ISSN 2395-1621

A Secured Data Sharing In Cloud Computing Using Key Based Agreement With Fault Tolerance

#1Tale Rohini Arun, #2Prof.V.N.Dhawas

1talerohini@gmail.com,
2vnd.sit@sinhgad.edu

#12Department of Computer Engineering

Sinhgad Institute of Technology, Lonavala

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.

Index Terms—Symmetric Balanced Incomplete Block Design (SBIBD), Fault Tolerance, Fault Detection, Cloud Computing

ARTICLE INFO

Article History

Received: 8th July 2019

Received in revised form :

8th May 2019

Accepted: 12th July 2019

Published online :

13th July 2019

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 be introduced 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 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 LITERAT URE

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 cpgcon/sysdia.jpg 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 hiding 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 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). Generating 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

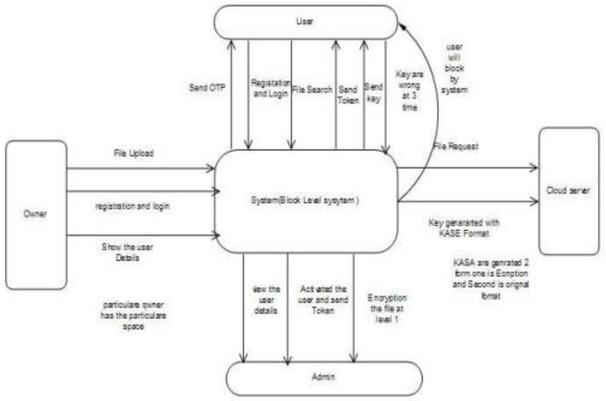
User
Send OTP
Registation and Login
File Search
Send Token
Send key
Key are wrong at 3 time
user will block by system
Owner
File Upload
registration and login
Show the user Details
particulare qwner has the particulare space
System(Block Level sysytem)
File Request
Cloud server
Key genarated with KASE Format
KASA are genrated 2 form one is Ecnption and Second is orignal fomat
View the user details
Activated the user and send Token
Encryption the file at level 1
Admin

Fig. 1. system architecture

Software Requirements Speciation :The operating system used can be window 7,8,10. The programming language used is java (JDK version 1.7), Server used is Apache tomcat 7 and database used is the MYSQL (version 5). Mathematical model : The Group Data Sharing model for the system is defined in following equation

$$B_{ij} = jk + 1 + MOD_k(i - j + (j - 1)(i - 1)/k) \qquad \ldots\ldots\ldots\ldots\ldots(1)$$

Where,

• Bi,j- participant is contained in the j’th column of the ith block..

• k- a prime no., indicating each block B contains k+1 different participants and each participants appears k+1 time in different blocks. Also the Common conference key for jth participants for the system is given by the equation

$$C_{i,j} = \prod^{K}{}_{1} M_x where, xsE_i{-}j \qquad (2)$$

Where,

• Ci,j- Common conference key of jth participants in ith block.

• Mx- Keys for xth message. Implementation Status : The system consists of four modules owner, user,and 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. Till now the project developed at encryption level of first and seconds level.

IV. SYSTEM ANALYSIS

In our system common conference key is used along with key agreement protocol. Our system can be able to provide fault tolerence level for perticular data user. The system can provide multiuser cloud security with the use of common conference key . Using fault tolerence factor perticular user can be blocked and hence security can be maintained. Two level of encryption can be given to data for security. To achive this we are using blowfish algorithm along with DES in oue system.

V. RESULT

In Cloud application Security of data is compulsory when data are stored in different dynamic group then our System get the solution of Data are dived into Block level. Our Application used the two latest algorithms Blowfish and DES and Reconstruction of Block. Our experiments are simulated by using Java programming language with Blowfish Algorithms and Reconstruction of Graph. In the first part, we present a comparative simulation analysis between Uploading Scheme and our scheme with respect to the time cost for each partic-ipant in different phases, which is illustrated in Graph. And Second Scheme is downloading with respect to time cost for each participant in different phases which in Second Graph.

VI. CONCLUSION

Group data sharing in cloud computing has opened many doors in web technology and network security. 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 conference key agreement has better qualities of higher safety and reliability as compared with conference key distribution. However, large amount of information interaction required for the conference key agreement in the system and more compu-tational cost. To overcome the problems in the conference key agreement, the SBIBD term is used in the protocol design.

ACKNOWLEDGMENT

The authors would like to thank the researchers as well as publishers for making their resources available and teachers for their guidance. We are thankful to the authorities of Savitribai Phule University of Pune and concern members of cPGCON2019 conference, organized by, for their constant guidelines and support. We are also thankful to the reviewer for their valuable suggestions. We also thank the college authorities for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members.

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.

[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.