SHARING SESSION KEY TO PROTECT DATA IN CLOUD STORAGE

V. Aarthi[1], P.R. Abeeragavi[2], T. Abinaya[3], Mrs. R. Kalaiselvi[4]

[1,2,3]Department of Computer Science and Engineering
[4]Assistant Professor, Department of Computer Science and Engineering,
Arasu Engineering College, Kumbakonam

ABSTRACT - Information retrieval in cloud is a technique that allows users to conveniently access information over the cloud. The data owner outsources their information in the cloud due to cost reduction and the great conveniences provided by cloud services. The main crises with sharing information in the cloud are the privacy and security issues. Data owner has lot of data on the cloud it should be classified based on importance of data using classification methodology. All information in cloud are encrypted so that cannot worried of information theft. Third party user request data owner, to retrieve information from cloud ,data owner can share a session key to retrieve information from cloud with sort term of period .session key is a 16 digit key contains hexa code which contains the key limitations. Session key had some more limitations to make information retrieval more secured.

KEYWORDS:

AES and DES encryption and decryption, privilege setting, hide setting, limitation, session key.

INTRODUCTION

Information retrieve as the name implies, concerns the retrieving of relevant information from databases. It is basically concerned with facilitating the users access to large amounts of(predominantly textual) information. In the simplest terms, cloud computing means storing and accessing data and programs over the internet instead of your computer's hard drive. A retrieval system stores units of information. Each unit is linked in the system to specifications of one or more documents or parts of documents. I will call them items. The user specifies particular units of information. Specific subjects and the system are designed to provide him with knowledge of all relevant items recorded in the system. To retrieve the information from the cloud makes more difficult when it comes to security issues particularly retrieve huge amount of data it will becomes more complex. Session key helps to retrieve information with some limitations and some protocols makes information retrieval more user.

CLOUD STORAGE

Cloud storage is one of the primary use of cloud computing. We can define cloud storage as storage of the data online in the cloud. A cloud storage system is considered as a distributed data centres, which typically use cloud-computing technologies and offers some kind of int erface for storing and accessing data. When storing data on cloud, it appears as if the data is stored in a particular place with specific name. There are four main types of cloud storage:

Personal Cloud Storage:

It is also known as mobile cloud storage. In this type storage, individual's data is stored in the cloud, and he/she may access the data from anywhere.

Public Cloud Storage:

In Public cloud storage the enterprise and storage service provider are separate and there aren't any cloud resources stored in the enterprise's data centre. The cloud storage provider fully manages the enterprise's public cloud storage. Private Cloud Storage: In Private Cloud Storage the enterprise and cloud

Private Cloud Storage:

In Private Cloud Storage the enterprise and cloud storage provider are integrated in the enterprise's data centre. In private cloud storage, the storage provider has infrastructure in the enterprise's data centre that is typically managed by the storage provider. Private cloud storage helps resolve the potential for security and performance concerns while still offering the advantages of cloud storage.

ALGORITHM

Advance Encryption Standard (AES)

AES is an encryption standard chosen by the national institute of standards and technology(NIST), USA to protect classified information. Symmetric key symmetric block cipher.

It has been accepted world wide as a desirable algorithm to encrypt sensitive data. It is a block cipher which operates on block size of 128 bits for both encrypting as well as decrypting.

Data Encryption Standard (DES)

The Data Encryption Standard(DES) is a symmetric-key block cipher published by the National Institute of Standards and Technology(NIST).

DES is an implementation of a Feistel Cipher. It uses 16 round Feistel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56 bits.

EXITING SYSTEM

In existing system the privacy of the cloud storage with respect to the server is not always guaranteed. In this system user can also download all file using the One Time Password. Users can stay online for a long period. Attackers can change current password without owner's knowled.

DEMERITS

In cloud data's are stored in remotely, it can't provide any security for that data so that it can accessed by others. A Third party user get authentication from data owner, but not restrict the time limit for third parties for that they can access cloud data in much time. And also, the data's are not separated in any categories for that third party user access all the cloud data's.

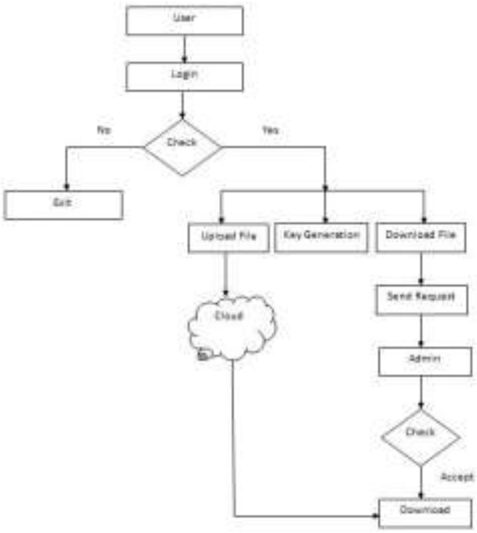
PROPOSED SYSTEM

In this proposed system common session key is shared to reduce the information leakage from cloud. Once the users make logout means they cannot again enter into the system. Session key will be expired after a period of time. The session key established by the protocol should only be known by the parties who are communicating with each other.

MERITS

Storage is space is separated into module and each module is secured with session password. This makes more efficient constructions this key can be used only once we propose a new secret sharing scheme that is computationally secure and can reducethenumbers.

SYSTEM ARCHITECTURE



LEVEL OF TESTING

In order to uncover the error present in different phases we have the concept of levels of testing. The basic levels of testing are

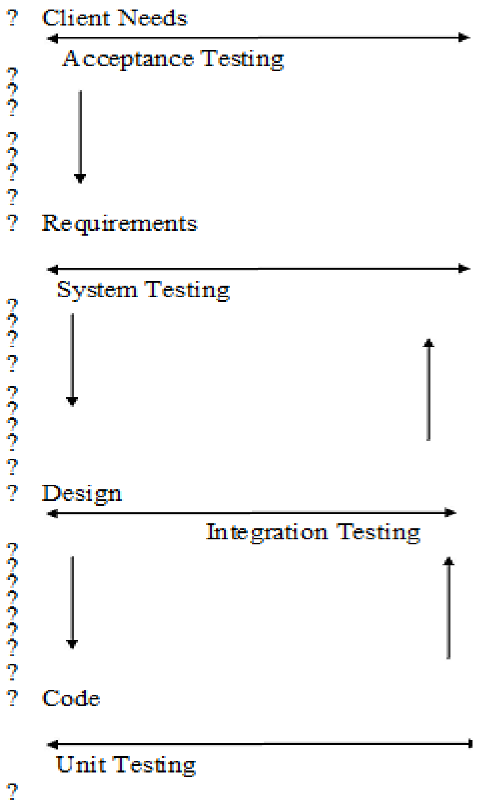


Figure 8.1 Levels of Testing

UNIT TESTING

Unit testing focuses verification effort on the smallest unit of software i.e. the module. Using the detailed design and the process specifications testing is done to uncover error within the boundary of the module. All modules must be in the unit test before the start of the interationg testing begins. When developing the modules as well as finishing the development so that each module works without any error. The inputs are validated when accepting from user.

INTEGRATION TESTING

After the unit testing we have to perform integration testing. The goal here is to see if modules can be integrated properly, emphasis being on testing interface between modules. This testing activity can be considered as testing the design and hence the emphasis on testing module interactions.

Sin this project "Real time investigation and classification system of air quality `", the main system performed by integrating all the modules.

When integrating all the modules I have checked whether the integration effects working of any of the services by giving different combinations of input with which the four services run perfectly before integration.

SYSTEM TESTING

Here the entire software system is tested. The reference document for this process is the requirements documents, and goal so to see if software meets its requirements. Here entire" Real time investigation and classification system for air quality using Big data Analysis" has been tested against requirements of projects and it is checked whether all requirements of project have been satisfied or not.

ACCEPTANCE TESTING

Acceptance test is performed with realistic data of the client to documents that the software is working satisfactorily. Testing here is focused on external behavior of the system: the internal logic of program is not emphasized. In this project" for Real time investigation and classification system for air quality " I have collected some data and tested whether project is working correctly or not. Test cases should be selected so that the largest number of attributes of an equivalence class is exercised at once. Testing phase is an important part of development. It is the process of finding errors and missing operations and also a complete verification to determine whether objectives are met and the user requirements are satisfied.

WHITE BOX TESTING

This is a unit testing method where a unit will be at a time and tested thoroughly at a statement level2 find the maximum possible errors. I tested step wise every piece of code, taking care that every statement in the code is executed at least once. The white box testing is also called glass box testing. I have generated the list of test cases, sample data, which is used to check all possible combinations of execution paths through the code at every module level.

BLACK BOX TESTING

This testing method considers a module as a single unit and checks the unit at interface and communication with other modules rather getting into details as statement level. Here the module will be treated as black generate output. Output for a given set of inputs combinations are forwarded to other modules box that will take some input.

CONCLUSION

Data sharing in the cloud is available in the future as demands for data sharing continue to grow rapidly. In this paper, we presented a session key to protect data in cloud storage from third party users using session key, third party users only access within a time duration of the data owner accept the request then only third party download the file. The study concludes that secure anti collision data sharing scheme for dynamic groups provides more efficiency supports access control mechanism and data confidentiality to implement privacy and security in dynamic group sharing.

FUTURE ENHANCEMENT

The future enhancement of the proposed Session key method involves securing online transaction in a cloud environment, wired environment, wireless environment and virtual network environment. The proposed hybrid encryption technique is also helpful in Mobile Banking and E- Banking. In virtual environment, data can be shared at two levels, such as Internet and Intranet. The proposed research work is used for sharing the secure data from one to others within the organization of the web server or virtual server at cloud environment. In Local Area Network, the proposed session key mechanism may be customized for transferring the sensitive data from work station to host based applications. In web based applications, the proposed mechanism enables the transfer of sensitive data from user to user, from user to server and from server to server which are located outside of the organization. In a cloud environment, more number of people are accessing the web server locally or globally to share the sensitive data. The proposed session key technique is very helpful to enhance the security for web based transactions in future.

REFERENCE

[1] M.R.Tribhuwan, V.A.Bhuyar, Shabana Pirzade,"Ensuring Data Storage Security in Cloud Computing through Two-way Handshake based on Token Management",2010International Conference on Advances in Recent Technologies in Communication and Computing.

[2] Latifur Khan and Bhavani Thuraisingham,"Security Issues for Cloud Computing", inTechnical Report UTDCS-02-10, February 2010.

[3] X. Wang, B. Wang, and J. Huang, "Clou Computing and its key techniques," inComputer Science and Automation Engineering(CSAE),2011IEEE International Conference on, vol. 2. IEEE, 2011, pp. 404–410

[4] E. M. Mohamed, H. S. Abdel kader, and S. El-Etriby, "Enhanced data security model for cloud computing," in Informatics and Systems (INFOS), 2012 8th International Conference on. IEEE, 2012, pp. CC–12.

[5] Arjun Kumar, Byung Gook Lee, Hoon Jae Lee, Anu Kumari, "Secure Storage and Access Data in Cloud Computing", 2012 International Conference on ICT Convergence (ICTC), 15-17Oct. 2012.

[6] Mr.Prashant Rewagad, Ms. Yogita Pawar, "Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in CloudComputing",2013 International Conference on Communication Systems and Network Technologies.

[7] Sultan Aldossary, William Allen, "Data Security, Privacy, Availability and Integrity in Cloud Computing: Issues and Current Solutions", in International Journal of Advanced Computer Science and Applications,Vol. 7, No. 4, 2016.