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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

A Review on Cryptographic Solution to the Predefined Bound of Ciphertext Classes in KAC

Rahul Suresh Tamkhane[1], Prof. Nilesh S.Vani[2], Prof. Pramod B. Gosavi[3]

M.E. Student, Department of CSE, GF's Godavari College of Engineering, Jalgaon, North Maharashtra University, India

Assistant Professor, Department of CSE, GF's Godavari College of Engineering, Jalgaon, North Maharashtra University, India

Head of Department & Associate Professor, Department of CSE, GF's Godavari College of Engineering, Jalgaon, North Maharashtra University, India

ABSTRACT: Cloud computing is the storing of data online which is accessible from multiple and connected resources. It is the fastest growing field in computer world which serves various services to users. One of the most important functionality is data sharing. Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services. This paper attempts to show how data is shared among cloud users securely, efficiently, and flexibly. On cloud anyone can share data as much they want to i.e. only selected content can be shared. With cryptography users can share the data to others in safe way. So user encrypts data and uploads on server.The proposed algorithm uses a new cryptosystem that is called as Key Aggregate Cryptosystem (KAC) [1] which generates a single key for multiple files.In particular, it uses a public key encryption which releases aggregate key for set of secret keys.

KEYWORDS: Cloud computing, Cloud Storage, Data Sharing, Key Aggregate Cryptosystem

I. INTRODUCTION

Cloud storage is very popular storage system. Cloud storage is storing of data off-site to the physical storage which is maintained by third party. By using cloud storage anybody can store data on "cloud" and can access information from any computer through internet. Nowadays, many websites provide users free accounts for email, file sharing, photos with different storage sizes, users can access their files from any corner of world.Data sharing is an important functionality in cloud storage because user can share data to anyone and anytime. The challenging task is to secure the data on cloud [2]. With traditional way to encrypt data before uploading on cloud and share with others. After downloading encrypted data, decrypt them and send them to other for sharing loses the value of cloud storage.Cloud-computing providers offer services according to different models which are Infrastructure as a Service (IaaS), Platform as s Service (PaaS), and Software as Service (SaaS). Also there are different types of cloud computing public cloud, private cloud and hybrid cloud.The main concern is to secure data from unauthorized access. With a special type of public key encryption which is called Key-Aggregate Cryptosystem anyone can share data with others secretly.

Data cryptography mainly is the encryption of the content of the data, such as text, image, audio, video and so forth to make the data unreadable, invisible or meaningless during transmission or storage. The aim of cryptography is to take care of data secure from attackers. The reverse process of getting original data back from encrypted data is known as decryption. To encrypt data at cloud storage both symmetric-key and asymmetric-key algorithms can be used.

Public-key cryptography, also known as asymmetric cryptography, is a class of cryptographic protocols based on algorithms that require two separate keys, one of which is secret (or private) and one of which is public.The public key is used, for example, to encrypt data; whereas the private key is used to decrypt data.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

II. RELATED WORK

Cloud computing is an internet base environment where users can store the data remotely in the cloud. Any cloud computing environment architecture can be divided basically into three layers, the characteristics layer, the models layer (infrastructure as a services, platform as a services, and software as a services), and the deployment layer [3].

Benaloh et al. [4] proposed an encryption scheme for transmitting large number of keys in broadcast scenario. It is designed for symmetric-key encryption.

D. Boneh and M. K. Franklin [5] proposed IBE (Identity Based Encryption) which is a public-key encryption in that public-key of user is its identity (e.g. an email address). The encryptor can take public parameter and a user identity to encrypt a message. The recipient then decrypts the message by his secret key.

Guo et al.[6] introduces IBE with key aggregation. In Identity Based Encryption the public key of user is the unique identity of user (e.g. email address).

V. Goyal, O. Pandey, A.Sahai, and B. Waters [7], proposed"Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data", he developed a new cryptosystem for fine-grained sharing of encrypted data. This scheme was called Key-Policy Attribute-Based Encryption (KP-ABE).

F. Guo, Y. Mu, Z. Chen, and L. Xu [8], introduced"Multi-Identity Single-Key Decryption without Random Oracles" This Paper produce Multi-Identity Single-Key Decryption (MISKD).It is an Identity-Based Encryption (IBE) system where a private decryption key can compress keys (identities). More exactly, in MISKD, a single private key can be used to decrypt multiple cipher texts encrypted with different public keys associated to the private key.

R. Canetti and S. Hohenberger proposed Proxy re-encryption (PRE) [9] scheme which allows user to delegate to the server the ability to convert ciphertext with other user's public key.

III. EXISTING SYSTEM

Data sharing is an important functionality in cloud storage. Because of honesty of technical staff or the security of trusted VM, users are motivated to encrypt their data with their own keys before uploading them to the server. The challenging problem is how effectively share encrypted data. Users can download the encrypted data from server, decrypt them and share to others, but it loses the value of cloud storage.

Our problem statement is that to introduce a new public-key encryption called key-aggregate cryptosystem. In that user encrypts message under public-key and ciphertext identifier. The key owner extracts secret keys for different classes using master-secret key.The key owner holds the master secret called master-secret key. More importantly, the extracted key have can be an aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys, i.e., the decryption power for any subset of ciphertext classes.

As shown in Fig1. Alice can share the uploaded files to Bob by creating an aggregate key. This aggregate key will be communicated with Bob by Email. He can download these files and decrypt them. Except sending multiple keys for two or more files Alice just send a single key to Bob.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

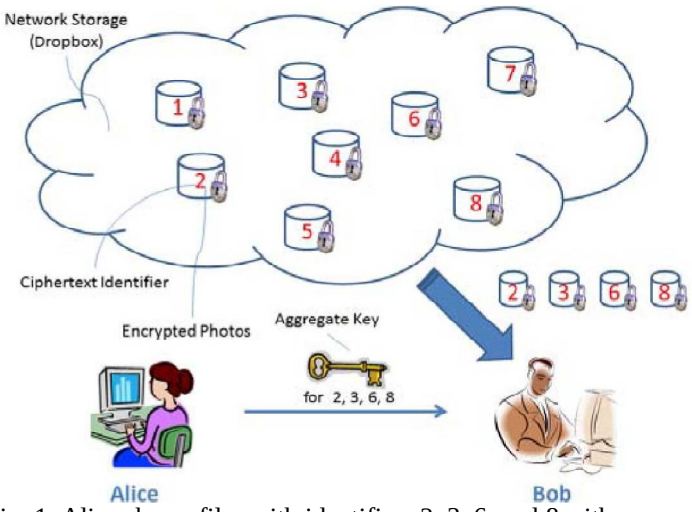

Fig. 1. Alice shares files with identifiers 2, 3, 6, and 8 with Bob by sending him a single aggregate key[1].

IV. PROPOSED SYSTEM

The proposed system is basedon key aggregation encryption.ElGamal encryption [10] is a type of public key encryption algorithm.The data owner having account on trusted server first generates public and master-secret key pair for encrypting data. Anyone who wants to encrypt data using this key pair an aggregate key will be generated. The public key of user can be any identity string (e.g. email address).The delegatee who received an aggregate key decrypts the data.

Here we are expanding public key so there will not be a limitation of ciphertext classes. With this the one more thing we are adding that is the sharing of different files on cloud like text files, multimedia files and so forth.

The proposed system is the based on key aggregation encryption. Here we are using two keys to encrypt data and a single key to decrypt the data. The data owner creates the public system parameter and generates a secrete key which is public key. Data can be encrypted by any user and he may decidesciphertext block associated with the plaintext file which want to be encrypted.The authenticated user having an aggregate key can decrypt any block of ciphertext.

This project consists of five modules.

1. **Setup Module:** In this module user creates an account on trusted cloud server.
2. **PMKGen Module:**In this module the public/master-secret key will be genarated.
3. **Encrypt Module:** In this module the anyone encrypt the data using public key and ciphertext class.
4. **AggKeyGen Module:** After encrypting a file this module generates an aggregate key which is send to delagatee via email.
5. **Decrypt Modele:** With this modulea delegateewith an aggregate key decrypt the file.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

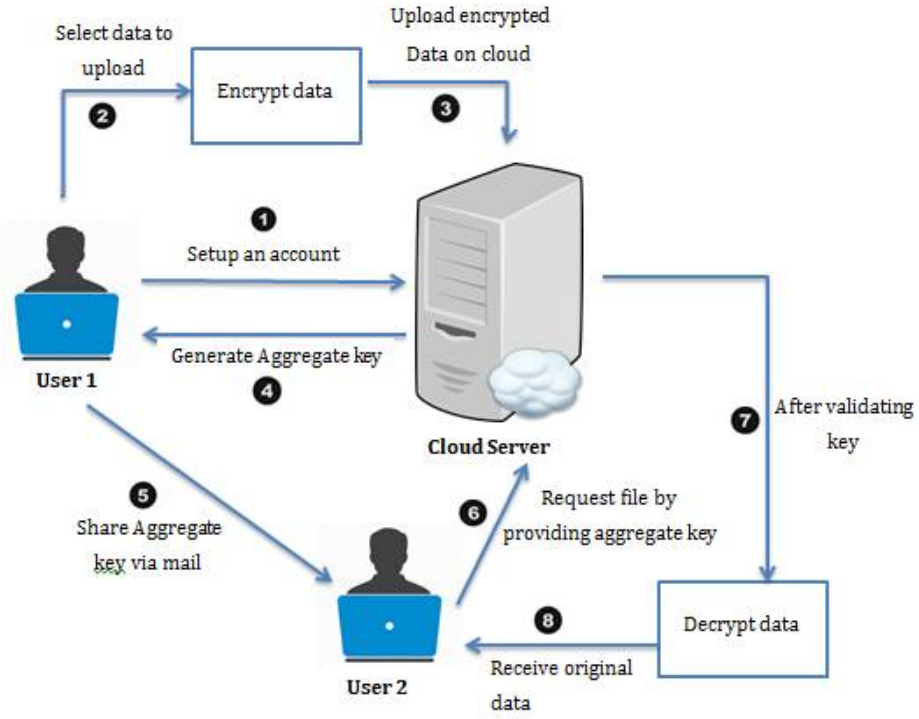

Fig2.Working of Proposed System

V. CONCLUSION& FUTURE WORK

In cloud storage data privacy is an important factor. In this project, we investigate the limitations of existing system which is predefined bound of number of maximum ciphertext classes. Uploading data to cloud server may lead to leakage of private data. The best solution is encryption. We consider how to compress number of secret keys into a single aggregate key. Our approach is more flexible than previous key aggregate cryptosystem.

In this paper, proposed system is found to be very efficient for sharing the data on cloud. For this we have used ElGamal and KAC algorithm which support delegation of secret keys for different ciphertext classes in cloud storage.

In future the research direction would be to find ways for a data owner to hold accountable any member that carries out malicious activities on their account.

REFERENCES

1. Cheng-Kang Chu, Sherman S.M. Chow, Wen-GueyTzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage" IEEE Transactions On Parallel And Distributed System, Vol 25, No. 2 February 2014.
2. L. Hardesty, Secure Computers Aren't so Secure. MIT press, http://www.physorg.com/news176107396.html, 2009.
3. G. Clarke, "Microsoft's Azure Cloud Suffers First Crash, The Register", http://www.theregister.co.uk/ 2009/03/16/azure_cloud_crash/,March 16, 2009.
4. J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "PatientControlled Encryption: Ensuring Privacy of Electronic MedicalRecords," Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.
5. D. Boneh and M.K. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Advances in Cryptology (CRYPTO '01), vol. 2139, pp. 213-229, 2001.
6. F. Guo, Y. Mu, and Z. Chen, "Identity-Based Encryption: How to Decrypt Multiple Ciphertexts Using a Single Decryption Key," Proc. Pairing-Based Cryptography Conf. (Pairing '07), vol. 4575, pp. 392-406, 2007.

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

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

7. 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.
8. F. Guo, Y. Mu, Z. Chen, and L. Xu, "Multi-Identity Single-Key Decryption without Random Oracles," Proc. Information Security and Cryptology (Inscrypt '07), vol. 4990, pp. 384-398, 2007.
9. 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.
10. ElGamal, Taher, "A public key cryptosystem and a signature scheme based on discrete logarithms". Advances in cryptology: Proceedings of CRYPTO 84. Santa Barbara, California, United States: Springer-Verlag. pp. 10–18, 1985.
11. S. S. M. Chow, Y. J. He, L. C. K. Hui, and S.-M. Yiu, "SPICE - Simple Privacy-Preserving Identity-Management for Cloud Environment," in Applied Cryptography and Network Security – ACNS 2012, ser. LNCS, vol. 7341., pp. 526–543, Springer, 2012

BIOGRAPHY

Mr. Rahul Suresh Tamkhane a Student in Computer Science Department, College of GF's Godavari College of Engineering, Jalgaon,North Maharashtra University, India.He received Bachelor of Engineeringdegree in 2010 from GF's Godavari College of Engineering, Jalgaon, NorthMaharashtra University, India. His researchinterests are in Cloud Computing and Data Security.

Prof. NileshS. Vani an Assistant Professor in Computer Science Department, College of GF's Godavari College of Engineering, Jalgaon, North Maharashtra University, India. He received M. Tech. degree from S.A.T.I., Vidisha (M.P.), India. His research interests are in Data Security.

Prof. Pramod B. Gosavian Associate Professor in Computer Science Department, College of GF's Godavari College of Engineering, Jalgaon, North Maharashtra University, India. He received M. Tech. degree from S.A.T.I., Vidisha (M.P.), India. His research interests are in Cloud Computing.