Distributed Cloud Data Storage using Fuzzy Authorization Framework

S. Sadesh[1], S. Geethapriya[2], M. Gowtham[3], M. Jeevitha[4]

[1]Associate Professor, VCET (Autonomous), Thindal, Tamilnadu

[2, 3, 4] B.E., Department of Computer Science and Engineering, VCET (Autonomous), Thindal, Tamilnadu

Abstract - The common issues found between cloud storage service providers and cloud application service providers are the interoperations and authorizations among the providers. Because the owner of the info and therefore, the cloud applications are from different cloud domains, building trust between them is challenging one. Another unwisely found issue is that quite one access token or secret keys needed if the info owner wants to authorize access right of several files. To deal with the above mentioned problems, a replacement secure authorization scheme for cloud storage is proposed which provides file divergence patience is named fuzzy authorization.

Keywords - Data Owner, Cloud Service Provider, End User, Time Limit

I. Introduction

Cloud storage is data storage where digital data is stored in logical storage disk, the physical storage is in across multiple servers, and therefore, the physical environment is usually owned and managed by the service provider. The cloud storage providers services as a further layer of knowledge privacy for the valuable and non-replaceable files. Backups are kept during a secure location but are physically far away from the originals or the source location. Storing confidential or sensitive information of the individuals or the business data within the cloud is usually more secured than storing local storage device. In addition with all the prevailing system mechanism, a correlated Authentication aspect with combination of the cloud storage provider and user is additionally considered. Additionally, deadline is provided to finish user to access the Cloud Service Providers (CSPs). So at the different time intervals, different sorts of tariffs are often applied to finish users to access the service. Likewise, the safety aspects provided by the cloud storage provider is additionally taken by data owner to extend the safety more. Additionally, trusted third party authentication mechanism is included.

II. Related Work

A. Problem Definition

Cloud computing provides unlimited storage for its users but secured transmission and retrieval of knowledge from the cloud are of great challenge. This work made use of atomic Advanced Encryption Standard (AES) algorithm to supply security for user data in cloud storage. 3DES and AES were adopted due to its robust security among the symmetric block ciphers.

B. Existing System

In existing system, the operations are carried out in the following aspects

- Data Owner: Data owner an entity who stores the info inside cloud storage and needs to use the cloud application services to process the info. A knowledge owner must register with cloud storage provider and must be logged-in to upload the info or access the info or authorize the info.
- Application Service Provider: An entity to be authorized to access the info which is stored in cloud storage. The appliance software be located in vendor's system or cloud and may be accessed by users through an internet browser or special purpose client software. For instance, PDFMerge is a web tool which may be wont to merge several PDF files into one PDF file. With proper authentication, PDFMerge fetches the source PDF files from the cloud storage. This results, uploading files from data owner's local device is avoided.
- Cloud Storage Provider: An entity which supplies storage as a service to its clients, and also provides access application programming interfaces to ASP when ASP holds a legitimate access token.

C. Drawbacks of Existing System

- Different types of access mechanism aren't applied then different client applications with varying processing capabilities got to execute the cloud data in same manner.
- Time limit isn't discussed then client wishes to access the info in same tariff for the entire period.
- Correlated Authentication aspects with combination of both cloud storage provider, application service provider and user isn't considered.

III. Proposed Method

In proposed system,

- Different sorts of access mechanism are applied then different client applications with varying processing capabilities got to execute the cloud data in same manner.
- Time limit is about then client likes to access the info in several levies for diverse time periods.
- Correlated Authentication aspects with mixture of both cloud storage provider, application service provider and user is additionally considered.
- Trusted third party authentication with no security violation is included.

IV. Module Description

The proposed system is designed and implemented with the following modules:

- Admin Module
- Cloud Service Provider Module
- Data Owner Module
- End User Module

A. Admin Module

In this module, the admin user can ready to add the cloud service provider details, and data owner details, the small print which is stored into the corresponding tables within the data base. Cloud Service Provider details include the Cloud Service Provider id, name of the Cloud Service Provider, website and password details are going to be stored into the CS Providers table. Data Owner details include the info owner id, name of the info owner and password details are stored into the data owner table. Also, the admin user assigns the assign Cloud Service Provider to Data Owner. And therefore, the admin user can ready to view the Cloud Service Providers details, Data Owners details; view Users details and consider downloads details.

B. Cloud Service Provider Module

In this Module, the Cloud service provider can ready to login with their provided credentials and may ready to view Data Owner details. In this module the payment from Data Owner are going to be performed. The small print includes of the payments are cloud storage provider id, data owner id, date of payment, file details and therefore, the payment amount.

C. Data Owner Module

In this data owner module, the info owner can upload the content, view CSP details after logged into the system. The data owner also can upload content to the cloud storage with the outline of file description, category of the file and Cloud Service Provider details alongside User details. The Data Owner also can view the download request from the users and supply keys to the download request files by the top users.

D. End User Module

In this module the top user can ready to view the Cloud Storage Provider Details, Users and Data Owner Details. The user also can look for content from the cloud storage and that they can download the file by means of send request to the info owner to get the key to download the contents.

V. Results and Discussion

In this paper, proposed FA (Fuzzy Authorization) which carries out a flexible file-sharing scheme between an owner who stores the info in one cloud party and applications which are registered within another cloud party. The safety analysis shows that our FA scheme provides a radical security of outsourced data, including confidentiality, integrity and secure access control. This approach reduces the storage consumption compared to other similar possible authorization schemes. This mainly addresses the reading authorization issue on cloud storage. This results to enable the TPA to perform audits for multiple users simultaneously and efficiently.

VI. Conclusion and Future Work

The existing system is describing the matter of secure authentication for storage in cloud. The proposed system provides Fuzzy authorization scheme to deal with the safety issues within the existing system. It also asserts that our scheme could efficiently achieve distance tolerance and realize fuzzy authorization in practice research study. The following enhancements are should be in future.

- The application if developed as multi web services, then many applications can make use of the records.
- The data integrity in cloud environment isn't considered. The error situation is often recovered if there's any mismatch.
- The internet site and database are often hosted in real cloud place during the implementation.

REFERENCES

[1] Babatunde Olaleye, Shri Kant, “Secure Use of Cloud Storage of Data on Smartphones using Atomic AES on ARM Architectures”, International Journal of Applied Engineering Research, ISSN 0973-4562, vol. 13, no. 5, pp. 2569-2581, 2018.

[2] D. D. Agrawal and P. Kulurkar, “A cloud-based system for enhancing security of android devices using Modern Encryption Standard-II Algorithm, International Journal of Innovations and Advancement in Computer Science, vol. 5, no. 4, pp. 60-66, 2016.

[3] A. M. Alsharani and S. Walker, “New approach in symmetric block cipher security using a new cubical technique”, International Journal of Computer Science and Information Technology (IJCSIT), vol. 7, no. 1, pp. 69-75, 2015.

[4] N. Balasubramanian, A. Balasubramanian and A. Venkataramani, “Energy consumption in Mobile Phones: A measurement study and implications for network applications”, In Proceedings of the 9th ACM SIGCOMM Conference on Internet Measurement, ACM IMC, Chicago, pp. 280-293, 2009.

[5] S. Banik, A. Bogdanov and F. Regazzoni, “Atomic-AES: A compact implementation of the AES Encryption/Decryption Core,” In Dunkelman O. and Sanadhya S. K. (Eds), (INDOCRYPT 2016), LNCS 10095, pp. 173-190, 2016.