches encrypted data on behalf of data users, multiple data owners who upload encrypted data to the cloud, and multiple data users who would like to retrieve encrypted data containing certain keywords. To outsource an encrypted document to the cloud, a data owner appends the encrypted document with keywords encrypted under the public parameter and uploads the combined encrypted document and encrypted keywords to the cloud. To retrieve all the encrypted documents containing keywords satisfying a certain access structure (i.e., predicate or policy) such as ("Illness = Diabetes" AND ("Age = 30" OR "Weight = 150- 200")), a data user first obtains a trapdoor associated with the access structure from the trapdoor generation center and then sends the trapdoor to the cloud server. The latter will conduct the search and return the corresponding encrypted documents to the data user.

ADVANTAGES OF PROPOSED SYSTEM:

- We define a security model for expressive SE, which takes into account all adversarial capabilities of the standard SE security notion.
- Using a randomness splitting technique, our scheme achieves security against offline keyword dictionary guessing attacks to the ciphertexts.

IMPLEMENTATION

MODULES

- Data Owner
- Data User
- Tapdoor Generation Center
- Cloud Server

MODULES DESCRIPTION

Data Owner:

- Data owners who outsource encrypted data to a public cloud.
- Data owner consists of two parts: the encrypted document generated using an encryption scheme and the encrypted keywords generated

Data User:

- Data users who are privileged to search and access encrypted data.
- A data user issues a trapdoor request by sending a keyword access structure to the trapdoor generation center.
- After obtaining a trapdoor, the data user sends the trapdoor and the corresponding partial hidden access structure (i.e., the access structure without keyword values) to the designated cloud server.

Tapdoor Generation Center:

- Trusted trapdoor generation center who publishes the system parameter and holds a master private key and is responsible for trapdoor generation for the system

- Trapdoor generation centre which generates and returns a trapdoor corresponding to the access structure to data user.
- Trapdoor generation center has a separate authentication mechanism to verify each data user and then issue them the corresponding trapdoors.

Cloud Server:

- Designated cloud server who executes the keyword search operations for data users. To enable the cloud server to search over ciphertexts, the data owners append every encrypted document with encrypted keywords
- The latter performs the testing operations between each ciphertext and the trapdoor using its private key, and forwards the matching ciphertexts to the data user.

SCREENS

Fig: Home Page

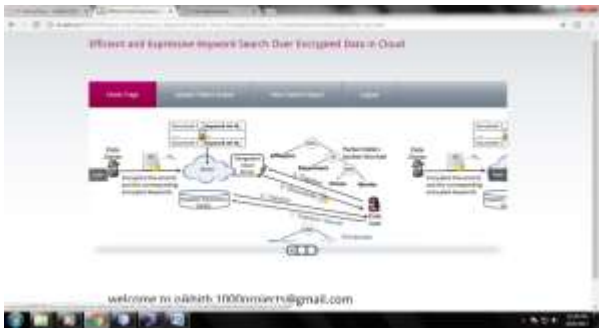

Fig: Owner Home

Fig: Upload Report

Fig: search Patient Report

Fig: Key Verification

CONCLUSION

In order to allow a cloud server to search on encrypted data without learning the underlying plaintexts in the publickeysetting, Boneh [7] proposed a cryptographic primitive called public-

key encryption with keyword search (PEKS).Since then, considering different requirements in practice,e.g., communication overhead, searching criteria and security enhancement, various kinds of searchable encryption systems have been put forth. However, there exist only a few public-key searchable encryption systems that support expressive keyword search policies, and they are all built from the inefficient composite-order groups . In this

Paper, we focused on the design and analysis of public-key searchable encryption systems in the prime-order groups that can be used to search multiple keywords in expressive searching formulas. Based on a large universe key-policy attribute-based encryption scheme given in , we presented an expressive searchable encryption system in the prime order group which supports expressive access structures expressed in any monotonic Boolean formulas. Also, we proved its security in the standard model, and analyzed its efficiency using computer simulations.

REFERENCES

[1] O. Goldreich and R. Ostrovsky, "Software protection and simulationon oblivious rams," J. ACM, vol. 43, no. 3, pp. 431–473, 1996.

[2] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques forsearches on encrypted data," in 2000 IEEE Symposium on Securityand Privacy, Berkeley, California, USA, May 14-17, 2000. IEEEComputer Society, 2000, pp. 44–55.

[3] E. Goh, "Secure indexes," IACR Cryptology ePrint Archive, vol.2003, p. 216, 2003.

[4] C. Cachin, S. Micali, and M. Stadler, "Computationally privateinformation retrieval with polylogarithmic communication," inSAdvances in Cryptology - EUROCRYPT '99, International Conferenceon the Theory and Application of Cryptographic Techniques, Prague,Czech Republic, May 2-6, 1999, Proceeding, ser. Lecture Notes inComputer Science, vol. 1592. Springer, 1999, pp. 402–414.

[5] G. D. Crescenzo, T. Malkin, and R. Ostrovsky, "Single database privateinformation retrieval implies oblivious transfer," in Advancesin Cryptology - EUROCRYPT 2000, International Conference on theTheory and Application of Cryptographic Techniques, Bruges, Belgium,May 14-18, 2000, Proceeding, ser. Lecture Notes in Computer Science,vol. 1807. Springer, 2000, pp. 122–138.

[6] W. Ogata and K. Kurosawa, "Oblivious keyword search," J. Complexity,vol. 20, no. 2-3, pp. 356–371, 2004.

[7] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Publickey encryption with keyword search," in Advances in Cryptology- EUROCRYPT

2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, May2-6, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol.3027. Springer, 2004, pp. 506–522.

[8] J. Lai, X. Zhou, R. H. Deng, Y. Li, and K. Chen, "Expressivesearch on encrypted data," in 8th ACM Symposium on Information,
Computer and Communications Security, ASIA CCS '13, Hangzhou,China - May 08 - 10, 2013. ACM, 2013, pp. 243–252.

[9] P. Golle, J. Staddon, and B. R. Waters, "Secure conjunctive keywordsearch over encrypted data," in Applied Cryptography and
Network Security, Second International Conference, ACNS 2004, Yellow Mountain, China, June 8-11, 2004, Proceedings, ser. Lecture Notes in Computer Science, vol. 3089. Springer, 2004, pp. 31–45.

[10] D. J. Park, K. Kim, and P. J. Lee, "Public key encryption with conjunctive field keyword search," in Information Security Applications,5th International Workshop, WISA 2004, Jeju Island, Korea, August 23-25, 2004, Revised Selected Papers, ser. Lecture Notes in ComputerScience, vol. 3325. Springer, 2004, pp. 73–86.

Author details:

Mr.UmamaheswaraRao Inkollu, Post Graduated in Computer Science Engineering (M.Tech) from JNTU Hyderabad in 2012 and Master of Computer Applications from JNTU Kakinada in 2009. Having 6 years of experience as Assistant Professor. He is presently working as Associate Professor in Computer Science and Engineering department in St. Martin's Engineering College, Hyderabad. His area of interest in Cloud Computing, Information Security, Bigdata.