ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

A Multi-Authority Access Control System in Cloud Computing Using Network Security

[1] Ms. Vibhute Shubhangi Prakash,[2] Prof. Mr. Kale Navnath D.
[1][2] Department of Computer Engineering
PVPIT College of Engineering, Bavdhan Pune, Savitribai Phule Pune University, Maharashtra.

***Abstract*— Data access control is an efficient way to provide the data security in the cloud.and Attribute-based Encryption (ABE) technique cryptographic conducting tool to guarantee data owners direct control on their data in public cloud storage. In this paper, from another point of view, system lead an edge multi-power CP-ABE access control plan for open distributed storage, named TMACS. In TMACS, exploiting (t; n) limit mystery sharing, When system verify to the user the TTP work like a SDN. Its having data controller that can evaluate the each request base on ad-hoc data table, if user is authenticated system can provide the access to specific user. Besides, by proficiently joining the customary multi-power plan with system, system build a half and half one, which fulfils the situation of traits originating from various powers and accomplishing security and framework level strength. The network security mechanism also fulfil with this approach, the system has evaluate on physical network environment with 2 to 4 physical devices and got satisfactory results than existing TMACS.**

***Index Terms*— Access Control, Attribute Based Encryp-tion, Cloud computing, CP-ABE, Identity-based encryption, multi-authority, Outsourcing, Revocation,SDN Controller,Wireless Router.**

1. INTRODUCTION

There are numerous focal points of distributed storage; there still information security is a noteworthy deterrent in the distributed computing [4]. 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 [6] 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 con-trol 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:

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

In KP-ABE plans [1], 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 arrange-ment 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 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[8] plans pro-posed, 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

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

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. An SDN Controller [7] is applications in Software-defined Network are the brains of the Network. Is this service manages flow control to enable intelligent network like as wireless router. In existing system like SDN Work as a controller serves as a sort of Operating system for the network. By taking the control plane off the network hardware and running it as software instead, the controller facilitates automated network management and makes it easier to integrate and administer business applications.

II.PROCEDURE FOR PAPER SUBMISSION

A. Review Stage

In paper [1] represents in access control systems for public cloud storage, brings a single-point bottleneck on both security and performance against the single authority for any specific attribute. First design multi-authority access control architecture to deal with the problem. By introducing the combining of (t, n) threshold secret sharing and multi-authority CP-ABE scheme, then proposes and realizes a robust and verifiable multi-authority access control system in public cloud storage, in which multiple authorities jointly manage a uniform attribute set. Data access control is an effective way to ensure the data security in the cloud.

In Paper [2] demonstrated that, with the component CUK a revoked user can transform the newly encrypted cipher-text to a previous version, which can be further decrypted with his/her revoked old-version secret keys. Author also proposed a multi-authority ciphertext-policy attribute-based encryption- based data access control for cloud storage, in which the authors claimed that the mechanism in dealing with attribute revocation could achieve both forward security and backward security. Unfortunately, our further analysis and investigation show that their work adopts a bidirectional re-encryption method in ciphertext updating, so security vulnerability appears. Our proposed attack method demonstrates that a revoked user can still decrypt new ciphertext that are claimed to require the new-version secret keys to decrypt.

In Paper [3] Author proposed a semi-anonymous attribute-based privilege control scheme AnonyControl and a fully-anonymous attribute-based privilege control scheme AnonyControl-F to address the user privacy problem in a cloud storage server. The proposed scheme was able to protect users privacy against each single authority. The scheme was tolerant against authority compromise, and compromising of up to (N 2) authorities did not bring the whole system down. Author provides detailed about security and feasibility of the scheme.

In Paper [4] Author is proposed a revocable multi-authority CP-ABE scheme, where efficient and secures revocation method introduced to solve the attribute revocation problem in the system. However, it is difficult to directly apply existing CP-ABE schemes to data access control for cloud storage systems because of the attribute revocation problem. Our attribute revocation method can efficiently achieve both forward security and backward security. The analysis and simulation results show that our proposed data access control scheme is secure in the random oracle model and is more efficient than previous works.

In paper [5] work proposes the first key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures (i.e., that may contain negated attributes) and with constant cipher text size. Then describe a new efficient identity-based revocation mechanism Attribute-based encryption comes in two favours. In key-policy ABE schemes (KP-ABE), attribute sets are used to annotate cipher texts and private keys are associated with access structures that specify which cipher texts the user will be entitled to decrypt. Cipher text-policy ABE (CP-ABE) proceeds in the dual way, by assigning attribute sets to private keys and letting senders specify an access policy that receivers' attribute sets should comply with.

In Paper [6] it shows that the proposed scheme is more versatile and supports many practical scenarios more naturally and efficiently. Attribute-Based Encryption (ABE) is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. CP-ABE is a form of ABE where policies

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

are associated with encrypted data and attributes are associated with keys. In this work author focused on improving the flexibility of representing user attributes in keys. Specially, they proposed Cipher text Policy Attribute Set. In this work they proposed CP-ASBE a form of CP-ABE that organizes user attributes into a recursive family of sets and allows users to impose dynamic constraints on how attributes may be combined.

In Paper [7] author has discuss SDN that manages flow control to enable intelligent networking by explaining its benefits, features and clarifying in detail its layers. The SDN controller serves as a sort of operating system (OS) for the network. It describes the multicontrollers briefly when it talks about system to enhance the control layer high performance and security

B. Final Stage

In this system, there are exist 6 entities:
1) Single i.e. global Certificate Authority(CA)
2) Multiple Attribute Authority(AAs)
3) Data Owner
4) User
5) TTP as SDN Controller
6) Cloud server
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)User gets his/her SK from any t out of n Aas.
3) Owners get PK from CA
4) Owners upload (CT) to the cloud server.
5) 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 back-ward security and forward security.[6]

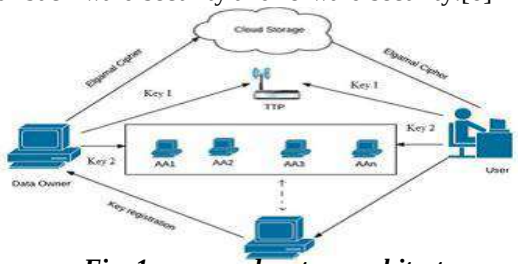

Fig. 1. proposed system architecture

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 assigns 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 users 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 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.
When system verify to the user the TTP work like a SDN Controller. Its can evaluate the each request base on ad-hoc data table, if user is authenticated system can provide the access to specific user. The network security mechanism also fulfil with this approach, the system has evaluate on physical network environment with 2 to 4 physical devices and got best result to TMACS.

I. MATH

Algorithm 1: Elgamal Encryption scheme
1.1 Key Generation phase
Input: Plain text as text data d.
Output: a,b,p,g all are private keys
Step 1: Initialize the random message from user as d. (it should be any kind of text data).
Step 2: initialize a,b,p,g for private key purpose.
Step 3: generate P as randomly base on bit length of d. so, Ans[]=GetRandomP(d.getbyte).bitlength base on probable prime no.
Step 4: p=Ans[0] g=Ans[1]
Step 5: Generate a using P a=RandomA(p)
Its calculate like p.bitLength()-1,Random. Step 6: Calculate b= calculateb(g, a, p); so, b= g.modPow(a, p);
Step 7: Key generation done

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

1.2 Encryption

Input: Text data d,p,b,g Output: cipher as C1 and C2.
Initialize BigInteger [] rtn = null,null;
Message=d.getbytes();
[]result= ElGamal.encrypt(message, p, b, g);
[] rtn = fnull; nullg;
k = ElGamal.getRandomk(p); C1 = g.modPow(k, p);
C2 = m.multiply(b.modPow(k, p)).mod(p);

1.3 Decryption

Input: input c1 and c2 as cipher a and p as private keys Output: Plain text d.
Step 1: m = C2.multiply (C1.modPow (a.negate(), p)).mod (p);
Step 2: return m.

Algorithm 2: SQL Injection and prevention algorithm for Database Security

1: Procedure SPMA (Query, SPL [ ]) INPUT: Query=User Generated Query SPL [ ]=Static Pattern List with m AnomalyPattern
2: For j = 0 to m do
3: If (AC (Query, String.Length(Query), SPL[j][0]) = =0)then
4: Calc anomaly score
5: If ( ) Score Value Anomaly = Threshold
6: then
7: RetrunAlarm .. Administrator
8: Else
9: Return Query. Accepted
10: End If
11: Else
12: Return Query .Rejected
13: End If
14: End For
End Procedure

IV. MATHEMATICAL MODEL

Lets,
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,C3Cn C1= key generation
C2= encryption of data
C3= Authentication and Authorities verification phase

$$t = \sum_{k=0}^{n} (Pk), TTP$$

C4 = decryption of data
Download the file using below function
DF = (IDgroup, IDdata ,CE, EK ,tdata), DF
C5=Revocation phase using polynomial function

$$f_p(x) = \prod_{j=1}^{m+1}(x - V_j) = \sum_{j=0}^{m+1} a_j x^j \pmod q$$

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
1. When user request for any file for cloud server

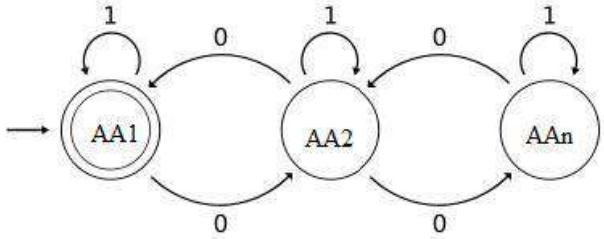

Fig. 2. State the each authority verification

2. Any t(n) return 1 then it will provide the private key otherwise state has change to another authority.
M = (Q, , , q0, F)
where Q = AA1, AA2,= 0, 1,
q0 = AA1,
F = AA1, and is defined by the following

TABLE I

	0	1
AA	AA1	AA2
AA	AA2	AAn

STATE TRANSITION TABLE

V. IMPLEMENTATION DETAILS

System requirements:

1) System interfaces: Windows Operating System
2) User interfaces: User interface using JSP and Servlet
3) Hardware interfaces: Processor: - Intel Pentium 4 or above

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 8, August 2017

Hard Disk: - 20GB
Memory: - 1GB
Other peripheral: - Printer
4) Software interfaces: Front End: Jdk 1.6.0, Netbeans 6.9.1, IE 6.0/above
Back-End: Mysql 5.1, Heidi SQL
5) Communication interfaces: System will use TCP/IP pro-tocol for establishing connection and transmitting data over the network. System will use Ethernet for LAN and Router
6) Services: Amazon EC2 for cloud

VI. EXPERIMENTAL RESULT

For the system evaluation system create 2 machines on physical environment with Wi-Fi and 10 VM with Amazon EC2 as public cloud environment.. The system is implemented on java 3-tiera architecture framework with INTEL 2.8 GHz i3 processor and 4 GB RAM with public cloud Amazon EC2 consol. For the system evaluation system create 2 machines on physical environment with Wi-Fi and 10 VM with Amazon EC2 as public cloud environment. After implementing some part of system to get system performance is satisfactory level. The below table shows the first algorithm perform for user plain data conversion into the encryption and decryption time in milliseconds. And use the less time to use this algorithm.

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 II
SYSTEM PERFORMANCE (ESTIMATED)

In second experiment Figure-3 shows data encryption per-formance which works to show that the data it will encrypt in how much time in seconds. Suppose there is a 100kb data is encrypted in 150 sec so the result will display automatically in that time of encryption data from the users.

Fig. 3. Data encryption performance based on data size

VII. 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 thats being shared in the cloud .This revocable multi-authority CPABE scheme with Verifiable outsourced decryp-tion and proved that it is secure and verifiable .The revocable multi-authority CPABE is an efficient technique, which can be applied in any remote storage systems and online social networks etc.

REFERENCES

[1] 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.24, NO. 06, October 2016.

[2] K. Yang, X. Jia, K. Ren, B. Zhang, and R. Xie, DAC-MACS: Effective data access control for multi-authority cloud storage systems, 2013 Proceedings IEEE INFOCOM Year: 2013. OR [2]. Jianan Hong; Kaiping Xue; Wei Li Comments on DAC-MACS: Effective Data Access Control for Multiauthority Cloud Storage Systems/Security Analysis of Attribute Revocation in

Multiauthority Data Access Control for Cloud Storage Systems IEEE Transactions on Information Forensics and Security, Year: 2015, Volume: 10, Issue: 6

[3] Taeho Jung, Xiang-Yang Li, Zhiguo Wan, and Meng Wan, Control Cloud Data Access Privilege and Anonymity with Fully Anonymous Attribute-Based Encryption, IEEE transactions on information forensics and security, VOL. 10, NO. 01, January 2015.

[4] Kan Yang and XiaohuaJia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage, IEEE Transactions on parallel and distributed systems, VOL. 25, NO. 07, July 2014.

[5] S. Kamara and K. Lauter, ”Cryptographic cloud storage,” in Proceedings of the 14th Financial Cryptography and Data Security.Springer, 2010, pp. 136-149. [6] R.Ostrovsky, A. Sahai, and B.Waters, ”Attribute-based encryption with nonmonotonic access structures,” in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2014, pp. 195-203.

[6] W. Xia, Y. Wen, C. Heng Foh, D. Niyato, and H. Xie, A survey on software-defined networking, IEEE Communications Surveys and Tutorials, vol. 17, no. 1, pp. 2751, 2015. View at Publisher View at Google Scholar View at Scopus

[7] Hideaki Ishii, Roberto Tempo, and Er-Wei Bai, Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud, IEEE Transac-tions on parallel and distributed systems, VOL. 24, NO. 06, June 2013.

[8] 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.

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

[10] Z. Liu and Z. Cao, ”On efficiently transferring the linear secret sharing scheme matrix in ciphertext-policy attribute-based encryption,” IACR Cryptology ePrint Archive, vol. 2010, p. 374, 2010.

[11] S. Patil, P. Vhatkar, and J. Gajwani, ”Towards secure and dependable storage services in cloud computing,” International Journal of Innovative Research in Advanced Engineering, vol. 1, no. 9, pp. 57-64, 2014.

[12] N. Attrapadung, B. Libert, and E. Panaeu, ”Expressive key policy attribute based encryption with constant-size ciphertexts,” in Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Springer, 2011, pp. 90 108.

[13] 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

[14] Open Networking Foundation (ONF), https://www.opennetworking.org/