International Journal of Pure and Applied Mathematics
Volume 118 No. 24 2018
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue

http://www.acadpubl.eu/hub/

Triple Data Encryption algorithm based Multiple Authority Access Control in cloud system using optimal threshold

Mr. Prashant MininathMane[1],
Dr.C.M.Sheela Rani[2]
Ph.D. Scholar, Professor
Computer Science and Engineering Department,
KLEF University,
Vijaywada ,A.P.,India

May 24, 2018

Abstract

Cloud storage is most important service provided by cloud system. In cloud storage service, data is stored on cloud server from different owners. Access control to the stored data is one of big challenge for data owners. Stored data can be accessed by cloud authority without knowledge of data owners. To overcome this problem the new technology is introduced known as Cipher text policy attribute dependent encryption. This encryption technique is one of the suitable technique to offer proper data access control in cloud storage. In existing Attribute dependant encryption techniques, single authority maintain the attribute key for encryption and decryption of stored data which carry single point blockage on security as well as performance. This paper suggested optimal threshold based multi Authentication attribute dependant data access control method which offer significant, proficient and revoked data access control scheme.

***Key Words*:**cloud storage space, Access control, multiple authentication encryption & decryption, Attribute Dependant encryption.

1 Introduction

Cloud storage is the main feature of computer world. Cloud storage system allows the on demand use of the resources due to which cost of required resources for computing is reduces. So it provides low-cost on-demand computing resources. But due to which we need to store the data on cloud server and because of this number of privacy issues are come out. The most primary service of cloud system is to store data on cloud server which enables different owners to store their data on cloud system. Data stored on cloud is accessed by different consumers. Ifa consumer wants any Resource; he can demand the resource to cloud. On demand resource can be provided by cloud by proper authentication [12]. Users can store their data on trustful servers. Cloud servers allowed accessing the information from any place from any device in appropriate manner. There are number of schemes proposed to secure stored data in cloud. The attribute based encryption scheme is the one among all the schemes to provide the proper fine gained access control [14]. In this scheme, every user has secrete key issued by Central authority. This encryption scheme is very much dominant and flexible which implement attribute dependent policy to provide proper access control [10]. ABE scheme is very potential approach for storing the data in cloud system that offers proper access control policy over data which is encrypted [13]. Attribute dependent Encryption (ABE) is viewing as one of the most suitable schemes to attain fine grained cloud data access control in cloud system. The data owner stores their confidential data on cloud system, but cloud server may be untrusted or compromised. So CP ABE and KP ABE techniques are introduced to solve this problem. The Idea behind CP-ABE Scheme is data owner encrypt their data with different attributes and store the encrypted data on cloud server. In KP ABE [15], User encrypts the data using different attributes and that data is decrypted by access structure policies. In CP ABE owners private key is created by attribute set and cipher text is associated with these attribute set. For example, if U is the sender wants to store

their data on cloud server then he creates their private key as collection of attributes. Let one teacher want to store the record of Class A students marks on cloud system. This data is sensitive and confidential which is decrypted by only his class professors and principal only not by students. Then he encrypts their data by attributes like Assistant Professor AND Class A OR Principal. Then this data is decrypted by only principal or Professors of Class A. the students cannot decrypt the Marks record. The encryption is performed using access structure policy which is generated using different attributes. Then central authority will generate private key on the basis of set of attributes. The decryption of data takes place if access structure policies are satisfied. Here single authority server distributes the private key for encryption and decryption. so if the single authority server is compromise then it gives blockage to performance and security.

Multi authority CP-ABE is solution to the problem of single point blockage.In DAC-MACS [4], the alternative solution was provided as attribute revocation mechanism to Multi authority CP-ABE [9]. In this scheme, Non-revoked user receives fresh private key with respect to date attribute once in a day from central authority. The main drawbacks of this scheme are: 1. in attribute revocation method every owner U required to periodically receive the fresh private key from central authority else U cannot able to decrypt the message. 2. It is an idle revocation method the revoked user is not removed from the system until the assigned time period terminates.3. This method needs an implicit time management. In multi authority cloud systems, the owners attributes can be vigorously customized. This paper presents revocable multi authority CP-ABE.

2 RELETED WORK

Sahai A. et al [2], the data can be stored on straightforward untrusted server in place of trusted server to perform authentication checks before delivering a document. But it not provides the fine grained access control.

Yu S et al. [3], permit the data owner to assign most of the calculated jobs involved in fine grained data access control to un-

trusted cloud system without knowing the content of data. But need to work on revocation as well as single point blockage problems.

Yu S et al. [4], KDC concept is introduced in DAAC scheme. In DAAC Algorithm, user encrypts their data using access structure. And encrypted data is stored on cloud server. KDC provides the private keys to all the users who want to access the data using users attribute set. By using this private key the user who have sufficient attributes can access the encrypted data. But DAAC is completely depends upon KDC. If KDC is compromised then security also compromised.

Hur J.et al [5], key escrow problem is solved by two way computation between Key distribution center and data storage server. Means private key is generated by agreement of both KDC and data storing server. That is no one individually use the key to decrypt the data present on cloud.

Jung T. [6,1], the multi authority CP-ABE introduced. In multiple authority means KDC can create the private key using the attributes of different authorities.

Yang K [7,11], this paper works on multi authority attribute base encryption to provide the fine grained access control. But need to work on attribute revocation.

3 PROBLEM DEFINATION

Data owners store their data on cloud system with the encryption of data using set of attributes. But stored data is not secured due to untrusted or compromised cloud server. Cloud server can use or delete the stored data intentionally or unknowingly. So multiple authority option is one of the solution in place of single authority. The cipher text policy is used to generate the access structure before uploading the data on cloud. Using this access control data uploaded and central authority generate the private keys dependant on set of attributes. Specifically, need to overcome some difficulties to improve the performance and cloud system security. Some difficulties are as follow:

In the existing schemes, set of attributes and the private keys are required to user to decrypt the data. But if any attribute is

revoked or any user is revoked then authorized user can not access the stored data. Therefore proper user revocation and attribute revocation is required.

The multiple authorities are sending attributes towards the different users; so there is high possibility of data collision.

In traditional Attribute based encryption methods involve single authority to assign the private key to different users from their attribute set, which will give a single point blockage on both data security and performance.

Above mentioned are the main limitations of diverse traditional schemes, which encourage doing the research on multiple authority attribute dependant access control system. Some of the objectives of proposed scheme are given as:

To design a Significant, Proper and Revocable fine grained information access control scheme using multiple authority attribute base encryption.

To solve key-escrow problem using Key distribution Authority and Central Authority.

To provide the efficient user and attribute revocation.

4 PROPOSED SYSTEM ALGORITHM

Cloud storage provides storage tohuge amount of data & provides the services to the users as per their demands. Therefore, it is very effective technique for accessing data from any location at any. The system proposed is multiple authority attribute dependant encryption to provide proper data access control, proper user revocation and Attribute revocation. The proposed system four parts: user, central authority, attributes authority and owner. The system contains eight algorithms to encryption and decryption of the data. The first algorithm is Global_Setup is system setup that creates system keys with the help of system parameters. The second algorithm CA_Setup uses the keys from Global_setup and generates the two keys CPK and CMK. The next algorithm AA_Setup uses CPK to generate the access control structure using attribute set and CPK. The encryption is performed using attribute key generated by AA_Setup and produces the cipher text. Then decryption key is generated by CA_Setup using the attribute key generated by

AA_Setup. Generation of the decryption keys both the Central and Attribute authorities are involved. No single entity responsible for key generation. This one is the solution for the key escrow problem. The cipher text is decrypted into plaintext by pre decryption and decrypt algorithm using the final key generated by both central authority and attribute authority.

Proper Attribute based revocation is performed by using the revocation list. The algorithms are used to perform proper revocation of attributes. The first algorithm is KEY_UPDATE, who update the Decryption key using CPK and revocation list periodically. The cipher text is again encrypted using updated key which is generated by KEY_UPDATE Algorithm. Therefore if any attribute or user is revoked then also data can decrypt using Updated key generated by KEY_UPDATE algorithm. The performance of system is monitored by time required for execution and utilized memory. The implementation is performed in Java in Cloud simulator. Proposed System composed following 8 algorithms to provide fine grained access control:

1. Global_Setup: the internal parameter issued to generate the GL_PK for the system which one required to generate the users private keys.
$$\lambda \rightarrow GL_{PK} \tag{1}$$

2. CA_Setup: central authority runs this algorithm using gl_setup and generates two keys CPK and masters secrete key CMK. CPK is used by attribute authority only.
$$GL_{PK} \rightarrow \{C_{PK}, C_{MK}\} \tag{2}$$

3. AA_SETUP: Each AA usingC_{PK}, set of attributesf and attribute domain uf generatesA_{PK} and A_{MK}.
$$(C_PK, f, u_f) \rightarrow \{A_{PK}, A_{MK}\} \tag{3}$$

4. Encryption: By using GL_{PK}, Message m, Access Structure A and public parameter generated by Attribute authority produces Ciphertext.
$$(m, A, GL\_PK, APK) \rightarrow CT \tag{4}$$

5. CA_Keygen: this algorithm generates Decryption key DSK, Group identity related private key CASK and Group Identity related public key CAPK using GL_PK and group identity gid.
$$(GL\_PK, gid) \rightarrow \{CAPK, CASK, DSK\} \quad (5)$$

6. AA_keygen: Attribute related key $ASK_{F,Sf,gidis}$ generated using set of attributes Sf,, GL_PK,AMK,CASK and CPK.
$$(Sf, GL_{PK}, AMK, CAS, CPK) \rightarrow \{ASK_F, Sf, gid\} \quad (6)$$

7. Pre Decryption: pre decryption key PD_KEY is generated using ASK, CT,GL_PK and C_ASK.
$$(CT, GL_{PK}, C_{ASK}, ASK) \rightarrow \{PD_KEY\} \quad (7)$$

8. Decrypt: the plaintext message is generated using CT, PD_KEY &DSK.
$$(CT, PD\_KEY, DSK) \rightarrow \{M\} \quad (8)$$

Also attribute base revocation is composed by following two algorithms:

1. Key_Update: to provide the attribute based revocation we need to calculate the ASK periodically. New ASK is calculated by Revocation List R and Old ASK.
$$(R, ASK) \rightarrow \{ASK'\} \quad (9)$$

2. Re_Encryption: Original CT is again encrypted by using newly generated ASK.
$$(CT, ASK') \rightarrow \{CT'\} \quad (10)$$

5 CONCLUSION

A multiple authority CP ABE scheme achieves fine grained Access control and attributes revocation. Multiple authorities improve the security mechanism by avoiding single point blockage. The key escrow problem is solved by two way calculation of key using KDC

and data storage server. This scheme enables the data supplier to define and imposeproper access policy. It also provides an attribute based user revocation technique depends on the proxy encryption

scheme. Also the decryption overhead of different owners is minimized by outsourcing the decryption policy to the cloud.

References

[1] Qi Li, Jianfeng Ma, Rui Li, XimengLiu,Xiong J, Danwei Chen, Secure, Efficient and revocable multiauthority access control system in cloud computing, Computers and security 59, 45-59.,Elsevier, 2016.

[2] Sahai A, Water B., Fuzzy Identity based Encryption, Advances in cryptology EUROCRYPT, Vol 3494,2005.

[3] Yu S, Wnag C, Ren K, Lou W, Achieving secure, scalable and fine grained data access control in cloud computing, INFOCOM IEEE, 1-9, 2010.

[4] Ruj S., Nayak A, DAAC: Distributed access control in clouds., IEEE Trustcom, 1-8, 2011

[5] Hur J, Improving security and efficiency in attribute based data sharing, IEEE Trans knowl Data Eng, 2271-82, 2013.

[6] Jung T, Li XY, Wan Z, Wan M, Privacy preserving cloud data access with multi authorities, INFOCOM IEEE, 2625-33, 2013.

[7] Yang K, Jia X, Ren K , Zhang B., Xie R , DAC-MACS :Effective Data access control for multi authority cloud storage systems., IEEE Trans inf forensics secur Data Eng, 1790-801, 2013.

[8] LewkoA,Okamoto T, Sahai A, Waters B., Fully Secure Functional Encryption : attribute based encryption and inner product encryption, EUROCRYPT, 62-91, 2011

[9] Chase M., Multi authority attribute based encryption , Theory of cryptography, vol: 4392, 515-34, 2007

[10] Chase M., Chow SS, Improving privacy and security in multi authority attribute based encryption, ACM, 121-30, 2009.

[11] Hur J, Noh DK., Attribute-based access control with efficient revocation in data outsourcing systems IEEE Trans Parallel DistribSyst 2011;22:121421

[12] Zhou, Lan, Vijay Varadharajan, and Michael Hitchens.,2013, "Achieving secure role-based access control on encrypted data in cloud storage." IEEE transactions on information forensics and security 8, no. 12,pp: 1947-1960.

[13] Liu, Zechao, Zoe L. Jiang, Xuan Wang, Siu-Ming Yiu, Chunkai Zhang, and Xiaomeng Zhao,2016, "Dynamic Attribute-Based Access Control in Cloud Storage Systems", In Trustcom/BigDataSE/I SPA, pp. 129-137.

[14] Jung, Taeho, Xiang-Yang Li, Zhiguo Wan, and Meng Wan., 2015, "Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption." IEEE Transactions on Information Forensics and Security 10, no. 1,pp: 190-199.

[15] Li, Wei, KaipingXue, YingjieXue, and Jianan Hong,2016, "TMACS: A robust and verifiable threshold multi-authority access control system in public cloud storage." IEEE Transactions on parallel and distributed systems 27, no.5,pp: 1484-1496.