# SECURE SEARCHING OF SHARED AND ENCRYPTED DATA IN MULTIPARTY ENVIRONMENT

Mr. Rahul Y. Mahadik

*Student of JSPM's Imperial College of Engineering & Research, Pune.*

Prof. Santosh T. Waghmode

*Asst. Prof. JSPM's Imperial College of Engineering & Research, Pune.*

**ABSTRACT**

*Encryption is well established technology for protecting sensitive data. Multiparty Searchable Encryption is a scheme in which multiple users store and shares their data with each other. The scheme classified in to two entities: A server and set of users. Achieving multiparty searching is challenging as existing systems are not reaching the secure, searchable encryption because of the set of users shares the key between them. 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. The proposed scheme, advanced Multi-Party Searchable Encryption allows a key server to solve the key sharing problem. The new scheme permits multi keyword searching with homomorphic encryption and additionally enables searching keyword within the form of checksum. Moreover, the evaluations show the speed of proposed scheme compared with the old MPSE scheme with respect to searching and encryption/decryption.*

**Keyword :** - *Data Privacy, Multi-party Searchable Encryption (MPSE), Pairing, Security, Trapdoor Privacy.*

## 1. Introduction

Most symmetric searchable encryption schemes aim at allowing a user to outsource her encrypted data to a cloud server and delegate the latter to search on user's behalf. These schemes do not qualify as a secure and scalable solution for the multiparty setting, where users outsource their encrypted data to a cloud server and selectively authorize each other to search. Due to the possibility that the cloud server may collude with some malicious users, it is a challenge to have a secure and scalable multiparty searchable encryption (MPSE) [1] scheme.

Searchable Encryption enables users to perform keyword based search on an encrypted database just as in normal database transactions [2]. The scheme limited to the single user setting where the data owner who generates the database allows a single user to perform searches on it. To support multi-user searches, share the secret key for database searches among all users. The scheme [1] allows only one user to upload the data, though multiple users are able to search. Then delegate the server to search on their behalf by issue a trapdoor. The index contains a list of encrypted keywords, as well as some authorization information that selectively authorizes different users to search over this index. In the proposed scheme, an individual user can act as a data owner and/or a data follower. Data owner is the user who uploads the file and allows others to search. Data follower is the user who will be authorized by others to search their data.
MPSE scheme [1] doesn't support multi-keyword searching and the user who want to search, send the keyword in the form of an index or ID. For that the key should be shared between the data owner and the data follower in a

secure way. File updating is another one important problem in MPSE scheme. This paper presents a new approach to provide multi-keyword searching and it allows file updating. The keyword searching can also be done with checksum converted.

Most of the existing approaches discussed with searchable encryption schemes [9] and follow up with many others. In the work of Bao et al. A new party namely, a user manager is introduced into the system to manage multiple user search capabilities. In this, then the user manager [3] needs to be fully trusted since it is capable of submitting to search queries and decrypting encrypted data. Most of these work discussed about order preserving encryption [8] [5], where the cipher text preserves the order of the plaintext so each entity will perform associate equality comparison.

### 1.1 Problem Definition

Design a system to implement MPSE (multiparty searchable encryption) and its security properties and then to provide a scalable and secure construction.

## 2. Existing System

In paper [2] it is stated that, a promising approach to prevention of confidential data disclosures due to adversaries that compromise servers is to store only encrypted data on servers, and to encrypt and decrypt documents only on customer machines. In the event of a multi-user application, each user may cause admittance to a different set of text files stashed away on the host; this can be accomplished by insuring that each document is coded with a separate per-document key, and setting for each user's client machine to receive entree to the winders of the documents that the corresponding user has access to. One challenge with this advance lies in bearing applications that permit users to look for documents that carry a given word. Many applications, such as document sharing, chat, forums, and calendars, support search over documents shared by different users. Prior work on searchable encryption schemes would require the customer to supply the server with a search token under each key that a matching document might be encrypted with, and hence the number of tokens scales with the number of documents to search. This can be tedious when there are a great number of text files.

In paper [3] it is submitted that, searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a secret manner, while preserving the ability to selectively search over it. This problem has been the focus of active inquiry and several security definitions and expressions have been nominated. In this paper, we set out by reviewing existing notions of protection and propose new and stronger security definitions. We then present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our expressions are more effective than all previous buildings. Further, prior work on SSE only considered the setting where only the possessor of the data is capable of submitting search queries.

In recent years, ascribable to the appealing features of cloud computing, large amount of data has been stored in the swarm. Although cloud based services provide many advantages, privacy and protection of the sensitive data is a great worry. To mitigate the concerns, it is desirable to outsource sensitive information in coded configuration. Encrypted storage protects the data against illegal access, but it complicates some basic, yet important functionality such as the search on the data. To achieve search over encrypted data without compromising the privacy, considerable amount of searchable encryption schemes has been offered in the literature. Yet, virtually wholly of them handle exact query matching but not similarity matching; a crucial prerequisite for real world applications. Although some sophisticated secure multi-party computation based cryptographic techniques are available for similarity tests, they are computationally intensive and do not scale for large data sources. In paper [4], an efficient scheme for similarity search over encrypted data is offered. To do so, a state-of-the art algorithm for fast near neighbor search in high dimensional spaces called locality sensitive hashing is used.

## 3. Proposed System

In this paper propose a new approach known as Advanced Multi Party Searchable Encryption (Advanced MPSE), in which searching can be done based on ranking of all documents. Ranking based on TFIDF value of all documents.

The proposed scheme mainly consists of two main components:

**Storage server:** A server in which all the encrypted documents are stored.
**Key Server:** A server in which all the public keys and the authorization information are stored.

Advanced MPSE scheme consists of following operations:

1. TFIDF Calculation
2. Checksum Calculation
3. Encryption of documents
4. Searching of keyword
5. Decryption

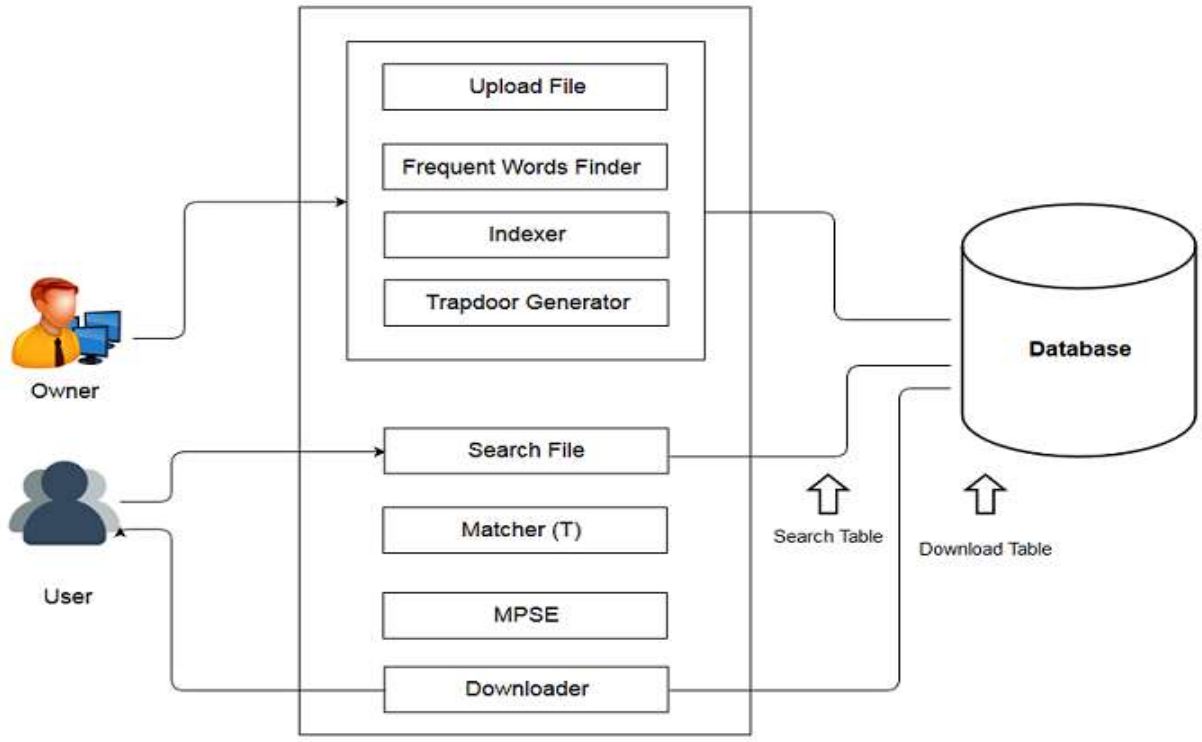


**Figure 1.** System Architecture

Key sharing is an important problem for MPSE scheme. I.e. the data follower wants a public key for the conversion of his keyword which is to be searched into index form. So this key retrieval should be done via a secure channel and also whenever the user wants the key, the owner should be ready to give the key. So the absence of the data owner affects this process. To overcome this problem, introduce a key server which has the responsibility for this key retrieval. When the follower wants the key, he should contact with the key server. If the user has the permission to access the document, then only the key server send the key for decrypting it.

Every document stored in index form; index in the sense which contains Ids of all the encrypted keywords within that document. Every data owner has the rights to search over his index because he has the corresponding key to decrypt it. There wouldn't be a key sharing between the data owner and follower so that the follower doesn't want to see the owners.

## 4. Algorithm

- **System Description:** Let S be the required system. S = {input, output, functions, success, failure} Input: Search Query Q = Q1, Q2, , Qn

- **Output:** Search Result R = File1, File2, .. , File n

- **Constraint:**
  1] User should search file with a valid trapdoor.
  2] User should be registered with the system.

- **Functions:**

Term Frequency (TF) and Inverse Document Frequency (IDF) are calculated for every uploaded document based on each keyword in that document for encryption.

$$TF = \frac{Total\ num.of\ documents}{Doc.containing\ particular\ word}$$

$$IDF = \frac{Num.of\ times\ the\ keyword\ appears}{Total\ num.of\ words\ in\ a\ doc.}$$

1] One user can upload many files. Hence one to many relationship is observed here
2] Many files can be accessed by many users. Hence many to many relationship is ob-served here.
3] One file can have many trap doors. Hence one too many relationships are observed here.

- **Success Conditions:** MPSE (multiparty search encryption) implemented successfully.

- **Failure Conditions:** MPSE (multiparty search encryption) not implemented successfully.

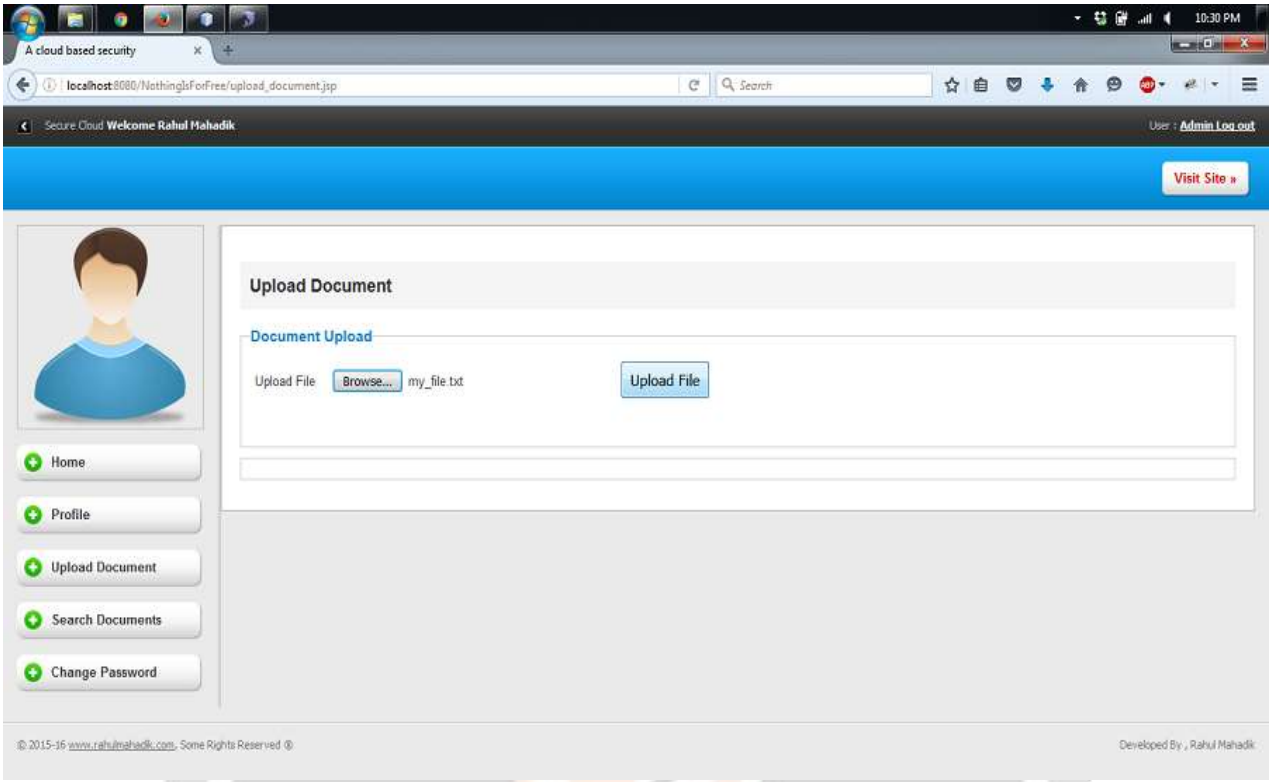


**Figure 2.** Upload File

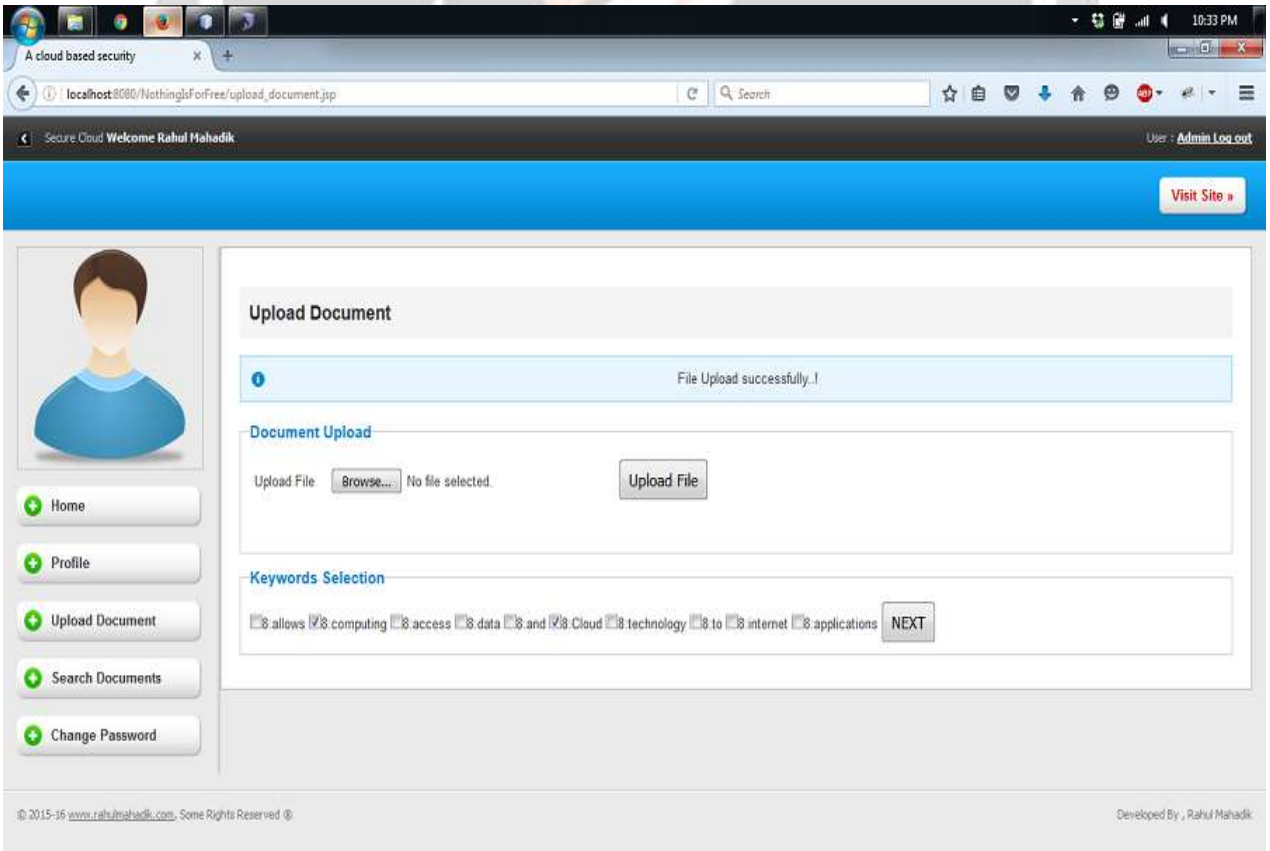


**Figure 3.** Trapdoor Generator

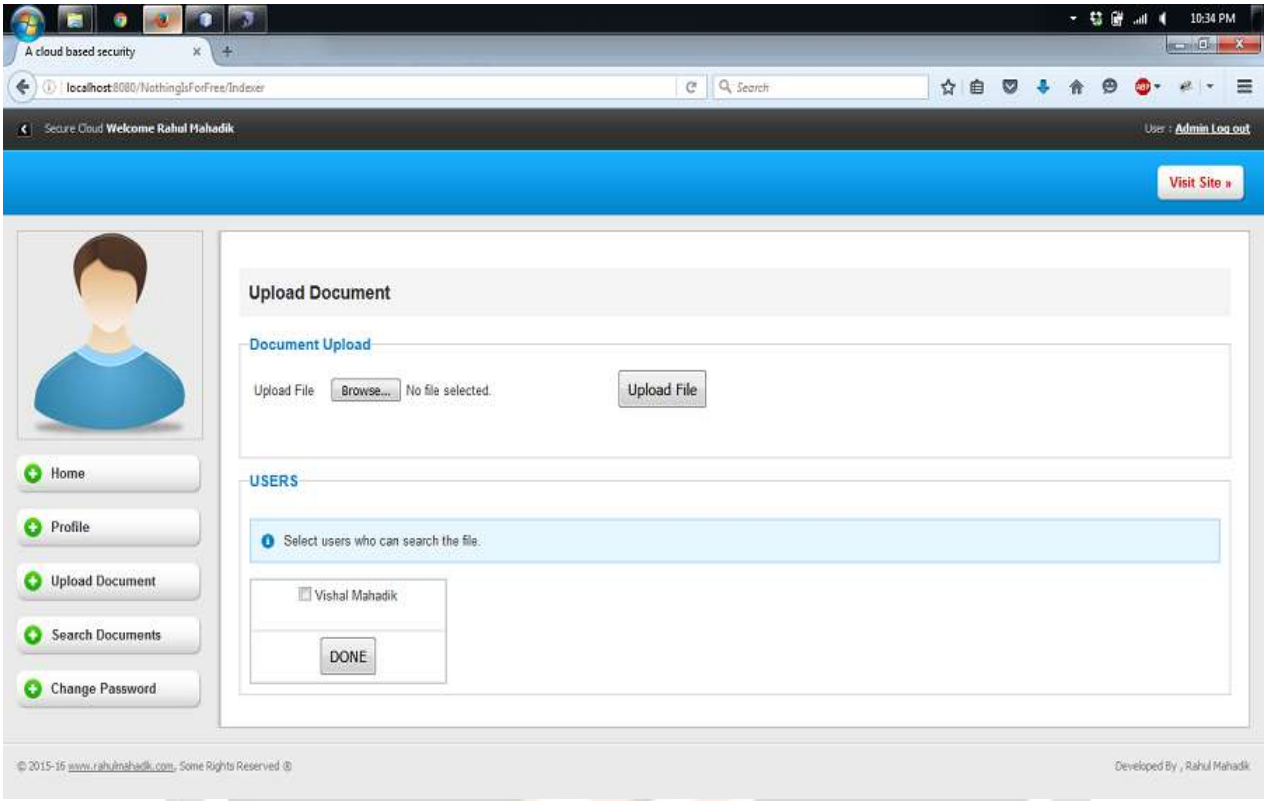


**Figure 3.** Select Users

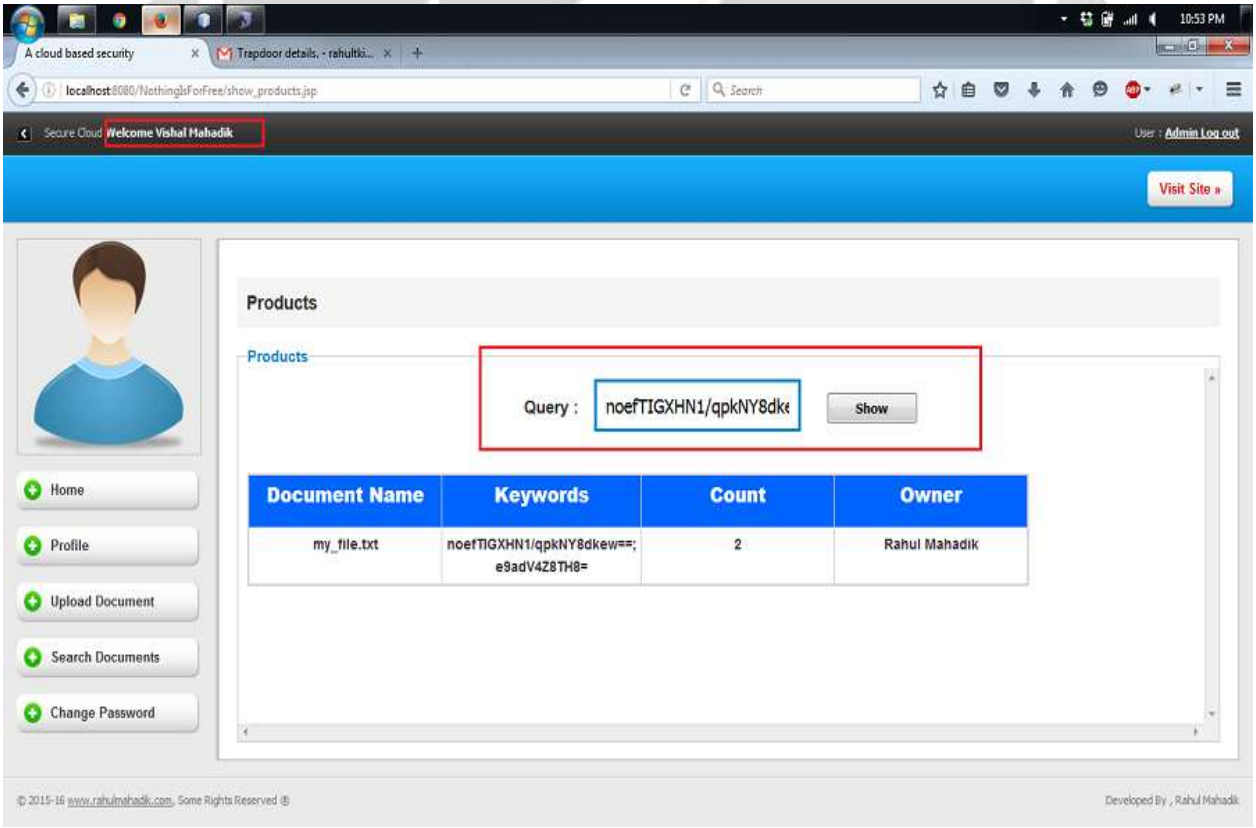


**Figure 4.** Search Data

## 5. Conclusion

The concept of searchable encryption provides a promising direction in solving the privacy problem when out sourcing 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. Conceptually, in the context of MPSE, an individual user can act as a data owner and/or a follower. As a data owner, data owner has more control over how the indexes are constructed. We introduce a Follow algorithm, which enables a data owner to assign a token to other authorized user's .With this token, other users search their documents without any further interaction with owner.

## 6. References

[1] Qiang Tang, "Nothing is for Free: Security in Searching. Shared and Encrypted Data," IEEE Trans. On Information Forensics and Security, Vol. 9, No. 11, Nov. 2014, pp. 1943-1952.

[2] R. Curtmola, J. Garay, S. Kamara, and R. Ostrovsky, "Searchable Symmetric encryption: Improved definitions and efficient constructions," in Proc. 13th ACM Conf. Comput. Commun. Security, 2006, pp. 79–88.

[3] F. Bao, R. H. Deng, X. Ding, and Y. Yang, "Private query on Pract. Encrypted data in multi-user settings," in Proc. 4th Int . Conf. Inf. Security Experience, vol. 4991. 2008, pp. 71–85.

[4] C. Bösch, Q. Tang, P. Hartel, and W. Jonker, "Selective document retrieval from encrypted database," in Proc. 15th Inf. Security Conf. (ISC), vol. 7483. 2012, pp. 224–241.

[5] Y.-C. Chang and M. Mitzenmacher, "Privacy preserving keyword searches on remote encrypted data," in Proc. 3rd Int. Conf. Appl. Cryptography Netw. Security, vol. 3531. 2005, pp. 442–455.

[6] M. Kuzu, M. S. Islam, and M. Kantarcioglu, "Efficient similarity search over encrypted data," in Proc. IEEE 28th Int. Conf. Data Eng., Apr. 2012, pp. 1156–1167.

[7] M. Raykova et al., "Usable, secure, private search," IEEE Security Privacy, vol. 10, no. 5, pp. 53–60, Sep./Oct. 2012.

[8] E. Shen, E. Shi , and B. Waters, "Predicate privacy in encryption systems," in Proc. 6th Theory Cryptography Conf. Theory Cryptography, vol. 5444. 2009, pp. 457–473.

[9] D. X. Song, D. Wagner, and A. Perrig, "Practical techniques for 2000, searches on encrypted data," in Proc. IEEE Symp. Security Privacy, May pp. 44–55.

[10] F. Bao, R. H. Deng, X. Ding, and Y. Yang,"Private query on Pract. Encrypted data in multi-user settings," in Proc. 4th Int. Conf. Inf. Security Experience, vol. 4991. 2008, pp. 71–85.

[11] A. Boldyreva, N. Chenette, Y. Lee, and A. O'Neill, "Order- preserving symmetric encryption," in Advances in Cryptology EUROCRYPT (Lecture Notes in Computer Science), vol. 5479, A. Joux, Ed. Berlin, Germany: Springer-Verlag, 2009, pp. 224–241.

[12] R. Agrawal, J. Kiernan, R. Srikant, and Y. Xu, "Order preserving encryption for numeric data," in Proc. ACM SIGMOD Int. Conf. Manage. Data, 2004, pp. 563–574.

[13] W. C. Barker and E. B. Barker, "Sp 800-67 Rev. 1. Recommendation for the Triple Data Encryption Algorithm Block Cipher," technical report, Nat'l Inst. of standards and Technology, 2012

[14] The MD5 Message-Digest Algorithm, RFC1321.

[15] Maha TEBAA, Saïd ELHAJJI, Abdellatif EL GHAZI, "Homomorphic Encryption Applied to the Cloud Computing Security" Proceedings of the World Congress on Engineering 2012 Vol I. WCE 2012, July 4, 2012, London, U.K