A Survey on Security in Searching Shared and Encrypted Data

Rahul Mahadik

Abstract— **Encryption is well established technology for safeguarding sensitive knowledge. Multiparty Searchable secret writing could be a theme during which multiple users store and share their knowledge with one another. The theme consists of 2 entities: A server and set of users. Achieving multiparty looking is difficult as existing schemes aren't achieving the secure searchable secret writing owing to the key sharing between set of users. Conjointly it's not forming ascendable resolution for multi-party looking and settings, wherever users source their encrypted knowledge to specific cloud server and by selection authorize one another to go looking. There are often an occasion that the cloud server could interact with some harmful users, it's a challenge to possess a safer and ascendable multiparty searchable secret writing (MPSE) theme. System then attempt to propose a MPSE theme by using the property linearity of Type-3 pairings and prove its security supported the bilinear Diffie–Hellman variant assumption within the oracle model. Moreover, the evaluations show the speed of planned theme compared with the previous MPSE theme with relevance looking and encryption/decryption.**

Index Terms—**Data Privacy, Multi-party Searchable Encryption (MPSE), Pairing, Security, Trapdoor Privacy.**

I. 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 the 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) scheme.

Due to the private nature of personal data, there is an inherent need for a user to selectively share her data with different recipients. In practice, what a user can do is to set some access control policies and then rely on the cloud server (e.g. Dropbox) to enforce them. Unfortunately, this approach is not realistic due to two reasons. One is that the users have no means to prevent the server from accessing their data. The other is that, even if the server is benign, it may also be forced to share users' data with other parties.

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 format an untrusted server, and then delegate the server to search on their behalf by issuing a trapdoor (i.e. Encrypted keyword). 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. A MPSE scheme allows every user to build an encrypted index for each of his documents and store it on 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.

To implement a more secured system by means of Encryption, keys of file, give access to file, retrieve access from file. And also if user tries to give false password more than 3 times while logging in to the account, it will be deleted. The account will renewed only by the real users. Our objective is first to formulate MPSE (Multiparty Searchable Encryption) and its security properties and then to provide a scalable and secure construction. To address these schemes, one needs to independently generate a key to protect each document (i.e. instantiate the scheme once for every document) and then shares the key with the users who will be authorized to search this document.

II. LITERATURE SURVEY

Without recognizing the underlying data contents searchable encryption allows an untrusted server to search on encrypted data. Traditional searchable encryption schemes focus only on a single keyword or conjunctive keyword search. To design more expressive search criteria, There are number of solutions have been recently proposed, but most of them are in the setting of symmetric key encryption. In this account, grounded on the composite-other groups, authors present an expressive and secure asymmetric searchable encryption (ESASE) scheme, which is the first that simultaneously supports conjunctive, disjunctive and negation search operations. They analyze the efficiency of ESASE and prove it is secure in the standard model. In sum, authors suggested that how ESASE could be extended to

ISSN: 2278 – 7798

support the range search and the multi-user setting [1].

Searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a clandestine fashion, while maintaining the ability to selectively search over it. This problem has been the focus of active inquiry and several security definitions and constructions have been made. In this report, authors set out by reviewing existing notions of protection and offer new and stronger security definitions.

They present two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our formulations are more effectual than all former constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. Here main consideration is the natural extension where an arbitrary group of parties other than the owner can submit search queries. Authors formally defined SSE in this multi-user setting, and present an efficient structure. [2]

A related scheme is the one of Bao et al. [3], whose consideration about setting where users have different keys, but all the information is encrypted with one key and the search happens over data encrypted with one key. I cannot directly apply their strategy for the multi-key setting by creating an instance of the scheme for every key because this results in many search tokens; the search tokens are tied to a secret different for every different key is the reason behind this scheme. Moreover, one requires different security definitions and security proofs when considering data encrypted under different keys with users only accessing a subset of them. [4]

III. Existing System

One challenge with this approach lies in supporting applications that allow users to search for documents that contain 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 client to provide the server with a search token under each key that a matching document might be encrypted with, and thus the number of tokens scales with the number of documents to search. This can be slow when there is a large number of documents.

In paper [3] it is stated that, searchable symmetric encryption (SSE) allows a party to outsource the storage of his data to another party in a private manner, while maintaining the ability to selectively search over it. This problem has been the focus of active research and several security definitions and constructions have been proposed. In this paper we begin by reviewing existing notions of security and propose new and stronger security definitions. Then they presented two constructions that we show secure under our new definitions. Interestingly, in addition to satisfying stronger security guarantees, our constructions are more efficient than all previous constructions. Further, prior work on SSE only considered the setting where only the owner of the data is capable of submitting search queries. We consider the natural extension where an arbitrary group of parties other than the owner can submit search queries.

In recent years, due to the appealing features of cloud computing, large amount of data have been stored in the cloud. Although cloud based services offer many advantages, privacy and security of the sensitive data is a big concern. To mitigate the concerns, it is desirable to outsource sensitive data in encrypted form. 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 have been proposed in the literature. However, almost all of them handle exact query matching but not similarity matching; a crucial requirement 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 [5], an efficient scheme for similarity search over encrypted data is proposed. To do so, a state-of-the art algorithm for fast near neighbor search in high dimensional spaces called locality sensitive hashing is utilized.

SSW scheme with similar security guarantees.[6] In recent years, due to the appealing features of cloud computing, large amount of data have been stored in the cloud. Although cloud based services offer many advantages, privacy and security of the sensitive data is a big concern. To mitigate the concerns, it is desirable to outsource sensitive data in encrypted form. 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 have been proposed in the literature. However, almost all of them handle exact query matching but not similarity matching; a crucial requirement 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 this paper, we propose an efficient scheme for similarity search over encrypted data. To do so, we utilize a state-of-the art algorithm for fast near neighbor search in high dimensional spaces called locality sensitive hashing. To ensure the confidentiality of the sensitive data, we provide a rigorous security definition and prove the security of the proposed scheme under the provided definition.

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

ISSN: 2278 – 7798

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. [7]

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). [8]

IV. PROPOSED SYSTEM

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). A detailed survey of searchable encryption schemes can be found in. In this work, we will be implementing multi-party searchable encryption (MPSE) schemes in the symmetric setting, which 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.

Due to the private nature of personal data, there is an inherent need for a user to selectively share her data with different recipients. In practice, what a user can do is to set some access control policies and then rely on the cloud server (e.g. Dropbox) to enforce them. Unfortunately, this approach is not realistic due to two reasons. One is that the users have no means to prevent the server from accessing their data. The other is that, even if the server is benign, it may also be forced to share users' data with other parties.

To implement a more secured system by means of Encryption, keys of file, give access to file, retrieve access from file. And also if user tries to give false password more than 3 times while logging in to the account, it will be deleted. The account will renewed only by the real users. Our objective is first to formulate MPSE (Multiparty Searchable Encryption) and its security properties and then to provide a scalable and secure construction. To address these schemes, one needs to independently generate a key to protect each document (i.e. instantiate the scheme once for every document) and then shares the key with the users who will be authorized to search this document.

V. CONCLUSION

In the formulation of MPSE, previous system assumed that authorization was granted on the index level, namely for each of our indexes we can determine 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 newfangled version of Multi Party Searchable Encryption Scheme which supports multi-keyword searching by means of homomorphic algorithm. The proposed system also avoids key sharing with the helper of a central server. All the uploaded documents can be stored in the encrypted configuration. File updating can also possible with the advanced MPSE scheme. The evaluations show the viability of the proposed mechanisms in comparing with MPSE scheme.

REFERENCES

[1] Zhiquan Lv1,2, Cheng Hong1, Min Zhang1, and Dengguo Feng1

[2] Feng Bao, Robert H. Deng, Xuhua Ding, and Yanjiang Yang. Private query on encrypted data inmulti-user settings. In ISPEC, pages 71–85, 2008.

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

[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] Q. Tang, Privacy preserving mapping schemes supporting comparison, in Proc. ACM Workshop Cloud Comput. Security Workshop , 2010, pp. 5358

[6] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, Public key encryption with keyword search, in Advances in Cryptology EUROCRYPT (Lecture Notes in Computer Science), vol. 3027, C. Cachin and J. Camenisch, Eds. Berlin, Germany: Springer-Verlag, 2004, pp. 506522

[7] 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.

[8] A. Boldyreva, N. Chenette, Y. Lee, and A. ONeill, Order-preserving symmetric encryption, in Advances in Cryptology-EUROCRYPT (Lecture Notes in Computer Science), vol. 5479

Rahul Mahadik received the B.E. Degree in Information Technology in 2014, From Tatyasaheb Kore Institute of Engineering and Technology, Warananagar. Now, Pursuing M.E. Degree in Computer Engineering from Imperial College of Engineering & Research, Wagholi in current academic year 2015-16.

ISSN: 2278 – 7798