A Flexible Approach for Class Based Encryption and Data Sharing in the Cloud Storage

vinutha.G [1], Dr.Aishwarya P[2]

[1] M.Tech, Student ,Atria Institute Of Technology, Bengaluru, Karnataka, India

[2] Professor, Atria Institute Of Technology, Bengaluru, Karnataka, India

---

Abstract-*Information sharing is a critical usefulness in cloud storage. The main objective is to safely, productively, and adaptably share data with others in cloud storage. The new public key cryptosystems which deliver the number of cipher texts such that proficient assignment of decryption rights for any set of cipher texts are conceivable.The utilization of public key encryption gives more adaptability for our applications. Our issue is to design an public key encryption plan which gives approval to flexible delegation for any subset of the cipher texts delivered by the encryption plan. To plan a productive public key encryption plan a class based encryption is used. A class based encryption plan comprises of polynomial algorithms.Here data owner creates a public and secret key pair. Data which is classified into classes is encrypted by the owner. Aggregate key is generated for any set of cipher texts by the data owner . The created keys can be gone to delegatees safely by means of secure e-mail. User with aggregate key can decrypt the ciphertexts from cloud interface. The data owner can aggregate any choices secret key and can discharge a single aggregate key. The aggregate key is stored in a smart card or advantageously sent to others through e-mail.*

Key words: Class based encryption, Symmetric based encryption, Identity based encryption, Attribute based encryption.

1. INTRODUCTION

Cloud storage is picking up fame as of now. In big business settings, we see the ascent popular for information outsourcing, which helps with the key administrationof corporate information. It is likewise utilized as a centre innovation behind numerous online administrations for individual applications.

Considering information protection [2], a conventional approach to guarantee it is to depend on the server to uphold the access control after validation, which implies any startling benefit heightening will uncover all information.. In big business settings, we see the ascent popular for information outsourcing, which helps with the key administration of corporate information. It is likewise utilized as a centre innovation behind numerous online administrations for individual applications.

Data sharing is a vital usefulness in cloud capacity. For instance, bloggers can let their companions view a subset of their private pictures; a venture might award her workers access to a segment of sensitive information. The testing issue is the way to adequately share encrypted information. Encryption keys additionally with two schemes-symmetric key or asymmetric key .Using symmetric encryption, when Alice needs the information to be started from an outsider, she needs to give the encryptor her secret key. obviously, this is not generally useful. By contrast, the encryption key and decryption key are diverse out in the public key encryption. The utilization of public key encryption gives more adaptability for our applications. For case, in big business settings, each representative can transfer encrypted data on the distributed storage server without the information of the organization's expert master secret key.

There for the best answer for the above issue is alice encrypts file with different public keys and just sends a bob single decryption key as shown inbelow fig 1.

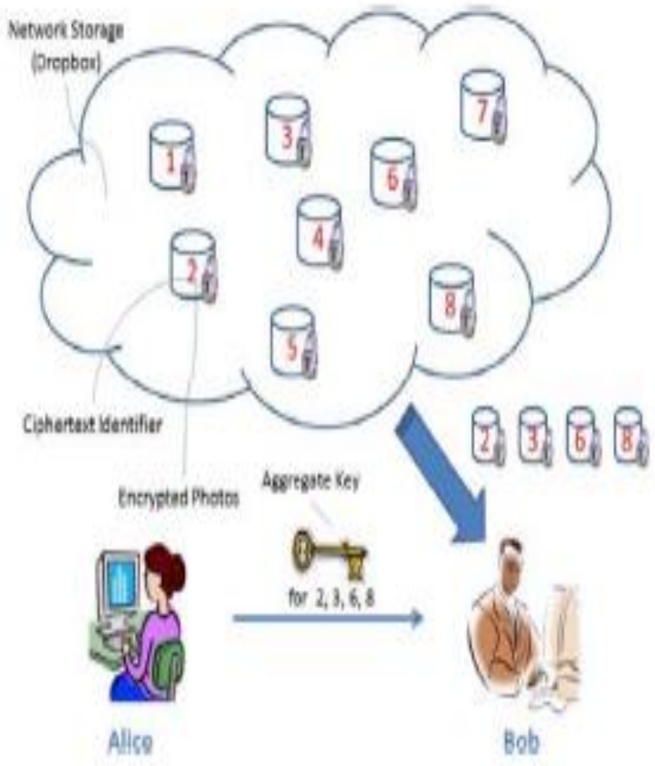

Fig1. Data sharing between the Alice and Bob

2. RELATED WORK

Symmetric key encryption [3] uses the hierarchical approach. This scheme is suitable hierarchies which have limited depths.The security of the plan depends just on the utilization of pseudo-arbitrary capacities [4].In this plan there is a central power that create appropriate keys for example administrator inside organisation. So the owner can’t depend on the outsider in the event of failure. A future piece of work is committed for enhancing proficiency of key deduction time for deep hierarchies.

In Attribute Based Encryption [5] system an attributes will be connected with cipher text. Advantages of attribute based encryption are encryption technique uses public key encryption and cipher text size is consistent. The major drawbacks are dealing with the keys is costly and requires more space for storing the keys.

Identity based encryption (IBE) [6] is an extraordinary instance of public key encryption.There is a trusted party called private key generator in identity based encryption which holds an master secret key and issues a secret key to every client regarding their identities. The encryption system is time intensive since it encrypts the plaintext not just with public key, secret key furthermore with numerous client identities. In identity based encryption transferring and storing the keys are more expensive. Key aggregation is constrained as in all the keys to be aggregated must originate from with distinctive identities.

4. PROPOSED SYSTEM

Our goal is to make an decryption key more capable as in it permits to decrypt a set of cipher texts. Data owner who classifies his files into classes, encrypts the data and then uploads to the cloud interface. For any set of cipher text which the data owner is willing to share with others can send aggregate key to the data user. So the data user is the delegatee who can decrypt the cipher texts from cloud interface only.To plan a productive public key encryption plan an class based encryption is used.As shown in the fig 2. Class based encryption scheme has three modules: Cloud server, data owner, data user. Data owner builds up the creates public and master secret key pair by keygeneration. Data owner encrypts a file by public key and class(which means identifier of cipher text) through encrypt.Data owner can utilize the master secret key to create aggregate key for an arrangement of ciphertext classes by means of Extract. The produced keys can be gone to user safely by means of secure e-mail or secure gadgets. Data user with an aggregate key can download the ciphertext from cloud interface anddecrypt ciphertext given that the cipher texts class is contained in the aggregate key.

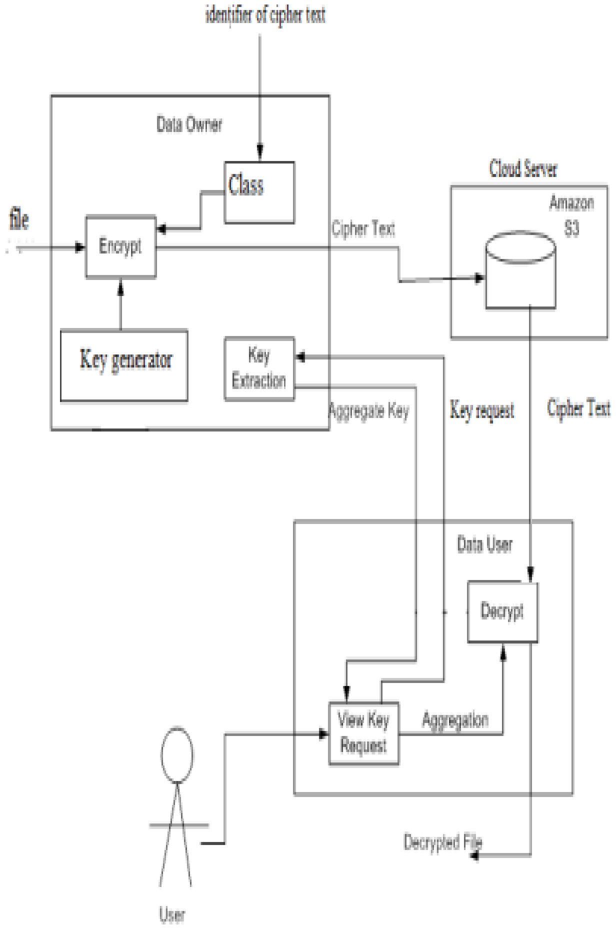

Fig2. System Architecture for class based encryption

Conclusion and Future work

Data security is the major issue in cloud storage. In this paper, we consider how securely and flexibly share the data with others in cloud storage and to design public-key encryption known as class based encryption.In cloud storage, the number of cipher texts normally grows quickly. So our approach can extend the public keys for n number of classes.

When one bears the delegated keys in a cell phone without utilizing exceptional trusted hardware the key is brief to leakage, planning a leakage versatile cryptosystem can be planned in future.

REFERENCES

[1] IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS," Key-Aggregate Cryptosystem for ScalableData Sharing in Cloud Storage" Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, Senior Member, IEEE.vol 24 FEBRUARY 2014

[2] S.S.M. Chow, Y.J. He, L.C.K. Hui, and S.-M.Yiu, "SPICE – Simple Privacy-Preserving Identity-Management for Cloud Environment,"Proc. 10th Int'l Conf. Applied Cryptography and NetworkSecurity (ACNS), vol. 7341, pp. 526-543, 2012.

[3] M.J. Atallah, M. Blanton, N. Fazio, and K.B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACMTrans.Information and System Security, vol. 12, no. 3, pp. 18:1-18:43, 2009.

[4] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," Proc. ACM Workshop Cloud Computing Security(CCSW '09), pp. 103-114, 2009

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,"Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[6] F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multipleciphertexts Using a Single Decryption Key,"Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575,pp. 392-406, 2007.

BIOGRAPHIES

VINUTHA G received B.E. degree in Computer Science and Engineering in Rajiv Gandhi Institute Of Technology, Bengaluru, Karnataka, India from VisvesvarayaTechnological University, Karnataka, India . Presently she is pursuing her final year M.Tech with specialization in Computer Science and Engineering in Atria Institute Of Technology, Bengaluru, Karnataka, India from Visvesvaraya Technological University, Karnataka, India. The proposed research work in this paper is part of her M.Tech thesis.

Dr. AISHWARYA P received B.E. degree from PeriyarManiammai College of Technology for Women, Bharadhidasan University in June 2000 and M.E from College of Engineering, Guindy, Anna University Campus in December 2001 and PhD from Manonmaniam Sundaranar University in March 2013. She is currently Professor of Computer Science and Engineering at Atria Institute Of Technology, Bengaluru, India and has been Teaching both UG and PG students of Computer Science and Engineering for nearly Fifteen years. She has published many research papers and also has attended many National and International Level Conferences.