ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Decentralised Access Control with Aggregate Key Encyryption For Data Stored In Cloud

Mr. Ashwin Chandra C, Ms. Dharani S

PG Student, M.E (CSE), Valliammai Engineering College, Chennai, India[1, 2]

ABSTRACT - We propose a perfect decentralized access control scheme with aggregate key encryption for data stored in cloud. This scheme provides secure data storage and retrieval. Along with the security the access policy is also hidden for hiding the user's identity. This scheme is so powerful since we use aggregate encryption and string matching algorithms in a single scheme. The scheme detects any change made to the original file and if found clear the error's. The algorithm used here are very simple so that large number of data can be stored in cloud without any problems. The security, authentication, confidentiality are comparable to the centralised approaches.

KEYWORDS: Aggregate key encryption, String matching algorithms, Attribute based encryption.

I. INTRODUCTION

Cloud is a market-oriented distributed computing system consisting of a collection of inter-connected and virtualized computers that are dynamically provisioned and presented as one or more unified computing resources based on service-level agreements (SLAs) established through negotiation between the service provider and consumers. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet.

Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).Security is needed because data stored in clouds is highly sensitive, for example, medical records and social networks. User privacy is also required so that the cloud or other users do not know the identity of the user. Thus it is a complex system which possesses highly securable processes. So it must need a proper systematic scheme to manage data.

Recently S. Yu, C. Wang, K. Ren, and W. Lou proposed a system which is based on attribute based encryption for Fine-Grained Access Control of Encrypted Data. To keep sensitive user data confidential against unauthenticated servers, existing schemes usually apply cryptographic methods by disclosing data decryption keys only to authorized users. We combine techniques of attribute-based encryption [2] (ABE)and several other techniques. The problem in this latest technique is that Single data owner will be easily be overwhelmed by the key management overhead. So apart from security concerns we have to concentrate on the key distribution also.

Search on encrypted data is also a major concern in cloud. Also [4] hiding of access policy is also needed. So encryption must be done in a perfect manner. Several recent encryption algorithm fails in searching process. But the best encryption algorithm which also makes search better is aggregate type encryption [1].Thus this encryption technique is used mostly.

Providing security only is very simple but providing security with privacy[2] is very much difficult. Maintaining the privacy is very much important because it is very easy for intruders to access the confidential data. Since very confidential data's are stored in cloud it is very much needed to maintain the security and privacy. Using homomorphic encryption, the cloud receives cipher text of the data and performs computations on the ciphertext and return's the encoded value. Now the user converts the value, but the cloud does not know what data it has operated on. These are the common problems in cloud. So this area must be concentrated.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Transactions done in the cloud should also be noted periodically. The user should be verified and should give appropriate permission for them. Permission criteria are carefully handled because users may change the data unnecessarily. So this area should be concentrated too much. Adding this kind of feature may automatically reduce the efficiency of the algorithm, so the algorithm designed must be very efficient. It must consider all the additional features and the system should be maintained accordingly.

Consider the following situation: A student from a college found out some malpractices done by some employees in college. Then the student takes steps to tell the details about the malpractice done in the college. Now he will report the malpractice done by the employees of the college to the university which controls the college. While reporting there are some conditions to be checked seriously. First the student should prove the identity because the university should believe that the message came from an authorised person. Second there should not be any interference. Also if any change is done for the original message then it should be found out and the file is recovered. Thus in this paper the above problems are described and rectified.

An area where access control is widely being used is health care[14]. Clouds are being used to store sensitive information about patients to enable access to medical professionals, hospital staff, researchers, and policy makers. It is important to control the access of data so that only authorized users can access the data. Using Aggregate key encryption [1], the records are encrypted under some access policy and stored in the cloud. Users are given sets of keys. Only when the users have matching set of keys, can they decrypt the information stored in the cloud. Access control is also gaining importance in online social networking.

Existing concepts in cloud are centralised nature so security can't be provided in a perfect manner. The schemes which use symmetric key encryption also not a better choice. Earlier work by Zhao provides privacy preserving authenticated access control in cloud[8]. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. Thus we propose a system which consider all the above situations and find solutions to the respective problems.

A. Our Contributions in this paper

The main contribution of this paper is

1) Distributed access control[11] of data stored in cloud so that only authorized users with valid key can access them.

2) Authentication of users who store and modify their data on the cloud.

3) The identity of the user is protected from the cloud during authentication.

4) The architecture is decentralized, meaning that there can be several KDCs for key management.

5) Encryption is based upon aggregate key encryption which is highly secure.

6) The protocol supports multiple read and write on the data stored in the cloud.

7) The costs are comparable to the existing centralized approaches and feature are more than the centralised approaches.

8) Access policy is defined so that valid user can read/write the data in the cloud.

B. ORGANISATION

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The paper is organised as follows. In section II the related work is presented. In section III the mathematical background and assumptions are presented. In section IV our scheme is presented. In section VI the security is analysed. In section VII the computation complexity and comparison with other work is presented. In section VIII the conclusion is presented.

II. RELATED WORK

Attribute based encryption[7][8][12][13](ABE) was proposed by Sahai and Waters [26]. In ABE, a user has a set of attributes based on the user in addition to its unique ID. In Key-policy ABE or KP-ABE (Goyal et al.[27]), the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes. In Ciphertext-policy, CP-ABE ([28],[29]), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.

All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase [2] proposed a multi-authority ABE, in which there are several KDC authorities(coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi-authority ABE protocol was studied in [7], [8], which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters [9] proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. However, as mentioned earlier in the previous section it is prone to replay attack.

To reduce or block replay attack we use string matching algorithms[3][5] which is more efficient and perfect in security. It works more efficient than all other matching algorithms.

III. BACKGROUND

In this section, we describe our cloud storage model, adversary model and the assumptions we have made in the paper.

A. Assumption

We make the following assumptions in our work.

1) The cloud is honest-but-curious, which means that the cloud administrators can be interested in viewing users.

2) Users can have either read or write or both accesses to a file stored in the cloud.

3) All communications between users/clouds are secured by Secure Shell Protocol, SSH.

IV. PROPOSED SCHEME

We explain public-key cryptosystems which produce a set of constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts is possible. The best thing is that it is very easy to combine aggregate key into a single key, but encompassing the power of all the keys being aggregated. The secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential and very much authenticated. This matching aggregate key can be easily send to others or be stored in a storage media with very limited secure storage. We provide formal security analysis of our

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

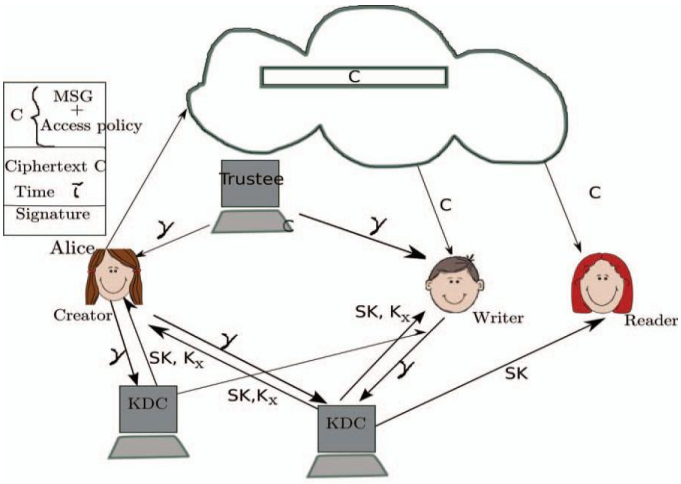
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

schemes in the standard model. This can also set for some other applications also. Our schemes give the first public-key patient-controlled encryption for flexible hierarchy and security, which was yet to be described.



ARCHITECTURE DIAGRAM

ALGORITHM FOR ENCRYPTION

1)Setup:Give A param =hg; g1; _ _ _ ; gn; gn+2; _ _ _ ; g2ni.
Randomly choosean index i_ where 1 _ i_ _ n. Define v = grg_1 i_where r 2R Zp. Give A the public-key pk = v.Since g; _ and r are chosen uniformly at random choice, the parameter and v have different distribution to that in the real construction.

2) Query phase 1. A may issue an OExt query for a set S. If i_ 2 S, abort; otherwise, return
KS = Yj2S
gr
n+1_jg_1
n+1_j+i_ :
We can see that gr
n+1_jg_1
n+1_j+i_ =(grg_1i_)_n+1_j=v_n+1_j= g
n+1_j .
Thus theaggregate key is computed correctly if i_ =2 S.
3) Challenge. A outputs two messages m0;m1 and an index ic. If ic 6= i_, abort. Otherwise, randomly choose a bit b 2 f0; 1g and return C_ =hh; hr;mb _ Zi. Let h = gt, t 2 Zp, then hr = gtr = (grg_1 i_ gi_)t = (vgic)t which means C_ is a valid encryption of mb under the index ic if Z = ^e(gn+1; h).

4) Query phase 2. Answer the queries as in phase 1.Note that B is not allowed to issue an OExt query on any set S which contains ic.

5) Guess. A outputs a guess b0. If b0 = b, output 0 (Z = ^e(gn+1; h)); otherwise, output 1.

The probability that B correctly guesses ic is 1=n.Therefore, if S is chosen from RBDHE, then Pr[B(S) = 0] =12 . If S is chosen from PBDHE, then j Pr[B(S) = 0] _ 1 2 j = AdvA=n _ "=n. So B has an advantage of at least "=n in solving decisional n-BDHE in (G;GT).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

The creator needs to encrypt the message and then he wants to sign it. Creator needs to calculate one pairing e(g, g). Encryption takes place with 2 exponentiations to calculate each of C1,x. So this requires 2mET time, where m is the number of attributes. User needs to calculate 3 exponentiation to calculate C2,x and C3,x. So time taken for encryption is (3m + 1)E0 + 2mET + τP. To sign the message Y,W, S_ is and Pjs have to be calculated as well as H(C). So, time taken to sign is (2l + 2)E1 + 2tE2 + τH. The cloud needs to verify the signature generated. Time taken to verify is (l + 2t)τ ˆ P + l(E1 + E2) + τH. To read, a user needs only to decrypt the cipher text. This requires 2m pairings to calculate e(H(u), C3,x) and e(skπ(x),u, C2,x) and O(mh) to find the vector c. Decryption takes 2mτP+τH+O(mh). Writing is similar to creating a record. The size of cipher text with signature is 2m|G0|+m|GT |+m2+ |MSG| + (l + t + 2)|G1|.

Some notations used are listed below.

TABLE II
NOTATIONS

Symbols	Computation
E_x	Exponentiation in group G_x
τ_H	Time to hash using function H
$\tau_{\mathcal{H}}$	Time to hash using function $\mathcal{H}$
$\tau_P/\tau_{\hat{P}}$	Time taken to perform 1 pairing operation in $e/\hat{e}$
$\|G\|$	Size of group G
a	Number of KDCs which contribute keys to user

ALGORITHM FOR DECRYPTION

Algorithm KMP(P[1; : : : ;m]; T[1; : : : ; n])

input: pattern P of length m and text T of length n
preconditions: 1 _ m _ n
output: list of all numbers s, such that P occurs with shift s in T
q =0;
i =0;
while (i < n) /* P[1; : : : ; q] == T[i _ q + 1; : : : ; i]
f;
if (P[q + 1] == T[i + 1])
f;
q = q + 1;
i = i + 1;
if (q == m)
f;
output i _ q;
q _(q); /*slide the pattern to the rightg
g
else /* a mismatch occurred
f
(q == 0) f i i + 1 g
else f q _(q) g g gif

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Whenever revocation required, C0 needs to be recalculated. e(g, g) is previously calculated. So, only one scalar multiplication is needed. If the user revoked is Uu, then for each x, C1,x has to be recomputed. e(g, g) is already computed. Thus, only two scalar multiplication needs to be done, for each x. So a total of 2m_ + 1 scalar multiplications are done by the cloud, where m_ is the number of attributes belonging to all revoked users. Users need not compute any scalar multiplication or pairing operations.

String matching algorithms looks very simple and works very fast than any other algorithms. Its computation cost is very much less. At the same time it maintain the confidentiality, authentication and privacy factors in a best way. The main advantage of using string matching algorithm is that it check one by one word for matching. So that a 100% recovery is done in a very simple way. This is the best way for confidential matching of strings.

COMPLEXITY

In this section we present the computation complexity of the privacy preserving access control protocol. We will calculate the computations required by users (creator, reader, and writer) and that by the cloud.

TABLE I
COMPARISON OF OUR SCHEME WITH EXISTING ACCESS CONTROL SCHEMES

SCHEMES	CENTRALISED /DECENTRALISED	WRITE/READ ACCESS	ACCESS CONTROL TYPE	PRIVACY PRESERVING	USER REVOCATION
Public key	Decentralised	1-w-m-r	Public key	No authentication	No
IBE	Decentralised	1-w-m-r	Identity	No authentication	No
ABE	Centralised	m-w-m-r	Attribute	No authentication	No
OURS	Centralised	m-w-m-r	Aggregate	authentication	Yes

TABLE III
COMPARISON OF COMPUTATION AND SIZE OF CIPHERTEXT WHILE CREATING A FILE

Schemes	Computation by creator	Computation by cloud	Size of cipher text
IBE	(m + 2)E0	0	mlog |G0| + |GT | + mlogm + |MSG|
ABE	(2m + 1)E0 + ET + τP (encrypt)	mE0 + mET + (m + 1)Tp	(2m + 1)|G0| + |GT | +m2 + |MSG|
Ours	(3m + 1)E0 +2mET + τP (encrypt) (2l + 2)E1 + 2tE2 + τH (sign)	2mτP + τH + O(mh) (decrypt)	(l + 2t)τ ˆ P + l(E1 + E2) + τH (verify)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

V. CONCLUSION

Thus we presented a decentralized access control technique with aggregate key encryption combined with string matching algorithms, which provides user revocation and prevents replay attacks with high security. The cloud does not know the type of the user who stores information in the cloud, but only verifies the user's credentials. Key distribution is done in a decentralized way so that the keys can be managed easily with perfect security. The access policy can be hidden by using some internal sql operations with the help of the algorithm used. The limitation behind this is that for every recovery of file it will take some time for checking and recovery.

REFERENCES

[1] "Supplementary Material forKey-Aggregate Cryptosystemfor Scalable Data Sharing in Cloud Storage" Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, andRobert H. Deng, Senior Member, IEEE.

[2] "Improving Privacy and Security in Multi-AuthorityAttribute-Based Encryption" Melissa ChaseMicrosoft Research1 Microsoft WayRedmond, WA 98052, USA.

[3] "A Matching algorithm based on the cloud and positioning systems to improve carpooling" S.Di Martino,R.Galiero,C.Giorio University of Naples

[4] "Expressive CP-ABE with partially hidden access structures' Junzuo Lai,Yingjiu Li

[5] "Understanding Cloud Data Using Approximate String matching and edit distance" Joseph Jupin,Justin,Philadelphia

[6]" Data sharing on untrusted storage with attribute based encryption" Shucheng,

[7] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive, 2008.

[8] ——, "Attribute-based signatures," in CT-RSA, ser. Lecture Notes in ComputerScience, vol. 6558. Springer, pp. 376–392, 2011.

[9] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

[10] D. R. Kuhn, E. J. Coyne, and T. R. Weil, "Adding attributes to role-based access control," IEEE Computer, vol. 43, no. 6, pp. 79–81, 2010.

[11] S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

[12] H. K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-based signatures: Achieving attribute-privacy and collusion-resistance," IACR Cryptology ePrint Archive, 2008.

[13] "Attribute-based signatures," in CT-RSA, ser. Lecture Notes in ComputerScience, vol. 6558. Springer, pp. 376–392, 2011.

[14] "Mobile cloud for health care" Doan Hoang, Ling Fesman, Australia.