Secure Data Sharing in Cloud Using Revocable-Storage Using Identity-Based Encryption

Prof. Harshal Kolhe[1], Gaikwad Dhanshri[2], Gholap Dhananjay[3], More Tushar[4], Vaishnav Shubham[5]
[1] *Asst Prof., Department of IT Engineering, PVGCOE, Nashik*
[2,3,4,5] *Students, Department of IT Engineering, PVGCOE, Nashik*

***Abstract*- Many cloud service provider such as Dropbox, Google Drive, OneDrive, etc are popular File Storage providers for the Cloud. For added security, It is essential to encrypt the files by the users before uploading them to the cloud. Many File encrypting tools like Veracrypt, AxCrypt, Boxcrypt, are in place to encrypt files. But they have implemented AES and RSA encryption algorithm which are not secure. Files are divided into multiple parts and stored in descrete, traceble locations. We have combined AES-256 for developing a dropbox client which encrypts the files and the file key sharing using base encode 64 base decode 64 method before uploading to dropbox(cloud). Before uploading the data in cloud it can be divide into chunks and then store in different locations. This scheme can be integrated with any cloud storage systems. In future we shall be designing schemes to share encrypted files with authenticated parties through cloud storage. Scalability of our implemented tool can be enhanced by doing parallel computation.**

***Index Terms*- T-Coloring algorithm, Cloud Security, Fragmentation, Performance.**

1. INTRODUCTION

Security is one of the most difficult task to implement in cloud computing. The paper basically deals with the security issues that are experienced during the storage of data on the cloud. The cloud vendors generally store the clients data and information in cloud without following any security measures. Cloud computing is a large-scale distributed computing paradigm in which a pool of computing resources is available to cloud consumers via the Internet. Cloud storage is a data storage model in which files are stored in logical partitions where as the physical storage spans multiple servers in multiple locations and the physical environment is owned and managed by a hosting company. These cloud storage providers are responsible for providing availability and security of user files. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data. When file is distributed then data is also segregated into many servers. So here the need of data security arises. Every block of file contains its own hash code, using hash code which will enhance user authentication process; only authorized person can access the data. Here, the data is encrypted using advanced encryption standard, so data is successfully and securely stored on cloud. Third party auditor is used for public auditing. The proposed design allows users to audit the data with lightweight communication and computation cost. Analysis shows that proposed system is highly efficient against malicious data modification attack and server colluding attack. Performance and extensive security analysis shows that proposed systems are provably secure and highly efficient. Cloud storage services may be accessed through a co-located cloud computer service, web service application programming interface (API) or by applications that utilize the API, such as cloud desktop storage, a cloud storage gateway or Web-based content management systems. Files are stored in cloud storage systems in plain text format. Again multiple copies of the files are maintained in multiple locations for 1faster access and availability. If proper security measures are not taken, malicious users can gain access to the files and misuse it.

2. LITERATURE SURVEY

RSA and AES algorithm is used for providing data security in cloud computing. Eliminate the data security concerns using encryption algorithms or enhance data security issues using encryption algorithms. The cloud provider provides some assurance in terms of service level agreement to

convince the customer for security concerns. It introduce some technologies to ensure data security in cloud storage, i.e. data transfer protection, authorization and storage protection. In storage protect, the basic requirement of data security is to keep a data safe during disaster. The cloud storage makes a data safety by splitting a data into small piece and store in distributed server. Due to this aspect, performance and system availability will be increased. In transfer protect, in cloud computing users are far away from storage device; data must transfer through network. For data availability, provider must spilt the data into different data centered. During data The division of a file into fragments is performed based on a given user criteria such that the individual fragments do not contain any meaningful information. Each of the cloud nodes; we use the term node to represent computing, storage, physical, and virtual machines; contains a distinct fragment to increase the data security. A successful attack on a single node must not reveal the locations of other fragments within the cloud. To keep an attacker uncertain about the locations of the file fragments and to further improve the security, we select the nodes in a manner that they are not adjacent and are at certain distance from each other. The node separation is ensured by the means of the T-coloring.

3. SYSTEM ARCHITECTURE

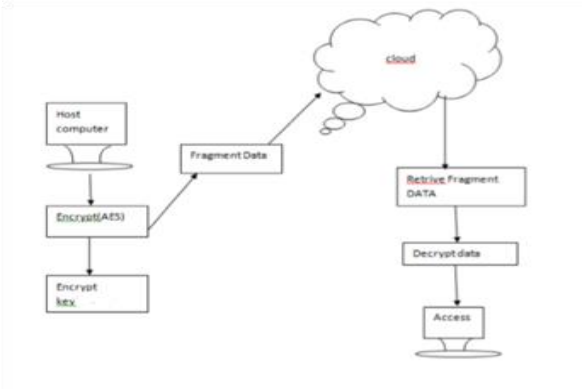

Fig -1: System Architecture

The architecture of the proposed system is shown in figure 1 The user is first authorized and authenticated .The service provider, provides the facility of file storage on the cloud. This files are first encrypted using AES 256 bit Algorithm ans a key is generated. This key is again encrypted. This files are fragmented are stored at traceable locations on cloud . This will help the authorized user to locate the required file correctly without complication. The user input query firstly encrypted with AES and encode64 base decode64 base. if the query matching conditions are satisfied then only the user can download and further decrypt the file. But if any unauthorized person tries to access the files, due to the complications in the reformation of files he will be unable to get the original copy. Here the security and the privacy measures are handled.

4. ALGORITHM

1) AES256

AES comprises three block ciphers: AES-128, AES-192 and AES-256. Each cipher encrypts and decrypts data in blocks of 128 bits using cryptographic keys of 128-, 192- and 256-bits, respectively. Symmetric (also known as secret-key) ciphers use the same key for encrypting and decrypting, so the sender and the receiver must both know -- and use -- the same secret key. All key lengths are deemed sufficient to protect classified information up to the "Secret" level with "Top Secret" information requiring either 192- or 256-bit key lengths. There are 10 rounds for 128-bit keys, 12 rounds for 192-bit keys and 14 rounds for 256-bit keys -- a round consists of several processing steps that include substitution, transposition and mixing of the input plaintext and transform it into the final output of ciphertext.

2)T-Coloring

G is a graph and T is a set of nonnegative integers. A T-coloring of G is an assignment of a positive integer $f(x)$ to each vertex x of G so that if x and y are joined by an edge of G, then $fff|f(x) - f(y)f|$ is not in T. T-colorings were introduced by Hale in connection with the channel assignment problem in communications. Here, the vertices of G are transmitters, an edge represents interference, $f(x)$ is a television or radio channel assigned to x, and T is a set of disallowed separations for channels assigned to interfering transmitters.

3) Fragmentation

Data fragmentation occurs when a collection of data in memory is broken up into many pieces that are not close together. It is typically the result of attempting

to insert a large object into storage that has already suffered external fragmentation. For example, files in a file system are usually managed in units called blocks or clusters. When a file system is created, there is free space to store file blocks together contiguously. This allows for rapid sequential file reads and writes. However, as files are added, removed, and changed in size, the free space becomes externally fragmented, leaving only small holes in which to place new data. When a new file is written, or when an existing file is extended, the operating system puts the new data in new non-contiguous data blocks to fit into the available holes. The new data blocks are necessarily scattered, slowing access due to seek time and rotational latency of the read/write head, and incurring additional overhead to manage additional locations. This is called file system fragmentation.

5. MATHEMATICAL MODEL

S=U, I, O, P
Where,
U = Set of users
Ui = {u1,u2,u3,... ... ...,un}
Where n>0
= ex. Primary user.
I = Set of Inputs
Ii = {i1, i2, i3,... ... ..., in}
Where n>0
= ex. Store data on cloud.
Output= {Acess data from cloud}
P = Set of Processes
Pi = {p1,p2,p3,... ... ...,pn}
Where n>0

6. RESULTS

Fig -2: System Overview

For the Login window the system provides the user authentication using password and username. This also provides the validations for password which helps the user to secure the password from attacker.

Fig -3: User Control Panel

In this module we can select the file which is to be store on cloud. This file can be get encrypted and then store on to dropbox using AES encryption algorithm. To secure the files from attacker we provide the key for each file. System also sends the mail to authenticated user which contains the encrypted key for file.

Fig -3: List of Uploaded Files

This module displays the list of files which stored by user on Dropbox. We can download it by clicking on download link, but it is encrypted. So that attacker will not get any information from files.

Fig -4: List of Files to Download

By clicking the download link all the files get downloaded into system. But we need to merge it. To merge the files we provide the key which is provided by user at the time of file upload. By this key only we can get the readable files.

7. CONCLUSION

A lots of effort is being utilized towards maintaining security over cloud storage. hence we have developed new security schemes. we have combined AES-256 with base encode64 and base decode64 encryption for developing a dropbox client which encrypts the files and the file key before uploading to dropbox. This scheme can be integrated with any cloud storage systems. In future we shall be designing schemes to share encrypted files with authenticated parties through cloud storage. Compression and decompression techniques can be added to files along with encryption and decryption, to save space in cloud storage.

REFERENCES

[1] C. Chiao-Chen and C. Yang-Chieh, Comparing consumer complaint responses to online and offline environment, Internet Research, vol. 21, pp. 124-137, 2011.

[2] Ozeki NG SMS Gateway, SMS Gateway-for Software developers and Service providers,Viewed Jul. 2012; http://www.ozekisms.com.

[3] Aditi Mhapsekar, Uma Nagarseka, Priyanka Kulkarni and Dhanan- jay R. Kalbande. Voice enabled Android application for vehicular com- plaint system using GPS and GSM-SMS technology, in World Congress on Information and Communication Technologies, 2012, pp. 520-524.

[4] Google Maps Javascript API v3. Internet: developers.google.com /maps/web/,[Apr. 25,2014]

[5] K. Coussement and D. Van den Poel, Improving customer complaint management by automatic email classification using linguistic style features as predictors, Decision Support Systems, vol. 44, pp. 870-882, 2008.

[6] R. Johnston, Linking complaint management to profit, International Journal of Service Industry Management, vol. 12, pp. 60-69, 2001.

[7] V. Bosch and F. Enriquez, TQM and QFD: exploiting a customer complaint management system, International Journal of Quality and Re- liability Management, vol. 22, pp. 30-37,2005.

[8] novel mobile interface to register citizens complaint. In iHCI IADIS International Conference In-terfaces and Human Computer Interaction 2008, Amsterdam, Nether- lands (25-27 July, 2008), 2008.

[9] Sunil Kopparapu, Natural Language Mobile Interface to Register Citizen Complaints, IEEE Technical Paper 2008.

[10] B. Schneier and J. Kelsey, Security audit logs to support computer forensics, ACM Trans. Inform. Syst. Security, vol. 2, no. 2, pp. 159176, May 1999.