RESEARCH ARTICLE OPEN ACCESS

A Threshold Multi-Authority Access Control System

Immanuel Joshua Paul[1], B.Prashanth[2] ,V.Kameshwaran[3],Ezhil Dyana[4]
[1,2,3,]U.G. Students, Dept of CSE, Alpha College of Engineering, Chennai.
[4]Asst.prof. Dept of CSE, Alpha College of Engineering, Chennai.

Abstract:

Bit-Exchange Encryption is the cryptographic conducting tool to assurance data owners enduring control above their data in public cloud storage. The earlier ABE plans include one and only power (Authority) to keep up the entire trait (Key) set, which can carry a solitary (single) point bottleneck on both safety and execution. In this way, some multi- power (Multi-Authority) plans are proposed, in which various powers independently keep up disjoint attribute subsets. In any case, the single-point bottleneck issue stays unsolved. In this paper, from another point of view, we conduct a threshold multi-authority 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, taking advantage of (t; n) limit mystery sharing, the expert (Master) key can be shared among numerous powers, and a legitimate client can produce his/her mystery (Private) 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 hybrid one, which fulfils the attributes originating from various authorities and accomplishing security.

Keywords — Bit-Exchange based encryption; Attribute Based Encryption(ABE); Threshold Secret Sharing(t,n).

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, people so far fear to mishandle the appropriated registering. Generally a couple of people trust that cloud is perilous spot and once you store your data 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. 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 as proposed, which can be divided into two categories:

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 proprietor 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. 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 show 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 (Multi-Authority) Bit-Exchange(BE) 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 BE plans, there is dependably a mystery key used to create trait private keys, we present (t, n) limit mystery (Private) sharing into our plan to share the mystery key among powers. In this plan, we reclassify the mystery key in the customary BE 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 primary attempt to address the single point bottleneck on both security and execution in BE access control plans in broad daylight distributed storage.

III. Our Proposed System Model

In this system, there are exist 5 entities.
1) Single i.e. Global Certificate Authority(CA)
2) Third Party Auditor(TPA)
3) Data Owner
4) Client
5) Cloud Server

The system will execute using below procedure:

1) TPA 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 TPA's.
4) Owners get PK from CA
5) Owners upload (CT) to the cloud server.
6) Clients download (CT) from the cloud server.

- The system can perform Attribute revocation method can efficiently achieve together 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.

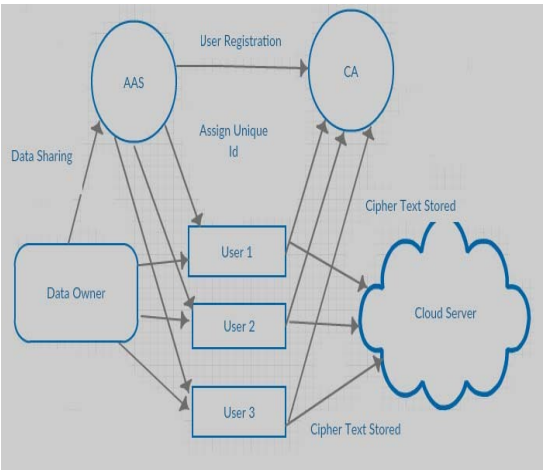

Fig 1.Proposed System Architecture

There are five sorts of substances in the framework as in Fig 1: an endorsement power (CA), Third Party Auditor (TPAs), information proprietor (proprietors), the cloud (server) and information purchasers (clients). The CA is a worldwide trusted testament power in the plan. It sets up the framework and acknowledges the enlistment of the considerable number of clients and TPAs in the framework. For each legitimate client in the framework, the CA appoints a worldwide one of a kind client character to it furthermore produces a worldwide open key for this client. Be that as it may, the CA is not included in any property association and the development of mystery keys that are associated with quality [6] [8]. For instance, the CA can be the Social Security Administration, an autonomous office of the United States government. Every client will be issued a Social Security Number (SSN) as its worldwide personality. Each TPA is a free trait impact that is in charge of entitling and repudiating client's credits as indicated by their part or personality in its area. In our plan, each characteristic is connected with a solitary TPA, yet every TPA can deal with a self-assertive number of qualities. Each TPA has full control over the structure and semantics of its qualities. Every TPA is in charge of producing an open characteristic key for every property it oversees and a mystery key. For every client mirroring his/her properties.

IV. Algorithm

DES with 64 bit encryption:
For user m1's ID attribute

Generate user m1 ID; Set of users m1's attribute for Domain B ;
Attribute check in Domain manager;
Now, Generate Random Value [unique] attribute = i;
Generate Random value [user] = r;
Secret key= (i+r).user m1's ID;

/*Encrypting client data along with ID.*/
Encrypt user ID. (i+r) + data).

/*Decrypting client data along with ID.*/
Decrypt (user ID. (i+r)+data)

In this proposed research work, we used 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.
2) **KeyGen(AUKP , 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 users private key, and be sent to an user.
3) **Encrypt(M, ACT , PK):** Data owner chooses a random number s from Zq and encrypts a message M belongs to 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, users private key, and nodes of the access structure in users private key. If i is equal to the leaf node, and i is in the access structure of users private key, it will call the decrypt node function, e(Dx, Ei) = e(g, g) sqx(0). If i is not in the access structure of an users 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) sqx(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. Security Analysis

In this system, we analyse that all the user's secrets *{Uuid}* are exposed to each *TPA*. If suppose the revoked user corrupts any *TPA* and some non-revoked users, then it can derive the key update key easily and apply it to update its secret key. This security weakness is addressed in our system [8]. For security purpose, we are using random character generating algorithm.

Random r = new Random ();
ch = (char) (Math.floor (26 * r.nextDouble () +65));

VI. Result Analysis

In the wake of executing some piece of framework we got framework execution on agreeable level. The beneath table demonstrates the principal calculation execution for client plain information change too encryption unscrambling.

TABLE I. TABLE OF SYSTEM PERFORMANCE

Data size in MB(MegaByte)	Encryption Time (Milliseconds)		Decryption Time (Milliseconds)	
	Existing	Proposed	Existing	Proposed
5	595	505	724	599
10	1120	1016	1132	1021
15	1680	1534	1687	1538
20	2260	2054	2231	2021

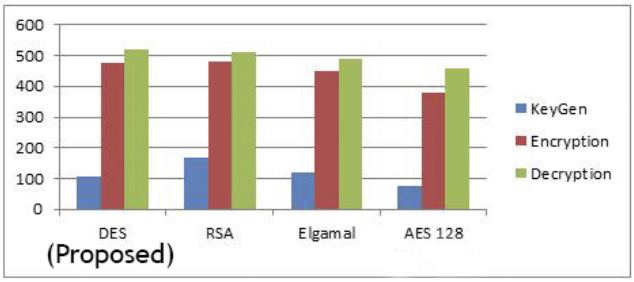

Fig. System Result Graph

Here above graph shows the system performance for cryptography algorithm. X shows the plain data size and Y show times required in Milliseconds. The base on analysis it is more efficient than all existing cryptographic techniques.

Conclusion

This analysis explains a revocable multi-authority CP-ABE proposal that can support capable attribute revocation. Then the helpful data access manage scheme for multi-authority cloud storage systems is planned. It eliminate Decryption slide for users according to attributes. This secure attribute based cryptographic technique for robust data security that's shared in the cloud .This revocable multi-authority CPABE scheme with Verifiable outsourced decryption and prove that it is protected and verifiable .The revocable multi-authority CPABE is the efficient technique, which can be applied in some remote storage system and online common networks etc.

FUTURE WORK

The current architecture is very efficient for security purpose, but sometime it's utilized multiple resources. When such a system allocates 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.

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. 121130.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving secure, scalable, and fine-grained data access control in cloud computing, in INFOCOM10. IEEE, 2010, pp. 534542.

[7] K. Yang, X. Jia, and K. Ren, Attribute-based fine-grained access control with efficient revocation in cloud storage systems, in AsiaCCS13.ACM, 2013, pp. 523528.

[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. 17901801, 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