Cloud based File Sharing

Pragathi Shetty, Rajkumari Sunanda, Sowmya Shree K S,
Swathi N G., Hemanth Kumar N P
Dept of Computer Science & Engineering,
AIET, Mijar, Mangalore, Karnataka, India

***Abstract*—Internet based online cloud services, provides enormous volume of storage space,secure and elastic data storage services are claim to be provided by cloud service provider that will adopt to various storage necessities.Cloud storage liberates organizations from establishing in-house data storage systems and migrate data to remote storage in cloud.However, cloud storage rises to security issues.Cloud security, authentication is very essential factor but the Cloud has security issues as it deals with different technologies like networking, database management, memory management and virtualization.**

Keywords— Access control, cloud computing, Snooping, Identity and Access(IAS), Access Control List(ACL).

I. INTRODUCTION

In a recent years, cloud computing have been very trending in IT that where computing and data storage is done in data centres rather than personal portable PC's. Cloud storage reduce the burden of local hardware and software management and enables users to remotely store their data and enjoy the cloud applications.When more people accessing their files online, an important part of file sharing today is done by taking advantage of cloud storage. Cloud Computing migrates thedatabases and application software to the large data centres, where the management of the data and services are not justifiable.Cloud platform services, concepts and applications such as storage, processing power, virtualization, and connectivity allow the use of sharing data. Ensure that user's privacy and security of data are the most concerned challenges. Cloud storage service providers provides secure and elastic data-storage services that will be suitable for various storage requirements. Once data is uploaded into the cloud, the data owner loses control of the data, hence new security risks towardconfidentiality andintegrity of the data arises. In the last recent years,the cloud storage are widely use as it provides various applications such asdata archival, file backupand file sharing. Cloud storage servicesimplements file sharing in different ways depending in the form they are applied and at the ordered permission types. To protect users and data from each other as well as from the hackers there is a need of data confidentiality and authenticity of users.With ever-rapid development of e-business, e-science and social networkinghuge amounts of data, is generated by these e- applications. For instance, everyday the famous social network websites, such as Twitter, Facebook store a large number of photos, serve billions of page views, and manage billions of contents.

II. LITERATURE REVIEW

In cloud computing shared resource are provided over the Internet. Various cloud storage threats are Data Leakage, Snooping, Data Loss, Business Risks in Shared Technology and Key Management. In data leakage Resources are shared in cloud, a multi-tenant environment which provides access to a customer's data. Sharing storage hardware and migrating private or confidential data in the cloud seems to be risky. There are number of threats which leads to data leakage, including unauthorized access of cloud user accounts or hacks of cloud providers. The tenant cannot thrust the cloud service provider with their data, the best strategy is to depend on stronger passwords and file encryption. The length of the key used to protect data in cloud is conventionally co-related to the time required to break down an encryption algorithm.In Snooping, files without security measures in the cloud are most susceptible of being hacked. Even if the cloud service provides encryption for files, on route to its destination data can still be cut-off. Security against this threat would be to ensure that the data is encrypted and transmitted over a secure connection, as it will prevent unauthorized users from accessing the cloud's data. In Data Loss, some of the cloud services like Microsoft Azure, Dropbox and Google Drive has become a part of various business processes it has to deal with new security issues such as loss of control over confidential data. Data loss can be costly for an enterprise. A lot of data that are not meant to be shared can end up being viewed by unauthorized user, user need to backup their data in real-time. The Business Risks in Shared Technology cloud computing such as Infrastructure, platforms, and applications are shared by cloud service providers. Entire environment of the system can be exposed by a single vulnerable activity. In Key Management the management of cryptographic keys has become huge security issues after the introduction of the cloud. It can be done by securing the key management process by being automated, inconspicuous, and active.

Identity and Access Management(IAS) method is for controlling access to the resources, because it provides enterprise access control over all of Google Cloud Platform, and it grand permissions granted to parent

resources. Mandatory access control (MAC) is a system control access limit to source entities, constructed on the level of permission or approval of the accessing data entity, it may be a person,a device or a process. Access control List(ACL) provide individual buckets or objects read or write access for users.

When a user wants to share some resource with another user, the user need to specify what are the capabilities of the other user with respect to the shared resource(s). Access-granting techniques specifies the permissions to be granted. Capabilities of the grantees of some resource are specified in each permission.

III. PROPOSED METHODOLOGY

Cloud Based File Sharing secures the sharing and forwarding of data among a group of user using AES encryption and decryption technique. Additional feature of sharing files with limited permission to access file and allotted time to view the file. The cloud provides storage services to the user. The cloud in this methodology only involves basic cloud operations of file upload and download. The cryptographic server (CS) is responsible for security operations, such as key management, encryption, decryption, the management of the ACL. Foreach data file, one user will be the owner of the file, where as the others in the group will be the data consumers. Cryptographic Keys methodology maintains a unique single cryptographic key for each of the data files.

Input:
F, the ACL, the SKA, the
256-bit hash function H_f
Compute:
N= {0,
1}^{256} K =
H_f(R)
I= SKA(F, K)
for each user in the ACL, do
K_i= {0, 1}^{256}
K_i= K $\oplus K_i$
Add Ki for user in the
ACL Send Ki for user i
end
for
delete
(K)
delete(
K'_i)
returnC to the owner or upload to the cloud

Algorithm 1 Key Generation and Encryption [3]

In the first step, a random number Nof length 256 bits is generated such that N= {0, 1}^{256}. In the next step, Nis passed through a hash function that could be any hash function with a 256-bit output. The second step completely randomizes the initial user-derived random number N. The output is termed as K and is used in encryption of symmetric key. TheCS generates K_i, for each users in the group such that

K_i= {0, 1}^{256}. K_i serves as the CS portion of the key whenever anencryption/decryption request is received by the CS, it is used to compute K. For every file user distinct K_i is generated. User Key Share K'_i is computed for each of the users in the group as :

$K'_i = K \oplus K_i$.

Input: I, the ACL, the SKA
Compute: K'_i from the requesting user.
Get I from the requesting user or download from the cloud
Retrieve K_i from the ACL.
If K_i does not exist in the ACL, then return the access denied message to the user else
$K = K_i \oplus K'_i$
F = SKA(I, K)
send F to the
user end if
delete
(K)
delete
(K'_i).

Algorithm 2 Decryption Algorithm K'_i[3]

A counter for the number of file that can be access by the user and the number of download that can be performed by a particular user can be specified during uploading the file and sharing with the contacts of users.

IV. EXPECTED OUTCOME

The Cloud based file sharing methodology is proposed to provide the following services to the outsourced data confidentiality, secure data sharing among the group, secure data from unauthorized access of valid insiders within the group and giving time and number limitation of file access to the users. Uploading File: Whenever sharing of data among the group arises, the owner of the file sends the encryption request to the CS. The request is accompanied by the file and a list of users that are to be granted access to the file. The owner set the number of downloads or views for a user that have access to the file or set time for the user to download the file before the set time or both. File Download: The authorized user sends CS the download request or downloads the encrypted file from the cloud and sends to the CS the decryption request. Through a locally maintained ACL the cloud verifies the authorization of the user. The user has to download the file before the limited countdown or set time provided by the owner.

V. CONCLUSION

Cloud based file sharing is a file sharing security in cloud. The required security from unauthorized access of the file in

the cloud is provided by the encryption and decryption function. The owner can provide file access option to the authorized users. This facilities limits the number and time of access of the shared files by the owner for the authorized user in the group.

REFERENCES

[1] Archana K Rajan, Surya Babu, "Privacy and Authenticity for Cloud Data using Attribute Based Encryption and Digital Signature" 2017 Unpublished work.

[2] J. Sánchez-García, J. M. García-Campos, D. G. Reina, S. L. Toral, F. Barrero. "On-siteDriverID: A Secure Authentication Scheme based on Spanish eID Cards for Vehicular Ad Hoc Networks."

[3] SeDaSC: Secure Data Sharing in Clouds MazharAli, Student Member, IEEE, RevathiDhamotharan, Eraj Khan, Samee U. Khan, Senior Member, IEEE, Athanasios V. Vasilakos, Senior Member, IEEE, Keqin Li, Fellow, IEEE, and Albert Y. Zomaya, Fellow, IEEE(2017)