International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Outsourcing Data on Cloud Using Aggregate Key

Ramakrishna Jadhav

[1]Savitribai Phule Pune University, RMD Sinhgad School of Engineering, Warje Pune, India

Abstract: ***Cloud computing has gained a lot of interest since last few decades due to its expanding services. Data sharing is one of the best options for gaining advantage of utilizing service for sharing the data being uploaded over cloud storage. But it's very essential that the data that is being uploaded over the cloud storage is to be maintained securely and data confidentiality is also the aspect to be considered with importance. To achieve this, the proposed system derives a novel algorithm or architecture which makes use of the public key cryptographic technique. This public key cryptographic system generates constant size cipher text. The keys are to be maintained secretly. These secret keys can be then delivered to obtain the actual plain text from the cipher texts. The encrypted files are maintained over cloud storage and the aggregate key, on request from the group user is sent to the corresponding users' mail id. This obtained aggregate key is then utilized for decrypting the download file. The proposed system shows how the KAC helps is maintaining the aggregate key architecture for managing the cloud storage for encrypted files.***

Keywords: convergent keys, cloud storages, data sharing, key-aggregate cryptosystem.

1. Introduction

Cloud computing has gained attention due to creation of logical pools for files being stored; the cloud stored data is owned and managed by hosting company or hosting management. It's a cloud service provider's responsibility to make the cloud data accessible and available for Read/Write on user demand and keep the environment secured and continuously running. Cloud users, may it be an individual or an organization, either buy or lease the storage space of the cloud from the CSP to store the corresponding data over clouds. Cloud storage can be easily accessed through various web services, APIs or desktop storage services.

Cloud services are highly virtualized in terms of resources, scalability, multi tenancy, etc. These services can be easily accessed from on premises deployed applications or off premises interfaces. Cloud storages are mainly briefed as hosted storage object service, but later this term has evolved to further include other various types of data which are available as a service, for an instance, block storage services.

Cloud architecture mainly supports data sharing and hence can be termed as key feature of clouds. Also a major feature of cloud is that one can store any kind of data over cloud and can download it or upload new data anytime over the clouds. So it's very clear that the data being stored or shared can either be a multimedia data or it can be in textual or document format. As data sharing is one of the features available on cloud, it should be done in a secure manner. Else the attackers or malicious users may damage your data and lead to its misuse.

So, for accomplishing such security of information sharing, the key total cryptosystem strategy is being utilized for specific information sharing. In this KAC structural planning, the information which is shared is kept in the encoded position. This encryption is completed utilizing a mystery key which makes cyphers of altered information size. By utilizing the total key these cyphers can be decode. This total key will decode just cluster of cyphers other remaining cyphers will be private.

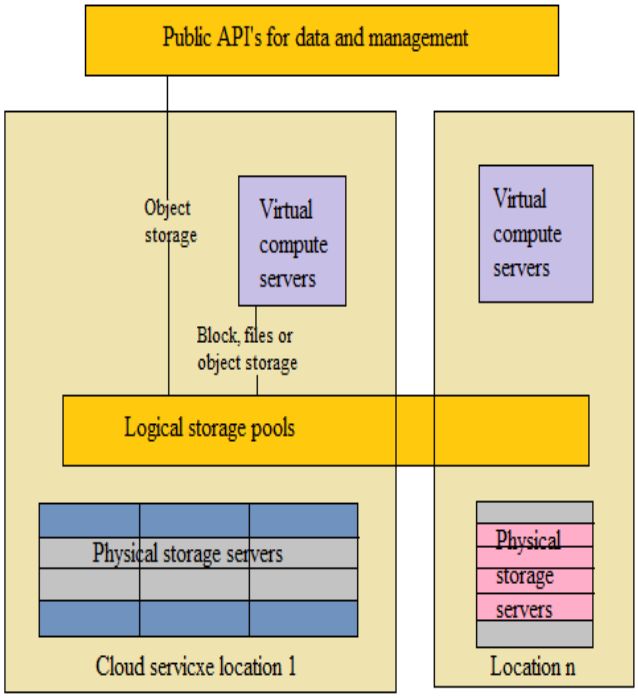

Figure 1: Architecture of data sharing in cloud storage.

2. Literature Survey

The significance of information sharing and the need to guarantee protection and security is talked about in various existing articles.

1. Security and privacy in the cloud

This paper diagrams the necessities for accomplishing protection and security in the Cloud furthermore quickly plots the prerequisites for secure information partaking in the Cloud. It gave an overview on protection and security in the Cloud concentrating on how protection laws ought to likewise mull over Cloud figuring and what work should be possible to counteract security and security breaks of one's close to home information in the Cloud. This investigated variables that influence overseeing data security in Cloud processing. It clarifies the important security requirements

for undertakings to comprehend the elements of data security in the Cloud.

2. Dynamic Broadcast Encryption:
This system uses Broadcast encryption which empowers a supporter to transmit encoded information or data to an arrangement of clients so that just a focused on subset of clients can decode the information. Other than above qualities, element show encryption it additionally permits the preserving so as to gather screen to incorporate new individuals already figured data, and client unscrambling mystery keys need not be registered over and over, the Aggregation rationale and size of figure writings are stay unaltered and the gathering encryption key requires no change.

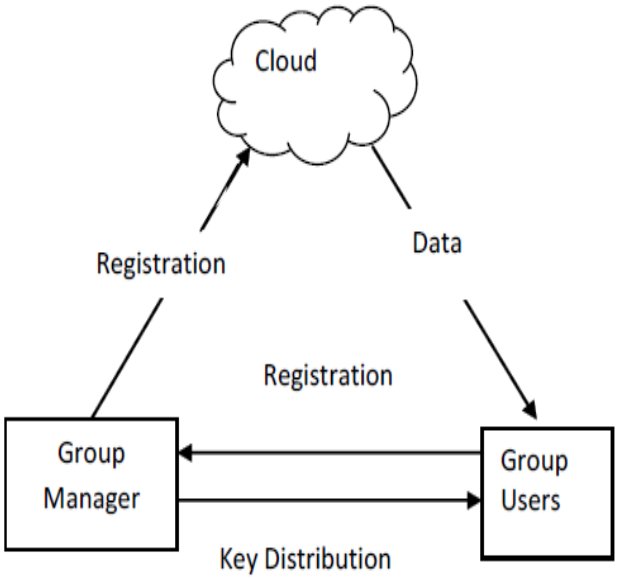

Figure 2: Dynamic Broadcast Encryption.

3. Data Sharing in Cloud Using Hybrid Cryptosystem
This framework utilizes the cut of information cloud to encode or unscramble the information. The first information are initially partitioned into various cuts, and afterward distributed to the distributed storage. At the point when a denial happens, the information proprietor needs just to recover one cut, and re-scramble and re-distribute it. The information proprietor recovers the mark from secure middle person and after that it permits client to transfer or download the information over the cloud.

4. Cryptographic Storage System
This framework permits sharing of secure document on untrusted servers. It partitions records into the gathering of document and scramble every gathering of document with a one of a kind document key. The information proprietor can impart the record gatherings to others by conveying the related lockbox key, where the lockbox key is utilized to encode the document piece keys. In any case, it achieves a substantial key conveyance overhead for extensive scale record sharing. Furthermore, the record key should be overhauled and disseminated again for a client renouncement.

3. Proposed System

The proposed framework is essentially outlined on the premise of key accumulation encryption. Here it utilizes two keys to scramble and decode the information which are mystery key and its total key. The information proprietor makes people in general framework parameter and creates an emit key which is open key pair. Information can be scrambled by any client and he may choose ciphertext square connected with the plaintext record which needs to be encoded. The information proprietor have rights to utilize the mystery key from which he can create a total key which is use for unscrambling of an arrangement of ciphertext pieces. The both keys can be sent to end client in extremely secure way. The confirmed client having a total key can decode any square of ciphertext.

New user gets registered over the shared cloud. Once the user gets registered he /she can upload files in two different privileges. If while uploading, user selects file type to be Individual, the uploaded file is kept hidden from the other users of the group. And if the file privileges while uploading is kept to be as group file, the file is made visible to other group members but only within the same group.After the file has been uploaded, the user can either place request for files uploaded by other group members over the cloud or can share the key to the users who have requested the file from current user.

When the file key is being shared, the file index for which the request has been placed is passed to aggregator function to create the aggregate key and there by the aggregate key is sent to the requesting users' registered mail id. Once the keys are shared, the entry from the request log of current user is removed so as to avoid stacking of requests from other users. This makes current user convenient to accept only the pending requests and hence avoids sharing keys to same request multiple times.

This undertaking comprise of five calculations which are utilized to perform the above operations. These calculations are:

Setup: the record is made on the untrusted server for sharing of information. This record is produced by information proprietor.

KeyGen: This calculation is use for the era of open key. The information proprietor produces an open emit key to encode the information over cloud. It additionally makes a total key to get to the square of figures of constrained size.

Encrypt: This calculation scrambles the information gave by the information proprietor by utilizing the discharge key. This encoded information is then share among the cloud.

Extract: The total key is use for removing the specific piece of the figures from the figure record. In any case, other encoded information stays secure.

Decrypt: The encoded information is then decoded by utilizing the same discharge key which is use for encryption.

As the above figure demonstrates, the key task is done in element way. The total key is use to unscramble just those figures which client needs. This key won't decode the other remaining figures. The primary encryption and unscrambling is finished by the emit key. On the off chance that any client enters the wrong emit key or wrong total key then the client contains will be obstructed by the information proprietor. What's more, the data which that client tries to recover is then included into non classified stockpiling. Just information proprietor can unblock that client substance and he may exchange the data from non-classified stockpiling to private stockpiling. The client can just get to the information on cloud on the off chance that he has emit key and the total key, else he will be piece until the end of time.

4. Mathematical Model

The proposed system can be mathematically represented using set theory as mentioned below:
S = {F, K, M, R, T}
F = Files being uploaded
K = Aggregate Keys getting generated as per user requests.
M = Master key formed to decrypt any file.
R = user requests for file download with file index.
T = user type is an Individual user or a group user.

User needs to place the request to access any shared file over the cloud along with its index. The authorized user who has uploaded the file can see the user requests and can further send the aggregate key to access the files requested by the users. The aggregate keys are generated on every request getting accepted by the file owner. Once the aggregate key if generated, it's sent to the requesting user's mail id for security purpose. If the user has registered as an individual user, his/her files are stored as private files and hence cannot be shared. This additional feature in the proposed system makes the shared cloud act as a private cloud too.

5. Results and Discussion

After successful registration to the system, user login to the system. For login, user must have to enter the valid username and password. If user entered credentials are not valid then, user cannot proceed further. If user credentials are valid then only he can proceed further.

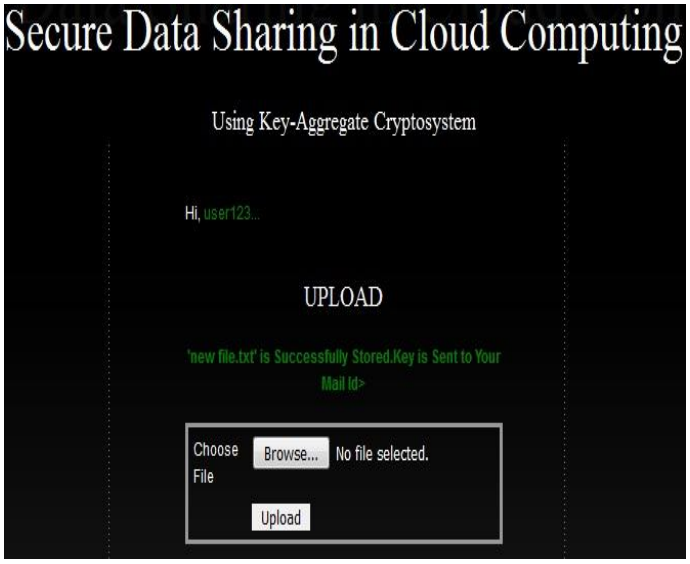

Figure 3: File Upload

After successful login to the system, user upload the file. For uploading the file, user select the file from directory and upload it to the system. The selected file first encrypted and then it uplaod on the cloud. The file uploaded on the cloud is encrypted format.Here; the details of uploaded files are shown fig 3.

Figure 4: Request decryption Keys

Once the data is uploaded the user with whom data is shared knows the data is uploaded on cloud. Then the user can send the request for decryption key as shown in fig 4.

Users can download the file. For file download, user first enters the aggragate key received over the mail in the text box. At back end the the entered aggragate key is splitted and apply the valid key to the file which should download. If key is valid then only file will be decrypted properly and downloaded, else encrypted data is downloaded as shown in fig 5.

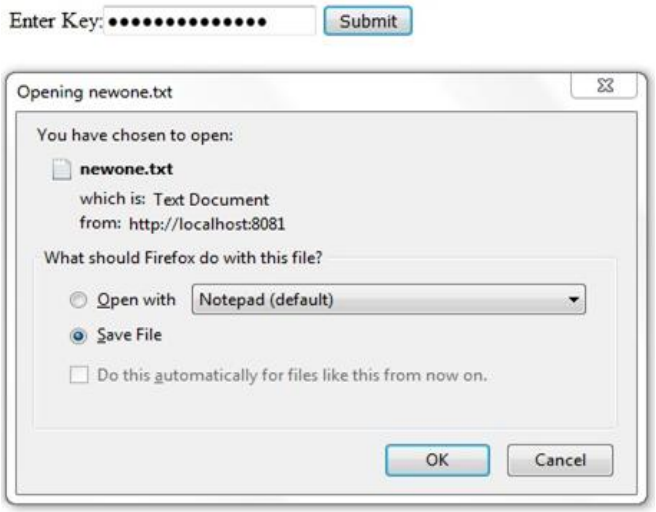

Figure 5: File decryption after receiving key

The proposed system is implemented and tested on 4 users as for result comparison where each user uploaded 10 files. So in general scenario if total files were to be counted, 40 files were uploaded and which would have required 40 separate keys to be stored and shared while user requested the files.

But the KAC proposed architecture, the number ofuploaded files and the number of requested files do not affect the number of keys to be shared, whate ever may be the count of files being requested , only a single key is being shared to the requesting user which is called as aggregate key.

The additional feature in the proposed system is that on a same cloud, user can upload the files as individual files which are not visible to the users working as group members. The numerical analysis of the various parameters can be seen in table 1 below. The table shows that the performance of the proposed system is not affected by number of users requesting files or number of files being uploaded. And hence the proposed system is proved to be a secure scalable data sharing system using aggregate keys.

Table 1: Performance Comparison

Details	General Scenario	KAC
No. of Files	40	40
No. of keys	40	1
Master Key	NA	1
Aggregate Key	NA	n
Storage Required	40	1
Private Storage	NA	Allowed
Performance	O(n)	O(1)

6. Conclusion

From above it presume that the proposed framework is observed to be exceptionally effective for sharing the information on cloud. This sharing is done in a safe and secret way. For this, it figures KAC calculation which means key aggregate encryption calculation. In this paper it has to keep up two open keys; Initial one is discharge key which is use for encryption and unscrambling of the information over cloud. Furthermore, the second key is total key which is use to unscramble restricted piece of figure. Other information stays private. This framework gives blocking component to the client whose conduct is by all accounts malevolent.

References

[1] 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.
[2] L. Hardesty, "Secure computers aren't so secure," MIT press, 2009, http://www.physorg.com/news176107396.html.
[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public Auditing for Secure Cloud Storage," IEEE Trans. Computers, vol. 62, no. 2, pp. 362–375, 2013.
[4] B. Wang, S. S. M. Chow, M. Li, and H. Li, "Storing Shared Data on the Cloud via Security-Mediator," in International Conference on Distributed Computing Systems - ICDCS 2013. IEEE, 2013.
[5] S. S. M. Chow, C.-K. Chu, X. Huang, J. Zhou, and R. H. Deng, "Dynamic Secure Cloud Storage with Provenance," in Cryptography and Security: From Theory to Applications - Essays Dedicatedto Jean-Jacques Quisquater on the Occasion of His 65th Birthday, ser. LNCS, vol. 6805. Springer, 2012, pp. 442–464.
[6] D. Boneh, C. Gentry, B. Lynn, and H. Shacham, "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps," in Proceedings of Advances in Cryptology - EUROCRYPT '03, ser. LNCS, vol. 2656. Springer, 2003, pp. 416–432.
[7] M. J. Atallah, M. Blanton, N. Fazio, and K. B. Frikken, "Dynamic and Efficient Key Management for Access Hierarchies," ACM Transactions on Information and System Security (TISSEC), vol. 12, no. 3, 2009.