ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 1 , January 2017

A Literature Survey on Revocation Storage System in cloud for Secured Data Sharing

Ramya , K Pramilarani

P.G. Student, Department of Computer Science, New Horizon College Of Engineering, Bangalore, Karnataka, India
Senior Assistant Professor, Department of Computer Science, New Horizon College Of Engineering, Bangalore, Karnataka ,India

ABSTRACT: Cloud computing has given the users the accessibility to deploy number of files to the centralized cloud and share those with number of users. Cloud computing is fast growing technology that enables the users to store and access their data remotely. The flexibility of cloud computing always comes with the hurdles of security concerns. While accessing the data from cloud, different users may have relationship among them depending on some attributes, and thus sharing of data along with user privacy and data security becomes important to get effective results. Most of the research has been done to secure the data authentication so that user's don't lose their private data stored on public cloud. The system proposes aggregate key for file in groups and searchable encryption. In this paper various research and challenges in this area are discussed in detail. It will definitely help the cloud users to understand the topic and researchers to develop a method to overcome these challenges.

KEYWORDS :Cloud Computing, Revocation System, Security, Privacy.

I. INTRODUCTION

Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. There is currently a push for IT organizations to increase their data sharing efforts. In enterprise settings, demand for data outsourcing is increased today. Data outsourcing should be assists in the strategic management of corporate data. This scheme is also used as a core technology behind many on line services. These on line services used for online application. Currently this scheme was easy to apply for free accounts for mail, photograph album, sharing of file with storage size more than 25GB. Together by using the current wireless technology, cloud users can access almost all of their files, directories and emails by a mobile phone in any corner of the world.

Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group. One trivial solution to achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the

Cloud provider and other malicious users. When the data owner wants to share his data to a group, he sends the key used for data encryption to each member of the group. Any member of the group can then get the encrypted data from the Cloud and decrypt the data using the key and hence does not require the intervention of the data owner.
The Cloud Security Alliance has summarized five essential characteristics that spotlight the relation to, and differences from, traditional computing paradigm .A cloud user may unilaterally acquire computing resources, like the server access and cloud storage, as on demand, without collaborating with the cloud provider. Cloud services are conveyed to users through Internet using standard mechanism that allow users to access the services using heterogeneous thin or thick client tools (e.g., PCs, mobile phones, and PDAs). The cloud providers pool the computing resources to serve the

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 1 , January 2017

multiple users through multitenant model, in which resources (physical or virtual) dynamically assigned or reassigned according to users demand. Some resources are storage, processing, memory, network bandwidth, and virtual machines. Users may increase the capabilities of services rapidly and elastically to quickly scale out or rapidly released the services capabilities to quickly scale in. Users have the ability to purchase unlimited capabilities of services in any quantity at any time. The cloud services purchased by users are quantified and measured. For both the provider and customers, resource usage will be monitored, controlled, metered, and reported.

II. PROBLEM FORMULATION

In public cloud, the user's data is stored in distributed data centers; so the control of data centers is not with single authority. Moreover the cloud providers are also able to access the data themselves if users stored the data in unencrypted format. Hence there is a need to design a mechanism to intensify the data security by using some cryptographic techniques to encrypt user's data before uploading to public cloud to prevent the misuse together by implementing hybrid cloud architecture by virtue of which the on one end the privacy and security can be achieved from private cloud and on the other end mass data storage feature of public clouds can be achieved.

The hybrid cloud architecture should develop from private cloud and public cloud, where the user's sensitive data such as roles structure, security related data will be stored on private cloud while the actual data will be stored on public cloud in encrypted form and later all extended ABAC policies are to be apply on it to make more secure. In this hypothetical architecture, the authenticated users who have the access to particular data can interact with the public cloud only for that data with dynamically key provisioning only for limited time; there is no access for public users to access the private cloud where the sensitive data is stored, which greatly weaken the attack surface for the private cloud. Using the data sharing from public cloud also enhance the productivity of organization, But security and user privacy is the main concern while sharing the user's data. This architecture not only will eliminate the organization's concerns about risks of leaking sensitive information, but will also takes full advantage of public cloud's power to securely store large volume of data with secure sharing of that data with enhanced privacy.

III. SYSTEM MODEL AND FRAMEWORK

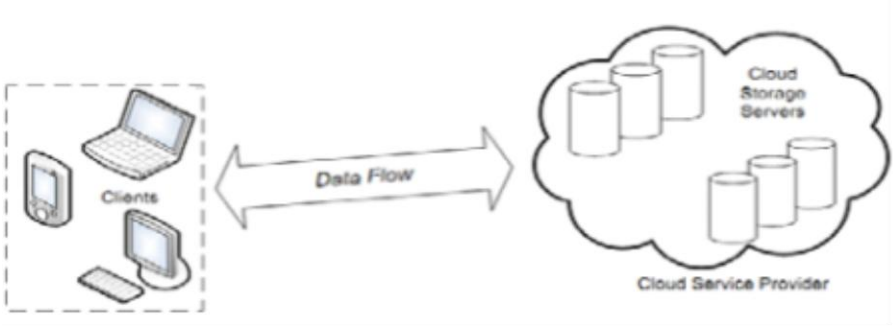

Fig. 1 Cloud data storage architecture

The cloud data storage architecture used in this work is based on the model proposed by Cong Wang, as shown in Fig - 1. The different entities are the Client and Cloud Storage Server. Client: The end user who has large amount of data to store in the cloud and relies on the service provider for maintenance. This can either be an individual user or a large organization. Cloud Storage Server: An entity, which is managed by a Cloud Service Provider, has significant storage space and computation resource to maintain client's data.

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 1 , January 2017

IV. DIFFERENT APPROACHES

A. ABAC

The proposed model of ABAC addresses the security features for data access, privacy preserving and secure sharing of data in cloud environment and use the hybrid cloud storage architecture.In the proposed model, the administrator only can create users and manage their attributes to access the data. There are restrictions on user per role, data usage, changing roles all are managed by administrator. In this design the key management is introduced according to the bank key management system. The key will be divided into two parts and these will be placed on different places. The users want to access the data never get these keys, they only get the authorization key which will be created dynamically for a particular time. The cloud provider or other user can never get the access to decryption keys. After the completion of design of this architecture this will be implemented on Microsoft Windows Azure, then only we can check the whole model against the access control based on attributes. The unauthorized users can't create new user id due to security measures. All this is shown in Figure 2.

Fig. 2 Secure Data Sharing in Cloud Computing using Hybrid cloud

B. KASE

Our system contains four different phases. First define a general framework of key aggregate searchable encryption (KASE) composed of seven polynomial algorithms for security parameter setup, key generation, encryption, key extraction, trapdoor generation, trapdoor adjustment, and trapdoor testing. We then describe both functional and security requirements for designing a valid KASE scheme. Then instantiate the KASE framework by designing a Concrete KASE scheme. After providing detailed constructions for the seven algorithms, analyze the efficiency of the scheme, and establish its security through detailed analysis. Discuss of various practical issues in building an actual group data sharing system based on the proposed KASE scheme, and evaluate its performance. The evaluation confirms our system can meet the performance requirements of practical applications. Both analysis and evaluation

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 1 , January 2017

results confirm that our work can provide an effective solution to building practical data sharing system based on public cloud storage.

C. KAC

Issues such as aggregation of key, constant size cipher text, secure storage of them have remained the most important challenges. For improving the constraints of the above techniques, we propose a new scheme Key - Aggregation cryptosystem (KAC). The KAC is an efficient and secured public-key cryptosystem for data sharing in the cloud storage. It produces constant-size cipher texts and any Number of secret keys can be aggregated.

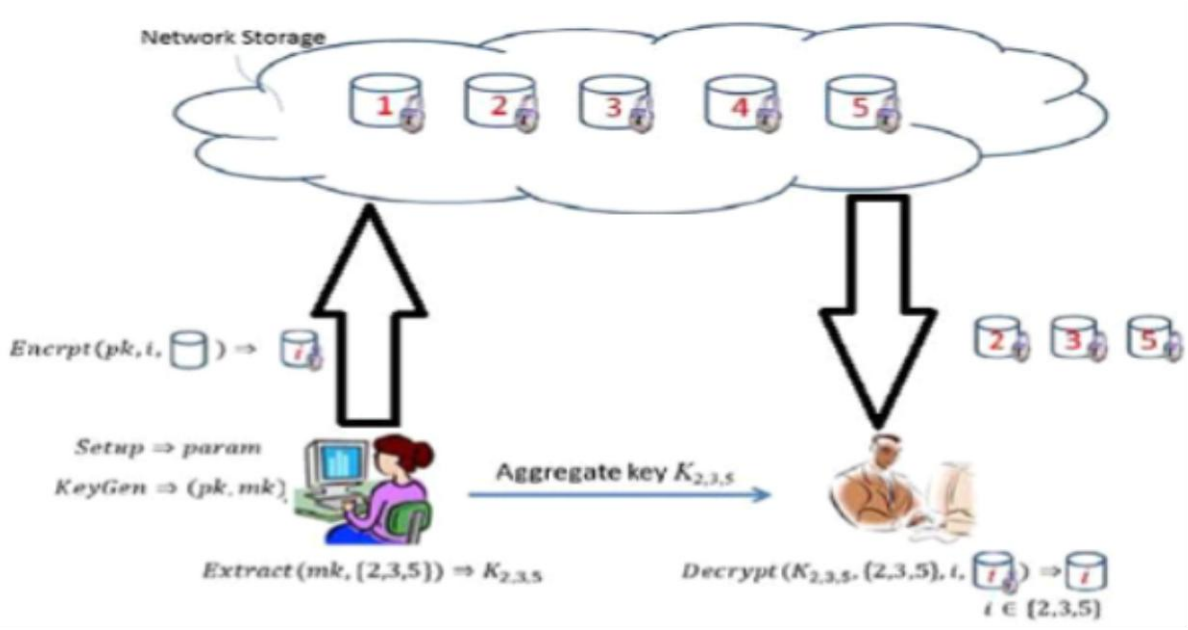

Fig. 3 KAC for data sharing in cloud storage.

In KAC, referring to Fig. 3 from, users encrypt the data using a public key under an identifier of cipher text known as class. These cipher texts are actually categorized into separate classes. The owner of the key holds a master secret called master secret key, which is used to obtain storage required to store these secret keys. There is no fuss of dealing with a hierarchy of delegation classes, more flexible than hierarchical approach. Regardless of the type among power set of classes, an aggregate key of constant size can be obtained. This will in turn reduce the secure storage and the overhead on the network.

D. MULTI-AUTHORITY ATTRIBUTE BASED ENCRYPTION SCHEME

In this scheme, every cipher text is associated with an attribute and secret key can be extracted by the Master -secret key holder to decrypt the cipher text if, its associated attributes abide by the policy. In each earlier ABE schemes, the user has to go to trusted party for proving his identity before getting a secret key which allows him to decrypt messages. Thus an efficient multi-authority ABE scheme was introduced in which the user's secret key is no longer authorized by a single center authority. It is authorized separately by cooperative and independent authorities. But the problem with this scheme is, there is no focus on the compactness of secret keys. There is linear increase in the number of keys with the number of attributes it contain. In ABE scheme, attribute plays a very major role. Attributes have been exploited to obtain a public key for encryption data and used to control user's access.

ISSN: 2350-0328

International Journal of Advanced Research in Science, Engineering and Technology

Vol. 4, Issue 1 , January 2017

E. REVOCATION SYSTEM

There exist a cloud which is available to the user and there exist a data owner. The basic ideology is that a user is provided a security key by the owner, the owner makes sure that the user can access only that data which is user liable to see making sure that he can't access other data uploaded. Now in this we are making sure that the data which is being uploaded should be safe and also taking care of the duplicate data. Supposed if a user has already uploaded ABC file and if user B tries to upload the same file then hash key of files are checked and as the hash key of the files are the same the user file is returned without the hassle of keeping duplicate file. Also it might happen that your id and password can be used other than you, so whenever you try to log in you are alerted either on your registered email id or the phone number. Example: Users are provided with private key. The private key of the user explain user access control. In this a plain file is encrypted using cipher algorithm. When encrypting the message, the sender chooses an access structure on attributes, and encrypts the message under the access structure via encrypting with the corresponding public key components. Users are able to decrypt a cipher text if and only if their attributes satisfy the cipher text access structure.

Fig 4. Basic Architecture Showing Encryption and Decryption Process

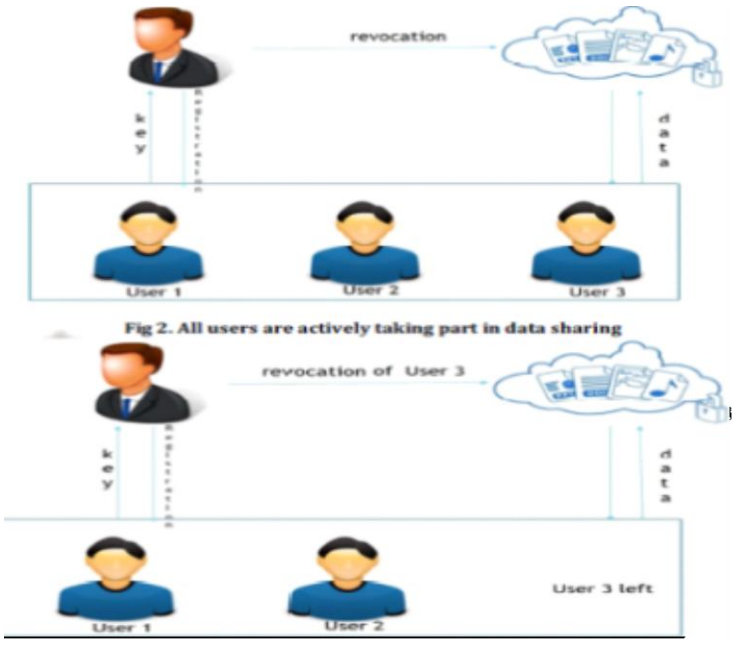

Fig 5. User 3 was revoked as user was no longer part of the organization/group/network

ISSN: 2350-0328
International Journal of Advanced Research in Science, Engineering and Technology
Vol. 4, Issue 1 , January 2017

Application of this Project is as follows:
1. Protection from eavesdropping.
2. Secret ballot internet voting.
3. Detection of misbehavior.

V. CONCLUSION

Cloud computing is a growing term in the field of computer science which is done over the internet. This increases the ease of access through any kind of internet connection. In this paper, the issues related to cloud security are being discussed and efficient way of user revocation has been done. The Proposed Idea of using Algorithms such as Huffman, RSA, MD5, KN Sharing and SHA1 would help us create cryptography which would help in creating a secure cloud server. In this way, it would provide load balancing over cloud.In this techniques the privacy is managed by the owner of the data itself and the secure sharing of data is provided. It is believed that the proposed model has the potential to be helpful in commercial situations as it uses the practical access policies based on user's attributes in a flexible manner and provides secure data storage and sharing in the cloud environment.

REFERENCES

[1] Atul Adya, William J Bolosky, Miguel Castro, Gerald Cermak, Ronnie Chaiken, John R Douceur, Jon Howell, Jacob R Lorch, Marvinv Theimer, and Roger P Wattenhofer. Farsite: Federated, available, and reliable storage for an incompletely trusted environment. ACM SIGOPS Operating Systems Review, 36(SI):1–14, 2002.
[2] Mihir Bellare, Alexandra Boldyreva, and Adam ONeill. Deterministic and efficiently searchable encryption. In Advances in Cryptology-CRYPTO 2007. Springer, 2007.
[3] Mihir Bellare, Sriram Keelveedhi, and Thomas Ristenpart. Dupless: Server-aided encryption for deduplicated storage. 2013.
[4] Mihir Bellare, Sriram Keelveedhi, and Thomas Ristenpart. Message-locked encryption and secure deduplication. In Advances in Cryptology–EUROCRYPT 2013. Springer, 2013.
[5] Kevin D. Bowers, Ari Juels, and Alina Oprea. Hail: a high-availability and integrity layer for cloud storage. In Proceedings of the 16th ACM conference on Computer and communications security, CCS '09, New York, NY, USA, 2009. ACM.
[6]M. Bellare and A. Palacio. Gq and schnorr identification schemes: Proofs of security against impersonation under active and concur- rent attacks. In CRYPTO, 2002.
[7] S. Bugiel, S. Nurnberger, A. Sadeghi, and T. Schneider. Twin clouds: An architecture for secure cloudcomputing. In Workshop on Cryptography and Security in Clouds (WCSC 2011), 2011.
[8]Pooja S Dodamani, Pradeep Nazareth, "A Survey on Hybrid Cloud with De-Duplication", International Journal of Innovative Research in Computer and Communication Engineering, December 2014.
[9] Boga Venkatesh, Anamika Sharma, Gaurav Desai, Dadaram Jadhav, "Secure Authorised Deduplication by Using Hybrid Cloud Approach", November 2014.W. K. Ng, Y. Wen, and H. Zhu. Private data deduplication protocols in cloud storage. In S. Ossowski and P. Lecca, editors, Proceedings of the 27th Annual ACM Symposium on Applied Computing. ACM, 2012.
[10] R. D. Pietro and A. Sorniotti. Boosting efficiency and security in proof of ownership for deduplication. In H. Y. Youm and Y. Won, editors, ACM Symposium on Information, Computer and Communications Security. ACM, 2012.
[11]Pasquale Puzio Refik Molva Melek Sergio Onen L. ClouDedup: Secure Deduplication with Encrypted Data for cloud storage. In Proceeding in 2013 IEEE International Conference on Cloud Computing Technology and Science
[12] I. Clarke, O. Sandberg, B.Wiley, and Hong T.W. Freenet: A distributed anonymous information storage and retrieval system.