A secure and efficient decryption and attribute revocation policy by using combination of access control and multi-authority cloud storage system

Vidhyashree B, Mr.Afroz pasha

***Abstract*— cloud provide different types of services to their users. cloud storage is used by general people as service. There are many cloud service providers like google that provide some amount of cloud storage for its Gmail account holders. But it should always concerned about security of the data stored in the cloud storage. The technique used for data access control is cipher-text policy attribute based encryption(CP-ABE).Efficient decryption and revocation for access control scheme is an effective and secure data for data access control for multi-authority cloud storage system. We achieve both forward and backward security by using efficient attribute revocation. The experimental analysis shows that our system is highly secure and efficient model**

***Index Terms*— cloud computing, decryption ,revocation ,cipher text policy**

I. INTRODUCTION

Cloud computing provides computing paradigm where computing resources are not physically present at user's location. These resources are collectively called cloud. The cloud service providers own and manage these cloud. There is a rapid shift from desktop to the cloud in the past few years. There is a rapid advancement of mobile smart phones and wireless network technologies. Based on the number of servers in the data centre, cloud computing is a large scale distribute network system that is implemented. Based on the layer concept cloud services are generally classified. In the upper layers of this paradigm, infrastructure as a service(Iaas),platform as a service, and software as a service(Saas) are stacked.

Data security in the cloud is provided by the data access control. The roles of the data owner is separated from the data service providers and it is separated by the cloud storage service. For each access different keys are used. By using a valid keys the user can access the required data. This is called key management in data access control in multi-authority cloud storage system. One of the most suitable technology for data access control for multi-authority cloud storage system is cipher text policy attribute based encryption(CP-ABE) because it provides access policies that are directly controlled by the data owner and the distribution of keys are not required by the data owner. Efficiency in computation is the major requirement in the designing of access control policies scheme. Decryption and revocation are the two important operations of access control policies. For example now a days the user's are using smart phones to access the required data but the computation ability of smart phone is not as efficient as PC. Thus the decryption of each user is efficient as possible. For efficient attribute revocation there are two important requirements that is backward security and forward security.

Manuscript received April 09, 2015

II. LITERATURE SURVEY

J. Bethencourt et al. Here we present a system for realizing complex access control on encrypted data that we call cipher text-policy Attribute Based Encryption by using our techniques encrypted data can kept confidential even if the storage server is un-trusted; moreover, our methods are secure against collusion attacks.

R. Ostrovsky et al. Here they construct an Attribute –Based Encryption (ABE) scheme that allows a user's private key to be expressed in terms of any access formula over attributes. Previous ABE scheme were limited to expressing only monotonic access structures. Here they provide a proof of security for their scheme based on the Decisional Bilinear Diffie-Hellman (BDH) assumption.

V. Goyal et al. In a cipher text policy attribute based encryption system , a user's private key is associated with a set of attributes (describing the user) and an encrypted cipher text will specify an access policy over attributes. A user will be able to decrypt if and only if his attributes satisfy the ciphertext's policy

M. Chase et al. In an identity based encryption scheme, each user is identified by a unique identity string. An attribute based encryption scheme (ABE), in contrast, is a scheme in which an be decrypted by anyone with a st of attributes. Such cipher texts can be decrypted by anyone with a set of attributes that fits the policy.

III. PROPOSED SYSTEM

Here the efficient decryption and efficient attribute revocation is constructed using a multi-authority CP-ABE. Then it is used to achieve access control for multi-authority cloud storage system. The main contributions are as .

1. An effective and secure data access control scheme for multi-authority cloud storage systems, can be achieved by proposing our DAC-MAC. It provide better performance than other existing scheme.
2. We built a new multi-Authority CP-ABE scheme to achieve working productively with no waste of money or effort decryption.
3. We achieve both forward security and backward security by using attribute revocation method for multi-authority CP-ABE scheme.

Our system consists of five different types of entities they are as follows: certificate authority(CA), the attribute authorities(AAs), the cloud server(server), the data owner(owner)and the user. It is as shown in the figure 1.

In this system CA is the global trusted certificate authority in the system. It will accept registrations of all the attribute authority and users in the system and it will setup the system .The CA will generates a pair of global secret key and global public key . However, the CA is not involved in any attribute management and any generation of secret keys that are associated with attributes.

Every AA is an independent attribute authority that is responsible for issuing, revoking and updating user's attributes according to their role or identity in its domain.

The data owner's stores the data in the cloud server and cloud server provides the required data to their users. It generates a decryption token for their users to decrypt a ciphertext according to their user's secret keys issued by the AAs

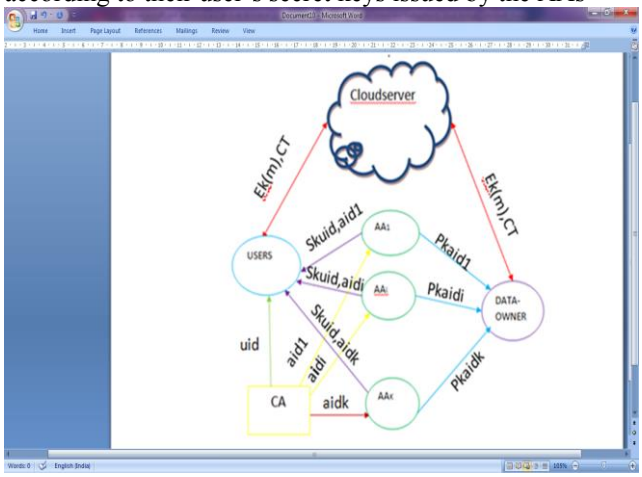

Figure 1:Data Access control for multi-authority cloud storage system

RESULT

Figure 2:generation of attribute set

Figure 3:attribute sets are generated

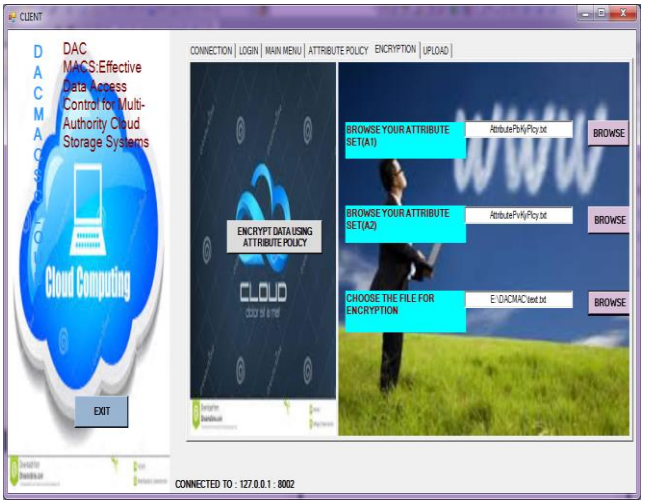

Figure 4:encrypting data using attribute policy

Figure 5:generation of key using symmetric algorithm

CONCLUSION

Here we analyze some of the existing model and identified its loop hole and problem it face. The existing system faces following problem such as inefficiency decryption process and suffers from attribute revocation policy.

In order to overcome these issues here we proposed a new efficient cloud model by using the combination of Access control mechanism and multiple authority. Here we design our system with efficient decryption with dynamic attribute revocation policy by achieving both forward and backward security. The experiment analysis shows that our system is highly secure and efficient model

In future we would like to develop this model by improving the security related issue in multiple authorities and find the sufficient solution for it.

REFERENCES

[1] P. Mell and T.Grance, "The NIST definition of cloud computing ," National Institute of Standards and Technology, Tech. Rep.,2009.

[2] J.Bethencourt, A.Sahai,and B.Waters,"Ciphertext-policy attribute based encryptin,"in S&P'07.IEEE Computer Society,2007,pp.321-334.

[3] B. Waters, "ciphertext-policy attribute based encryption: An expressive, efficient, and provably secure realization," inPKC'11.Springer, 2011,pp 53-70.

[4] V. Goyal.A. Jain .O. Pandey, and A. Sahai,"Bounded ciphertext policy attribute based encryption " in ICALP'08,Springer ,2008,pp. 579-591.

[5] R.Ostrovsky, A. sahai, and B.Waters,:Attribute based encryption with non-monotonic access structures,"in CCS'07. ACM, 2007, PP. 195-203.
[6] A. B. Lewko, T. Okamoto, A. Sahai,K. Takashima, and B. Waters,"Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption ," in EUROCRYPT'10.Springer,2010,pp. 62-91.
[7] M. Chase,"Multi-authority attribute based encryption," in TCC'07.Springer,2007, pp. 515-534.
[8] S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attribute based encryption," in ICISC'08.Springer, 2008,pp. 20-36.
[9] M. Chase and S.S.M.Chow,"Improving privacy and security in multi attribute based encryption ," in CCS'09.ACM, 2009,pp. 121-130.
[10] A.B.Lewko and B.Waters, "Decentralizing attribute based encryption," in EUROCRYPT'11.Springer, 2011, pp. 568-588.
[11] M. Green, S.Hohenberger, and B. Waters, "outsourcing the decryption of abe ciphertexts," in proceedings of the 20th USENIX security symposium. USENIX Association,2011.
[12] J.Hur and D.K.Noh ,"Attribute based access control with efficient revocation in data outsourcing systems,"IEEE Trans.parallel Distrib.syst., vol. 22,no.7,pp. 1214-1221,2011.
[13] S. Ruj,A. Nayak, and I.Stojmenovic,"DACC:Distributed Access Control in Clouds," in TrustCom'11.IEEE,2011,PP.91-98 .
[14] K. Yang, X. Jia and K. Ren,"Dac-macs:Effective data access control for multi-authority cloud storage systems," IACR Cryptology eprint Archive,vol. 419, pp. 1-12, 2012.
[15] M. Kallahalla, E.Riedel, R. Swaminathan, Q. Wang, and K. Fu, "plutus: Scalable secure file sharing on untrusted storage," in FAST'03. USENIX,2003.