**International Journal of Management, IT & Engineering**
Vol. 8 Issue 4, April 2018,
ISSN: 2249-0558 Impact Factor: 7.119
Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

# LITERATURE SURVEY ON KAC SCHEME FOR SCALABLE DATA SHARING IN CLOUD STORAGE

**S. R. Jankar**[*]

## Abstract

Cloud computing is web based computing where one of a kind service–such as server, storage and applications are delivered to an organization's computer gadgets via internet and there are central remote servers to keep records and applications. Cloud storage allows user to share information remotely, access it and additionally user share this information with other. So, Data sharing is an essential functionality of cloud storage. Data sharing is now not secured as user totally depends on cloud server for data privacy and data management. So, user prefers to encrypt their information earlier than importing on cloud. In the Key Aggregate Cryptosystem for data sharing, an efficient public key encryption scheme which helps in extensible delegation it means that any subset of cipher text is decryptable by using a fixed size decryption key. The secret key holder can release a fixed size aggregate key for extensible alternatives of cipher text in cloud storage. This paper come out with an overview and find out about cryptographic approach for security and effectively data sharing in cloud storage.

*Keywords:*

Cloud storage;

Data sharing;

Key aggregate encryption;

Cryptography

[*] **M.E. Student,Department of Computer Science & Engineering,M.S. Bidve Engineering College Latur, Maharashtra, India**

## 1. Introduction

Cloud system can be used to allow user for getting access to all the utility and files from anywhere in the world and additionally allow data sharing capabilities. Cloud storage is online data storage facility provided by cloud computing where the data stored in and can be accessed from more than one distributed and linked resources that include in a cloud.

Cloud storage is gaining popularity specifically in commercial enterprise as it offers a lot of way to store large data, it offers worthwhile ways to back up data, in additional we can see increase in demand for data outsourcing to minimize hardware cost, and in additional it offers facility to organizations to subscribe to online services for a nominal fee. Because of today's Wi-Fi technology everybody can access their emails and nearly all files on cellphone in any corner in the world.

Nowadays, it is not difficult to sign in for free account of email, file sharing, and remote access. So, the data sharing is an essential functionality in cloud storage. This is now not a secure sharing with encrypted data due to the fact cloud user is completely depend on cloud server for data privacy in which cloud server offers an access control after the authentication. It means any privilege escalation will expose all the data.

Cloud server look over the availability of files on behalf of the data owner and due to the shared tenancy conditions data on one virtual machine(goal) can be stolen by any other virtual machine (co-resident with goal) as they are situated on same physical machine. It can be said that cloud user can't trust that cloud server is doing job properly in terms of security and confidentiality.

In cloud storage, efficient public key encryption technique is used which helps in extensible delegation in such way that any subset of cipher text is decryptable by a fixed size decryption key. In different words we can say that the secret key holder can release a fixed size aggregate key for extensible alternatives of cipher text set in cloud storage.

In KAC, user can encrypt message not just under a public key, but additionally under identifier of cipher texts known as class. The cipher texts are again classified in to distinct classes. The key owner holds master secret key which can be used to extract secret keys for distinct classes. The extracted keys can be aggregated  that is aggregate key which is as compact as a single secret key for single class, but combines the strength of many such keys i.e. decryption strength of any subset of cipher text classes. And the data files outside that distinct class remains confidential. This scheme allows a content provider to share their information in a private and selective way, with fixed and small cipher text expansion, by distributing to each and every authorized user a single, compact, aggregate key.

In KAC, user can encrypt message not just solely under a public key, but additionally under identifier of cipher texts known as class. Cryptography helps the data owner to share the information in secure way; cryptography is the discipline and study of hiding information. It is the facility given by science to translate simple and plain intelligible information into an unintelligible information (i.e. encryption) and again retranslating that message into its initial means original form (i.e. decryption).It gives confidentiality, integrity, and accuracy. A cryptographic solution, with proven security relied on variety of theoretic assumption is more suited data sharing is essential functionality of cloud storage. Some cryptographic approaches can be determined in section 2. Detailed study of these approaches helps to introduce a new public key cryptosystem i.e. Key aggregate cryptosystem.

## 2. Literature Survey

In this section we studied some different approaches, which are the feasible solutions on sharing in secure cloud storage, and we compare this with our fundamental KAC scheme.

### 2.1. Key assignment scheme for a predefined hierarchy

Key assignment scheme intends to reduce the rate of storing and managing secret keys for generic cryptographic use. Key assignment scheme is like non-constant decryption key size, symmetric or public key for a predefined hierarchy is used. Only hash functions are used for a node to derive a descendant's key from its own key.  Atallah [2] addresses the hassle of key management for such hierarchies and proposes the solution with The space complexity of the public information is similar as that of storing hierarchy and is asymptotically optimal; the private information at a node consists of a single key related with that node and updates are managed regionally in the hierarchy; this scheme is provably secure to face collusion; and every node can derive the key of any of its descendant with a number of symmetric-key operations bounded by the length of the path between the nodes.  Tzeng [3] addresses the hassle in key assignment scheme is that to assign cryptographic keys to a set of partially ordered classes so that the cryptographic key of higher category can be used to derive the cryptographic keys of a lower class. It means if hacker receives the key of root node then he or she can definitely receive the keys of leaf nodes. So he proposes the solution for this hassle by introducing a time bound cryptographic key assignment scheme in which cryptographic keys of class are distinct for each time period, each user holds some secret parameters whose number is independent of variety of classes in the hierarchy and total time bound.

These hierarchical approaches can partly resolve the hassle if one intends to share all information (documents) under a certain branch in the hierarchy.

### 2.2 Symmetric key encryption with compact key

The identical hassle of supporting flexible hierarchy in decryption power delegation is observed in case of symmetric-key setting. Benaloh [4] introduced an encryption approach which is initially proposed for concisely transmitting large range of keys in broadcast scenario. It makes use of Symmetric-key encryption with Compact Key. This paper construct an environment friendly system that permits patients both to share partial access rights with others, and to perform searches over their records. They formalize the necessities of a Patient Controlled Encryption approach, and provide a number of instances, primarily based on current cryptographic primitives and protocols, each achieving a distinct set of properties. However, it is designed for the symmetric-key setting instead. The encryptor must have the corresponding secret keys to encrypt information, which is not appropriate for many applications. Since their approach is used to generate a secret value instead of a pair of public/secret keys, it is doubtful how to follow this notion for public-key encryption scheme.

### 2.3. IBE with compact key

Boneh [5] proposed Identity Based Encryption is a kind of public-key encryption in which the public-key of a user can be place as an identity-string of the user (e.g., an email address). There is a private key generator (PKG) who is a trusted party in IBE which holds a master-secret key and broadcasts a secret key to each and every user regarding with their identity. The encryptor can take the public parameter and a user identity to encrypt a message. The recipient can decrypt this cipher text by using his secret key. Guo [6] proposed Multi identity single key decryption (MISKD) in which a private decryption key can design more than one public key (identities) e.g. e-mail address, cell phone number, IP addresses; a single private key can be used to decrypt more than one cipher text encrypted with distinct public keys related to the private key. In this approach, key aggregation is restricted in the sense that all keys to be aggregated have to come from distinct "identity divisions". While there are an exponential number of identities and accordingly secret keys, only of them a polynomial number of secret keys can be aggregated. This significantly increases the expenses of storing and transmitting cipher texts, which is impractical in many conditions such as shared cloud storage. So we can say that this approach is very expensive and impractical.

## 2.4. Attribute based encryption

Sensitive information stored and shared on cloud by cloud server; so cloud user prefers to encrypt this sensitive information before importing on cloud. One downside of encrypting information is that it can be selectively shared only at a coarse-grained level(unprocessed/common) i.e., giving any other party your private key (secret key) which is no longer desirable. Goyal [7] proposes Attribute based encryption for fine grained (processed/weak/selective) access control of encrypted data. This approach permits each cipher text to be related with an attribute. Master secret key holder can extract a secret key for a policy of these attributes; so that cipher text can be decrypted by using this key e.g. the secret key for the information (2V3V6V8). Then we can decrypt information as using cipher text 2, 3, 6and 8.

Table 1. Summary on Literature Review

| **Reffered paper** | **Description** | **Conclusion** |
|---|---|---|
| Dynamic and Efficient Key Management for Access Hierarchies[2] | In this defined a key allocation mechanism that implements such an access graph, that is, an assignment of keys to users and objects where a user | The number of keys increases with the number of branches. It is unlikely to come up with a hierarchy that can save the number of total keys to be granted. |

| | | |
|---|---|---|
| | can access an object if he has a key for that object. | |
| Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records[4] | In this paper build an efficient system that allows patients both to share partial access rights with others, and to perform searches over their records. | The encryptor needs to get the secret keys to encrypt data which is not suitable for many applications. It is unclear how to apply this method for public key encryption scheme. |
| Identity-Based Encryption from the Weil Pairing[5] | Identity-based encryption (IBE) is a type of public-key encryption in which the public-key of a user can be set as an identity-string of the user (e.g., an email address). | Different secret keys have to be generated for the same identities, and as a result it is more difficult to apply leakage resilient techniques. |
| Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data[7] | In this scheme multiple attribute authorities monitor different sets of attributes and issue corresponding decryption keys to user and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. | The size of the key often increases with the number of attributes it encompasses or the ciphertext-size is not constant. |

## 3. Proposed System

In KAC, users encrypt a message not just under a public key, but additionally under an identifier of cipher text known as class. That means the cipher texts are again classified into distinct classes. The key owner holds a master-secret key, which can be used to extract secret keys for distinct classes. 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 strength for any subset of cipher text classes. With our solution, cloud user can simply or directly send retriever a single aggregate key through a secure e-mail. Retriever can download the encrypted photos or information from user’s Dropbox area and then use this aggregate key to decrypt these encrypted photos (information). The scenario is shown in Figure 1.

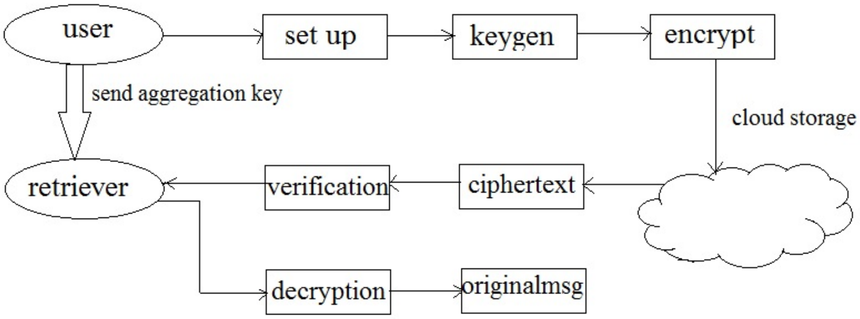

Figure 1. System Architecture

A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows.

*1. Setup Phase:* It is performed by the data owner to setup an account on an entrusted server. On entering an entering inputs a security level parameter and the number of cipher text classes n (i.e., class index must be an integer bounded by 1 and n), it gives outputs the public system parameter param, which is ignored by the input of the other algorithms for briefness.

*2. KeyGen Phase*: It is performed by the data owner to generate at random a public/master-secret key pair (pk, msk).

*3. Encrypt Phase (pk, i, m)*: It is performed by every user who desires to encrypt information. On entering inputs a public-key pk, an index i denoting the ciphertext class, and a message m, it gives output a ciphertext C.

*4. Extract (msk, S)*: It is performed by the data owner for delegating the decrypting strength for a certain or absolute set of ciphertext classes to a delegate. On entering inputs the master secret key msk and a set S of indices corresponding to distinct classes, it gives output the aggregate key for set S denoted by KS.

*5. Decrypt (KS, S, I, C)*: It is performed by a delegate who obtained an aggregate key KS generated by Extract. On entering inputs KS, the set S, an index i denoting the ciphertext class the ciphertext C belongs to, and C, it gives output the decrypted end result m(original message) if i belongs to S .

**4. Scope**

1. With the developments in Cloud computing, there is now a developing center of attention on enforcing data sharing capabilities in the Cloud. It is additionally used as a core technology at the back of many online services for personal purposes.
2. On cloud each person can share information as much they want to i.e. only chosen or selected content can be shared.
3. Cryptography helps the data owner to share the information in secure way. So user encrypts information and import on server.
4. Key aggregate cryptosystem approach used for data sharing in cloud storage is more secure.
5. This approach is beneficial for securely, efficiently, and flexibly share information with others in cloud storage.
6. It is an efficient public-key encryption scheme which supports flexible delegation.

## 5. Conclusion

In this survey we studied distinct cryptographic approaches for data sharing security. One trivial solution to achieve secure data sharing in the cloud is for the data owner to encrypt his information earlier than storing into the Cloud, and therefore the data remain information-theoretically secure against the Cloud provider and different malicious users. With extra mathematical tools, cryptographic schemes are getting extra versatile and often involve more than one key for a single application. Thus it considers how to compress secret keys in public-key cryptosystems which support delegation of secret keys for distinct cipher text classes in cloud storage. Our approach is more extensible (flexible) than hierarchical key assignment.

## References

[1] Cheng-Kang Chu et.al, “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, *IEEE Transactions on Parallel and Distributed Systems*. Volume: 25, Issue: 2. Year: 2014.

[2] 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.

[3] W.-G. Tzeng, “A Time-Bound Cryptographic Key Assignment Scheme for Access Control in a Hierarchy,” *IEEE Transactions on Knowledge and Data Engineering* (TKDE), vol.14,no.1,pp.182–188, 2002.

[4] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” in Proceedings of ACM Workshop on Cloud Computing (CCSW ’09). ACM, 2009, pp. 103–114

[5] D. Bonehand M.K. Franklin, “Identity-Based Encryption from the Weil Pairing,” in Proceedings of Advances in Cryptology - CRYPTO ’01, ser. LNCS, vol. 2139. Springer, 2001, pp. 213–229

[6] F. Guo, Y. Mu, Z. Chen, and L. Xu, “Multi-Identity Single-Key Decryption without Random Oracles,” *in Proceedings of Information Security and Cryptology* (Inscrypt ’07), ser. LNCS, vol. 4990. Springer, 2007, pp. 384–398.

[7] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data,” *in Proceedings of the 13th ACM Conference on Computer and Communications Security* (CCS ’06). ACM, 2006, pp. 89–98.