Integrated Cryptosystems with Aggregate Keys for Online Data Sharing on the Cloud Server

GANAPATHIRAJU RAMANA RAJU [#1] & Y.SRINIVASA RAJU [#2] & D.D.D.SURIBABU [#3]
[#1] MCA Student, Master of Computer Applications, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#2] Assistant Professor, Master of Computer Applications, D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.
[#3] Head & Associate Professor, Dept of CSE, D.N.R. College of Engineering, Bhimavaram, AP, India.

Received: January 14, 2019 Accepted: February 21, 2019

ABSTRACT: *In the current cloud servers, the major limitation is data which is stored and shared over the cloud users has no security and there is also no security for accessing the data in the current cloud servers. This is mainly because all the data which is stored in the current cloud servers is stored in the form of plain text rather than in a cipher text manner. Even though if there was any cloud with a facility like encrypting the data before it is stored into its memory location, it may use any of the cryptography primitive algorithms like public ,private or secret key encryption algorithms. But all these algorithms have some or other limitations when it is compared one with other. There was no facility like aggregation of Keys which was generated by the server while storing the data into the cloud. In this paper, we address this practical problem, which is largely neglected in the literature, by proposing the new concept of novel key aggregate cryptosystems for secure data sharing in the cloud. In this paper for the first time we have introduced a new technique like aggregation in which a data owner only needs to distribute a single key to a set of cloud users for sharing a large number of documents.*

Key Words*: Encryption, Decryption, Key Aggregate, Cipher Text, Cryptosystems.*

I. Introduction

Now a day's cloud domain has occupied a major role in each and every part of the information processing and information storage centers. As the cloud has became a valuable resource for all parts of information processing centers, the data which is to be stored will be stored on the remote systems not on their local hardware, and accessed remotely via internet by connecting various servers. As the data will be stored on remote server, the data user need to retrieve the data from the remote server, whenever he want any data from that remote hardware. In the current cloud servers, the major limitation is data which is stored and shared over the cloud users has no security and there is also no security for accessing the data in the current cloud servers [1]. This is mainly because all the data which is stored in the current cloud servers is stored in the form of plain text rather than in a cipher text manner.

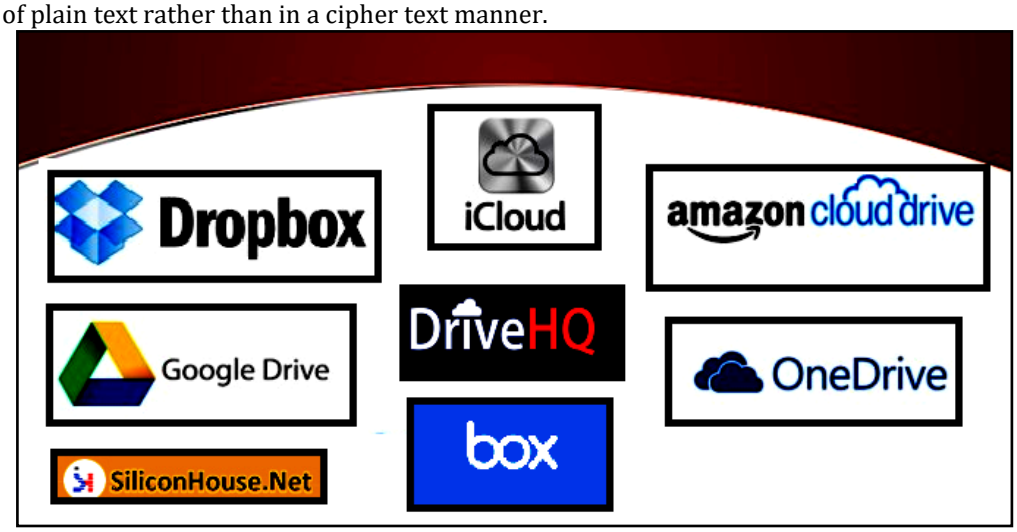

Figure.1. Represents various types of Cloud Service Providers both Public and Private Service Providers

As we know that cloud has grabbed user attention in storing their valuable or sensitive information however limits in allocating resources dynamically. As we know that cloud has received more and more user's attention towards data storage, it still has some restrictions in size constraints. In enterprise settings, we tend to see the increase in demand for knowledge outsourcing that assists within the strategic management of corporate knowledge. In the recent cloud service providers, it is straightforward to use without charge accounts for email, image album, file sharing and/or remote access, with storage size a lot of than Fifteen GB (for free usage) and up to 1 TB or more for the premium users [2].

From the above figure 1, we can clearly find out that there are many cloud service providers that are available in the current days for storing and accessing the data remotely. Here in the above figure, there are some public clouds which takes no amount for storing the data till 1GB,some clouds are their which will give access only for the premium members like those who have premium account. Also there are some cloud service providers like hybrid cloud, which can provide public and private services at a time also known as hybrid cloud service provider. For our project we are using the DRIVEHQ.com as the cloud service provider for storing and accessing the data in a secure manner .In this project we take a DRIVEHQ public account like which can accept any data up to 1 GB, which is almost the max size and if the data exceeds then it will ask to pay the amt greater than 1 GB for the cloud data user [3], [4].

II. Background Work

In this section we mainly discuss about the background work that was carried out inorder to find out the key aggregate cryptosystems for sharing the data security over encrypted cloud data. Now let us discuss about that in detail as follows:

Preliminary Knowledge

There are mainly 3 different types of cloud service providers available in the realtime environment for storing and accessing the data from remote systems rather than local systems.

A. Public Cloud Service Provider
B. Private Cloud Service Provider
C. Hybrid Cloud Service Provider

A. Public Cloud Service Provider

This is one of the cloud service provider which is used to store and access the information to and from the remote servers rather than from the local systems.For any public cloud service,the CSPs provide min 1 GB and Max 2 GB of storage space [5]-[7] and the end user can able to access his files within the permitted space.If the user wish to add more than 2 GB of cloud space,then he/she need to pay amount for the excess data to the CSP.

B. Private Cloud Service Provider

This is one of the cloud service providers which is used to store and access the information to and from the remote servers rather than from the local systems. For any private cloud service, the CSPs provide various plans according to the user requirement and based on the plan he choose he/she can able to access the server space for storing and accessing the files in a secure manner. For the private cloud there will be several plans like short time cloud service or long term cloud service, depends on the user requirement the appropriate plan can be choosen for data storage and retrieval.

C. Hybrid Cloud Service Provider

This is one of the cloud service providers which is used to store and access the information to and from the remote servers rather than from the local systems. For any hybrid cloud service, the CSPs provide initially upto 2 GB free space and once the end user crosses the min specified space constraint then he will be charged extra cost for the memory location which is consumed by the end user.

In our proposed application we try to use Hybrid cloud for accessing the files to and from the cloud server in order to show the performance of our proposed approach.

III. Proposed Integrated Cryptosystems with Aggregate Keys for Online Data Sharing on the Cloud Server

In this section we will mainly discuss about Integrated Cryptosystems with Aggregate Keys for Online Data Sharing on the Cloud Server. Now let us discuss about this proposed model in detail as follows:

Scope

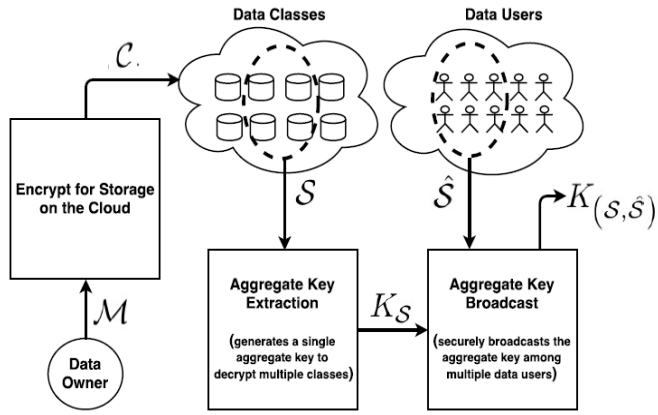

Figure.2. Represents the Proposed Model for Key Aggregate Broadcast For Secure Data Storage

In this proposed system model, we mainly discuss about the various primitives that were used in our current thesis. For any cloud service provider, it contains three main entities like:

1. Data Owner,
2. Data User/Search User.
3. Data Classes
4. Aggregate Key Extraction
5. Aggregate Key Broadcast

Initially the data owner is the person who may be an individual or sometimes an enterprise, who wishes to outsource a collection of documents D = (D1, D2, . . . , Dn) in encrypted form C = (C1, C2, . . . , Cn) to the cloud server and still preserve the search functionality on outsourced data. Here we assume that documents are labeled with D [8] and if there are many documents to be out sourced they are represented as D1, D2 and so on. Here the documents what we take in our current paper consists of a general documents or text files and need to be stored in a secure manner inside a cloud server. Here the sensitive data is initially encrypted and then ready to store inside the cloud server, they are termed as C1, C2 and so as they were encrypted[9] by the data owner at his level before out sourcing into the cloud server.

From the above 2,we can clearly find out that the data administrator try to upload the files into the cloud server in an encrypted manner and once the data is uploaded the data need to be stored in the form of encrypted manner,so that data will be stored in a secure manner inside the cloud server.As there are many files inside the cloud server [10] ,the data users need to be registered with their valid details into the cloud server and they will try to request the files which are available in the cloud server from the data owners [11].Once the data owners receive multiple use requests for a group of common files,then the data owner need to generate a aggregate key (S) for the end users group and if the same end users are requesting multiple files commonly then the cloud server need to broad cast this aggregate key to the end users commonly with a single key for that selected users.Finally those who are having aggregate keys can able to decrypt the data in a plain text manner and remaining all cant able to access the data from their login account if they don't have a valid id and password[12].

IV. Conclusion

In this proposed thesis we finally implemented and analyzed a secure, and efficient approach to broadcast single aggregate to multiple users. In this paper, we propose CPA(Chosen Plain Text Attack) and CCA (Chosen Cipher Text Attack) secure KAC (Key Aggregate Cryptosystems) constructions that are efficiently implementable and finally proved KAC is best in providing solution again two CPA and CCA attacks.By conducting various experiments on our proposed model, we finally came to a conclusion that our proposed approach is best in broadcast single key for the end users over encrypted cloud data.

VI. References

1. "About Dropbox". Dropbox, Inc. Retrieved 2013-06-03. Dropbox was founded by Drew Houston and Arash Ferdowsi in 2007, and received seed funding from Y Combinator.

2. M. Chase paper on "Improving Privacy and Security in Multi-Authority Attribute-Based secret writing," Proc. ACM Conf. laptop computer and Comm. Security, pp. 121-130. 2009.
3. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based secret writing for Fine-Grained Access management of Encrypted info,"Proc. thirteenth ACM Conf. laptop computer and Comm. Security (CCS '06), pp. 89-98, 2006.
4. "Meet the Team! (Part 1)". The Dropbox Blog. Dropbox, Inc. Retrieved April 24, 2010 by Ying, Jon (February 5, 2009)..
5. Jon Fingas (2013-03-15). "Dropbox acquires Mailbox, teases an email and cloud collaboration". Engadget. Retrieved 2013-03-15.
6. R. A. Popa ,N. Zeldovich. "Multi-key searchable encryption". Cryptology ePrint Archive, Report 2013/508, 2013.
7. J.Li, X.F. Chen, M.Q. Li, J.W. Li, P. Lee, Wenjing Lou. "Secure Deduplication with Efficient and Reliable Convergent Key Management", IEEE Transactions on Parallel and Distributed Systems, 25(6): 1615-1625, 2014.
8. C. Chu, S. Chow,W. Tzeng, et al. "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions on Parallel and Distributed Systems, 2014, 25(2): 468-477.
9. J. Li, Q. Wang, C. Wang. "Fuzzy keyword search over encrypt-ed data in cloud computing", Proc. IEEE INFOCOM, pp. 1-5, 2010.
10. IDC Enterprise Panel. It cloud services user survey, pt. 3: Whatusers want from cloud services providers, august 2008.
11. Sherman SM Chow, Yi-Jun He, Lucas CK Hui, and Siu Ming Yiu.Spice–simple privacy-preserving identity-management for cloudenvironment. In Applied Cryptography and Network Security, pages526–543. Springer, 2012.
12. Cong Wang, Sherman S.-M. Chow, Qian Wang, Kui Ren, andWenjing Lou. Privacy-preserving public auditing for securecloud storage. Cryptology ePrint Archive, Report 2009/579, 2009.http://eprint.iacr.org/.