International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

SECURE DATA SHARING SCHEME FOR MOBILE CLOUD COMPUTING USING SeDaSc

Preethi P[1], Priyadarshini J[2], Soniya V[3], A.S. Balaji[4]

[1,2,3]*Student, Department of computer science, Anand Institute of Higher Technology Chennai, India*
[4]*Assistant Professor, Department of Computer Science Engineering, Anand Institute of Higher Technology, Chennai, India*

Abstract - *Cloud storage liberates organizations from establishing in-house data storage systems. However, cloud storage gives rise to security concerns. Cloud-specific and conventional insider threats are faced by data in case of group-shared data. The important issue is the Secure data sharing among a group that counters insider threats of legitimate yet malicious users. In this paper, we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control 6) One time download 7) Share Time Expire 8) Secret Key Management. The SeDaSC methodology encrypts a file with a single encryption key. The user gets only one share among the two different key shares that are generated for each user. The possession of a single share of a key allows the SeDaSC methodology to counter the insider threats. The other key share is stored by a trusted third party, which is called the cryptographic server. The SeDaSC methodology is applicable to conventional and mobile cloud computing environments. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations. We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be encouraging and show that SeDaSC has the potential to be effectively used for secure data sharing in the cloud.*

Key Words: **SeDaSc, reencryption, Key, cloud, Z3solver, etc…**

1. INTRODUCTION

CLOUD computing combining a set of existing and new techniques from research areas such as service-oriented architectures (SOA) and virtualization is considered as the next step in the evolution of on-demand information technology. It is routine for users to leverage cloud storage services to share data with others in a friend circle, e.g., Dropbox, Google Drive and Ali Cloud. The shared data in cloud servers, however, usually contains users' sensitive information (e.g., personal profile, financial data, health records, etc.) and needs to be well protected. As the ownership of the data is separated from the administration of them, the cloud servers may migrate users' data to other cloud servers in outsourcing or share them in cloud searching. Therefore, the big challenge is to protect the privacy of those shared data in cloud, especially in cross-cloud and big data environment. This challenge can be met by designing a comprehensive solution to support user-defined authorization period and to provide fine-grained access control during this period. After the user-defined expiration time the shared data should be self-destroyed. The data is stored in a common encrypted form to alleviate the problems. The user cannot share his/her encrypted data at a fine-grained level which is an disadvantage of encrypting data. The owner must know exact details of the one he/she wants to share with. In many applications, the data owner wants to share information with several users according to the security policy based on the users' credentials. The significant advantages of Attribute based encryption (ABE) is that it is based on the tradition public key encryption instead of one-to-one encryption because it achieves flexible one-to-many encryption. To achieve both data security and fine-grained access control, the powerful method is provided by ABE scheme. In the key-policy ABE (KP-ABE) scheme the ciphertext is labeled with set of descriptive attributes. The user can get the plaintext only when the set of descriptive attributes satisfies the access structure in the key. In general, the owner has the right to specify that certain sensitive information is only valid for a limited period of time, or should not be released before a particular time. In Timed-Release Encryption (TRE) an encryption key is associated with a predefined release time, and a receiver can only construct the corresponding decryption key in this time instance. On this basis, Paterson et al. proposed a time specific encryption (TSE) scheme, which is able to specify a suitable time interval such that the ciphertext can only be decrypted in this interval (decryption time interval, DTI). It can be used in many applications, e.g., Internet programming contest, electronic sealed-bid auction, etc. Electronic sealed-bid auction is a method to establish the price of goods through the Internet while keeping the bids secret during the bidding phase. That is, the bids (ciphertext) should be kept secret during the bidding phase (a specific time interval). Thus, in this paper, we attempt to solve these problems by using KPABE and adding a constraint of time interval to each attribute in the set of decryption attributes.

2. EXISTING SYSTEM

In existing system, sharing data among users is perhaps one of the most engaging features that motivate's cloud storage. Regarding availability of files, without the permission of the data owner, third party cannot access the files and without compromising the data owner's anonymity. When a file is shared to multiple users, the problem occurs.

3. PROPOSED SYSTEM

In this project, a key-policy attribute-based encryption with time-specified attributes (KP-TSABE), a novel secure data Autolysis of Data scheme in cloud computing. In the KP-TSABE scheme, every ciphertext is labeled with a time interval while private key is associated with a time instant. The ciphertext can only be decrypted if both the time instant is in the allowed time interval and the attributes associated with the ciphertext satisfy the key's access structure. we propose the Secure Data Sharing in Clouds (SeDaSC) methodology that provides: 1) data confidentiality and integrity; 2) access control; 3) data sharing (forwarding) without using compute-intensive reencryption; 4) insider threat security; and 5) forward and backward access control 6) One time download 7) Share Time Expire 8) Secret Key Management.

4. OVERALL ARCHITECTURE

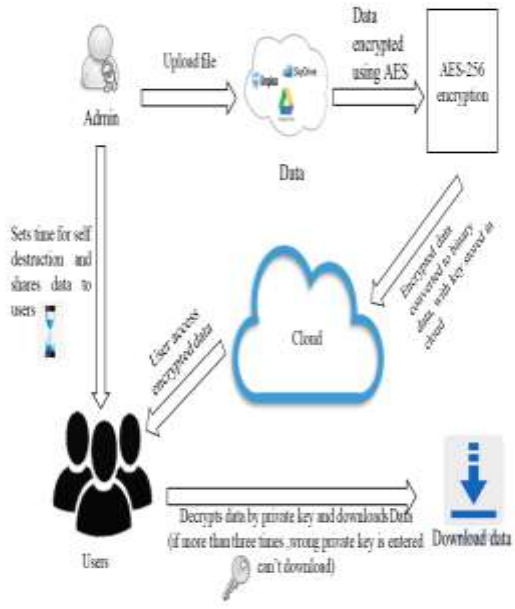

Fig -1: overall architecture diagram

4.1 Authentication and Authorization

First the user has to register and then the data base has to be accessed. After registration the user can login to the site. The whole mechanism from unauthorized usage will be protected and protect itself due to authorization and authentication. The user who wants to use this application, they have to register the details given.

4.2 File Encryption and data storing to cloud

User shares the file which he want to Upload. At first the uploaded files are stored in the Local System. Then the user upload the file to the real Cloud Storage (In this application, we use Dropbox). The file gets encrypted by using AES (Advanced Encryption Standard) Algorithm and Private Key will be produced while uploading to cloud. Again the Encrypted Data is converted as Binary Data for Data security and Stored in Cloud.

4.3 File Sharing

The files which are uploaded in the cloud is shared to the friends or users. The user who uploaded the file has to set the time to expire the data in Cloud. The Private Key of the Shared file will be send through Email.

4.4 File Decryption and download from cloud

The user can download the data by decryption by using AES (Advanced Encryption Standard) Algorithm. Corresponding Private Keys should be given by the user to decrypt the data. The data will be deleted if the user enter the Wrong Private Key for Three times. The intimation email will be sent to the Data owner if the file got deleted. The Downloaded Data will be stored in Local Drive.

4.5 File Autolysis of data and access control

The Data will be automatically deleted if the User does not downloaded the file successfully with in the time given by the data owner. If the user download the data, then the File Autolysis will be disabled. If the File got deleted by File Autolysis scheme, the intimation Email will be sent to Data Owner. If data owner attach any malicious in our shared file then will intimate to shared user. In our website to block the backward access. Example. If a user to logout account then can't go back our previous page.

5. CONCLUSION

The proposed system the SeDaSC methodology, which is a cloud storage security scheme for group data. The proposed methodology provides data confidentiality, secure data sharing without reencryption, access control for malicious insiders, and forward and backward access control. Moreover, the SeDaSC methodology provides assured

deletion by deleting the parameters required to decrypt a file.

6. FUTURE ENHANCEMENT

The future enhancement of the project is focused on the attempt to enhance security and also different types of advanced algorithm for Encryption may be used to develope this application. We use Dropbox as a Cloud Server. In Future, we may developed that the user can select the Cloud Server such as Google Drive, Hostinger, Dropbox, AppBox He/She want.

REFERENCES

1) Addressing Techniques for Secure Data Sharing in Cloud. Arti Bhagat, Nisha Rathee. IEEE, ICICCT 2018.

2) Secured Cloud Data Sharing Using Auditable Aggregate Key. Pooja Pol and Amrit Priyadarshi. IEEE and ICAECCT 2016.

3) Modified Secret Sharing Algorithm for Secured Medical Data Sharing in Cloud Environment.Mr.K.A.Muthukumar and Dr.M.Nandhini. 2016 IEEE and ICONSTEM.

4) Hybrid Encryption Techniques for Secure Sharing of a Sensitive Data for Banking Systems Over Cloud.Prachi More , Shubham Chandugade , Shaikh Mohammad Shafi Rafiq and Prof. Priya Pise. 2018 IEEE and ICACCT 2018

5) A Seamless Secret Sharing Scheme Implementation for Securing Data in Public Cloud Storage Service.Nelmiawat and Wahyudi Arifandi.2018 IEEE

6) B. Wang, B. Li, and H. Li, "Oruta: Privacy-preserving public auditingfor shared data in the cloud," Cloud Computing, IEEE Transactions on, vol. 2, no. 1, pp. 43–56, 2014.

7) J. Xiong, Z. Yao, J. Ma, X. Liu, Q. Li, and J. Ma, "Priam: Privacy preserving identity and access management scheme in cloud," KSII Transactions on Internet and Information Systems (TIIS), vol. 8, no. 1, pp. 282–304, 2014.

8) P. Jamshidi, A. Ahmad, and C. Pahl, "Cloud migration research: A systematic review," Cloud Computing, IEEE Transactions on, vol. 1, no. 2, pp. 142–157, 2013.