International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 3, Issue 4, April 2016

Security in Searching Shared and Encrypted Data in Multi Party Environment

[1] Amarja Jagtap-Patil [2] Pranav Chavan [3] Ashish Chaturvedi [4] Nagraj Kiwade [5] Jyoti Kshirsagar
[1][2][3][4][5] Department of Computer Engineering, Rajarshi Shahu College of Engineering, Pune.
Savitribai Phule Pune University
[1] amarja014@gmail.com, [2] chavanpranav25@gmail.com,
[3] ashish.chaturvedi2810@gmail.com, [4] nagrajkiwade127@gmail.com [5] jyotikshirsagar@gmail.com

Abstract: **Encryption is well established technology for protecting sensitive data. Multiparty Searchable Encryption is a scheme in which multiple users store and share their data with each other. The scheme consists of two entities: A server and set of users. Achieving multi-party searching is challenging as existing schemes are not achieving the secure searchable encryption due to the key sharing between set of users. Also it is not forming scalable solution for multi-party searching and settings, where users outsource their encrypted data to particular cloud server and selectively authorize each other to search. There can be a possibility that the cloud server may collude with some harmful users, it is a challenge to have a more secure and scalable multiparty searchable encryption (MPSE) scheme. This is shown by analysis on the Popa–Zeldovich scheme, which says that an honest user may leak all search patterns even if user shares only one of the documents with any unknown malicious user. Based on these analysis, system present a new security model for MPSE by considering the scenarios from best case to worst case, which capture different server user collusion possibilities. System then try to propose a MPSE scheme by employing the property linearity of Type-3 pairings and prove its security based on the bilinear Diffie–Hellman variant assumption in the oracle model. Moreover, the evaluations show the speed of proposed scheme compared with the old MPSE scheme with respect to searching and encryption/decryption.**

Keywords**: Multi-Party, Searchable Encryption, Trapdoor privacy, Data privacy, Pairing Holomorphiv, Encryption**

I. INTRODUCTION

Some Existing Multi-User Schemes: Curtmola et al.Proposed the concept of multi-user searchable encryption schemes, where a user can authorize multiple other users to search her encrypted data. However, the proposed primitive does not take into account the fact that the same user may also be authorized to search other users' data and the corresponding security issues. As a result, the primitive from offers a solution for a much more simplified problem than ours, and it seems not trivial to construct a scalable solution for our problem based on their scheme.

In the work of Bao et al. A new party, namely user manager, is introduced into the system, to manage multiple users' search capabilities (e.g. enable them to search each other's data). In this extension, the user manager needs to be fully trusted since it is capable of submitting search queries and decrypting encrypted data. This conflicts with our security criteria (i.e. there should not be additional TTP involved). The schemes of Dong, Russello and Dulay have similar issues. In the work from the above authors have investigated order preserving encryption, where the cipher texts preserve the order the plaintexts so that every entity can perform an equality comparison. Clearly, these schemes also conflict with our security criteria (i.e. leak minimal information to the server).

II. RELATED WORK

In the formulation of MPSE, previous system assumed that authorization was granted on the index level, namely for each of our indexes we can decide whether another user can search or not (if authorized user can try all keywords) We will try to introduce Advanced Multi Party Searchable Encryption as a new version of Multi Party Searchable Encryption Scheme which supports multi-keyword searching by means of holomorphic algorithm. The proposed scheme also avoids key sharing with the help of a key server. All the uploaded documents can be stored in the encrypted form. File updating can also possible with advanced MPSE scheme.

III. SYSTEM ARCHITECTURE

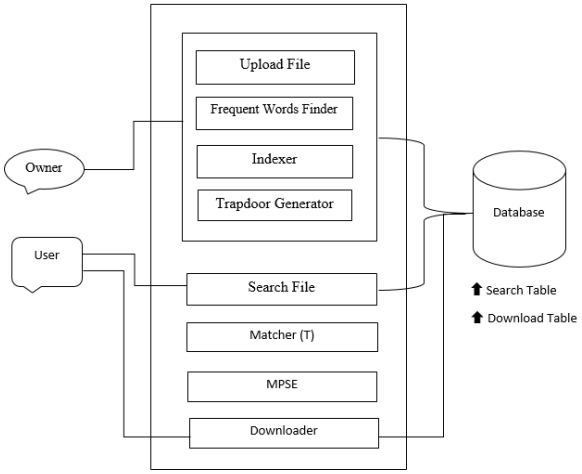


Fig.1. System Architecture

Basically system architecture is divided into four modules, they are as follows:-

***1. User Login*:** In this module if a user gets logged in, he should give his email id and password.

***2. Give Access*:** After User gets logged in he can view The concept of searchable encryption provides a promising direction in solving the above problem. Such schemes allow users to store their data in encrypted form at an untrusted server, and then delegate the server to search on their behalf by issuing a trapdoor (i.e. encrypted keyword). other users who are ready to access his files. User can see the list and give permission to access the file.

***3. Retrieve Access*:** After User gets logged in he can view other users who are ready to access his files. User can see the list and deny access for the user to access the file.

***4. Server*:** Cloud Service Provider (CSP) see the file list and upload the encrypted files in cloud database along with the owner name of the file, which acts as match word. If A's file will be uploaded to cloud and A give permission to B, then B can download the file only when the owner of B(i.e. A) will get matches with the owner of the(A's) file in cloud. Users can follow other user and there should be match between them, then only file download will be possible.

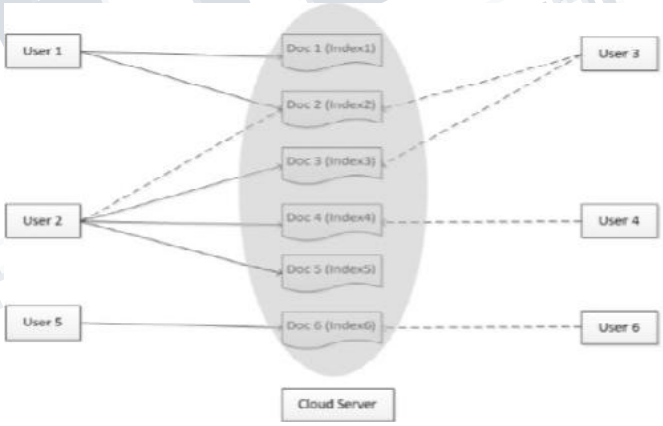
***DATABASE USED*:** MYSQL version 5.5

IV. PROPOSED SCHEME

The concept of searchable encryption provides a promising direction in solving the privacy problem when outsourcing data to the cloud. Such schemes allow users to store their data in encrypted form at an un trusted server, and then delegate the server to search on their behalf by issuing a trapdoor (i.e. encrypted keyword). A detailed survey of searchable encryption schemes can be found.

As to the specific setting where multiple users store and share their data with each other in the cloud, we need a new primitive, namely multi-party searchable encryption (MPSE) schemes in the symmetric setting. MPSE can be regarded as a multi-party version of the symmetric searchable encryption proposed by Song et al. briefly, a MPSE scheme allows every user to build an encrypted index for each of her documents and store it at a cloud server.

The index contains a list of encrypted keywords, as well as some authorization information which selectively authorizes other users to search over this index. Our objective is first to formulate MPSE and its security properties and then to provide a scalable and secure construction.



V. IMPLEMENTATION DETAILS

***CORE TECHNOLOGIES*:**

1.Java Development Kit 7(JDK7)
2.JSP and Servlet

DESIGNING DETAILS:

1.Cascaded Style Sheet (CSS)
2. JavaScript

Our project provides a promising direction in solving the privacy problem when outsourcing data to the cloud. Such schemes allow users to store their data in

encrypted form at an untrusted server, and then delegate the server to search on their behalf by issuing a trapdoor (i.e. encrypted keyword). We will be formulating a new primitive, namely multiparty searchable encryption (MPSE), for enabling users to selectively authorize each other to search in their encrypted data. Due to the user status dynamics, we will present a security model by considering the worst-case and average-case collusion scenarios simultaneously, and also proposed a new scheme with provable security.

VI. PROJECT OVERVIEW

Our project provides a promising direction in solving the privacy problem when outsourcing data to the cloud. Such schemes allow users to store their data in encrypted form at an untrusted server, and then delegate the server to search on their behalf by issuing a trapdoor (i.e. encrypted keyword). We will be formulating a new primitive, namely multiparty searchable encryption (MPSE), for enabling users to selectively authorize each other to search in their encrypted data. Due to the user status dynamics, we will present a security model by considering the worst-case and average-case collusion scenarios simultaneously, and also proposed a new scheme with provable security.

As to the specific setting where multiple users store and share their data with each other in the cloud, we need our new primitive, namely multi-party searchable encryption (MPSE) schemes in the symmetric setting. The index contains a list of encrypted keywords, as well as some authorization information which selectively authorizes other users to search over this index.

VII. CONCLUSIONS AND FUTURE SCOPE

In the formulation of MPSE, previous system assumed that authorization was granted on the index level, namely for each of our indexes we can decide whether another user can search or not (if authorized user can try all keywords) We will try to introduce Advanced Multi Party Searchable Encryption as a new version of Multi Party Searchable Encryption Scheme which supports multi-keyword searching by means of holomorphic algorithm. The proposed scheme also avoids key sharing with the help of a key server. All the uploaded documents can be stored in the encrypted form. File updating can also possible with advanced MPSE scheme. The evaluations demonstrate the viability of the proposed mechanisms in compared with MPSE scheme.

The future scope is use of hybrid cloud to store and retrieve data instead of single one and provide multiple domain accessibility services like PaaS (Platform as a Service), IaaS (Infrastructure as a service).

REFERENCES

[1] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky. Searchable symmetric encryption: improved definiti- ons and efficient constructions. In Proceedings of the 13th ACM conference on Computer and Communications Security,pages 7988. ACM, 2006.

[2] A. Popa and N. Zeldovich. Multi-key encryption. http://eprint.iacr.org/2013/508,2013.

[3] C. Bsch, Q. Tang, P. Hartel, and W. Jonker, Selective document retrieval from encrypted database, in Proc. 15th Inf. Security Conf. (ISC), vol. 7483. 2012, pp. 224241.

[4] M. Kuzu, M. S. Islam, and M. Kantarcioglu, Efficient similarity search over en-crypted data, in Proc. IEEE 28th Int. Conf. Data Eng. ,Apr. 2012, pp. 11561167.

[5] C. Dong, G. Russello, and N. Dulay. Shared and searchable encrypted data for untrusted servers. In V. Atluri, editor, Data and Applications Security XXII, 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security, volume 5094 of LNCS, pages 127–143. Springer, 2008.

[6] D. X. Song, D. Wagner, and A. Perrig. Practical Techniques for Searches on Encrypted Data. In IEEE Symposium on Security and Privacy, pages 44–55. IEEE Computer Society, 2000.

[7] Q. Tang. Privacy preserving mapping schemes supporting comparison. In Proceedings of the 2010 ACM 2010.

[8] Q. Tang. Theory and Practice of Cryptography Solutions for Secure Information Systems, chapter Search in Encrypted Data: Theoretical Models and Practical Applications, pages 84–108. IGI, 2013.