A Development of Novel Encryption for Secured Data Sharing Using KAC

T.Dhivya Bharathi
P.G.Scholar, Department of I.T.,Dr.Sivanthi Aditanar College of Engineering,TamilNadu,India.

Dr.S.Sivananaitha Perumal
Head of the Department of I.T.,Dr.Sivanthi aditanar College of Engineering,TamilNadu,India.

Abstract – Data sharing is the very important functionality in cloud storage. Cipher text Policy Attribute-Based Encryption (CP-ABE) has a very large cipher text size, which increases linearly with respect to the number of attributes in the access policy. The other hand, existing privacy preserving schemes protect the anonymity but require bulky, linearly increasing ciphertext size. It proposed a new construction of CP-ABE, named Privacy Preserving Constant CP-ABE (denoted as PP-CP-ABE) that significantly reduces the ciphertext to a constant size with any given number of attributes.Key Aggregate Cryptosystem(KAC) concept is used for sharing this data from one to another. Key-aggregate cryptosystem produce constant size cipher text . That is very efficient delegation rights of decryption for any set of cipher text are possible. Any set of secret keys can be aggregated and make them as single key, which groups all the key by making it a aggregate key.

Index Terms – Cloud storage, Secret Key, Attribute Based Encryption, Encryption, Decryption, Ciphertext-Policy.

1. INTRODUCTION

Cloud Computing provides us a means by which can access the application as utilities,over the internet. It allows us to create, configure, and customize application online. With Cloud Computing users can access database resources via the internet from anywhere for as long as they need without worring about any maintenance or management of actual resources. Cloud Computing refers to manipulating, configuring, and accessing the application online. It offers online data storage,infrastructure and application.Cloud Computing is both a combination of software and hardware based computing resources delivered as a network services.

In the Ciphertext-Policy Attribute-Based Encryption, each attribute is a descriptive string and each entity may be tagged with multiple attributes. Many entities may share common attributes, which allows message encryptor's to specify a secure data access policy over the shared attributes to reach a group of receivers. A decryptor's attributes need to satisfy the access policy in order to recover the message. These unique features make CP-ABE solution appealing in many system,where expressive data access control is required for a large number of users.

In this concept contain symmetric key encryption.

1. Symmetric Key

Single Key is used for both encryption and decryption during data sharing in cloud storage.

2. Asymmetric Key

Two different keys are used for encryption and decryption during data sharing in cloud storage.

In this concept Alice and Bob are friend.Alice put her personal photo or data in her cloud storage.She does not want to expose her photo to everyone. Due to various data leakage so she encrypts all her photo using her own secret key before uploading in cloud storage.Oneday Bob asks her to share his particular photo .Alice use this ways to share his photo.

i) Alice encrypt all her photo with single secret key and share that secret key directly with the Bob

ii) Alice aggregate all the secret key and make as compact as single key after that she sends to Bob for getting his photo.

2. RELATED WORK

SYMMETRIC KEY ENCRYPTION

In this method select two prime number p and q. A master key is chosen at random and every distinct prime number has been achieved with associated class. These prime number store in the public system parameter. After that a constant size key is generated as well as generated access rights for S. This method is used to generate a secret value rather than a pair of public/secret keys, by using this method to reduce the key size of symmetric key encryption.

ATTRIBUTE BASED ENCRYPTION

In CP-ABE, each user's private is associated with a set of attribute and each ciphertext is encrypted by an access policy. To decrypt the message, the attribute in the user private key need to satisfy the access policy. PP-CP-ABE significantly reduces the ciphertext size from linear to constant and supports expressive access policies.

Attribute Based Encryption is also called as Public key Encryption which associated with a secret key of the users. In Ciphertext Policy Attribute Based Encryption scheme, the encryptor can fix the policy, who can decrypt the encrypted message. The policy can be formed with the help of attributes. In CP-ABE, access policy is send along with the ciphertext and access policy need not sent along with the ciphertext, by which are able to preserve the privacy of the encryptor.

KEY AGGREGATE CRYPTOSYSTEM

Key aggregate cryptosystem is encrypted using public key, identifier of ciphertext is also known as class. Ciphertext contain different classes. A master secret key is used to maintain the master secret holds by key owner. Master secret key is used to extract secret keys from different classes, the extracted key have an aggregate key which is as compact as secret key for each and every single class.

FRAMEWORK

Key aggregate encryption having five modules.

Setup : The entire accounts are maintain by the data owner.

Keygen : It is used to generate master and secret key which is executed by the data owner.

Encrypt: It is used to encrypting the data using secret key.

Extract: It is used to extract the particular set of ciphertext classes and it is also executed by data owner.

Decrypt: It is executed by a delegate who got, an aggregated key generated by Extract. On input, set, an index denoting the ciphertext class belongs to and output is decrypt result.

3. PROPOSED MODELLING

DATA SHARING USING KAC

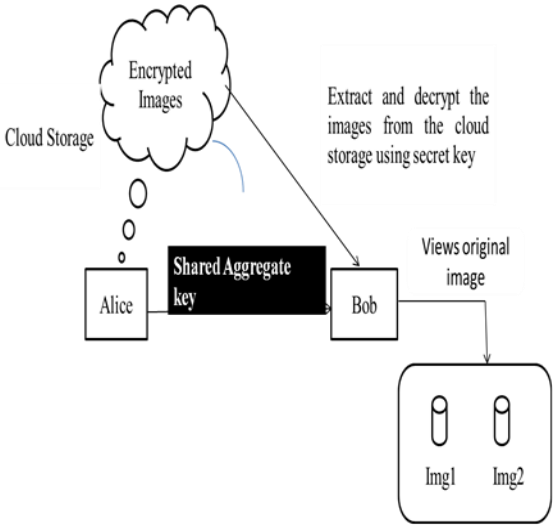


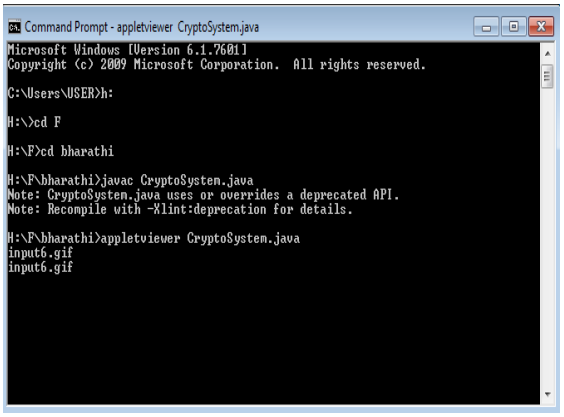
Fig1. Data Sharing Using KAC

This diagram shows how to share data using key aggregate concept.A canonical application of KAC is data sharing. The key aggregate property is useful when we expect delegation to bE efficient and flexible. In this method used to avoid unauthorized access due to providing aggregate key. Data sharing using KAC, Figure1. Suppose Alice wants to share her data m1,m2……..,mn on the server. Alice first perform setup to get param and used KeyGen to get the public/master key pair. Encrypted data are uploaded to the server and decrypt the extract data. Finally Bob receive their original data using KAC.

4. EXPERIMENTAL RESULT

Encrytpion

Ciphertext and two images had been given as a input



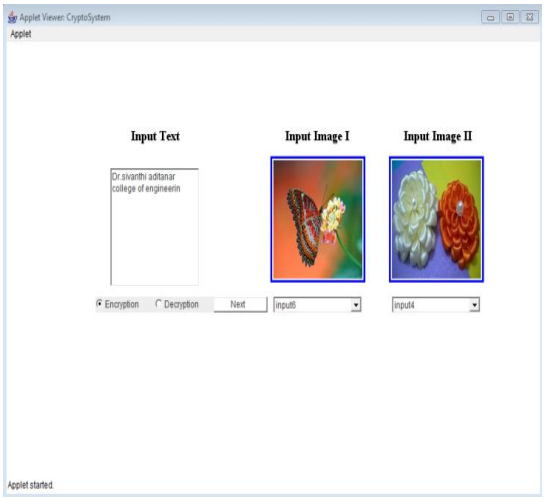


Fig1.Encryption Window

KeyGeneration

Encrypted image is placed behind the input text.Publickey gets generated automatically according the given images.Hexadecimal code that ie) private key is generated by

using ABE algorithm.The encrypted version stored in particular file.

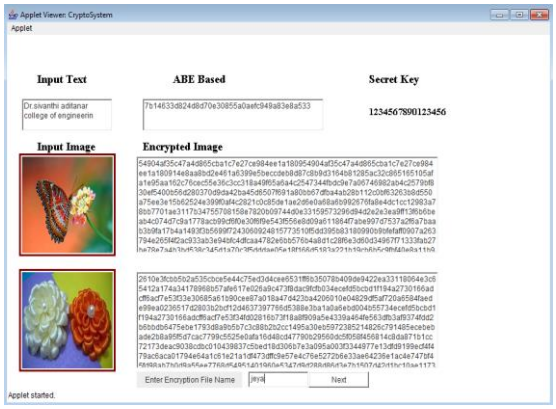


Fig 2. KeyGeneration window

Encryption process is finished in this window.

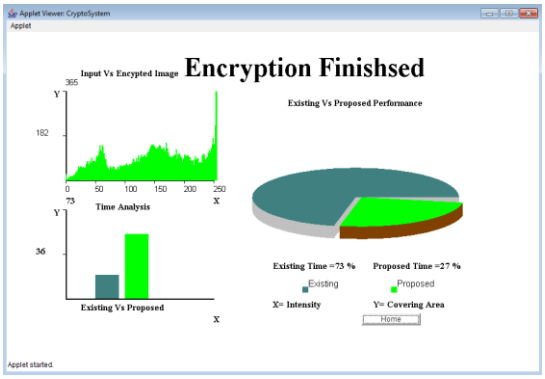


Fig 3. Encryption finished window

Decryption

By choosing the radio button decryption process starts. By giving user name, paasword and key value.and ciphertext Ok button has to be clicked.If its correct only it will be move to next process.

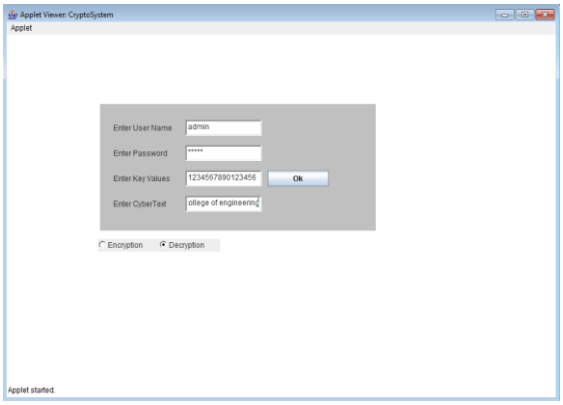


Fig 5. Decryption Window

Decrypted file window open choose the encrypted file name in comobox and click next.

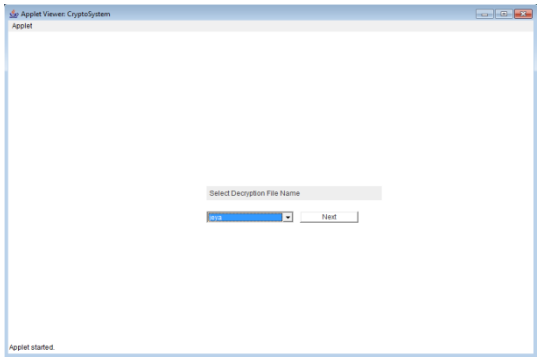


Fig 6. Decryption File Name Window

The corresponding file name given before displays the decrypted text, image and key.

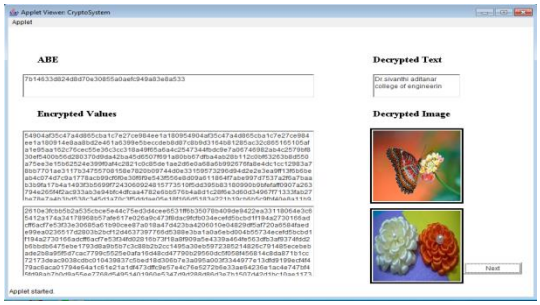


Fig 7. Decryption Process Window

5. CONCLUSION

KAC concept is used for sharing the information in secure manner. Public key cryptosystem support extract the original data from the cloud storage. And also used to transfer the data very securely, and also used to avoid unauthorized access. A Constant Cipher text Policy Attribute Based Encryption (PP-CP-ABE) is proposed. Compared with the existing CP-ABE constructions, PP-CP-ABE significantly reduces the cipher ext size to constant and supports expressive access policies. Thus, PP-CP-ABE can be used in many communication constrained environments.

REFERENCES

[1] Y. Sun and K.J.R. Liu, “Scalable Hierarchical Access Control in Secure Group Communications,” Proc. IEEE INFOCOM ’04, 2004.
[2] M. Chase and S.S.M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” Proc. ACM Conf. Computer and Comm. Security, pp. 121-130. 2009.
[3] R. Canetti and S. Hohenberger, “Chosen-Ciphertext Secure Proxy Re-Encryption,” Proc. 14th ACM Conf. Computer and Comm Security (CCS ’07), pp. 185-194, 2007.
[4] S.S.M. Chow, J. Weng, Y. Yang, and R.H. Deng, “Efficient Unidirectiona Proxy Re-Encryption,” Proc. Progress in Cryptolog (AFRICACRYPT ’10), vol. 6055, pp. 316-332, 2010.

[5] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamicand Efficient Key Management for Access Hierarchies," ACM Trans. Information d System Security, vol. 12, no. 3, pp. 18:1-18:43,2009.
[6] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Proc. Automata, Languages Program. Springer, 2008, pp. 579-591.
[7] S. Roy and M. Chuah, "Secure data retrieval based on ciphertext policy attribute-based encryption (CP-ABE) system for the DTNs," Tech. Rep., 2009.
[8] Z. Zhou and D. Huang, "On efficient ciphertext-policy attribute based encryption and broadcast encryption," in Proc. 17th ACM Conf. Comput. Commun. Security, 2010, pp. 753-755.
[9] K. Emura, A. Miyaji, A. Nomura, K. Omote, and M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length," in Proc. 5th Int. Conf. Inf. Security Practice Experience. Springer Verlag, 2009, pp. 13-23.
[10] S. Yu, K. Ren, and W. Lou, "Attribute-based content distribution with hidden policy," in Proc. 4th Workshop Secure Netw. Protocols, 2008, pp. 39-44.