© 2019 IJSRST | Volume 6 | Issue 4 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST196446

ABE Technique and Erasure Code for Secure Cloud Storage with Revocation

Jayesh Sahebrav Patil*, Prof. Prashant Mininath Mane, Dr. S. M. Sangve
Department of Computer Engineering, ZCOER, Narhe, Pune, Maharashtra, India

ABSTRACT

Now a day, Information Security has primarily more attractive concern and today when most of the sensitive data is stored on Cloud with client organization having lesser control over the outsourced data, the fundamental way to fix this problem is to do encryption of data. So, a secure user can impose with information get to control system must be given before the clients store any information on the cloud storage. Attribute Based Encryption (ABE) is an asymmetric key based crypto system that has received much focus that provides fine-grained data access control to data files deployed on the cloud. Here, we present a more proficient and most important type of ABE 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; the keys are updated once a specific user is removed from the group, and these updated new keys are shared between the existing users also our system supports the keyword search on encrypted data in the remotely storage of cloud. In multi keyword search; users and data owners can establish the index of keywords and pursuit trapdoor, without depending on the online trusted authority. Here erasure codes are used to ensure the 100 percent of data availability. Experimental results demonstrate that the performance of the proposed system is superior than existing system in terms of security, data availability, time consumption and memory utilization.

Keywords: Cloud Computing, Searchable Encryption, Erasure Codes, Attribute Based Encryption, Attribute Revocation

I. INTRODUCTION

Cloud Computing is received as another option to conventional data innovation because of low-maintenance attributes and its intrinsic resource-sharing. In cloud computing, the service providers for example, Amazon, etc provides different services to users of cloud with the aid of intense data centers. With merging of private data management frameworks and cloud servers together, clients can acknowledge top indent services and recover huge stab on their nearby infrastructures. Data storage is a basic service provided by cloud system. By making use of the cloud, the cloud users can get total relief from the issues arises while storing and maintaining the local data. Also, it has a noteworthy risk to keep up the protection of those put away documents. In particular, clients could not trust totally on the cloud servers managed by CSP, just due to information files deployed on the cloud may be delicate and private, similar to marketable strategies. To give data secrecy, encryption of data files is an efficient solution, so upload file by encoding data into the cloud. Unfortunately, the data sharing among the groups securely in the cloud is definitely not a straightforward undertaking as a result of the accompanying testing issues.

In the first place, identity protection is the major downfall for the development of cloud computing. With no security of user id protection, users might be reluctant to participate in cloud systems in light of the fact that their genuine identities could be effectively uncovered to cloud providers and attackers. Second, it is exceptionally suggested that any member in a group can have the capacity to utilize the data sharing and storing administrations given by the cloud, which is stated as multi owner way. related with the single- proprietor manner, in which simply the group administrator can reserve and alter data in the cloud, the numerous-owner manner is more flexible in real time applications. To wrap things up, groups are dynamic in practice. The alterations of participation make secure data sharing very difficult. Toward one side, the anonymous system challenges new conceded clients to become familiar with the substance of information documents stored before their participation, because of its unrealistic for new granted users to contact with obscure and unknown data owners, and obtain the corresponding decryption keys. At opposite end, a proficient membership revocation mechanism without refreshing the secret keys of the other clients is likewise wanted to limit the unpredictability 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. ABE has gained much focusing the research community. And ABE 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 named with descriptive attributes set and a particular key can decrypt a particular ciphertext just if there is a match between the characteristics of the ciphertext and the users key attributes.

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, a productively revocable and searchable ABE (RSABE) scheme for the remote cloud storage is proposed. Catchphrase seek is likewise upheld, in which information proprietors and clients can deliver the watchwords list and scan for trapdoor, without relying upon continually online confided in power.

The section II explains the literature review of existing
systems. Section III presents the proposed system implementation details which includes searchable encryption, attribute revocational 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. REVIEW OF LITERATURE

Here [1] author provide search keywords over encoded information without leaking data keywords and that is possible due to Secure Encryption in such a cryptographic primitive. Here, the catchphrase seek is upheld and a while later the entrance structure is mostly covered up to guarantee information security in figure writings is proposed.

In Dynamic searchable encryption (DSE) of big Databases [2], author present a DSE scheme. this scheme the newly inserted records are reserved in other tuples and database that are deleted are inserted in list of a revocation and finally it excludes the tuples in the revocation list for obtaining final result. Scheme presented by Yet, Cash et al does not recognize the multi-keyword ranked search functionality.

In paper [3] authors consider another necessity of ABE without sourced decryption that is termed as verifiability of transformations. Informally, it ensures that a customer can capably check if the change is done effectively or not. Their system demonstrate that the new plan is both secure and unquestionable, without relying upon arbitrary 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, an ABE system is proposed by Green et al. [4] with outsourced decryption that to a great extent takes out the overhead of decryption for clients. In ABE system, a client keeps up an untrusted server, say a CSP, with a change key that allows the cloud to decipher any ABE ciphertext fulfilled by that clients' properties and it simply think of some computational overhead for the customers to recoup the plaintext from the changed ciphertext. Security of an ABE framework with redistributed decoding guarantees that an enemy (Including a malignant cloud) won't have the ability to analyses anything related to the encrypted message; in any case, it does not give any assurance of definiteness of the transformation performed by the cloud.

Author Yu et al. [5] consider the issue of user revocation
which involves re-encrypting the data that is obtainable to the customer 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 elaborate with the expansion in 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 ABE scheme known as ciphertext policy attribute based encryption (CP-ABE) where every private key is set with properties, and each ciphertext is named with an access strategy. Decryption is done if and just if the client property set achieve the ciphertext access structure. This can get fine-grained access control on shared information in various useful settings. Here, Author can take just CP-ABE in record designs in which get to structures are AND gates on positive and negative qualities. Their important arrangement has been shown to be picked plaintext assault (CPA) secure underneath the decisional bilinear Diffie-Hellman presumption however the usage of autonomous occasions of CP-ABE encryption, and furthermore the security of this proposition stays as an open issue.

In this paper [7], the authors proposed a cryptosystem that provides fine-grained access control to encoded information that they called Key Policy ABE(KP-ABE). In their cryptosystem, ciphertext are classified with different characteristics and secrete keys are set with access structures that limits which ciphertext a

user is capable to interpret. They have applied their construction in forensic analysis and broadcast encryption. However, their systems fail 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 for achieving minimal search time these are (SSE-1 and SSE- 2). The SSE-1 contrive is secure against picked catchphrase attacks (CKA1) and SSE-2 is secure against flexible picked watchword ambushes (CKA2). These early fills in as a solitary watchword boolean pursuit conspires, that are most straightforward as far as usefulness. At that point, loads of work have been evolved under numerous danger models to accomplish different seek profitableness, similar to single catchphrase look, comparability seeks, multi-watchword boolean hunt, positioned inquiry, and multi-watchword positioned pursuit, and so on.

The notion of ABE was proposed in this paper [9] as fuzzy version of Identity Based Encryption (IBE). In Fuzzy IBE, Sahai et al. consider identity as a practical characteristics set. A Fuzzy IBE scheme considers a private key for an identity, to interpret a ciphertext combined with a personality, if and just if the identities w and w are near one another judged by some metric. A Fuzzy IBE approach can be joined with secure encryption utilizing biometric contributions as personalities; the rupture obstruction characteristics of a Fuzzy IBE course of action has accurately what considers if its utilization of a biometric characters. Moreover, they demonstrate that Fuzzy- IBE can be utilized for different kind of use that they term ABE. Here they exhibit two head ways of IBE Fuzzy orchestrates. Their progressions can be seen as an IBE under two or three attributes that make a (delicate) character of a message. Their IBE arrangements are couple oversight patient and private against plot attacks. Besides, the key advancement does not use arbitrary prophets. Creator exhibit the privacy of their arrangements under the Selective-ID security display.

Here Searchable encryption schemes [8] used by clients to store encoded information on the cloud and execute keyword search over ciphertext area. Because of different cryptography natives, accessible encryption plans can be built by utilizing public key based cryptography or symmetric key based cryptography.

III. PROPOSED APPROACH

A. Problem Statement

We formally define our problem as follows.

1) ABE is reasonable for remote cloud storage to secure data privacy and acknowledge fine-grained data access control.

2) It is important for ABE schemes to accomplish attribute revocation as clients' characteristics might be changed often.

3) Keyword search over encrypted data likewise require to be solved in the remote cloud storage. Likewise, computational effectiveness is a idea for the resource constrained mobile device.

4) As such, with the evolution of sharing confidential private corporate information over CS, it is essential to adopt a proficient encryption framework to encrypt outsourced data. To achieve this, we propose a secure, searchable and proficient ABE technology to provide malleable access control of encrypted data stored in the cloud that overcomes the drawbacks of existing ABE schemes.

B. Proposed System Overview

1) Attribute Based Encryption (ABE): ABE is kind of public key cryptography. In conventional public key

cryptography, a message is encrypted utilizing the receivers public key for a particular beneficiary. Identity based cryptography and specifically IBE changed the conventional comprehension of public key cryptography by enabling general public key to be a discretionary string, e.g, the email address of the recipient. ABE goes above and beyond and characterizes the identity not atomic but rather as a lot of attributes sets, e.g., roles, and messages can be encoded as for subsets of properties (key-strategy ABE - KP-ABE) or strategies characterized over a lot of traits (ciphertext-approach ABE-CP-ABE). The key issue is, that somebody should possibly have the capacity to decode a ciphertext if the individual holds a key for" coordinating properties" where client keys are constantly issued by some confided in gathering. Ciphertext-Policy ABE and Key-Policy ABE are two sorts 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 designating the task of dispatching 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

5) Erasure Codes

C. System Architecture

The Fig.1 shows the proposed system architecture.

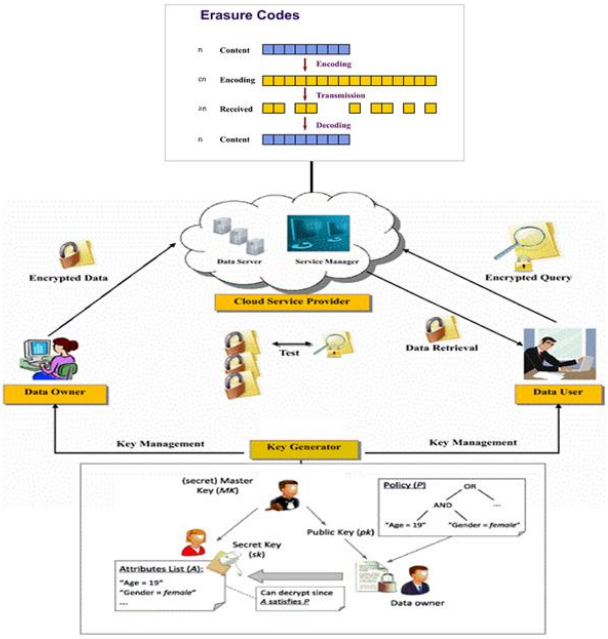

Figure 1: Proposed System Architecture

1) Existing system provide a ABE scheme parallel outsourced key decryption and delegating. With the aid of DSP and KGSP, this scheme achieves constant proficiency at both authority and user sides.

2) Limitations of Existing System:

(a) System does not give user revocation.

(b) ABE plans are not ready to at the same time achieve

productive trait denial and keywords look.

3) The contributions of our system is as follows.

(a) The proposed RSABE underpins productive characteristic renouncement and watchword seek in versatile cloud condition all the while.

(b) With the high effectiveness framework gives a prompt denial technique. In RSABE plot, the characteristic specialist safely delegates the most refresh undertakings to cloud server. Amid the whole renouncement, the mystery key segment that customer holds keeps unaltered, which brings mind boggling solace for portable clients.

(c) The framework additionally gives seek catchphrases

on the encoded information. The cloud server will restore the list items just when the lists and keywords are correlated and the attribute set of client satisfies the entrance arrangement in ciphertext. Additionally, information proprietor and client can make the keywords
file and inquiry trapdoor independently without relying
upon confided in outcast.

D. Algorithms

1. ABE Algorithm

Step 1: ABE Setup: The setup algorithm takes input as a
security parameter I. It gives output as a public key PK and a master key MK.
Step 2: KeyGen: For delegated key generation the initialization algorithm gets an access policy (or attribute set) and the master key MK as input for each user's private key request, it outputs the key partial transformation key.
Step 3: To achieve the same results with less time Encrypt: A message M and an attribute is taken as a input in the encryption algorithm.
Step 4: Decrypt: the ciphertext (ct) and the private key sk is taken as a input in the decryption algorithm. It outputs the original message M
Step 5: User revocation: when there is a user to be revoked, an updates affected user's private keys by using KGSP.
Step 6: end for

IV. RESULT 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

Here, the performance between existing and proposed system is compare. The following graph shows the time require to generate encryption key over the of number of attributes. In Figure 2 X-axis show number of attributes used while Y-axis show required time to run the key generation algorithm in seconds. Table 1 shows the reading from which the below graph is generated.

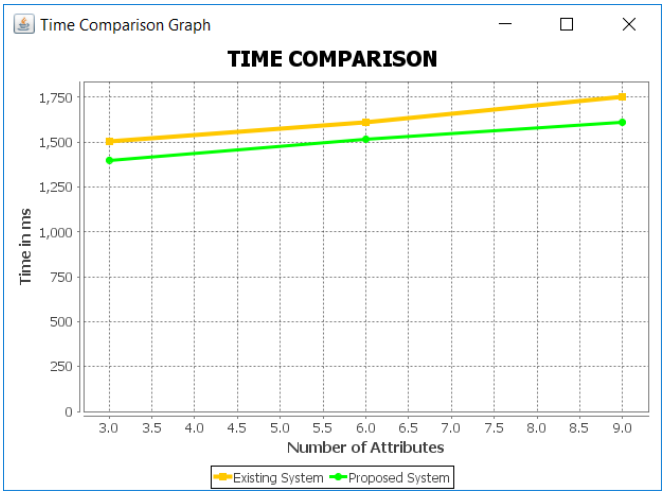

Figure 2: Time Comparison Graph

TABLE I

TIME COMPARISON

No. of Attribute	Existing System (Time in ms)	Proposed System (Time in ms)
3	1501	1420
6	1628	1508
9	1750	1612

TABLE III

STORAGE SPACE COMPARISON

Original File Size	Existing System (KB)	Proposed System (KB)
100	200	150

Figure 3 shows storage space comparison graph between existing system and proposed system. In Fig. 3 X-axis show systems while Y-axis shows required storage space at cloud server to store the encrypted file in KB. Table 2 shows the reading from which the fig. 3 graph is generated.

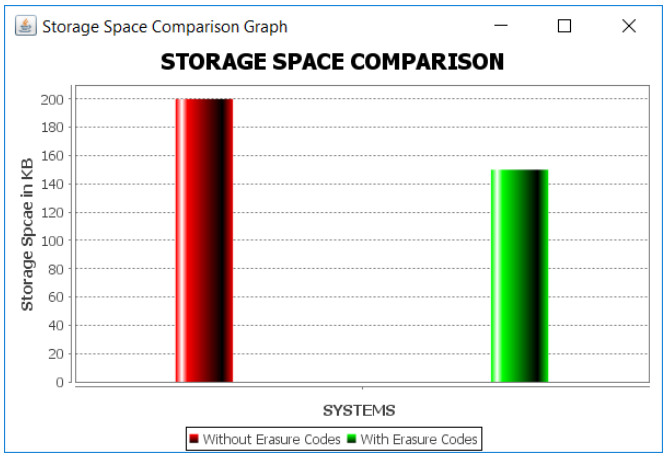

Figure 3: Storage Space Comparison Graph

TABLE IIIII

COMPARISON WITH SIMILAR SYSTEM

Parameters	Proposed System	Base Paper[1]	Paper [9]
Keywords Search	✓	✓	×
Revocation	Attribute	Attribute	System
Access Control	LSSS	LSSS	AND Gate
Erasure Codes	✓	×	×

V. CONCLUSION

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 ABE 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 minimize the computation overhead of the user, the system provides modified outsourced ABE scheme which supports the outsourced key-decryption and issuing by utilizing Key Generation Service Provider. One of the advantage of system is supports secure searching over encrypted data. Results shows that our system is proficient as well as practical.

VI. REFERENCES

[1]. Y. Li, F. Zhou, Y. Qin, M. Lin, and Z. Xu, -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. 14thACM 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 13thACM 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.

Cite this article as :

Jayesh Sahebrav Patil, Prof. Prashant Mininath Mane, Dr. S. M. Sangve, "ABE Technique and Erasure Code for Secure Cloud Storage with Revocation", International Journal of Scientific Research in Science and Technology (IJSRST), Online ISSN : 2395-602X, Print ISSN : 2395-6011, Volume 6 Issue 4, pp. 222-229, July-August 2019.
Journal URL : http://ijsrst.com/IJSRST196446