Cloud Based Two Tier Security Scheme To Manipulate The Private Data

Aswini G
PG Scholar
Dept Of Computer Science & Engg
Saveetha Engineering College , Chennai
TamilNadu , India

Mervin R
Associate Professor
Dept Of Computer Science & Engg
Saveetha Engineering College , Chennai
TamilNadu , India

***Abstract*—Cloud computing as a technology is being used for software related work by which the users create a software working environment. It connects the large scale computing resources for effective communication. The security plays a major role in cloud and cloud computing services. Auditing is done with the help of the third party or private auditing were the data owners need to be online to manage the auditing. In this system own auditing is done based on the token generation. Using this token generation technique the token values are compared. From original tokens, changes done to the files can be identified. Users can login into their account and upload the files. In this system two tier security is provided for the uploaded files. The files will be converted into the smaller blocks and it will be stored into three different cloud server locations. Data are not only stored but also the content will be encrypted in the cloud server. It is not possible to break the two tier block for the hackers at the cloud end. The users first have to decrypt the files and also combine the split up files from three different locations which is tedious. Anyone can download the files from the server with the file owner permission. At the time of download, key is generated (code based key generation) and it will be send to the file owner. To download the files, these keys are being used which does the verification on whether the correct secret key has been entered by the user. A effective auditing is performed with the help of AES algorithm were the resulting method would be a secure and easy to use method.**

Keywords*—*Cloud computing, token generation; two tier security; encryption; code based key generation, AES

I. Introduction

Cloud Computing has been imagined as the next generation information technology (IT) engineering for endeavors, because of its extensive rundown of phenomenal preferences in the IT history: on-interest self-administration, universal system access, area autonomous asset pooling, quick asset flexibility, utilization based estimating and transference of danger Security has remained a constant issue for open Systems and internet. Lack of security is the only hurdle in wide adoption of cloud computing. Cloud computing is surrounded by many security issues like securing data, and examining the utilization of cloud by the cloud computing vendors. Several mechanisms have been used for privacy preserving of shared data in the cloud but these may fail to end the direct server attacks and other similar attacks. Public auditability allows an external party, in addition to the user himself, to verify the correctness of remotely stored data. However, most of these schemes do not support the privacy protection of users' data against external auditors, i.e., they may potentially reveal user data information to the auditors. This drawback greatly affects the security of these protocols in Cloud Computing. From the perspective of protecting data privacy, the users, who own the data and rely on TPA (third part auditor) just for the storage security of their data, do not want this auditing process introducing new vulnerabilities of unauthorized information leakage towards their data security .

As clients no more physically have the capacity of their information, customary cryptographic primitives with the end goal of information security insurance can't be specifically embraced. Specifically, just downloading all the information for its respectability confirmation is not a useful arrangement because of the cost in I/O and transmission cost over the system. Plus, it is regularly inadequate to recognize the information defilement just while getting to the information, as it doesn't give clients rightness confirmation for those unaccessed information and may be past the point where it is possible to recoup the information misfortune or harm. Considering the huge size of the outsourced information and the client's compelled asset ability, the undertakings of examining the information accuracy in a cloud domain can be imposing and costly for the cloud clients. In addition, the overhead of utilizing cloud storage ought to be minimized however much as could reasonably be expected, such that client does not have to perform an excess of operations to utilize the information.

Without a properly designed auditing protocol, encryption itself cannot prevent data from "flowing away" towards external parties during the auditing process. Here the main challenge is to provide secure ways of data analysis.Thus, it does not completely solve the problem of protecting data privacy but just reduces it to the one of managing the encryption keys. Unauthorized data leakage still remains a problem due to the potential exposure of encryption keys. In these mechanisms data is stored in one server. In this project integrity of the data in the cloud is also ensured. Using token generation technique comparison of the token values from original tokens is done to find out the changes in the file. This mechanism improves the storage and security related problems. It improves the security problem from unauthorized user. It provides dynamic data operations to data owner and privileged user.

II. RELATED WORK

Cloud Computing gets to be flourishing and standard plan of action ascribe enchanting alternatives. Additionally to the current event, the past choices moreover prompt genuine cloud particular security issues. Jules [13] portrayed a formal "verification of retrievability" (POR) model for guaranteeing the remote information trustworthiness. Their plan combines spot-checking and error correcting code to guarantee both ownership and retrievability of documents on file administration frameworks.

The utilization of numerous distinct cloud all the while shows different particular architecture and are talked about as per their security and protection capacities and prospects[7]. Cloud computing supply a replacement of figuring with shifted administrations models that encourages totally distinctive services to the clients. As all the data of partner degree ventures handled remotely and trades through totally distinctive system. Security is vital parameter furthermore the service supplier ensures that there no approved access to the sensitive data of partner degree venture all through the data [6]. This security and outline gives a proficient decoding, furthermore plan an effective property denial technique that can accomplish both forward in reverse security [10]. This should be possible once, various times, or persistently. Associate degree offender that furthermore has admittance to the process logic of the cloud can even modify the capacities and their input and output information. regardless of the way that inside the dominant part of cases it will be legitimate to accept a cloud supplier to be completely forthright and responsible way taking care of the clients' issues amid a conscious, there still remains a danger of malicious staff of the cloud supplier, palmy assaults and compromisation by outsiders, or of activities requested by a subpoena.

III. ARCHITECTURE OF THE TWO TIER SECURITY SCHEME

An effective and flexible distributed scheme with explicit dynamic data support to ensure the correctness of users' data in the cloud is proposed. Erasure correcting code is relied upon in the file distribution preparation to provide redundancies and guarantee the data dependability. This construction drastically reduces the communication and storage overhead as compared to the traditional replication-based file distribution techniques. By utilizing the homomorphic token generation with distributed verification of erasure-coded data, our scheme achieves the storage correctness insurance as well as data error localization.

This system consists of user profile interface, key generator and validation of key policy, encryption and decryption of splited files. A user profile created by the user is utilized for accessing of the files available in the cloud storage space. Also the account created by the owner can provide necessary access to the users who are in need of the data. Advanced encryption schemes are being followed to provide security to the data. Using token generation technique compare the token values from original tokens to find out the changes about the file. Two tier security scheme is provided for our uploaded files. The files does not stored directly it will be converted into the blocks, it will be stored into three different cloud server locations. If anyone try to hack at the cloud end, it is tedious to break the two tier block.

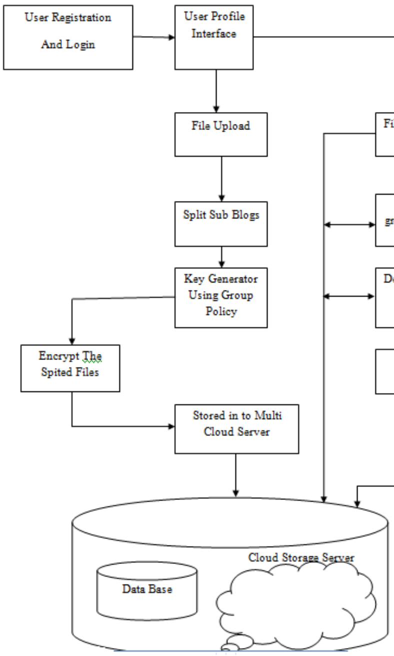


Fig 1. Architecture of Cloud two tier security scheme

IV. IMPLEMENTATION METHOD

Development Phases:

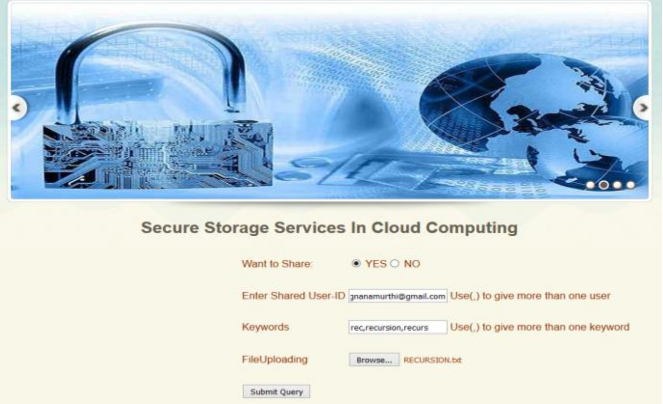
A. User Interface

Users can use this from anywhere at any time. For example, the email service is probably the most popular one. Cloud computing is a concept that treats the resources on the Internet as a unified entity, a cloud. Users just use services without being concerned about how computation is done and storage is managed. Here the main focus is on designing a cloud storage system for robustness and confidentiality. A cloud storage system is considered for user interface entry level creation in this module. The user interface can arguably include the total "user experience" which may include many aspects, and the content that is presented to the user within the context of the user interface. It provides the user an ability to interact with the computer online.

A simple login page is created to ensure that the data access is provided only to the registered users. Various levels of validation is done during the registration for correct entry of mail-id, password and mobile number. Authentication is provided to the existing users who forget their passwords by means of generating OTP. Successful users who have logged in can upload their files into the cloud server. The files to be uploaded are selected and respective names are given which gets updated into the database.

B. File split and encryption

Owner uploads the file into the cloud server by which the data can be accessed by the others on the server with the help of the owner Fig.2. The uploaded files gets split up into three parts by means of secure erasure technique. These split files are being stored at three different storage locations on the cloud server. Token values are initially created for the contents of the file which are being uploaded into the cloud server. These token values are used to ensure the integrity of the data.By means of comparing these token values of the current file and the existing file correctness is ensured. Also the files which are uploaded are not just directly stored, they are being encrypted before being stored. These encrypted splits are stored at different locations. . In coding technique, the user encrypts the information together with his public key and uploads the cipher texts to the Cloud. Obviously, key generation algorithms are used to download the files, were a decryption is necessary before to download. Further on authentication is provided to the file access in the upcoming modules.



Secure Storage Services In Cloud Computing

Want to Share: ● YES ○ NO

Enter Shared User-ID gnanamurthi@gmail.com Use(,) to give more than one user

Keywords rec,recursion,recurs Use(,) to give more than one keyword

FileUploading RECURSION.txt

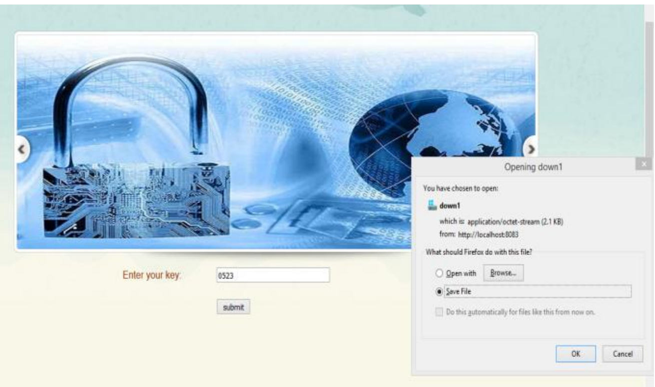
Fig 2: Uploading files with access permissions

Storing data over storage servers - one way to provide data robustness is to replicate a message such that each storage server stores a message. Another way is to encode a message of k symbols into a codeword of n symbols by erasure coding. To store a message, each of its codeword symbols is stored in a different storage server. As long as the number of servers is under the tolerance threshold of the erasure code, the message can be recovered from the codeword symbols stored in the available storage servers by the decoding process. The data is divided into fine-grained components and these components area unit distributed to different location.In coding technique, the user encrypts the information together with his public key and uploads the cipher texts to the Cloud. The cloud will severally figure on the encrypted knowledge to get the encrypted result, that solely the user will decode. The AES algorithm is used for encryption were, AES relies on a style principle referred to as a substitution-permutation network, combination of each substitution and permutation, and is quick in each package and hardware. Not like its precursor DES, AES doesn't use a Feistel network.

C. Key Generation and Key Sharing

Users get the permission from owner to download the files from cloud server. For each try of accessing the files, random keys are generated which are then shared with the user by the owner . These random keys are being generated by means of random key generation algorithm Fig.3. The owner provides access to the users if and only if it is authorized.

Unauthorized users are not allowed to access the data in the cloud server. The owner of the data can avoid this in to ways either not to share the secret key with the unauthorized user trying to access the file or to block a particular user if he is unauthorized, so that we cannot access the data.



Enter your key: 0523

Opening down1

You have chosen to open:

down1

which is: application/octet-stream (2.1 KB)

from: http://localhost:8083

What should Firefox do with this file?

○ Open with

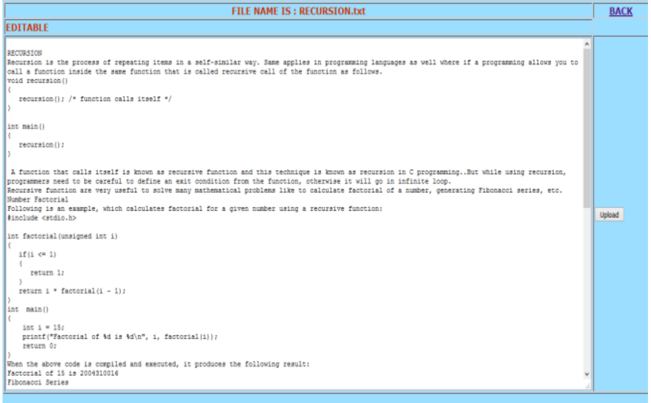
● Save File

□ Do this automatically for files like this from now on.

Fig 3: Downloading the files from cloud server

D. File Sharing and Auditing

Owner after sharing the key, checks for the integrity of the data by doing the token value matching .Once the key is shared the authorized user either views the document or download it and modify it Fig.4. Changes done to the document are to be approved by the owner before it is being uploaded into the cloud server Fig.5. Here the owner checks for the integrity of the data. If the changes are authorized then the document is uploaded into the cloud server by the owner, if not then it is being removed by the owner.



FILE NAME IS : RECURSION.txt

EDITABLE

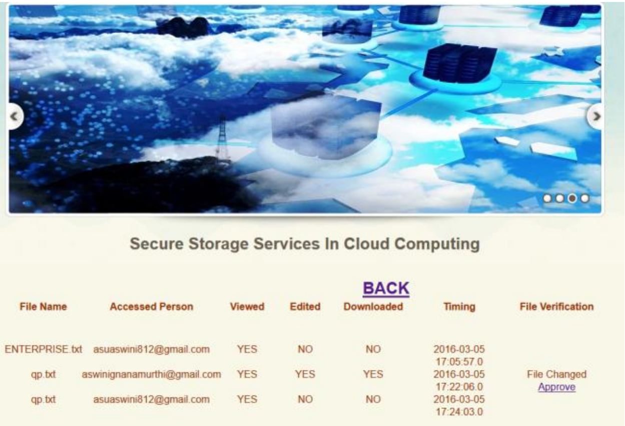
```
RECURSION
Recursion is the process of repeating items in a self-similar way. Same applies in programming languages as well where if a programming allows you to
call a function inside the same function that is called recursive call of the function as follows.
void recursion()
{
   recursion(); /* function calls itself */
}

int main()
{
   recursion();
}

 A function that calls itself is known as recursive function and this technique is known as recursion in C programming..But while using recursion,
programmers need to be careful to define an exit condition from the function, otherwise it will go in infinite loop.
Recursive function are very useful to solve many mathematical problems like to calculate factorial of a number, generating Fibonacci series, etc.
Number Factorial
Following is an example, which calculates factorial for a given number using a recursive function:
#include <stdio.h>

int factorial(unsigned int i)
{
   if(i <= 1)
   {
      return 1;
   }
   return i * factorial(i - 1);
}
int  main()
{
    int i = 15;
    printf("Factorial of %d is %d\n", i, factorial(i));
    return 0;
}
When the above code is compiled and executed, it produces the following result:
Factorial of 15 is 2004310016
Fibonacci Series
```

Fig 4: Updation to the files downloaded



Secure Storage Services In Cloud Computing

BACK

File Name	Accessed Person	Viewed	Edited	Downloaded	Timing	File Verification
ENTERPRISE.txt	asuaswini812@gmail.com	YES	NO	NO	2016-03-05 17:05:57.0	
qp.txt	aswinignanamurthi@gmail.com	YES	YES	YES	2016-03-05 17:22:06.0	File Changed Approve
qp.txt	asuaswini812@gmail.com	YES	NO	NO	2016-03-05 17:24:03.0	

Fig 5: Auditing and approving the file changes

V. EXPERIMENTAL RESULTS

A comparison is being drawn out between the split up files and the direct files which are being stored into the cloud space. Rather than directly storing the files into the cloud we split it into blocks, as it is more advantageous while considering certain factors. Considering security, it is obvious that on storing the files as a whole, hacker attacks are done in an easy manner rather than split up storage where it is tedious for the hackers to identify each split of data and group them to get the original text. In terms of integrity, storing the file in split up blocks is better than the entire file storage. During split file storage the data gets distributed among multiple locations were changes done to any single location can be managed with the files stored in other locations. But in case of whole file storage modifications done at one point can distort the entire file which is difficult to recover. Speed denoted the encryption speed were encrypting the file as separate blocks is advantageous than encrypting as a whole, because parallel processing is faster than encrypting a single large file.

VI. CONCLUSION

Privacy-preserving public auditing system is proposed for data storage and security in cloud computing. Homomorphic linear authenticator and random masking is done to guarantee that the TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou(2010), "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou(2012), "Towards secure and dependable storage services in cloud computing," Service Computing, IEEE Transactions on, vol. 5, no. 2, pp. 220–232.

[3] H. Chen and P. Lee(2014), "Enabling data integrity protection in regeneratingcoding-based cloud storage: Theory and implementation," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 407–416.

[4] K. Yang and X. Jia(2013), "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726.

[5] Nisha D. Dable , Nitin Mishra(2014)," Enhanced File Security using Encryption and Splitting technique over Multi-cloud Environment, International Journal on Advanced Computer Theory and Engineering (IJACTE), ISSN (Print): 2319-2526.

[6] Prashant Kumar, Lokesh Kumar(2013)," Security Threats to Cloud Computing", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 2, No. 1.

[7] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Ninja Marnau, "Security and Privacy Enhancing Multi-Cloud Architectures", IEEE Transaction on Dependable and Secure Computing, Jan 2013.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou(2009), "Enabling public verifiability and data dynamics for storage security in cloud computing," in Computer Security–ESORICS 2009. Springer, 2009, pp. 355–370.

[9] Selvakumar G. Jeeva Rathanam M. R. Sumalatha(2012)," PDDS Improving Cloud Data Storage Security Using Data Partitioning Technique," IEEE.

[10] Kan Yang, Ren, Xiaohua Jia, Bo Zhang, and Ruitao Xie, "DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems," IEEE 2013.

[11] Z.Wilcox-O'Hearn and B. Warner(2008), "Tahoe: The Least-Authority Filesystem,"Proc. Fourth ACM Int'l Workshop Storage Security and Survivability (StorageSS), pp. 21-26.

[12] Zhifeng Xiao and Yang Xiao(2012), "Security and Privacy in Cloud Computing", IEEE Communication Survey & Tutorials, Accepted for Publication.

[13] A. Jules and J. Burton S. Kaliski, "Pors: Proofs of retrievability for large files," in Proc. of CCS'07, Alexandria, VA, October 2007, pp. 584–597.