International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-7, Issue-2, March 2019
DOI: 10.21276/ijircst.2019.7.2.3

A Review on Multilevel Approaches for Security in Cloud by Using ABE

Akhilesh Kumar Soni, Nitya Khare

***Abstract*: Public Key Encryption acts as the basic technique for ABE where it provides one to many encryptions, here, the private key of users & the cipher-text both rely on attributes such that, when the set of the attributes of users key matches set of attributes of cipher-text with its corresponding access policy, only then decryption is possible. Thus, an opponent could grant access to the sensitive information that holds multiple keys, if it has at least one individual key for accession. Medical organizations find it challenging to adopt cloud-based electronic medical records services, due to the risk of data breaches and the resulting compromise of patient data. Hence there is a need of developing a proper authorization delegation mechanism for safe, secure and easy cloud-based EHR management.In this research work a centralized, attribute based authorization mechanism is developed that uses Attribute Based Encryption (ABE) and allows for delegated secure access of patient records.**

***Keywords*:Cloud computing, Data sharing, Data confidentiality, Security, ABE, Access controls.**

I. INTRODUCTION

Data stored in cloud, means it is stored with cloud provider. The problem of privacy and security threatens us a lot. When dealing with cloud environments, confidentiality implies that a customer's data and computation tasks are to be kept confidential from both the cloud provider and other customers[10]. The threats on outsourced data can be prevented by encrypting the data before putting it into the cloud. Several Encryption schemes are available however the one that suitsfor data that is to be accessed by multiple users end always atAttribute Based Encryption (ABE).In case of ABE themessages are encrypted based on the role of the users. TheDecryption is possible only for those who really play the rolesinfo).

Manuscript Received March 19, 2019

Akhilesh Kumar Soni, M.Tech Scholar Department of Computer Sciecne& Engineering SIRT-Excellecne, Bhopal (email:amar.soni86@gmail.com)

Nitya Khare, Associate Professor Department of Computer Sciecne& Engineering SIRT-Excellecne, Bhopal,

A. Applications of ABE

A straight forward application of KP-ABE includes downloading the encrypted data from the cloud by data holder, and decrypting it to extract the unique data, then again re-encrypting it beneath the new access policies and yet again uploading it for the end user. The task becomes intimidating when the quantity of data involved is massive. Hence, KP-ABE is broadly practiced in applications of data distribution such as, Facebook, Amazon, Google Drive, and Drop box etc., where remote servers are semi-trusted, so as the access control method is insured by the encryption technique and not by the cloud storage server. Also, KP-ABE application could be explained in a way for example: Suppose an organization required to introduce its personal cloud as an Application, so the organizational group has to form a confidential team for an IT project. Then, this Team needs a cloud server on rent so they could help for sharing of data to its internal group. This confidential group consists of only those individuals which are authorised person to those shared data outsourced to the cloud that they been provided on rent. However, the access control authority confirms that only authorised person of the confidential team are permitted to access those data. Whereas, in CP-ABE, it is applicable in encryption of cloud data phenomenon for example: In any industrial department, the description provided on a new product could permit access to only those departments that pursue during the design and testing stages. Then, as the product is ready to be launched in the market, product specifications and its access shall need to be transferred from the engineering department to the advertising and transactions departments.

B. Advantages & Limitations of ABE

There are few common advantages & limitations of Attribute based Encryption schemes & their types which could need the enhancement in it.

Advantages

In ABE, it provides well security & privacy with fine grained access but less than KP-ABE method. Also, for huge storage of records it offers elasticity. Ultimately, advantage of ABE is that there is no one-to-one relationship in its encryption and decryption keys; means an encryption key can correspond to multiple keys for decryption. In the ABE technique, specific access policies and attribute sets could differ according to time, which is a versatile nature of the scheme. Whereas, KP-ABE has more advantage then ABE. It is further reconstructed with different techniques which provide better access control such as when it's combined with Re-encryption method. Also, it offers well security & privacy than ABE which is thus more efficiently available in version of expressive KP-ABE scheme where public parameters of constant size had been shown. Now-a-days,

more feasible experiences had also been explained by adopting ABE on resource-controlled devices with IOT applications. Some advantages could be described in CP-ABE kind of encryption where it affords fine grained access alike KP-ABE. It has better efficiency in its security methods but consumes time. Similar to KP-ABE, also it can be merged to re-encryption techniques & hidden policy variants which provide adequate access control method & good security to the schemes.

Limitations

In ABE the public key of every authorized user is essential for the data owner but it prohibited in actual environment. As in ABE it suffers from high computational overhead whereas KP-ABE possesses less. And in KP-ABE, decryption of the encrypted text couldn't be decided by the person which encrypts it. It is more complex than ABE, as it is incompatible in some application because a data owner necessarily should trust the key issuer. Therefore, in CP-ABE, compared to ABE cons are limited, but in its variant of verification built on a collision-resistance hash function provides large computation overhead which is required to minimize.

C. Preliminary

Access structures:

In [1] the access tree in KP-ABE scheme defines the access scope of a user's private key. Each non-leaf node of an access structure is labelled as children of a root node. Here, every non-leaf node represents a Threshold Gate which has its own threshold value corresponding to it. Suppose a node x has number of children represented as num(x) correspondingly it has its onset value, say kx, then 0<kx<num(x). Hence in every access tree or an access structure, each leaf node of the tree is termed by an attribute and it has its onset value kx =1. Therefore, for different onset values of an attribute provides a unique Threshold Gate. Such as for kx =1, OR gate is a Threshold Gate, whereas for kx =num(x) it provides AND gate as a Threshold Gate. Therefore, to enable working of an access tree, there are few functions to describe its operations i.e.

- parent (x): signifies the parent of the node x in the tree i.e. we can say as root node.
- att (x): it is defined only if x is a leaf node, and indicates the attribute connected to the leaf node x in the tree.
- index(x): it represents the order of the root node x between its brothers. The nodes are numbered from 1 to num.

Here, maximum in all the schemes they have focused on the monotonic access structure. For satisfying an access structure,

Let $\boldsymbol{x} = \{\boldsymbol{x1} \ldots \ldots \ldots \boldsymbol{xn}\}$be a group of events. A collection of party A ⊆ 2x is monotone for ∀B and C, if B ∈ A, B ∈ C, then C ∈ A. An access structure (respectively, monotone access structure) is a monotone collection. A of nonempty subsets of x1... xn, i.e., A ⊆ 2P\{∅}. The arrays in A are termed as authorized arrays, and the absent sets in A are called unauthorized set.

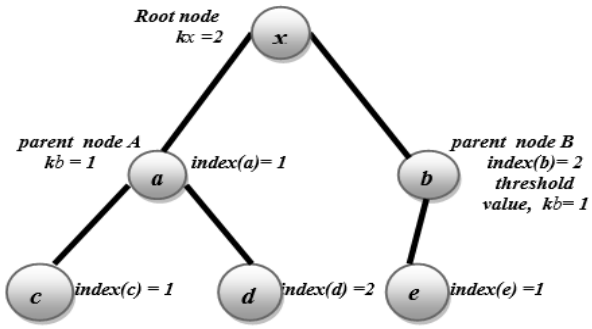

Fig 1: Access Tree Structure

Linear secret sharing schemes

In [1] in this, vital uses of linear secret-sharing structures are revised from definitions from those given in Beimel, A.: Secure Schemes for Secret Sharing and Key Distribution. A secret-sharing scheme Π over a group of parties P is called linear (over Zp) if:

1) The shares for each party form a vector over Zp.

2) There exists a matrix an M with rows and n columns called the share generating matrix for Π. For all i =1.....l the i'th row of M, we let the function ρ defined the party labelling row i as ρ(i). When we consider the column vector, v=(s,r2,...,rn), whereas a ∈Zp is the secret to be shared, and r2,...,rn∈Zp are randomly chosen, then Mv is the vector of l shares of the secret s according to Π. The share (Mv) i belongs to party ρ(i).

Suppose that Π is an LSSS for the access structure A. Let S ∈ A be any authorized set, and let I⊂{1,2,...,l} be defined as I = {i : ρ(i) ∈ S}. Then, there exist constants {ωi∈Zp} i∈ I such that, if {λi} are valid shares of any secrets according to Π, then$\boldsymbol{£i \in I \omega i \gamma i = s}$.

Access structures could be described in monotonic Boolean formulas, which can be transformed to an LSSS representation. When considering a Boolean formulation as an access tree with l nodes, the corresponding LSSS matrix consists of l rows.

3) Bilinear groups: Bilinear Maps: [1] Let G0 and G1 be two multiplicative cyclic groups of prime order p. Let g be a generator of G0 and e be a bilinear map,

e: G0 × G0 → G1.

The bilinear map e has the following properties:

- Bilinearity: for all u,v∈ G0 and a,b∈Zp, we have $\boldsymbol{e(u^a, v^b) = e(u, v)^{ab}}$
- Non-degeneracy: e(g, g)≠ 1.

We say that G0 is a bilinear group if the group operation in G0 and the bilinear map e are both efficiently computable. Notice that the map e is symmetric since,

$$\boldsymbol{e(g^a, g^b) = e(g, g)^{ab} = e(g^b, g^a)}$$

II. LITERATURE REVIEW

Under survey cryptographic techniques proposed by various authors has been reviewed and a brief review on each of them are included below.In Sadia et al. [7]analysis of security problem in cloud identifies the threats mainly as inside and outside attackers. Inside attackers includes malicious employees at client side, malicious employees at cloud provider side and cloud provider itself. They arrived at findings that client data on cloud data base must in the form cipher text [8].

ISSN: 2347-5552, Volume-7, Issue-2, March 2019
DOI: 10.21276/ijircst.2019.7.2.3

In [9] the authors had done a survey on the various proposed security models for cloud and found that the insider threats from cloud provider itself and also the use of high cost pairing operations in most of security models as the demerits insecure cloud models.

Vidhate et al. [10] propose a scheme that integrates cryptography with Role Based Access Control (RBAC).AES isthe encryption technique used. The scheme uses private cloud to get parameters regarding the roles for which the encryption document is accessible. The owner then uploads the cipher text into cloud by seeking a dedicated server for performing encryption. During decryption public cloud forward the request to the private cloud; if the roles are having permission to access thecipher text they will be forwarded to the dedicated server to perform decryption. Advantages of the proposed system includes single key for decryption and a role based access. The system takes greater amount of time for role checking since it has to wait for the replies from private cloud regarding role based access permission.

Chu et al. [11] proposed a key aggregate cryptosystem(KAC) to decrypt a subset of cipher texts by generating anaggregate key for secret keys of different classes. In this proposal sender can broadcast the document to be shared by transferring a secret key through a public key cryptosystem.

Table 1: Comparative Review of ABE

Author name	Description	Results
Maithilee Joshi et al. [1]	An attribute based, field level, document encryption is proposed for managing the access and data security of cloud-based EHRs	Provided authentication to users with respect to read and write access.
Priya et al. [2]	Discussed about the various security techniques and relations based on Attributes Based Encryption, especially, the type KP-ABE over data attributes which explains secured methods & its schemes related to time specifications.	Provided that KP-ABE scheme is more efficient with respect to time.
Yong Yu et al. [3]	Proposed an attribute-based cloud data integrity auditing protocol to simplify the key management issues.	Less calculation in verifying the Response of auditing and thus cause less time consumption.
Y. Li et al. [4]	An fuzzy identity based attribute-based cloud data auditing protocol is designed.	Protocol offers the property of error-tolerance.
Ming-quan et al. [5]	Proposed Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing	Achieves better efficiency in terms of computation and communication cost as compared to RSA &Paillier scheme.
Yong Yu et al. [6]	Investigated data privacy issues in remote data integrity-checking protocols	Practically proved that the best size of the block is between 4 and 8 KB, which delivers the best performance

III.PROPOSED SYSTEM

According to the proposed methodology, the model explains about the flourishment of data security, its confidentiality & its integrity by using KP- ABE scheme for fine grained access in cloud computing. The proposed methodology works in following steps:

Step (1): Cloud Authority Server -- CAS when distributes PUK to cloud users then he send his PUK to Data owner.

Step (2): Data Owner --Then data owner generates SK by Elgamal algorithm and encipher it and transfers the encrypted data CT1 to CSP.

Step (3): Cloud Service Provider -- CSP thus alters the enciphered cipher-text, re-encrypts it into another cipher CT2.

Step (4): Data Centre --Then the data send by the data owner to the CSP is saved into Data centre.

Step (5): Authority Server—Hence, Authority Server generates the license for data user and after generation of license he sends it to CSP with PUK and timer starts running.

Step (6): Data User -- Thereafter Data user sends a request for retrieval of data from authority server and unless until he gets permission to retrieve by satisfying his authentication, end user cannot decrypt it.

Step (7): CSP and Timer Expires --When the data user credentials are satisfied then CSP provides encrypted data to the data end user, it generates two conditions; if Timers gives NO condition then data end user has authenticated himself as an authorized user and has time decrypt data in that interval of time and if Timers YES condition comes, then it seems that user had not decrypted the data in a certain time interval and data is self-destructed.

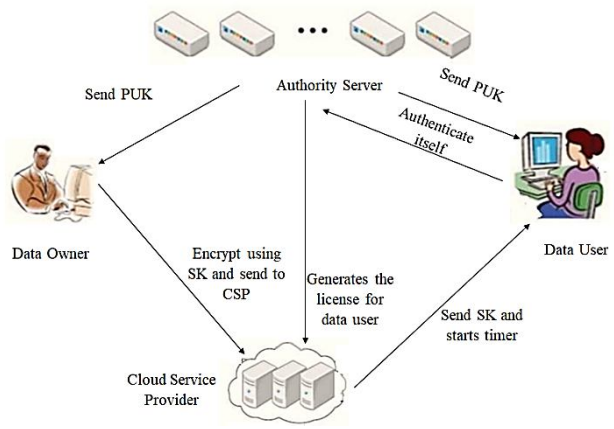

Fig. 2: Flowchart of Proposed Methodology

IV. CONCLUSION

In this paper various data sharing schemes have been analysed. Confidentiality and Authentication (security parameters) is achieved while designing an algorithm for achieving security in cloud. The proposed methodology implemented here provides efficient results. This research work also uses the concept of authentication of the user. Although the technique implemented here is efficient in terms of security and computational time, but further enhancements can be done for the communication overhead that may appears during the encrypted data retrieval.

REFERENCES

[1] Maithilee Joshi, Karuna P. Joshi and Tim Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems", IEEE, International Conference on Cloud Computing, 2018.

[2] Priya, A., and Tiwari, R., "A Survey: Attribute Based Encryption for Secure Cloud", IJOSTHE, 5(3), 12, 2018. https://doi.org/https://doi.org/10.24113/ojssports.v5i3.70 .

[3] Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai, "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage", IEEE Transaction on Emerging Topics in Computing, Vol. 14, No. 8, 2017.

[4] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, K-K. R. Choo. "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems". IEEE Transactions on Dependable and Secure Computing, 2017.

[5] Ming-quanHong,Wen-bo Zhao, Peng-yu Wang, "Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing", IEEE, 2016.

[6] Yong Yu · Man Ho Au · Yi Mu · Shaohua Tang · Jian Ren · Willy Susilo · Liju Dong, "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage", Springer, 2014.

[7] Sadia Marium, Qamar Nazir, Aftab Ahmed, SairaAhthasham Mirza AamirMehmood," Implementation of Eap with RSA for Enhancing The Security of Cloud Computing", International Journal of Basic and Applied Sciences, pp 177-183, 2012.

[8] Saira Varghese, S.Maria Celestin Vigila," A Comparative Analysis on Cloud Data Security", Proceedings of 2015 Global Conference on Communication Technologies, pp 507-510,IEEE, 2015.

[9] RohiniVidhate, V.D. Shinde," Secure Role-Based Access Control on Encrypted Data in Cloud Storage using Raspberry PI" International Journal of Multidisciplinary Research and Development, Volume: 2, Issue: 7, pp 20-27,July 2015.

[10] Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2,pp 468-477, February 2014.

[11] G. Yamamoto, S. Oda, K. Aoki. "Fast integrity for large data". Proc. ECRYPT workshop Software Performance Enhancement for Encryption and Decryption. Amsterdam, Netherlands 2007, 21-32.

[12] Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member, IEEE, Kui Ren, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, "Privacy-Preserving Public Auditing for Secure Cloud Storage" IEEE Transactions on Computers, vol. 62, no. 2, February 2013.

