ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

A Secured Data Sharing in Cloud Computing Using Key Based Agreement with Fault Tolerance

Komal C. Khandale, Ms. Kanchan Varpe,

Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India

Assistant Professor, Department of Computer Engineering, RMD Sinhgad School of Engineering, Pune, India

ABSTRACT: In Cloud Computing, sharing of data helps number of participants to freely share different group data,which helps to improve the efficiency of working in cooperative manner. To ensure security constraints of data sharing within the same group and also the outsourced data in group is challenging task. To solve this problem Symmetric Balanced Incomplete Block Design (SBIBD) is used for key security so, un- authorized user cant access the data from different group. The common conference key K is generated using SBBID scheme for multiple participants. The algorithms used for this system are DES and blowfish algorithm.The key protocols have played vital role in securing groups in cloud computing. As result of storing data from dynamic group and data are divided into blocks the system performance can be greatly improved.

KEYWORDS: Fault Tolerance, Fault Detection, Cloud Com-puting.

I. INTRODUCTION

In cloud computing, to store and share data securely,there are multiple cloud service providers offers various cloud services. i.e. Amazon Simple Storage Service (S3).

Cloud providers offers large storage space with abstraction for simplicity of the user. The membership in the cloud is frequently changing and because of this, security-preserving causes challenging issues in the cloud. Company employees in the same department can share and store files in the cloud.

However, there is a significant risk to the confidentiality of those stored files. For security purpose, it is necessary to encrypt data before uploading files in the cloud.These schemes do not support for secure data sharing for dynamic groups. Some systems have used techniques for securing data sharing called cryptography among multiple group members in an untrustworthy cloud, but these systems additionally experiences cost overheads and security risks. These systems are not supportive to dynamic group concept. In some systems, different combined approaches of key policy attribute based encryption, lazy re-encryption and proxy re-encryption are used to achieve efficient data access control without disturbing the content of data. Some system uses the cipher text-policy and the group signatures attribute based encryption techniques. The efficient user revocation is not supported, so the security feature can be violated. The attribute-based techniques can be used by multi-owner schemes. the security issues can beintroduced if any owner revokes from an application.

Therefore, this approach is not so suitable for data sharing. Many approaches are there in public cloud based on privacy-preserving policies. Collusion attack is one of the security concern for these approaches. For dynamic groups the existing approach supports secure data sharing scheme in a single cloud. The attribute-based techniques are used for such secure data sharing schemes. Secure user revocation is not supported. The role-based techniques are used in proposed systems for secure data sharing and key distribution for dynamic groups by taking the use of multiple clouds. In multiple clouds, storage space is partitioned into multiple groups. The files are first partitioned and then can be stored in multiple groups with two level of encryption. The system supports secure user revocation and anti-collision

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

attack. Our system can overcome the issue of cost overhead. Our approach deals with the space overhead by using the term, virtual storage server. Therefore, the time and space constraints are considered in the system. If the space of storage became full then according to the time and space constraint, stored data is automatically transferred to the virtual server. The aim of this system is to propose a scheme that provides the security, data sharing in dynamic group. , if hacker hack any file of owner the tolerance level increases and hence the the fault tolerance and fault detection of user side can be calculated . The system ensures, data Security in Cloud, mechanism to store data in Cloud, mechanism to fetch data from cloud, access control lists with respects to roles on Data, performance improvement with using lightweight and flexible encryption mechanism to secure data from cloud providers. In cloud computing sharing of group data can be well supported by block design based key agreement protocol as mentioned in our system. For group data sharing the structure of a (v,k+1,1) design can be used and multiple participants can use the common conferences key for such participants are derived. To make a protocol more practical and more secure the fault tolerance property is introduced in our system.

II. REVIEW OF LITERATURE

In [1], Hybrid cloud is most popular cloud architecture used in large companies that outsource the data to the public cloud. However, some serious security concerns, such as data confidentiality and access policy regularity to the data stored in public cloud are involved in such public cloud data out-sourcing. To address this issue, this system designed a hybrid
cloud architecture that supports data sharing in very secure and efficient manner, even with resource-limited devices. An attribute-based encryption technique is used, which provides flexible access control in the cloud and privacy-preserving in data utilization. This scheme is able to resist some attacks between private cloud and data user by employing anonymous key agreement but in this approach only AES algorithms is applied on the data. In [2], To secure an electronic communi-cation the fundamental building blocks are authentication and key establishment. The protocols and key establishment should be essentialy proper in their specific purpose. This paper provided key establishment protocol in the asymmetric (public key) manner that is based on MTI (Matsumoto, Takashima and Imai)-which is two pass key agreement protocol and is much efficient. This protocol is strong enough against most of the potential attacks like secrecy, small subgroup attack, unknown key-share attack, key compromise impersonation with some what low complexity. It serves the authentication process between two parties before exchanging the session keys. but, data integrity cannot be performed and user know which parties share such keys.

In [3], As we know that now a days the demand of applications based on cloud servers and even to store a data securely on a cloud server has very high demand. If user loses the local control on data there is urgent need from user side to check weather his data is secured. So the research on design of a protocol related to the secure data storage on cloud is tremendously increasing day by day. This paper, introduces an efficient public auditing protocol with global and sampling block less verification and batch auditing, but using this scheme only structured data can be stored on the dynamic group.

In[4], The role-based access control (RBAC) schemes have been introduced to provide protection of the privacy of data stored in the cloud, also to ensure that data can be accessed by only those to whom the access policies allowed.To provide security for data stored in cloud storage system, This system introduces trust models to improve the security that use crypto-graphic RBAC schemes. Cryptography is used only for RBAC schemes. In [5] Users generally avoid to submit negative feedback about the systems due to the fear of similarity from the recipient user. for such cases, a privacy preserving reputation protocol provides protection to the users by hid-ing their feedback and providing only the reputation score. The system presents a privacy preserving reputation protocol for the malicious adversarial model. The protocol does not require trusted third parties,centralized entities or specialized platforms, such as trusted hardware and anonymous networks. User get the request data and user also can give the negative feedback. In [6], To ensure the truthfulness of data in storage outsourcing Waters Provable Data Possession (PDP) term is used as performance parameter. to support the scalability of service and data migration in this paper, the author focuses on the construction of an efficient PDP scheme for distributed data storage. For which they consider the continuation of multiple data service providers to store and maintain the clients data in

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

cooperative manner. In [7] To ensure the integrity of data in outsourcing storeroom service the term waters provable data possession is used. The system experiments a demonstration with verification of their scheme involving that there must a small and constant amount of overhead. Further, which minimizes communication complication verification scheme and data is stored on constant way. In [8], At present, there is no strong confirmation that multiple copies of the data are actually stored in such storage systems. The system address this shortcoming through multiple-replica attestable data possession (MR-PDP) term. Using MR-PDP to lay up t replicas is computationally much more resourceful than using a single-replica PDP format to store t separate, dissimilar files (e.g.,each file encrypting separately prior to storing it). Gen-erating further replicas on demand is another benefit of MR-PDP at little expense, when some of the accessible replicas fail. Using cryptologic multi linear maps are terribly helpful in cryptography however their construction is one among the long-standing open drawback. Recently, 2 candidates of the cryptologic multi linear map are planned from plan of the somewhat holomorphic secret writing theme[9]. They have a tendency to give a summary of the planned 2 candidates for the multi linear map and to compare their structures with the underlying somewhat holomorphic encryptions[10].

III. SYSTEM ARCHITECTURE AND SYSTEM OVERVIEW

The system consists of four modules owner, user, admin and cloud service provider. User enters in application by registration and log in. Then admin activate the user and give the specific token. After entering the token user can login successfully. After login user search the owner file and cloud services provider give the key in format of KASE. If user enter the wrong key (KASE) then level of fault tolerances is increases and if level goes up to 3 then owner knows the user information and if owner block that user then after words user can be blocked from particular owner or system so the user will not able to get file of particular owner. Therefore, system ensures security constraints.

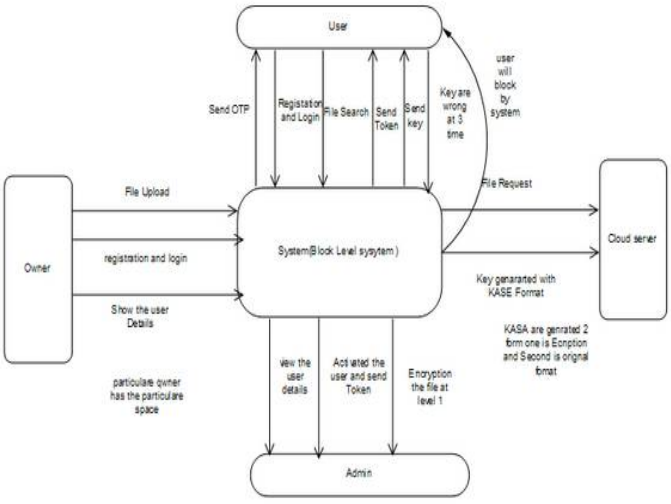

Fig. 1. system architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

Mathematical model :

Let,

Input : Data File, Fault Tolerances Values. let,

S=DO, U, A, C, DG S1, D, FT

Where Do, U, A, C are the element of the Set Do=Data Owner

U=user
A=Admin

C=Cloud Server provider S1=Search File.

G=Get Key from user. DG= Dynamic Group.
D=Download the File using key FT=Fault Tolerances.

Do Upload the Data in DG.

Admin activated the user and Encryption at level FT value are decided by the Data Owner

FT=k1∩k2

If both entered keys are correct then only file can be accessible.

Algorithms used:

1)Blowfish Algorithm 2)DES Algorithm

Blowfish Algorithm steps:

1. Initialize first the P-array and then the four S-boxes, in order, with a fixed string. This string consists of the hexadecimal digits of pi (less the initial 3): P1 = 0x243f6a88, P2 = 0x85a308d3, P3 = 0x13198a2e, P4 = 0x03707344, etc.

2. XOR P1 with the first 32 bits of the key, XOR P2 with the second 32-bits of the key, and so on for all bits of the key (possibly up to P14). Repeatedly cycle through the key bits until the entire P-array has been XORed with key bits. (For every short key, there is at least one equivalent longer key; for example, if A is a 64-bit key, then AA, AAA, etc., are equivalent keys.)

3. Encrypt the all-zero string with the Blowfish algorithm, using the data file described in steps (1) and (2).
4. Replace P1 and P2 with the output of step (3).

5. Encrypt the output of step (3) using the Blowfish algorithm with the modified data
6. Replace P3 and P4 with the output of step (5).

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

IV. SYSTEM ANALYSIS

Our system is be able to provide fault tolerance level for particular data user.The system provide multiuser cloud security with the use of fault tolerance value. Using fault tolerance factor particular user can be blocked and hence security can be maintained.Two level of encryption can be given to data for security. To achieve this we used blowfish algorithm along with DES in our system.

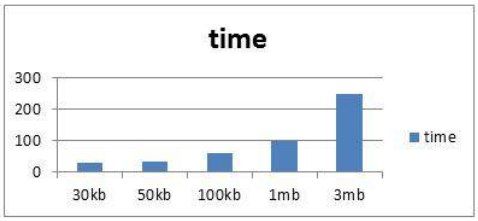

Fig. 2. Comparative graph of Uploading File

Number	File Size	X –axis	Y- axis
1	30	0.30	30 KB
2	50	30	50KB
3	100	70	100 KB
4	1 MB	100	1 MB
5	3 MB	230	3MB

Fig. 3. Comparative Table of Uploading File

V. CONCLUSION AND FUTURE SCOPE

Group data sharing in cloud computing has opened many doors in web technology and network security. Since cloud technology brought more popularity,it involve some security issues also. Therefore using the cloud services requires data confidentiality.With the help of our proposed technique of conference key agreement protocol performance can be greatly improved. Data which is outsourced by the data owner is encrypted by common conference key and can be protected from attackers. the term fault tolerance is used to ensure data confidentiality. System provides two levels of security to the data. If particular user is entering the wrong keys than expected ones then that user will be blocked by the system and hence data is handled securely.

In our future work, In advanced with this system uploading Video and Audio File can be done.We would like to extend our protocol to provide more properties to make it applicable for a variety of environments.

REFERENCES

[1] A Secure and Efficient Data Sharing Framework with Delegated Ca-pabilities in Hybrid Cloud Information Forensics and Security IEEE Transactions on, vol. 10, no. 11, pp. 23812395, 2015.
[2] n Efficient Protocol For Authenticated Key Agreement L. Law, A. Menezes, M. Qu, J. Solinas, and S. Vanstone
[3] An Efficient Public Auditing Protocol with Novel Dynamic Structure for Cloud Data Mohamed Nabeel, Student Member, I Ning Shang, Elisa Bertino 2013 IEEE
[4] Trust Enhanced Cryptographic Role-based Access Control for Secure Cloud Data Storage Information Forensics and Security IEEE Transac-tions on, vol. 10, no. 11, pp. 23812395, 2015.
[5] A Decentralized Privacy Preserving Reputation Protocol for the Malicious Adversarial Model O. Hasan, L. Brunie, E. Bertino, and N. Shang.
[6] D. Boneh, C. Gentry, and B. Waters, Collusion resistant broadcast encryption with short ciphertexts and private keys, in Proc. Adv. Cryptol ., 2005, vol. 3621, pp. 258275.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 6, June 2018

[7] D. Boneh, A. Sahai, and B. Waters, Fully collusion resistant traitor tracing with short ciphertexts and private keys, in Proc. 25th Int. Conf. Theory Appl. Cryptographic Tech., 2006, vol. 4004, pp. 573592.
[8] D. Boneh and M. Naor, Traitor tracing with constant size Cipher text, in Proc. 15th ACM Conf. Comput. Comm. Security, 2008, pp. 501510.
[9] D. Boneh and A. Silverberg, Applications of multilinear forms to cryp-tography, Contemporary Math., vol. 324, pp. 7190, 2003.
[10] C. Blundo, L. A. Mattos, and D. R. Stinson, Generalized Beimel- Chor schemes for broadcast encryption and interactive key distribution, Theor. Comp. Sci., vol. 200, no. 12, pp. 313334, 1998.