International Journal of Innovative Research in Science and Engineering
Vol. No.3, Issue 04, April 2017
www.ijirse.com
ISSN (O) 2454-9665
ISSN (P) 2454-0663

A ROBUST MULTI AUTHORITY VERIFICATION IN CLOUD USING ELGAMAL ENCRYPTION SCHEME

Prof. Priyanka Mane[1], Shital Bade[2], Shilpa Jadhav[3], Kalyani Pakhare[4]

Department Information Technology, Genba Sopanrao Moze College of Engineering, Balewadi, Pune, (India)

ABSTRACT

Attribute base Encryption (ABE) is the cryptographic conducting tool to assurance data owner's enduring control above their data in public cloud storage. The proposed ABE plans include one and only power to keep up the entire trait set, which can carry a solitary point bottleneck on both safety and execution. In this way, some multi-power plans are proposed, in which various powers independently keep up disjoint trait subsets. In any case, the single-point bottleneck issue stays unsolved. In this paper, from another point of view, we lead an edge multi-power CP-ABE access control plan for open distributed storage, named TMACS, in which various powers together deal with a uniform characteristic set. In [9] TMACS, exploiting (t; n) limit mystery sharing, the expert key can be shared among numerous powers, and a legitimate client can produce his/her mystery key by cooperating with any t powers. Security and execution investigation results demonstrate that system is not just undeniable secure when not as much as t powers are traded off, additionally dynamic when no not as a great deal as t powers are alive in the framework. Besides, by proficiently joining the customary multi-power plan with system, we build a half and half one, which fulfils the situation of traits originating from various powers and accomplishing security and framework level strength.

Keywords: Identity-based encryption; Revocation; Outsourcing; Cloud computing.

I. INTRODUCTION

There are numerous focal points of distributed storage, there still information security is a noteworthy deterrent in the distributed computing [10]. Information proprietor stores his information in trusted servers, which are controlled by completely trusted executive. In any case, individuals are as yet dreading to abuse the distributed computing. For the most part a few individuals trust that cloud is hazardous spot and once you store your information to the cloud, you lose complete control over it. Information proprietor can't trust on the cloud server to direct secure information access control. In this way, secure information access control issue has turned into the most basic testing issue in general society distributed storage. So any customary security advances can't be connected straightforwardly on it.

Quality based Encryption (ABE) [14] is a standout amongst the most suitable plans to lead information access control in broad daylight distributed storage which it can promise information proprietors' immediate control over their information and gives the fine-grained access control administration. Earlier, there are many ABE scheme was proposed, which can be divided into two categories:

ISSN (O) 2454-9665
ISSN (P) 2454-0663

1) Key-Policy Attribute-based Encryption (KP-ABE)
2) Cipher text-Policy Attribute-based Encryption (CPABE),

In KP-ABE plans, decode keys are connected with access structures while cipher texts are just marked with the extraordinary trait sets. Then again, in CP-ABE plans, information proprietors can characterize an entrance arrangement for every document in view of clients' traits, which can insurance proprietors' more straightforward control over their information. Subsequently, when contrasted with KP-ABE, CP-ABE is a best decision for outlining access control openly distributed storage.

In most existing CP-ABE [13, 14] plans, there is entirely one-power in charge of property administration and key conveyance. This one and only power situation can bring a solitary point bottleneck on both security and execution. Once the power is traded off, an enemy can without much of a stretch get the stand out power's expert key, then he/she can create private keys of any ascribe subset to decode the particular encoded information. Once the one and only power is slammed, the entire framework can't function admirably. In this way, these CP-ABE plans are still a long way from being broadly utilized for access control as a part of open mists.

In any case, some multi-power CP-ABE plans proposed, regardless they can't manage the issue of single-point bottleneck on both security and execution. In these multi-power CP-ABE plans, the entire property set is separated into numerous disjoint subsets and every characteristic subset is still kept up by one and only power. Despite the fact that the foe can't increase private keys of all traits on the off chance that he/she hasn't traded off all powers, bargaining one or more powers would make the enemy have a larger number of benefits than he/she ought to have. Also, the foe can acquire private keys of particular traits by trading off particular one or more powers. What's more, the single-point bottleneck on execution is not yet explained in these multi-power CP-ABE plans. Accident or logged off of a particular power will make that private keys of all characteristics in trait subset kept up by this power can't be produced and appropriated, which will even now impact the entire framework's successful operation.

The remaining part of this paper is organized as follows. In section II, we introduce the related work. In section III, we review the literature survey. In section IV, we present our proposed system model. In section V, we shows result and performance of our system. And remaining part is that, we conclude the paper and explain the future work.

II. RELATED WORK

In this paper, we propose a vigorous and evident limit multi-power CP-ABE access control plan, which manages the single-point bottleneck on both security and execution. In this plan, numerous powers mutually deal with the entire property set however nobody has full control of a particular characteristic [9]. Following in CP-ABE plans, there is dependably a mystery key used to create trait private keys, we present (t, n) limit mystery sharing into our plan to share the mystery key among powers. In this plan, we reclassify the mystery key in the customary CP-ABE plans as expert key. The idea of (t, n) limit mystery sharing ensures that the expert key can't be acquired by any power alone. This plan is not just undeniable secure when not as much as t powers are bargained, additionally hearty when no not as much as t powers are alive in the framework. This plan is the

ISSN (O) 2454-9665
ISSN (P) 2454-0663

primary attempt to address the single point bottleneck on both security and execution in CP-ABE access control plans in broad daylight distributed storage.

III. LITERATURE SURVEY

R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption" [1]

In this paper, the author has introduced Ciphertext approach quality based encryption framework, that proposed CP-ASBE which is a form of CP-ABE, which organizes user attributes into a recursive family of sets and also allows to users to establish dynamic constraints on how attributes may be combined. And also this system shows how CP-ASBE can support compound attributes, and numerical attributes with multiple those value assignments. In their work, design of CP-ASBE system is secure in the standard model but extending for a multi-authority system.

Sahai and B. Waters, proposed the approach "Fuzzy identity-based encryption" [2].

The author [2] has presented another kind of Identity Based Encryption (IBE) plan that called Fuzzy Identity Based Encryption. A Fuzzy IBE plan takes into consideration a private key for a character id to unscramble a Ciphertext scrambled with another personality id0 if and just if the personalities id and id0 are near one another as measured by some metric (e.g. Hamming separation).

Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption" [3]

In this paper, author has introduced the full security by achieving the dual system encryption strategy. The main challenge of applying dual system encryption strategy to ABE is the structure of keys and Ciphertext. In IBE or HIBE system, structure of keys and ciphertexts are both associated with the same type of simple object that is identities. In this paper, author presents two completely secure useful encryption plans. Their first result is a completely secure property based encryption (ABE) plan.

N. Attarpadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts,"[4]

This paper [4] proposes the principal of key-approach characteristic which is based on encryption (KP-ABE) with consideration of non-monotonic access structures and with regular ciphertext size.

M. Chase and S. Chow, "Improving privacy and security in multi authority attribute-based encryption," [5]

The author has described that, system has single authority which can monitor every single attribute of all users is unrealistic. Therefore Multi-authority attribute-based encryption which enables a more realistic classification of attribute-based access control, such that the advantage is that different authorities are responsible for assigning different sets of attributes to users.

IV. PROPOSED SYSTEM MODEL

In this system, there are exist 5 entities:

1) Single i.e. global **Certificate Authority(CA)**
2) Multiple **Attribute Authority(AA's)**

ISSN (O) 2454-9665
ISSN (P) 2454-0663

3) **Data Owner**

4) **User**

5) **Cloud server**

A) The system will execute using below procedure:

1. AA registers to CA to get (aid,aid.cert)
2. User register to CA to get (uid,uid.cert)
3. User gets his/her SK from any t out of n Aas.
4. Owners get PK from CA
5. Owners upload (CT) to the cloud server.
6. Users download (CT) from the cloud server.

- The system can perform Attribute revocation method can efficiently achieve both forward security and backward security. An attribute revocation method is efficient in the sense that it incurs less communication cost and computation,
- Cost, secure in the sense that it can achieve both backward security and forward security.

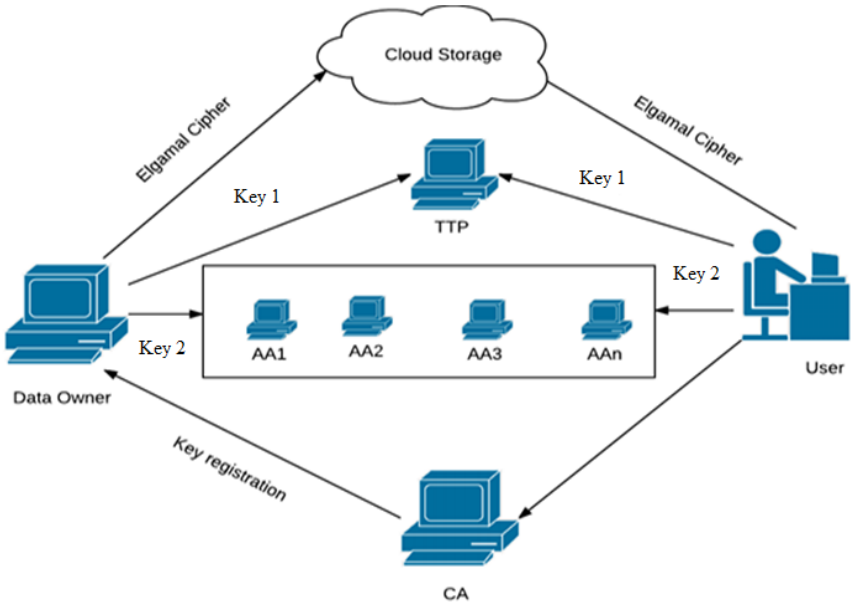

Fig. 1: proposed system architecture

There are five types of entities in the system as in Fig 1: a certificate authority (CA), characteristic authorities (AAs), data owner (owners), the cloud server (server) and data consumers (users). The CA is a global trusted certificate authority in the scheme. It sets up the system and accepts the registration of all the users and AAs in the system. For each legal user in the system, the CA assign a global unique user identity to it and also generates a global public key for this user. However, the CA is not involved in any attribute organization and the formation of secret keys that are connected with attribute [6] [8]. For example, the CA can be the Social Security Administration, an independent agency of the United States government. Each user will be issued a Social Security Number (SSN) as its global identity. Every AA is an independent attribute influence that is responsible for entitling and revoking user's attributes according to their role or identity in its domain. In our scheme, every attribute is associated with a single AA, but each AA can manage an arbitrary number of

ISSN (O) 2454-9665
ISSN (P) 2454-0663

attributes. Every AA has full control over the structure and semantics of its attributes. Each AA is responsible for generating a public attribute key for each attribute it manages and a secret key. For each user reflecting his/her attributes.

B) Mathematical Module:

Let's,

D is denoted by dataset which includes the n number of paragraphs in file

D={Ci1,Ci2,Ci3…..Cin}

Here, C is the intermediate module which holds the data processing for security as well as data privacy.

C={C1,C2,C3…Cn}

C1= key generation

C2= encryption of data

C3= Authentication and Authorities verification phase

C4 = decryption of data

C5=Revocation phase

C6=Resign key generation

Here R is web base approach which handles the parallel searching, the result of query classified into n number of result pages. All R instances might be different authorities which will holds the data and when intermediate module generate the requires it will execute parallel.

R={R1, R2,R3….Rn}

4.3 Algorithms:

MD5 AES 128 with 16 bit encryption

For user m1's ID attribute

{Generate user m1 ID; Set of users m1's attribute -> Domain B;

Attribute checks in Domain manager;

Now, Generate Random Value[unique] attribute = i;

Generate Random value [user] = r;

Secret key= (i+r).user m1's ID; }

/* Encrypting user data along with ID */

Encrypt (user ID. (i+r)+data)

/* Decrypting user data along with ID */

Decrypt (user ID. (i+r)+data)

In this proposed research work, we are going to use four algorithms to be executed: Setup, KeyGen, Encrypt, and Decrypt. And the parameters described in this scheme and parameters of the ABE scheme are the same. It will be depicted as follows.

1) Setup(d): The authority chooses several uniform and random numbers t1, ..., tn, y from Zq, and makes public the public key, PK =(T1 = g t1 , ..., Tn = g tn , Y = e(g, g) y). And keeps the master key, MK = (t1, ..., tn, y) be secret.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

2) KeyGen(AU−KP , PK, MK): The authority generates private key components for each leaf node x in the access structure. The private key components are Dx = g qx(0) ti , where i is equal to a leaf node in the access structure. These components will be merged into the user's private key, and be sent to a user.

3) Encrypt (M, ACT , PK): Data owner chooses a random number s from Zq and encrypts a message M ∈ G2 with a set of attributes ACT , and then he generates the encrypted data.

4) Decrypt (CT, D): This algorithm can be executed by a recursive algorithm, It inputs the encrypted data, user's private key, and nodes of the access structure in user's private key. If i is equal to the leaf node, and i is in the access structure of user's private key, it will call the decrypt node function, e(Dx, Ei) = e(g, g) s·qx(0). If i is not in the access structure of an user's private key, it will call the decrypt node function; and it outputs invalid. If i is not equal to the leaf node, it will call decrypt node function and input all children nodes of node x, z, and use lagrange coefficient to compute to obtain e(g, g) s·qx(0). Finally, the decryption algorithm call the decrypt node function on the root of the access structure and compute e(g, g) ys = Y s , if and only if the encrypted data satisfies the access structure of private key. And the message M = E Y s can be obtained.

V. RESULT

After implementing some part of system we got system performance on satisfactory level. The below table shows the first algorithm performance for user plain data conversion as well encryption decryption.

Data Size in MB	Encryption time (Milliseconds)		Decryption time (Milliseconds)	
	Existing	Proposed	Existing	Proposed
5	595	515	724	612
10	1120	1026	1132	1033
15	1680	1547	1687	1556
20	2260	2064	2231	2033

Table 1: System performance (Estimated)

VI. CONCLUSION

This investigation explains a revocable multi-authority CP-ABE scheme that can support efficient attribute revocation. Then the effective data access control scheme for multi-authority cloud storage systems is proposed. It eliminates Decryption overhead for users according to attributes .This secure attribute based cryptographic technique for robust data security that's being shared in the cloud .This revocable multi-authority CPABE scheme with Verifiable outsourced decryption and proved that it is secure and verifiable .The revocable multi-authority CPABE is a efficient technique, which can be applied in any remote storage systems and online social networks etc.

FUTURE WORK

The current architecture is very efficient for security purpose, but sometime its utilized multiple resources. When the such system allocate multiple resources it will generate a lot of dependencies. For the next updation we can focus on minimum resource utilization with system flexibility like power, VM's, network, memory etc.

ISSN (O) 2454-9665
ISSN (P) 2454-0663

REFERENCES

[1] R. Bobba, H. Khurana, and M. Prabhakaran, "Attribute-sets: A practically moticated enhancement to attribute-based encryption" 2009.

[2] Sahai and B. Waters, proposed the approach "Fuzzy identity-based encryption" 2005.

[3] Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, "Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption" 2005.

[4] N. Attarpadung, B. Libert, and E. Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in 2011.

[5] M. Chase and S. Chow, "Improving privacy and security in multi authority attribute-based encryption," in *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, pp. 121–130.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," in INFOCOM'10. IEEE, 2010, pp. 534–542.

[7] K. Yang, X. Jia, and K. Ren, "Attribute-based fine-grained access control with efficient revocation in cloud storage systems," in AsiaCCS'13.ACM, 2013, pp. 523–528.

[8] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, "DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEE Trans. Info. Forensics Security, vol. 8, no. 11, pp. 1790–1801, 2013.

[9] Wei Li, KaipingXue, YingjieXue, and Jianan Hong, "TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage", IEEE Transactions on Parallel and Distributed Systems,Vol. PP,Issue 99, pp.1-12, 2015.

[10] Mohamed Nabeel and Elisa Bertino, Fellow, IEEE, "Privacy Preserving Delegated Access Control in Public Clouds", IEEE Transactions on Knowledge and Data Engineering, Vol. 26, Issue 9, pp.2268-2280, 2014

[11] Kan Yang, Student Member, IEEE, and XiaohuaJia, Fellow, IEEE, "Expressive, Efficient, and Revocable Data Access Control for MultiAuthority Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 7, pp. 1735-1744,2014

[12] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and MircoMarchetti, "Scalable Architecture for Multi-User Encrypted SQL Operations on Cloud Database services", IEEE Transactions on Cloud Computing, Vol. 2, Issue4, pp. 448-458, 2014

[13] Luca Ferretti, Fabio Pierazzi, Michele Colajanni, and MircoMarchetti, "Performance and cost evaluation of an adaptive encryption architecture for cloud databases", IEEE Transactions on Cloud Computing, Vol. 2, Issue 2,pp.143-155, 2014

[14] Luca Ferretti, Michele Colajanni, and MircoMarchetti, "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases", IEEE Transactions on Parallel and Distributed Systems, Vol. 25, Issue 2, pp.437-446,2014