International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 8 | ISSN : 2456-3307
DOI : https://doi.org/10.32628/CSEIT183895

Survey on Regenerating Code Based Revocable and Searchable ABE Scheme for Mobile Cloud Storage

Jayesh Sahebrav Patil*, Prashant Mininath Mane
Department of Computer Engineering, Zeal College of Engineering & Research, Savitribai Phule University, Pune, Maharashtra, India

ABSTRACT

From the time in memorial, Information Security has remained a primary concern and today when most of the sensitive data is stored on Cloud with client organization having lesser control over the stored data, the fundamental way to fix this issue is to encrypt such data. So, a secure user imposed data access control system must be given, before the users outsource any data to the cloud for storage. Attribute Based Encryption (ABE) system is one such asymmetric key based cryptosystem that has received much attention that provides fine-grained access control to data stored on the cloud. In this paper, we propose a more proficient and richer type of Attribute Based Encryption technique (RSABE) that not only considers the Outsourced ABE construction but also address the issue of revocation in case of change of attributes of the group user or organization; once a user is removed from the group, the keys are updated and these new keys are distributed among the existing users also our system supports the Keyword search over encrypted data in the mobile cloud storage. In multi keyword search; data owners and users can generate the keywords index and search trapdoor, respectively, without relying on always online trusted authority. Experimental results prove that the performance of the proposed system is greater than existing system in terms of security, time consumption and memory utilization & data availability.

Keywords : Attribute Based Encryption, Cloud Computing, Revocation, Searchable Encryption, Data Availability.

I. INTRODUCTION

Cloud Computing perceived as another option to conventional data innovation because of its intrinsic resource-sharing and low-maintenance attributes. In cloud computing, the cloud service providers (CSPs, for example, Amazon,) can send different services to cloud clients with the assistance of intense data centers. By combining the local data management frameworks into cloud servers, clients can appreciate top-notch services and recovery of 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. In addition, it also has a significant risk to the confidentiality of those stored files. Specifically, users do not trust the cloud servers managed by cloud providers totally, 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. Finally yet importantly, 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 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 skill-fullness 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 flaw in the standard ABE system is the huge size of the ciphertext and the computational complexities in decryption phase are highly taxing. Therefore, 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. Our proposed system also considers the revocation of users in the system to achieve authenticity and privacy.

The organization of this document is as follows. Section II presents the literature survey of research papers. While section III present proposed research findings and analysis of those findings. Section IV presents conclusion of research work. Section V presents the research paper.

II. LITREATURE SURVRY

In paper [2] author Y.Li, F. Zhou proposed Secure Encryption scheme; they stated that 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 ciphertexts is proposed.

In paper [3], 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 [4] 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.

In Paper [5], Green et al. 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 user's 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 ciphertext. Security of an ABE system with outsourced decryption ensures that an adversary (Including a malicious cloud) won't have the capacity to learn anything about the encrypted message; in any case, it doesn't promise the correctness of the transformation performed by the cloud.

In paper [6], 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. [7] 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 fine-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 paper [8], the authors proposed a cryptosystem that provides fine-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.

In Paper [9] Curtmola et al. 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.

[10] The notion of ABE was proposed in this paper 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 we 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.

In paper [11] authors proposes searchable encryption schemes that 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. SYSTEM OVERVIEW

A. System Architecture

Fig. 1 shows the proposed system architecture.

The contributions of our scheme are as follows.

A) An RSABE [1] scheme is proposed. Which simultaneously supports efficient attribute revocation, and keyword search in mobile cloud environment.

B) The system provide 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.

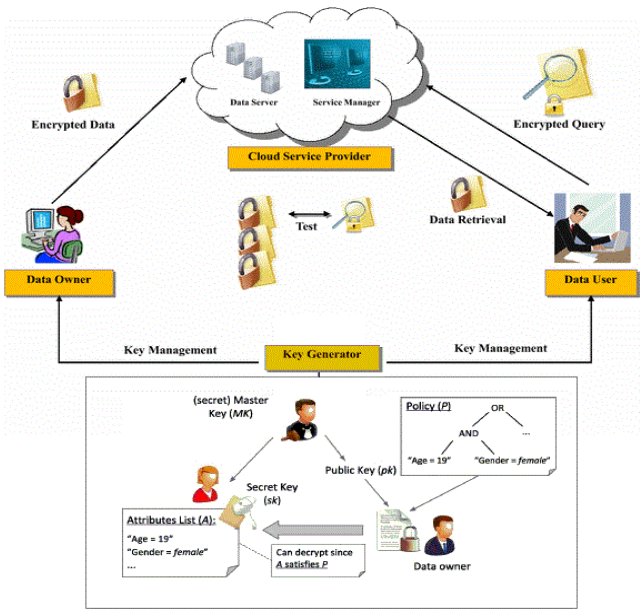

Figure 1. System Architecture

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.

D) To Improve Data Availability Erasure Codes are used.

IV. CONCLUSION

The proposed system presents a revocable and searchable Attribute Based Encryption with data recovery using erasure codes, which 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 ABE scheme which supports the outsourced key issuing by utilizing Key Generation Service Provider. One of the advantage of system is that it supports secure searching over encrypted data. In addition, system provides data recovery, if encrypted data stored at cloud server is modified or corrupted.

V. REFERENCES

[1] Shangping Wang1, Duo Zhang2, Yaling Zhang3, and Lihua Liu4, "Efficiently Revocable and Searchable Attribute-Based Encryption Scheme for Mobile Cloud Storage", in IEEE Access, vol. 6, pp. 30444-30457, 2018.

[2] Y. Li, F. Zhou, Y. Qin, M. Lin, and Z. Xu, "Integrity-verifiable 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.

[3] 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.

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

[5] 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.

[6] 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.

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

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

[9] 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.

[10] 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.

[11] D. Boneh, G. Di Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search", in Advances in Cryptology-Eurocrypt 2004. Springer, 2004, pp. 506-522.