International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) ISSN: 2395-5325
Volume 3, Special Issue 2 (March '2017)
Proceeding of - National Conference on Recent Trends in Information Technology and Communication,
Conference held at Velammal Engineering College,Chennai,India.

# CRYPTOGRAPHIC IMPLEMENTATION OF AGGREGATE-KEY ENCRYPTION FOR DATA SHARING IN CLOUD STORAGE

**Sangeetha,**
Velammal Engineering College,
Chennai,India.

**Shruthi,**
Velammal Engineering College,
Chennai,India.

**Sharmilee,**
Velammal Engineering College,
Chennai,India.

**S.Ahamed Ali,**
Assistant Professor,
Department of Information Technology,
Velammal Engineering College,
Chennai,India.

**Abstract:** Using cloud storage, users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. Data sharing is an important functionality in cloud storage. In this paper, we propose a Key Aggregate Cryptosystem is to show how to securely, efficiently, and flexibly share data with others in cloud storage. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. We describe new public-key cryptosystems which produce constant-size cipher texts such that efficient delegation of decryption rights for any set of cipher texts are possible. The innovation is that one can aggregate any set of secret keys and make them as compact as a single key, but encompassing the power of all the key being aggregated. In other words, the secret key holder can release a constant-size aggregate key for flexible choices of cipher text set in cloud storage, but the other encrypted files outside the set remain confidential.erabilities towards user data privacy, and introduce no additional online burden to user. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and Enabling public audit ability for cloud storage is of critical importance so that users can resort to a third-party auditor (TPA) to check the integrity of outsourced data. To securely introduce an effective TPA, the auditing process should bring in new vulnerable performance analysis show the proposed schemes are provably secure and highly efficient.

***Keywords: Key Aggregate Cryptosystem Third Party Auditor, Key Distribution Centre,Role Based Access Control, Personal Health Record, Bone-Lynn-Sachem, Advance Encryption Standard, Data Encryption Standard, Triple Data Encryption Algorithm, Multiple Access Control.***

## I.INTRODUCTION

In which a data owner needs to distribute a single key to a user for sharing a large number of documents or files and the user only needs to submit a single trapdoor to the cloud for querying the shared documents. The security analysis and performance evaluation, both to confirm that our proposed schemes are provably secure and practically efficient. The single key distribution center used for distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. In Cipher text-policy contain the secret key that can decrypt the file. So when the user tries to access a file, the system will match the user attributes that associated with user key. If those attributes satisfies the access policy associated with the file, the system will decrypt the file, otherwise it will not be decrypted. The problem here is that the data records must have keywords associated with them to enable the search. The key distribution center is a single key management uses a symmetric key approach and does not support authentication. The KDC is not only a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. A user can create and store files and other users can only read the file. Write access was not permitted to users other than the creator. In the Proposed system we introduce a new decentralized access control scheme used for secure data storage. The scheme has some added feature of access control which means authorized users can access the data. The costly certificate verification in the traditional public key infrastructure. In KAC, users encrypt a message or data not only under a public-key but also under an identifier of cipher text called class. Cipher texts are further classified into various classes. The key owner holds the master-secret called master-secret key, which can be used to extract the secret keys for different classes. More importantly, the extracted key can be the aggregate key which is as compact as a secret key for a single class, but aggregates the power of many such keys.The sizes of cipher text, public-key, and master-secret key and aggregate key in our KAC schemes are of constant size.

## II.RELATED WORK

[1] In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper 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 be kept confidential even if the storage server is un trusted; moreover, our methods are secure against collusion attacks. Previous Attribute-Based Encryption systems used attributes to describe the encrypted data and built policies into user's keys; while in our system attributes are used to describe abuser's credentials, and a party encrypting data determines policy for who can decrypt. Thus, our methods are conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC).In addition, we provide an implementation of our system and give performance measurements.

[2]The broadly accepted and undisputed economic benefits notwithstanding, cloud computing, and particularly cloud storage, raises many security-related and legal qualms.Every enterprise considering to utilize cloud storage has to deal with compliance and security restrictions. In order to address these, cloud providers offer more and more security mechanisms for their services.At closer inspection, however, such mechanisms often are of limited value. In order to assess the security of existing cloud storage services, we build a generic usage model for public cloud storage integrating perspectives from the law and from economic agency theory as well as respective basic threat model. Using these models, we then examine selected security mechanisms of two well-known public cloud storage services—Amazon S3 and Google Cloud Storage—and briefly sketch auspicious starting points for future research.

[3]Cloud technology is very constructive and useful in present new technological era, where a person uses the internet and the remote servers to give and maintain data as well as applications. Such applications in turn can be used by the end users via the cloud communications without any installation. Moreover, the end users‟ data files can be accessed and manipulated from any other computer using the internet services. Despite the flexibility of data and application accessing and usage that cloud computing environments provide, there are many questions still coming up on how to gain a trusted environment that protect data and applications in clouds from hackers and intruders Cloud storage should be able to store and share data securely, efficiently, and flexibly with others in cloud storage. The costs and complexities involved generally increase with the number of the decryption keys to be shared. The encryption key and decryption key are different in public key encryption. Since we are proposing new era of Aggregate key cryptography. To produce constant length ciphertext is also one of important task that we have materialized. In this paper, we propose a simple, efficient, and publicly verifiable approach to ensure cloud data security while sharing between different users. Since we introduce here, aggregate- key cryptosystem. Cryptographic methods are usually applied to address this data sharing issue.

[4] Personal health record is maintain in the centralize server to maintain patient's personal and diagnosis information. Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. The security schemes are used to protect personal data from public access. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. In this paper we propose novel patient-centric framework and suite of mechanism for data access control to PHR'sstored in semi trusted servers. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE)techniques to encrypt each patient's PHR file. Data owner update the personal data into third party cloud data centers. Multiple data owners can access the same data values. Our scheme supports efficient on-demand user/attribute revocation.

[5] This paper introduces Panda, a software framework for Pairings and Arithmetic. It is designed to bring together advances in the ancient computation of cryptographic pairings and the development and implementation of pairing-based protocols. The intention behind the Panda framework is to give protocol designers and implementers easy access to a toolbox of all functions needed for implementing pairing-based cryptographic protocols, while making it possible to use state-of-the-art algorithms for pairing computation and group arithmetic. Panda Aoers an API in the C programming language and all arithmetic operations run in constant time to protect against timing attacks. The framework also makes it easy to consistently test and benchmark the lower level functions used in pairing-based protocols.an example of how easy it is to implement pairing-based protocols with Panda, we use Bone-Lynn-Sachem (BLS) signatures. Our Panda-based implementation of BLS needs only 434640cycles for signature generation and 5832584 cycles for signature frication on one core of an intel i5-3210M CPU. This includes full protection against timing attacks and compression of public keys and signatures

## III.PROCESS OF KEY AGGREGATE CRYPTOSYSTEM

This work is done by focusing on the following modules

**Modules with Description**

- Secure Storage.
- Key Re-Authentication.
- Integrity Checking.
- Data Sharing.
- Dynamic Data Forwarding.

**Secure storage**

In this module, the user registration process is done by admin. Here every user's give their personal details for registration process. After registration every user will get an ID for

accessing the cloud space. If any of the user wants to edit their information they have to submit the details to the admin after that the admin will do the edit and update information process. This process is controlled by the Admin. In this module, every user's share their information and data's in their own cloud space provided by the admin. That information may be sensitive or important data's. For providing security for their information every user's storing the information in their specific cloud. Registered users only can store the data in cloud.

**Key Re-Authentication**

In this module, the information and data's shared by the user in the cloud is encrypted by using AES (Advance Encryption Standard) algorithm. All the information shared by every user is encrypted based on the data sensitivity and stored in the cloud. Involves in client side configuration, performs two actions. The two actions are access control and permission control. Access control-AES algorithm. Permission control – Iconic Encryption algorithm. Access control process is based on the server control features. Permission control process is based on the client control features.

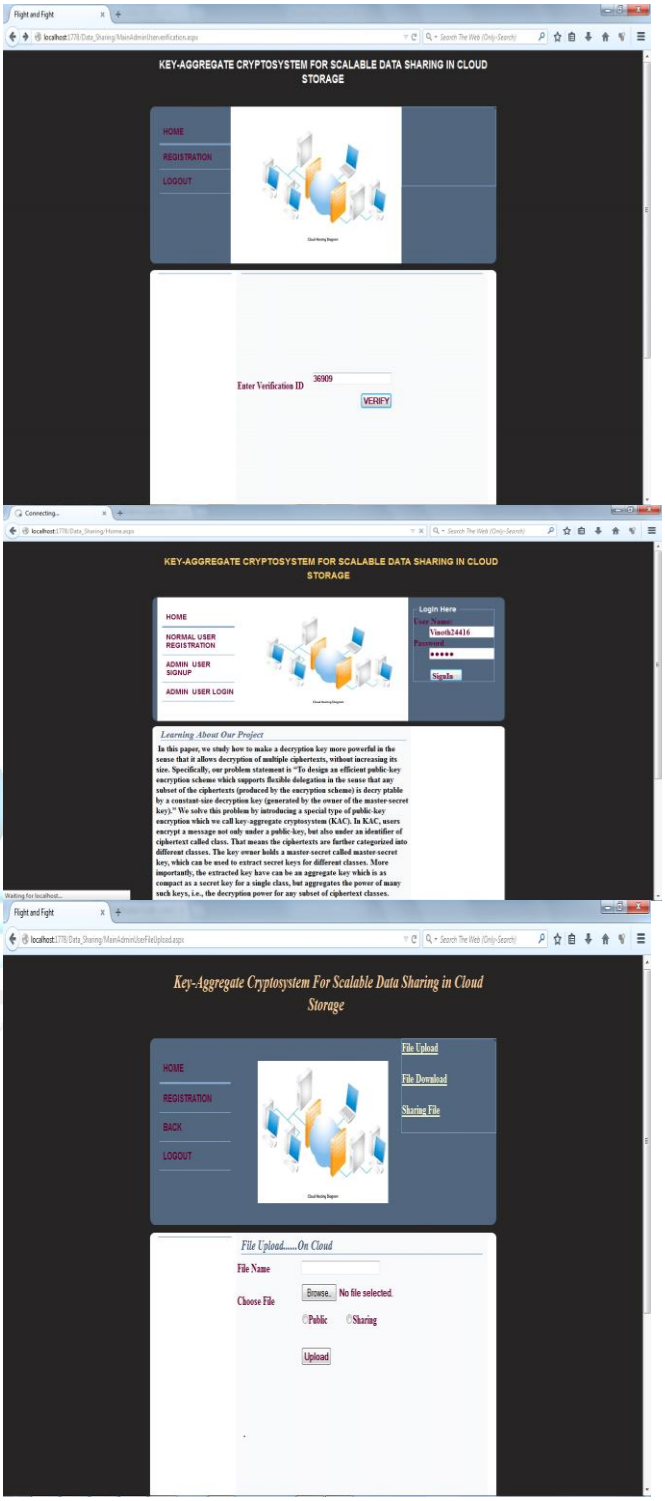
**Integrity Checking**

Integrity checking is the process of comparing the encrypted information with altered cipher text. If there is any change in detection a message will send to the user that the encryption process is not done properly. If there is no change in detection means then it will allow doing the next process. Integrity checking is mainly used for anti-malware controls. In this module, the encrypted data is decrypted by the user using the public key given by the owner of the data. Decryption is the process of converting cipher text into plain text. MES algorithm is used for encrypting and decrypting the data. The user can view the information and also can download the data with high security.

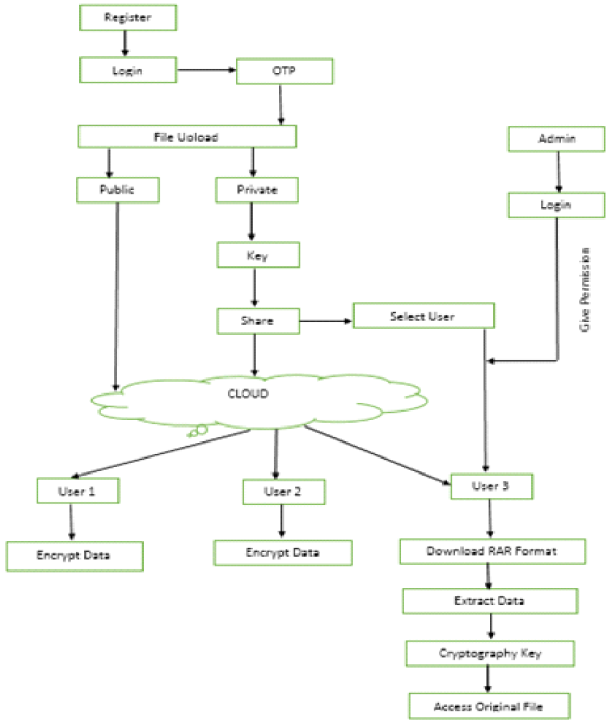
**Data Forwarding**

In this module, the encrypted data or information stored in the cloud is forwarded to another user account by using that user's public key. If any user wants to share their information with their friends or someone they can directly forward the encrypted data to them. Without downloading the data the user can forward the information to another user.

## IV.IMPLEMENTATION RESULTS



**FLOW CHART**




In order to upload and share the file in the cloud, user have to register by giving their details .once the user has registered, username and password is been sent to users mail ID. The user has to login with the given username and password and the OTP (One Time Password) is sent to the users mail ID for security purpose. To upload the file the user has to choose the file upload option and provide the file details like, file name, key and select user .once the file is uploaded the dialog box appears saying that your file is uploaded successfully. To share the uploaded file user has to choose the file sharing option and provide the file details as given before. now to download the uploaded file by other user , he/she need to get the approval from the admin once the user is authorized he/she can download the file. Suppose if the user dint get the approval from the admin the downloaded file will be in the encrypted format.

## V.CONCLUSION

The delegation of decryption can be effectively implemented with the aggregate key which is only of fixed size. The Multiple Key Distribution Centers used for distributing secret keys and attributes to users. It is provided with the high security by using encryption and decryption keys for sensitive information. The cipher text is sent to the cloud based on the attributes and the cloud verifies the key and stores the cipher text. The user wants the data, the cloud sends the cipher text. If the user has key matching with access policy, it can decrypt and get back original message.

## REFERENCE

[1]. Author: John Bettencourt ,Year of publication:2015
[2]. Author:Silvia Balaban,Year of publication:2014
[3]. Author:Sativa Kacheshwar Dab hade,Year of publication:2014
[4]. Author:Y.B.Guravl,Manjiri Deshmukh,Year of publication:2013
[5]. Author:Michael Naehrig,Year of publication:2013
[6]. Eric Zavattoni, Luis J. Dominguez Perez, Shigeo Mitsunari, Ana H.S´anchez- Ramirez, Tadanori Teresa, and Francisco Rodr´ıguez-Henr´ıquez. Software implementation of an attribute-based encryption Scheme. IEEE Trans. Computers, 64(5):1429–1441, 2015.
[7]. Erik C Shall man. Up in the air: Clarifying cloud storage protections. Intell. Prop. L. Bull., 19:49, 2014.
[8]. Cheng-Kang Chu, Sherman SM Chow, Wen-Guey Zeng, Jitneying Zhou, and Robert H Deng. Key-aggregate cryptosystem for Scalable data sharing in cloud storage. Parallel and Distributed Systems, IEEE Transactions on, 25(2):468–477, 2014.
[9]. Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wending Lou.Scalable and secure sharing of personal health records in cloud Computing using attribute-based encryption. Parallel and Distribute Systems, IEEE Transactions on, 24(1):131–143, 2013.
[10]. Chitchanok Chuengsatiansup, Michael Naehrig, Pance Ribarski, And Peter Schwa be. Panda: Pairings and arithmetic. In Pairing- Based Cryptography - Pairing 2013 - 6th International Conference, Beijing, China, November 22-24, 2013, Revised Selected Papers, pages 229–250, 2013.