International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 5 Issue: 5 174 – 178

A Cryptographic Solution to the Predefind Bound of Ciphertext Classes in KAC

Mr. Rahul Suresh Tamkhane
ME Student
Department of Computer Engineering
GF's Godavari College of Engineering,
Jalgaon, Maharashtra, India
rahul.tamkhane@gmail.com

Mr. Nilesh S. Vani
Assistant Professor
Department of Computer Engineering
GF's Godavari College of Engineering,
Jalgaon, Maharashtra, India
nileshvani@gmail,.com

Mr. Pramod B. Gosavi
Head & Associate Professor
Department of Computer Engineering
GF's Godavari College of Engineering,
Jalgaon, Maharashtra, India
gosavi.pramod@gmail.com

Abstract— In Cloud Computingsecure data sharing is an important functionality. 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. 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 that user encrypts data and upload it on cloud 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. With this aggregate key others can decrypt ciphertext set and remaining encrypted files outside the set are remains confidential.

Keywords- *Cloud computing,Cloud storage, Data sharing, Key Arregate Cryptosystem, Encryption and decryption*

*****

I. INTRODUCTION

Nowadays Cloud storage is very popular storage system. By using cloud storage anybody can store data on "cloud" and can access information from any computer through internet anywhere at anytime. There many websites which 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] [11]. 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. In modern cryptography, a fundamental problem is leveraging the secrecy of data. In this work, we study how to make a decryption key more powerful which allows decryption of multiple ciphertexts without increasing its size. 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. 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.

In this paper, design, and implementation of solution to the predefined cipher text classes in Key-Aggregate Cryptosystem are described. Section I introduce the system to be developed. Section II gives thebasic concepts related to cloud computing. Section III discusses the existing system and analysis with their drawback and objective. Section III describes the system methodology. Section IV describes the implementation details. Section V gives the flow of proposed system. Section VI gives the implementation of system. Section VII describes the results and related discussions. Finally, Section VIII concludes the research work.

II. BASIC CONCEPTS

A. What is Cloud?

The term "Cloud" refers to a Network or Internet. In other words, we can say that Cloud is something, which is present at remote location. Applications such as e-mail, web conferencing, customer relationship management (CRM) execute on cloud.

B. What is Cloud Computing?

Cloud Computing refers to manipulating, configuring, and accessing the hardware and software resources remotely. It offers online data storage, infrastructure, and application.

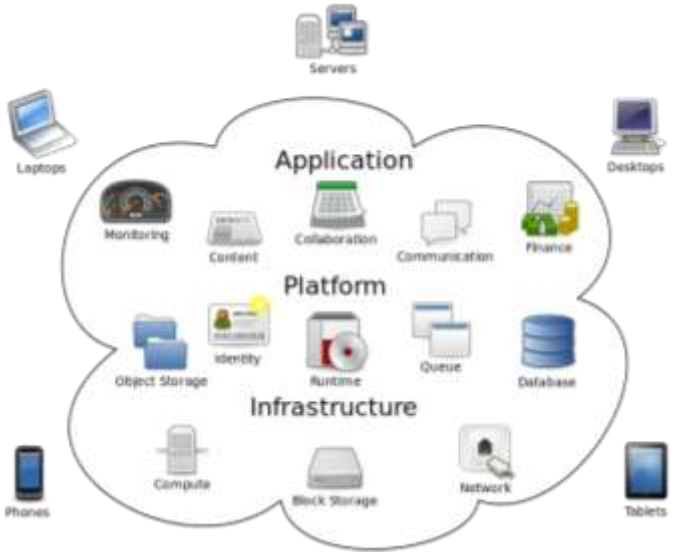

Figure 1. Cloud computing architecture

C. Cloud Service Models

Cloud computing is based on three basic service models [3]. Fig. 1 shows the architecture of cloud computing.

a) *Infrastructure-as-a-Service (IaaS)* - Provides access to fundamental resources such as physical machines, virtual machines, virtual storage, etc.
b) *Platform-as-a-Service (PaaS)* - Provides the runtime environment for applications, development and deployment tools, etc.
c) *Software-as-a-Service (SaaS)* - Allows to use software applications as a service to end-users.

D. Characteristics of Cloud Computing

The National Institute of Standards and Technology identifies the following five essential characteristics:

- *On-demand self-service:*Provision of computing capabilities, such as server time and network storage as needed.
- *Broad network access:*Capabilities are available over the network and accessed through standard mechanisms (e.g., mobile phones, tablets, laptops and workstations).
- *Resource pooling:*The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model.
- *Rapid elasticity:*Capabilities can be elastically provisioned and released, in some cases automatically.
- *Measured service:*Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts).

III. Literature Survey

In this section we compare our proposed system scheme with other possible solutions on sharing in secure cloud storage.

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.

In existing system [1], there is a limitation of predefined bound of ciphertext classes in Key-Aggregate Crptosystem the proposed work will overcome this limitation.

IV. Proposed System

The proposed system is based on 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.

In this system, 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 six modules.

1. ***Setup Module:***
   In this module, the new user creates an account on trusted cloud server. After creating an acoount successfully he/she can login in to the system. The user gets unique registration id of the account.

2. ***PMKGen Module:***
   In this module, the public/master-secret key will be generated. The public key is public to others but the master-secret key is private to the cloud server. After generating the public/master-secret key pair user can upload the file on cloud.

3. ***User Module:***
   In this module, the user can select the files to be uploaded on cloud server. After selecting particular file it is encrypted first and then saved on cloud using Encrypt Module. User can download the saved files or he can download the shared files.

4. ***Encrypt Module:***
   In this module, the data is encrypted with encryption algorithm.It uses the file identifier, public key and master-secret key of user before encryption.

5. ***AggKeyGen Module:***
   This module generates the aggregate key which is a combination of two or files. This aggregate key will be send to delagatee via email.

6. ***Decrypt Module:***
   In this module, the data is converted into original form which is called as decryption process. With this module a delegatee with an aggregate key decrypt the contents of file.

Working of proposed system is shown in Fig. 2.

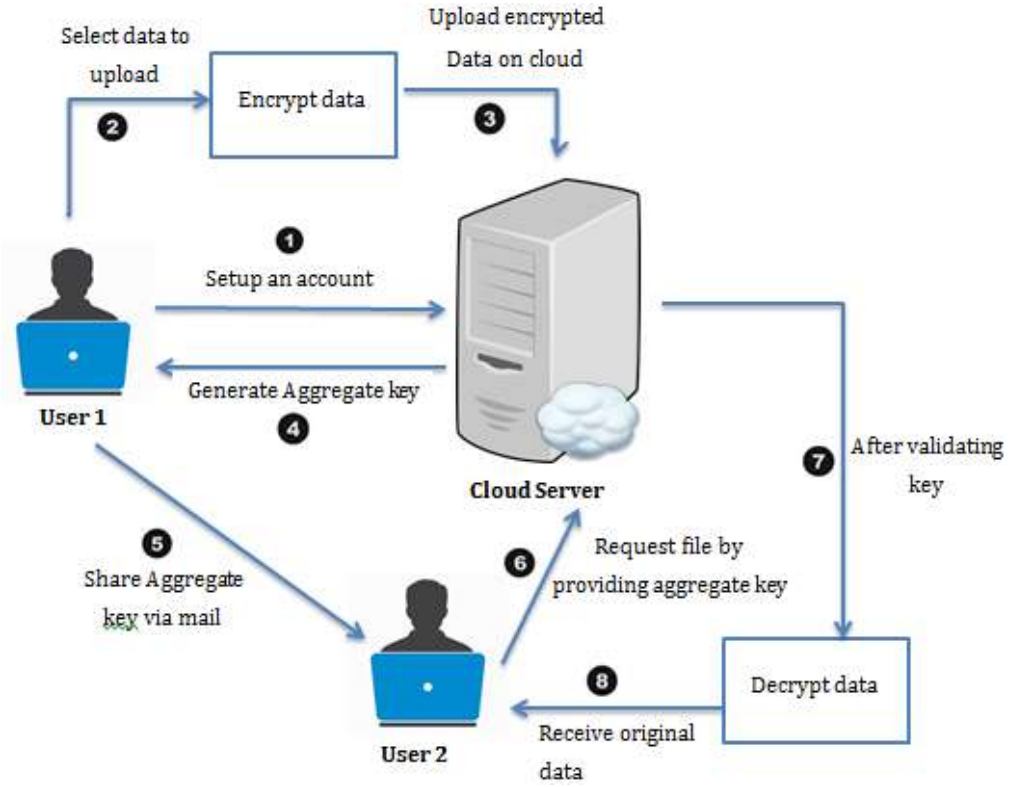

Figure 2. Working of proposed system

V. FLOW OF SYSTEM

The flow of proposed system is shown on Fig. 3. First the new user needs to create an account and login into the system. Then he upload the file on cloud. While uploading file his file gets encrypted using public and master-secret key pair of himself. For sharing files with other he may choose multiple files according to that the aggregate key will be generated and send to end user via email. The cloud server does the job of generating aggregate key. Finally, to download the shared fileshe inputs the key and after verifying the key it will be allow to download the files.

 ISSN: 2321-8169
174 – 178

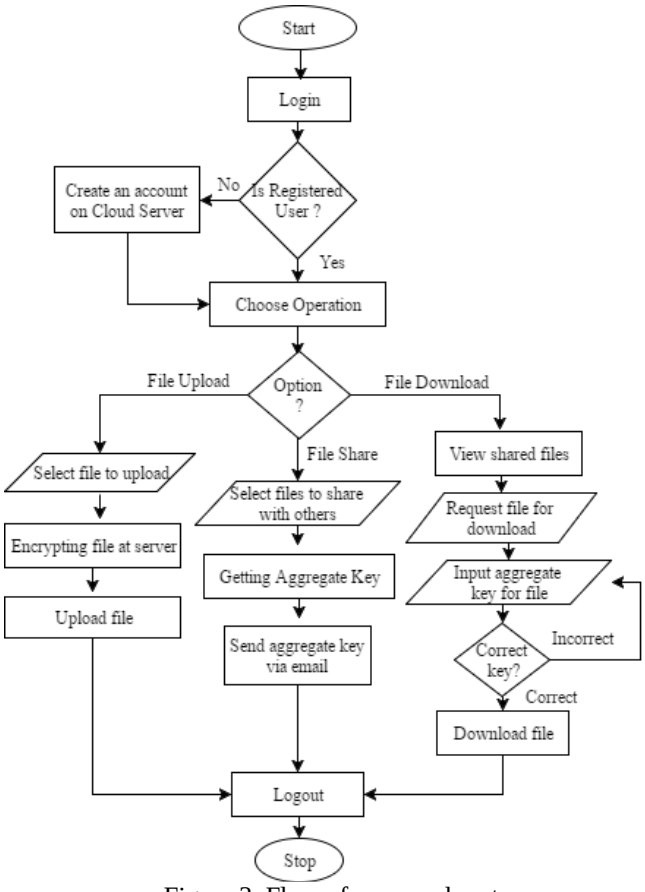

Figure 3. Flow of proposed system

VI. IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus itcan be considered to be the most critical stage in achieving a successful new system and in giving the user, confidencethat the new system will work and be effective.

Our system works in following four phases:

1. ***Setup phase:*** In this phase, the user first creates a account on clod server and login into system.
2. ***Upload phase:***In this phase, the data owner uploads the file on cloud server. It will be encrypted by Encrypt module as shown in Fig.4.
3. ***Share phase:***Data owner can share the uploaded files with other user (end user) by generating the aggregate key. This aggregate key will be shared to end user via email as in Fig. 5.
4. ***Download phase:***End user can download the files shared by other user. He can also download the own uploaded file as shown in Fig. 6.

Figure 4. Encrypting file before uploading on cloud server

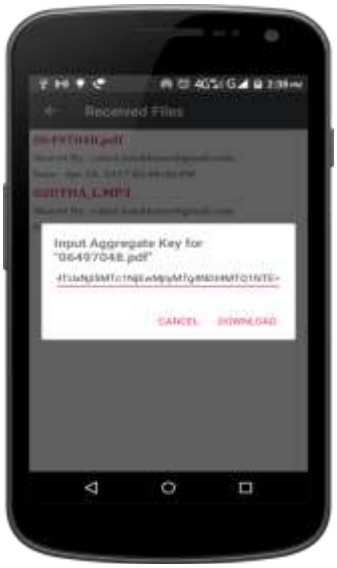

Figure 5. Entering aggregate key for downloading requested file whichis received by user via email

Figure 6. Decrypting file contents after downloading file.

VII. Results And Discussion

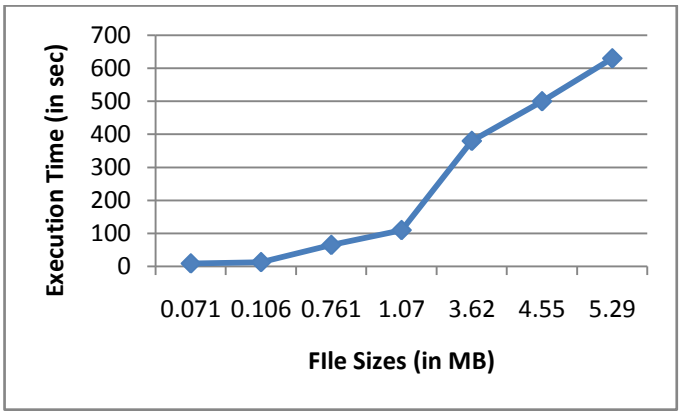

Figure 7. Computational time requiredfor encrypting files

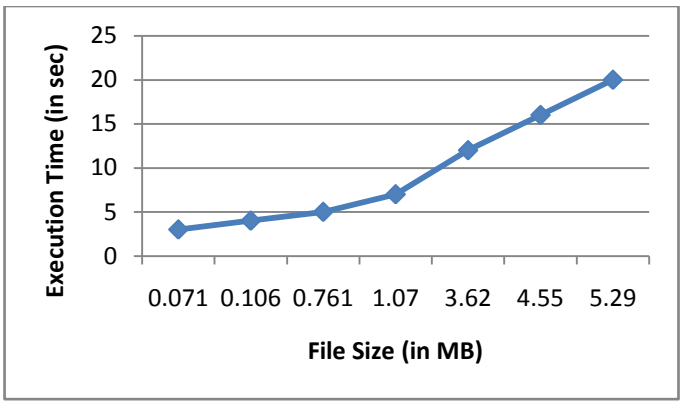

Figure 8. Computational time requiredforuploading file

VIII. Conclusion

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.

Acknowledgment

I would like to extend my gratitude to many people who helped me to bring this paper fruition. I would like to thank Prof. PramodGosavi and Prof. NileshVani. I am so deeply grateful for his help, professionalism, and valuable guidance throughout this paper. This accomplishment would not have been possible without them. Thank you.

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, March 16, 2009, http://www.theregister.co.uk/ 2009/03/16/azure_cloud_crash/

[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] 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.

[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. Springer, 2012, pp. 526–543