Journal of Information Security and Applications 41 (2018) 124–133

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Fine-grained search and access control in multi-user searchable encryption without shared keys

Manju S Nair[a,*], Rajasree M.S[b]

[a] College of Engineering Trivandrum, India
[b] Government Engineering College Barton Hill, India

ARTICLE INFO

Article history:

Keywords:
Cloud storage
Multi-user searchable encryption
Bilinear map accumulator
Fine-grained access control
Pairing based cryptography

ABSTRACT

Searchable encryption schemes enable secure sharing and efficient retrieval of encrypted documents stored in the cloud. Multi-user symmetric searchable encryption allows multiple users to upload encrypted data to the cloud and selectively authorize other people to search and retrieve documents without revealing any information about either the search query or sensitive information. This however, poses major challenges since it involves managing the access control policies of a set of users by a third party. Selectively sharing files among an arbitrary set of users is more challenging than allowing all members of a group to access a set of documents. The proposed scheme ensures that the search returns only those documents that are accessible to the querier and guarantees that only authorized users are allowed to decrypt a document. A bilinear map accumulator combined with pairing based cryptography ensures that only authorized users can decrypt a shared document. Prior schemes have addressed the problem using shared keys or by using trusted third parties. The proposed scheme supports both keyword searches and selective sharing of data among multiple users in the cloud without requiring shared keys or trusted third parties. The security of our scheme is proved using rigorous security analysis.

1. Introduction

Advancement in internet technology has made cloud storage a promising technology which offers several advantages such as high accessibility, usability and disaster recovery. At the same time it removes the burden of infrastructure management and handles large scale data in a very cost effective manner. Increasingly, people are relying on cloud for various services and are willing to move their data to the cloud due to it's versatility; the ability to access data from anywhere at any time using simple hand held devices. Many business organizations generally outsource their storage requirement to the cloud as a solution to tackle with the Big Data demand. The major concern however in moving data to the cloud are issues regarding the privacy and security [1,2] of sensitive data since the data is with the third party, the cloud provider. Cloud storage is also listed as the most risky cloud application according to "The Cloud Usage: Risks and Opportunities Report" [3] from the Cloud Security Alliance.

The canonical way of dealing with this issue of security is to retain the control of data with the data owner and ensure security and privacy by encrypting [4] the data. Encryption is one of the essential privacy enhancing technologies that could be explored and employed in the cloud computing Big Data environment. Data centric protection through encryption renders the data inaccessible to anyone who does not have the key to decrypt it. Encryption also renders the data in such a way that no computation can be performed on it. Moreover, homomorphic encryption schemes that support computations to be carried out on cipher text and producing encrypted results are computationally very intensive, require large storage overhead and has not proven to be practical as yet. One of the major requirements when we outsource data to the cloud is to selectively retrieve the documents based on some keywords.

Searchable encryption schemes [5–9] are cryptographic primitives that support search on encrypted data stored in a remote storage without revealing the search query or any other information about the sensitive data. Moreover, the area of encrypted search [10] has emerged as one of the most exciting and potentially powerful tool, particularly for Big Data analytics, supporting full search capability without disclosing any private information. For supporting fast and efficient retrieval of information, most of the practical searchable encryption schemes [5] use an encrypted index. To search for a keyword the client generates a trapdoor using a secret key and the keyword to be searched and sends it to the provider. Using this trapdoor the cloud provider retrieves the

* Corresponding author.
E-mail address: manjusnair@cea.ac.in (M.S. Nair).

https://doi.org/10.1016/j.jisa.2018.06.006
2214-2126/

documents containing the keyword without knowing the search query or any other information. The two common approaches are, one is constructing a single master inverted index for all the documents in the set or constructing separate index for each document in the set. The first approach result in highly efficient search protocol with sub linear search complexity. However, the downside is that it is less flexible in handling dynamic data and multi-keyword ranked queries. On the other hand the second approach offers better flexibility in handling dynamic data as well as conjunctive queries, but the search complexity is linear to the total number of documents in collection. The major research challenges involved in searchable encryption schemes are briefly outlined below.

- Handling of conjunctive queries and query expressiveness. Query expressiveness refers to supporting rich queries such as queries supporting wild characters, ranges, subset, and comparison.
- Supporting multiple user's needs. Enterprises require outsourced data to be accessed by multiple clients based on authorized access control policies.
- Managing dynamic data. Techniques to update encrypted index to handle dynamic data should not cause any additional leakage and should be optimal.
- Handling massive data sets. This require low complexity search protocol with highly parallelizable implementation.
- Efficient ranking techniques are desirable to ensure the relevance of results and to reduce the communication cost.
- Managing unstructured data like image collections, videos, and social network data which exhibit a different and more complex structure.
- Factors such as such as I/O latency [11] and storage utilization should be considered which will otherwise degrade the practical performance. Techniques and data structures used to reduce information leakage can result in more disk access and communication between server and client which can adversely affect the performance of the search protocol.

Theoretical expectation of security for a searchable encryption scheme is that there should not be any leakage of information. Oblivious RAM [12] based solution addresses this issue to an extent by hiding all information, but the high communication overhead, and the storage requirement make this scheme less efficient for practical application. Hence the tradeoff is between efficiency and information leakage. Encryption of documents, index, and queries ensures the privacy of the same from any outsider, but a statistical analysis over the access and search pattern can uncover a significant amount of sensitive data. Symmetric encryption schemes are widely recommended to be used in the cloud and Big Data environments due to the security and efficiency offered.

The proposed system addresses the problem in a multi-user scenario where a user is allowed to outsource the encrypted documents to the cloud and selectively authorize other users to access it. However, the most challenging point here is that no entity in the system can be fully trusted. Therefore, managing access control policies of dynamic users by a third party is very challenging. A naive way to enforce data access without depending on the cloud provider is to distribute the corresponding decryption key to authorized users. This approach however, does not scale well when the number of documents and users increases. Further it makes the user revocation expensive.

Extending single user symmetric searchable encryption(SSE) to multi-user symmetric searchable encryption(MSSE) also has to address the security threats caused by the possibility of malicious users colluding with the cloud server. Cloud server can collude with a dishonest user and may try to access files beyond their access privileges by combining the secret key values each one poses. Further they can learn the keys of other users and decrypt all encrypted data.

The two major requirements in extending SSE to MSSE are, providing fine grained search and access control to authorized users. Enforcing fine grained search control involves allowing only authorized users to generate valid trapdoors for searching and providing only those document-ids that are made accessible to him by the data owner containing the keyword as search result. Providing fine-grained access control ensures that only the selected set of users authorized by the owner can decrypt a document. Sharing encryption keys and trapdoor generation key among a set of users can support data sharing without loosing confidentiality. However, sharing key among multiple users will make user revocation expensive, needs efficient key management schemes, and further the key exposure by a malicious user can lead to system failure. From the users perspective, key sharing also has the disadvantage of having to keep several keys to access multiple user's data. The number of keys to be stored scales with the number of files shared by other users. This in turn can prevent the user from using inexpensive hand held devices for accessing cloud data from anywhere.

In traditional broadcast encryption based access control schemes, the symmetric key of a document is encrypted using the public keys of all permitted users. This meta data is added along with each document to support sharing of a document. But the size of the meta data associated with each file increases with the number of users who can access the file. Compared with pairing based broadcast encryption scheme [13], the proposed system has no header part associated with each document and the decryption requires only a single paring operation which is an important factor while using simple hand held devices.

Elegant cryptographic techniques like attribute based encryption can provide fine grained access control in MSSE. However, re-encryption of data and re-distribution of keys are required in case of user revocation, which are computationally very expensive. In addition to this in CP-ABE, the computational overhead in decrypting the documents increases with the number of attributes in the access policy and the length of the secret key increases linearly with the number of attributes.

Absence of practical homomorphic encryption schemes and management of data by a third party makes the problem very challenging with several factors to be addressed as highlighted above. In this paper we have addressed the problem of providing fine grained search control and access control to a set of users without using shared keys or trusted third parties.

The discussion above highlights the complexity of the problem which this study attempts to address. The proposed system is divided into two modules based on the requirements mentioned above and to reduce the design complexity.

1.1. Our contributions

The strengths of the proposed multi-user searchable encryption scheme are

- Any user can flexibly and selectively share encrypted documents with an arbitrary set of users without distributing data encryption keys and trapdoor generation keys.
- Our system supports both secure sharing of data at document level and keyword search by multiple users.
- The scheme doesn't require any central authority or group manager, the system is entirely distributed and any user can flexibly share files with an arbitrary number of users.
- Efficient user revocation. The revocation of a user doesn't require key renewal or a major change in the encrypted index and hence will not affect other non revoked users