© 2019 IJSRST | Volume 6 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X
Themed Section: Science and Technology
DOI : 10.32628/IJSRST1962114

Searchable Attribute-Based Encryption Scheme over Cloud Data

[1]Prajot Deshmukh, [2]Prof. Gajanan Patle, [2]Prof. Ektaa Meshram

[1]PG Scholar, Department of Computer Science Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, Maharashtra, India

[2]Assistant Professor, Department of Computer Science Engineering, Abha-Gaikwad Patil College of Engineering, Nagpur, 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 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 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.

Keywords: Attribute-Based Encryption, Attributes Revocation, Fine-Grained Access Control, Keywords Search, Mobile Cloud Storage.

I. INTRODUCTION

Cloud Computing is seen as another choice to customary information advancement as a result of its inborn asset sharing and low-upkeep attributes. In cloud registering, the cloud specialist co-ops (CSPs, for instance, Amazon, can send diverse administrations to cloud customers with the help of extreme datacenters. By consolidating the neighborhood information the board structures into cloud servers, customers can value first class administrations and recuperation gigantic theories on their adjacent frameworks. Information storage is a fundamental administration given by cloud framework. By utilizing the cloud, the clients can be totally discharged from the troublesome nearby information storage and support. Additionally, it likewise has a huge hazard to the secrecy of those putaway documents. In particular, the cloud servers overseen by cloud suppliers are not trusted absolutely by clients while the information records put away in the cloud might be touchy and secret, for example, marketable strategies. To give information security, as a fundamental arrangement is to scramble information records, and after that transfer the encoded information into the cloud. Sadly, structuring proficient and secure information sharing a philosophy for gatherings in the cloud isn't a simple assignment because of the accompanying testing issues.

To begin with, personality security is a significant defeat for the improvement of cloud processing. With no security of personality protection, clients might be reluctant to participate in cloud registering frameworks on the grounds that their genuine characters could be effectively revealed to cloud suppliers and aggressors. Second, it is exceedingly suggested that any part in a gathering can almost certainly utilize the information putting away and sharing administrations given by the cloud, which is defined as the various proprietor way. Contrasted and the single-proprietor way, in which just the gathering director can store and adjust information in the cloud, the numerous proprietor way is increasingly adaptable progressively applications. To wrap things up, bunches are dynamic practically speaking. The alterations of participation make secure information sharing extremely troublesome. Toward one side, the mysterious framework provokes new conceded clients to get familiar with the substance of information records put away before their cooperation, because of its unrealistic for new allowed clients to contact with obscure information proprietors and get the relating unscrambling keys. At the opposite end, an effective enrollment revocation system without refreshing the mystery keys of different clients is additionally wanted to limit the unpredictability of key administration.

To settle this issue, data which is to be put away is encoded in mixed structure. Anyway, such encoded information must be pleasing to the sharing and access control. Different private and open key cryptographic procedures are not receptive to versatile access control. So as to settle this issue Revocable and Searchable Attribute-Based Encryption method was proposed. Attribute-Based Encryption (ABE) has increased much consideration in the research network. Attribute-Based Encryption is a lopsided key based cryptographic method which improves the skillfulness of access control systems.

In a Revocable and Searchable ABE system, a client's keys just as ciphertext are marked with sets of engaging attributes and a specific key can decode a specific ciphertext just if there is a match in the attributes of the ciphertext and the client's critical. Be that as it may, a defect in the standard ABE framework is the immense size of the ciphertext and the computational complexities in the decoding stage are very saddling. In this way, there is a need to upgrade the capability of ABE. To unravel this issue, a proficiently revocable and searchable ABE (RSABE) conspire for the mobile cloud storage is proposed. Watchword search is additionally upheld, in which information proprietors and clients can produce the keywords list and search trapdoor, separately, without depending on constantly online confided in power. Our proposed framework likewise thinks about the revocation of clients in the framework to accomplish legitimacy and security.

II. LITERATURE REVIEW

In this paper [1], the capacity of attribute revocation is productively accomplished by assigning the update of mystery key and ciphertext to the ground-breaking cloud server. Catchphrase search is additionally bolstered, in which information proprietors and clients can create the keywords list and search trapdoor, individually, without depending on constantly online confided in power. Moreover, a redistributed decoding innovation is utilized to diminish the computational heap of unscrambling on the client side.

In [2] a Secure Encryption is such a cryptographic crude, that empowers clients to search keywords over the scrambled information without spilling keywords data. In this paper, the catchphrase search is upheld and afterward the access structure is in part covered up to ensure protection data in ciphertexts is proposed.

In this paper [3], the creator proposed a dynamic searchable encryption plot. In their development, recently included tuples are put away in another database in the cloud, and erased tuples are recorded in a revocation list. The last search result is accomplished through barring tuples in the revocation list from the ones recovered from unique and recently included tuples. However, Cash et al. dynamic search plot do not understand the multi-watchword positioned search usefulness.

In this paper [4] the creators considered another need of ABE with redistributed unscrambling that is the certainty of changes. Casually, it ensures that a client can effectively check if the change is done precisely or not. Their framework exhibit that the new plan is both secure and certain, without relying upon arbitrary forecasts. In their work, they propose an alternate view for ABE that, everything considered, clears out the overhead for customers. Anyway, their development does not consider overhead calculation at the attribute specialist associated with the key-issuing process.

Here in [5], Green et al. proposed an ABE framework with re-appropriated unscrambling that, all things considered, take out the decoding overhead for customers. In such a framework, a client gives an untrusted server, state a cloud specialist organization, with a change key that allows the cloud to interpret any ABE ciphertext satisfied by that client's attributes or access arrangement into a basic ciphertext, and it just achieves somewhat computational overhead for the client to recuperate the plaintext from the changed ciphertext. Security of an ABE framework with redistributed unscrambling guarantees that a foe (Including a vindictive cloud) won't have the ability to get the hang of anything about the encoded message; regardless, it doesn't guarantee the rightness of the change performed by the cloud.

In this paper [6], Yu et al. consider the issue of client revocation which includes re-scrambling the information that is accessible to the client leaving the framework and refreshing the private keys of clients staying in the framework. They have proposed a plan that empowers the proprietor of the information to re-appropriate the errand of re-encryption and private key updates to an outsider without uncovering the substance and the client data. They have great accomplished the finely grained and versatile access in cloud processing. Anyway, the unpredictability in client revocation increments with the expansion in the number of clients which makes the framework complex. What's more, their plan does not bolster client responsibility.

Cheung et al. in [7] have proposed yet each other kind of Attribute-Based Encryption plot known as ciphertext approach attribute-based encryption (CP-ABE) where each mystery key is named with attributes, and each ciphertext is set with an access strategy. Unscrambling is done if and just if the customers characteristic set fulfills the ciphertext access structure. This gives fine-grained access control on shared information in different commonsense settings, including secure databases and secure multicast. In this paper, they consider CP-ABE designs in which access structures are AND doors on positive and negative attributes. Their essential arrangement has been ended up being picked plaintext assault (CPA) secure under the decisional bilinear Diffie-Hellman presumption however the utilization of autonomous occurrences of CP-ABE encryption, and furthermore, the security of this proposition stays as an open issue.

In this paper [8], the creators proposed a cryptosystem that gives fine-grained access control to scrambled data that they called Key-Policy Attribute-Based Encryption (KP-ABE). In their cryptosystem, ciphertext is marked with sets of attributes and private keys are set with access structures that control which ciphertext a client can translate. They have connected their development in the measurable examination and communicate encryption. Anyway, their frameworks neglect to conceal the attributes that do the encryption. Thus the issue of attribute stowing away is left open.

Here Curtmola et al. [9] proposed two plans (SSE-1 and SSE-2) which accomplish the ideal search time. Their SSE-1 plot is secure against picked catchphrase assaults (CKA1) and SSE-2 is secure against versatile picked watchword assaults (CKA2). These early works are single watchword boolean search plans, which are exceptionally straightforward as far as usefulness. A short time later, plenteous works have been proposed under various risk models to accomplish different search usefulness, for example, single watchword search, similitude search, multi-catchphrase Boolean search, positioned search, and multi-watchword positioned search, and so forth.

The thought of ABE was proposed in this paper [10] as a fluffy form of Identity-Based Encryption (IBE). In Fuzzy IBE, Sahai et al. see the way of life as a lot of sensible characteristics. A Fuzzy IBE course of action thinks about a private key for a personality, to interpret a ciphertext blended with a character w, if and just if the personalities w and w' are near one another made a decision by some measurement. A Fuzzy IBE course of action can be united with secure encryption utilizing biometric contributions as characters; the break opposition property of a Fuzzy IBE plan is exactly what considers the utilization of biometric personalities, which ordinarily will have some confusion each time they are explored. Furthermore, they demonstrate that Fuzzy-IBE can be utilized for a kind of use that the term" attribute-based encryption". In this paper, they show two progressions of Fuzzy IBE orchestrates. Their progressions can be viewed as an Identity-Based Encryption of a message under two or three attributes that make a (delicate) character. Their IBE plans are both oversights tolerant and secure against plot assaults. Plus, the key progression does not utilize self-assertive prophets. Maker displays the security of their game plans under the Selective-ID security demonstrate.

Searchable encryption plans empower the customers to store the encoded information to the cloud and execute a catchphrase search over the ciphertext area. Because of various cryptography natives, searchable encryption plans can be developed utilizing open key based cryptography or symmetric key based cryptography [11].

III. Proposed Work

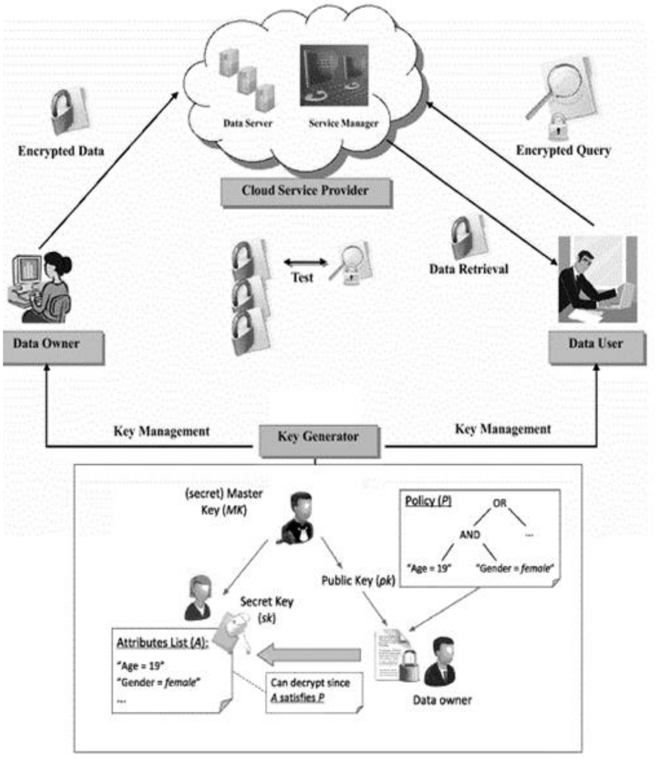

Figure 1. System Architecture

1. Attribute Based Key Generation

Initially user needs a key for file encryption or decryption before storing or downloading from cloud server. To minimize the key management overhead a separate outsourcing Key Generation Service Provider (KGSP) is used. And for data security purpose, Attribute Authority (AA) is introduced in the system. In this, upon receiving the key request from user, AA verifies the attributes of users, if they are valid then and only then KGSP generate and distribute the key for that user.

2. File Encryption and upload

For data confidentiality purpose, each and every data files are stored on server in encrypted format. After verification of attributes, user get key. Upon receiving this key, user encrypt their files and upload on cloud server.

3. File Download and Decryption

As user does not have capability to decrypt whole downloaded file, Decryption Service Provider (DSP) is introduced in proposed system. Initially, user requesting to DSP with partial key to download the file from cloud server. Then cloud server identify that file and calculate its size. If the size of file is greater than threshold size then cloud server send that file to DSP. At DSP, that file is partially decrypted and send to requested user. Otherwise Cloud server directly send that file to user and at user side this file is decrypted using key obtained from KGSP.

IV. 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 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.

V. REFERENCES

[1]. SHANGPING WANG, DUO ZHANG, YALING ZHANG, AND LIHUA LIU, "Efficiently Revocable and Searchable Attribute-Based Encryption Scheme for Mobile Cloud Storage", IEEE Access Volume 6, June 2018.

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

Cite this article as :

Sh