International Conference on Modern Trends in Engineering Science and Technology
© 2019 IJSRSET | Volume 5 | Issue 5 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section : Engineering and Technology

Efficient and Searchable ABE Scheme in Cloud Computing

Navin Sethiya[1], Hrishikesh Patel[1], Akshay Harshe[1], Alekh Gaigole[1], Harshvardhan Donadkar[1], Prof. Priya Karemore[2]

[1]UG Scholar, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of Computer Technology, Priyadarshini College of Engineering, Nagpur, Maharashtra, India

ABSTRACT

Searchable Attribute based encryption is a promising technique that achieves flexible and fine-grained data access control over encrypted data, which is very suitable for a secure data sharing environment such as the currently popular cloud computing. However, traditional attribute-based encryption fails to provide an efficient keyword based search on encrypted data, which somewhat weakens the power of this encryption technique, as search is usually the most important approach to quickly obtain data of interest from large-scale dataset. To overcome this issue, the fundamental way is to do encryption of data. So, a secure user can have imposed with data access control system must be given before the users store any data to the cloud for storage. Attribute Based Encryption (ABE) system is one of the asymmetric key based cryptosystems that has received much focus that provides fine-grained access control to data outsourced on the cloud. In this paper, we propose a more proficient and most important type of Attribute Based Encryption technique that not only considers the Outsourced ABE construction but also address the issue of revocation in case of user leaving the group or organization; once a user is removed from the group, the keys are updated and these updated new keys are shared between the existing users also our system supports the keyword search over encrypted data in the mobile cloud storage. In multi keyword search; users and data owners can establish the keywords index and search trapdoor, respectively, without relying on the online trusted authority. Experimental results show that the performance of the proposed system is better than existing system in terms of security, data availability, time consumption and memory utilization.

Keywords : Attribute-Based Encryption, Cloud Computing, Searchable Encryption, Attribute Revocation.

I. INTRODUCTION

Cloud Computing is received as another option to conventional data innovation due to its intrinsic resource-sharing and low-maintenance attributes. In cloud computing, the cloud service providers (CSPs, for example, Amazon), can provide different services to cloud clients with the assistance of intense datacenters. By combining the local data management frameworks into cloud servers, clients can appreciate top notch services and recovery huge speculations on their nearby infrastructures. Data storage is a basic service provided by cloud system. By making use of the cloud, the users can be completely released from the troublesome local data storage and maintenance. Also, it also has a significant risk to the confidentiality of those stored files. Specifically, the cloud servers managed by cloud providers are not trusted totally by

users while the data files stored in the cloud may be sensitive and confidential, such as business plans. To provide data privacy, as basic solution is to encrypt data files, and then upload the encrypted data into the cloud. Unfortunately, designing an efficient and secure data sharing methodology for
groups in the cloud is not an easy task due to the following challenging issues.

First, identity privacy is the major downfall for the development of cloud computing. Without any security of identity privacy, users may be unwilling to join in cloud computing systems because their real identities could be easily disclosed to cloud providers and attackers. Second, it is highly recommended that any member in a group can be able to use the data storing and sharing services given by the cloud, which is defined as the multiple-owner manner. Compared with the single-owner manner, in which only the group manager can store and modify data in the cloud, the multiple-owner manner is more flexible in real time applications. Last but not least, groups are dynamic in practice. The modifications of membership make secure data sharing very difficult. At one end, the anonymous system challenges new granted users to learn the content of data files stored before their participation, due to its not possible for new granted users to contact with unknown data owners, and obtain the corresponding decryption keys. At other end, an efficient membership revocation mechanism without updating the secret
keys of the other users is also desired to minimize the complexity of key management.

To solve this issue, information which is to be stored is encoded in scrambled form. However such encoded data must be agreeable to the sharing and access control. Various private and public key cryptographic techniques are not responsive to scalable access control. In order to solve this issue Revocable and Searchable Attribute Based Encryption technique was proposed. Attribute Based Encryption (ABE) has gained much attention in the research community. Attribute Based Encryption is an asymmetric key based cryptographic technique which improves the skillfulness of access control mechanisms.

In a Revocable Searchable ABE framework, a user's keys as well as ciphertext are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match in the attributes of the ciphertext and the user's key.

However, a raw in the standard ABE system is the huge size of the ciphertext and the computational complexities in decryption phase are highly taxing. So, there is a need to enhance the proficiency of ABE. To solve this issue, an efficiently revocable and searchable ABE (RSABE) scheme for the mobile cloud storage is proposed. Keyword search is also supported, in which data owners and users can generate the keywords index and search trapdoor, respectively, without relying on always online trusted authority.

Literature review is described in the section II. Section III presents the proposed system implementation details which includes searchable encryption, attribute revocation algorithm. Section IV presents experimental analysis, results and discussion of proposed system. Section V concludes our proposed system. While at the end list of references paper are presented.

II. LITERATURE REVIEW

Y. Li, F. Zhou, Y. Qin, M. Lin, and Z. Xu, [1] Here Secure Encryption is such a cryptographic primitive that enables users to search keywords over the encrypted data without leaking keywords information. In this paper, the keyword search is supported and then the access structure is partially hidden to protect privacy information in cipher texts is proposed.

Author's D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.-C. Rosu, and M. Steiner [2] present Dynamic searchable encryption in very large databases: Data structures and implementation, in Proc. of NDSS, vol. 14, 2014. In this paper[2], the author proposed a dynamic searchable encryption scheme. In their construction, newly added tuples are stored in another database in the cloud, and deleted tuples are recorded in a revocation list. The final search result is achieved through excluding tuples in the revocation list from the ones retrieved from original and newly added tuples. Yet, Cash et al. dynamic search scheme does not realize the multi-keyword ranked search functionality.

In paper [3] J. Lai, R. Deng, C. Guan, and J. Weng, Attribute-based Encryption with Verifiable Outsourced Decryption, the authors considered another necessity of ABE with outsourced decryption that is the verifiability of transformations. Informally, it makes sure that a user can efficiently check if the transformation is done accurately or not. Their system demonstrate that the new scheme is both secure and verifiable, without depending on random predictions. In their work, they propose a different view for ABE that, all things considered, wipes out the overhead for clients. However their construction does not consider overhead computation at the attribute authority involved in the key-issuing process.

Here, Green et al. [4] proposed an ABE system with outsourced decryption that to a great extent takes out the decryption overhead for clients. In such a system, a user provides an untrusted server, say a cloud service provider, with a transformation key that permits the cloud to translate any ABE ciphertext fulfilled by that users attributes or access policy into a simple ciphertext, and it just brings about a little computational overhead for the user to recover the plaintext from the changed ci-phertext. Security of an ABE system with outsourced decryption ensures that an adversary (Including a malicious cloud) wont have the capacity to learn anything about the encrypted message; in any case, it doesnt promise the correctness of the transformation performed by the cloud.

In this paper [5], Yu et al. consider the issue of user revocation which involves re-encrypting the data that is accessible to the user leaving the system and updating the private keys of users remaining in the system. They have proposed a scheme that enables the owner of the data to outsource the task of re-encryption and private key updates to a third party without revealing the content and the user information. They have very well attained the finely grained and scalable access in cloud computing. However the complexity in user revocation increases with the increase in the number of users which makes the system complex. In addition, their scheme does not support user accountability.

Cheung et al.[6] have proposed yet one another type of Attribute Based Encryption scheme known as ciphertext policy attribute based encryption (CP-ABE) where every secret key is labelled with attributes, and each ciphertext is set with an access policy. Decryption is done if and only if the clients trait set satisfies the ciphertext access structure. This gives _ne-grained access control on shared data in various practical settings, including secure databases and secure multi-cast. In this paper, they consider CP-ABE plans in which access structures are AND gates on positive and negative characteristics. Their principal plan has been proved to be chosen plaintext attack (CPA) secure under the decisional bilinear Diffie-Hellman assumption but the use of independent instances of CP-ABE encryption, and also the security of this proposal remains as an open problem.

In this paper [7], the V. Goyal, O. Pandey, A. Sahai, and B. Waters authors proposed a cryptosystem that provides _ne-grained access control to encrypted information that they called Key- Policy Attribute Based Encryption (KP-ABE). In their cryptosystem, ciphertext are labelled with sets of characteristics and private keys are set with access structures that control which ciphertext a user is able to interpret. They have applied their construction in forensic analysis and broadcast encryption. However their systems fails to hide the attributes that does the encryption. Hence the issue of attribute hiding is left open.

Here Curtmola et al.in [8] proposed two schemes (SSE-1 and SSE-2) which achieve the optimal search time. Their SSE-1 scheme is secure against chosen-keyword attacks (CKA1) and SSE-2 is secure against adaptive chosen-keyword attacks (CKA2). These early works are single keyword boolean search schemes, which are very simple in terms of functionality. Afterward, abundant works have been proposed under different threat models to achieve various search functionality, such as single keyword search, similarity search, multi-keyword boolean search, ranked search, and multi-keyword ranked search, etc.

The notion of ABE was proposed in this paper [9] as fuzzy version of Identity Based Encryption (IBE). In Fuzzy IBE, Sahai et al. view identity as a set of realistic qualities. A Fuzzy IBE arrangement considers a private key for an identity, to translate a ciphertext mixed with an identity w, if and only if the identities w and w are close to each other judged by some metric. A Fuzzy IBE arrangement can be joined with secure encryption using biometric inputs as identities; the breach resistance property of a Fuzzy IBE arrangement is precisely what considers the use of biometric identities, which typically will have some commotion each time they are investigated. Besides, they show that Fuzzy-IBE can be used for a sort of utilization that they term attribute based encryption. In this paper they demonstrate two advancements of Fuzzy IBE arranges. Their advancements can be seen as an Identity-Based Encryption of a message under a couple of characteristics that make a (soft) character. Their IBE arrangements are both oversight tolerant and secure against plot attacks. Besides, the key advancement does not use arbitrary prophets. Creator exhibit the security of their arrangements under the Selective-ID security model.

Searchable encryption schemes[10] enable the clients to store the encrypted data to the cloud and execute keyword search over ciphertext domain. Due to different cryptography primitives, searchable encryption schemes can be constructed using public key based cryptography or symmetric key based cryptography.

III. PROPOSED APPROACH

Problem Statement

We formally define our problem as follows.

1. Attribute-based encryption (ABE) is suitable for mobile cloud storage to protect data confidentiality and realize fine-grained data access control.

2. It is essential for ABE schemes to achieve attribute revocation as users' attributes may be changed frequently.

3. Keyword search over encrypted data also needs to be solved in the mobile cloud storage. In addition, computational efficiency is a consideration for the resource-constrained mobile device.
4. In other words, with the emergence of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data.

To achieve this, we propose a secure, searchable and efficient ABE technology to provide flexible access control of encrypted data stored in the cloud that overcomes the drawbacks of existing ABE schemes.

Proposed System Overview

1. Attribute Based Encryption (ABE): Attribute-based encryption (ABE) is type of public-key cryptography. In traditional public-key cryptography, a message is encrypted for a specific receiver using the receivers public-key. Identity-based cryptography and in particular identity-based encryption (IBE) changed the traditional understanding of public-key cryptography by allowing the public-key to be an arbitrary string, e.g., the email address of the receiver. ABE goes one step further and defines the identity not atomic but as a set of attributes, e.g., roles, and messages can be encrypted with respect to subsets of attributes (key-policy ABE - KP-ABE) or policies defined over a set of attributes (ciphertext-policy ABE- CP-ABE). The key issue is, that someone should only be able to decrypt a ciphertext if the person holds a key for "matching attributes" where user keys are always issued by some trusted party. Ciphertext-Policy ABE and Key-Policy ABE are two types of ABE.

2. Outsourced Key-issuing: The tasks of attribute authority are decreased by out-sourcing the key-issuing task to a third party by delegating the task of issuing private keys for users to a Key Generation Service Provider to reduce the local overhead.

3. User revocation: If a user leaves a system, he should no longer have the access to the files and this issue is taken care of by the revocation feature that revokes the user that is no longer the part of the system.

4. Searchable Encryption

Searchable encryption (SE) allows a server to perform search over encrypted data according to a search token submitted by a data user.

The Fig. 1 shows the proposed system architecture.

1. Existing system provide a ABE scheme simultaneously supporting outsourced key issuing and decryption. With the aid of KGSP and DSP, this scheme achieves constant efficiency at both authority and user sides.

2. Limitations of Existing System:
(a) System does not provide user revocation.
(b) ABE schemes are not able to simultaneously achieve efficient attribute revocation and keyword search.

3. The contributions of our scheme can be concluded as follows.

(a) An RSABE scheme is proposed, which simultaneously supports efficient attribute revocation, and keyword search in mobile cloud environment.
(b) The system provides an immediate revocation method with high efficiency. In RSABE scheme, the attribute authority securely delegates the most update tasks to cloud server. During the whole revocation, the secret key component that user holds keeps

unchanged, which brings great convenience for mobile users.

(c) The system also supports solution to search keywords on the encrypted data. The cloud server will return the search results only when the keywords and indexes are matched and the attributes set of user satisfies the access policy in ciphertext. Moreover, data owner and user can generate the keywords index and search trapdoor respectively without relying on trusted third party.

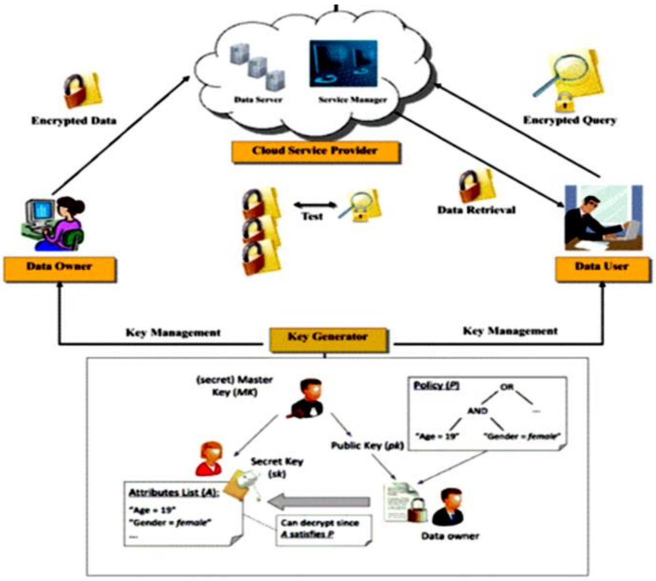

Figure 1.Proposed System Architecture

Algorithm

1) ABE Algorithm

a) ABE Setup: The setup algorithm takes as input a security parameter I. It outputs a public key PK and a master key MK.

b) KeyGen : For each users private key request, the initialization algorithm for delegated key generation takes as input an access policy (or attribute set) and the master key MK. It outputs the key partial transformation key.

c) To achieve the same results with less time Encrypt: The encryption algorithm takes as input a message M and an attribute.

d) Decrypt: the decryption algorithm takes as input the ciphertext (ct) and the private key sk. It outputs the original message M.

e) User revocation: when there is a user to be revoked, aa updates affected users' private keys with the help of KGSP.

IV. RESULTS AND DISCUSSION

A. Experimental Setup

All the experimental cases are implemented in Java in congestion with Netbeans tools and MySql as backend, algorithms and strategies, and the competing rule generation approach along with various encryption technique, and run in distributed environment with Master System having configuration of Intel Core i5-6200U, 2.30 GHz Windows 10 (64 bit) machine with 8GB of RAM and Slave System with configuration of Intel Core i5-2430M, 2.40 GHz Windows 7 (64 bit) machine with 4GB of RAM.

B. Dataset Description

The Input for Project is real time dataset such as news dataset or email dataset from the UCI Machine Learning Repository, News Dataset is a text data set which contains sports and political related data.

C. Result and Discussion

Table 2 show the attribute / parameters comparison between similar type of system.

Table 2. Result Comparison with Similar System

Parameters	Proposed System	Base Paper [1]	Paper [8]
Keyword Search	✓	✓	×
REVOCATIO N	Attribute Level And User Level Revocatio n	Attribute Level Revocatio n	System Level User Revocatio n
ACCESS CONTROL	LSSS	LSSS	AND Gate

V. CONCLUSION AND FUTURE SCOPE

The most important aspect that is to be considered in storing data is the security mechanisms associated with it. The proposed system presents a revocable and searchable Attribute Based Encryption scheme that is much more efficient than the previous systems. It provides security for appropriate users by using the user based access control attributes. In order to reduce the computation overhead of the user, the system provides modified outsourced ABE scheme which supports the outsourced key-issuing and decryption by utilizing Key Generation Service Provider. One of the advantage of system is that is supports secure searching over encrypted data. Results show that our system is proficient as well as practical.

VI. REFERENCES

[1] Y. Li, F. Zhou, Y. Qin, M. Lin, and Z. Xu, \Integrity veriable conjunctive keyword searchable encryption in cloud storage," Int. J. Inf. Secur., vol. 17, pp. 1 20, Nov. 2017, doi: 10.1007/s10207-017-0394-9.

[2] D. Cash, J. Jaeger, S. Jarecki, C. Jutla, H. Krawczyk, M.- C. Rosu, and M. Steiner, "Dynamic searchable encryption in very large databases: Data structures and implementation", in Proc. of NDSS, vol. 14, 2014.

[3] J. Lai, R. Deng, C. Guan, and J. Weng, Attribute-based Encryption with Verifiable Outsourced Decryption Trans. Inf. Forensics Security, vol. 8, no. 8, pp. 1343-1354, Aug. 2013.

[4] M. Green, S. Hohenberger, and B.Waters, \ Outsourcing the decryption of ABE ciphertexts," in Proc. 20th USENIX Conf. Secur. (SEC). Berkeley, CA, USA: USENIX Association,2011, p. 34.

[5] S. Yu, C.Wang, K. Ren, and W.Lou, Achieving Secure, Scalable, Fine-Grained Data Access Control in Cloud Computing, in Proc. IEEE 29th INFOCOM, 2010, pp.534-542.

[6] L. Cheung and C. Newport, Provably Secure Ciphertext Policy ABE, in Proc. 14th ACM Conf. CCS, 2007, pp. 456- 465.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, Attribute- Based Encryption for Fine-Grained Access Control of Encrypted Data, in 2006, Proc. 13th ACM Conf. Comput. Commun. Security, pp. 89-98.

[8] 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 Computer and communications security. ACM, 2006, pp. 79-88.

[9] A. Sahai and B. Waters, Fuzzy Identity-Based Encryption, in Proc. Adv. Cryptol.-EUROCRYPT, LNCS 3494, R. Cramer, Ed., Berlin, Germany, 2005, pp. 457-473, Springer-Verlag.