International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Preserving Privacy In Public Auditing For Data Storage Security In Cloud Computing

Geethamani G. S.[1], Ranjani S[2]

[1]Assistant Professor, PG Department of (IT), Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

[2]PG Student, Department of (IT) , Hindusthan College of Arts and Science, Coimbatore, Tamil Nadu, India

ABSTRACT

This paper is proposed "to computerize the cloud computer. This system was developed in Asp.net as front end, the Microsoft SQL Server as the back end and Windows XP as platform. Computers today have become indispensable tools. They are fast changing the way in which work is done by their speed, accuracy and diligence. Almost all good businesses practices have embraced computers for increasing the productivity and efficiency, which ultimately results in profits. Cloud computing is the long dreamed vision of computing as a utility, where users can remotely store their data into the cloud so as to enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By data outsourcing, users can be relieved from the burden of local data storage and maintenance. Thus, enabling public auditability for cloud data storage security is of critical importance so that users can resort to an external audit party to check the integrity of outsourced data when needed. To securely introduce an effective Third Party Auditor (TPA), the following two fundamental requirements have to be met:

1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data.

2) Introduce no additional on-line burden to the cloud user.

Keywords : Network Traffic, Network Security, Protocols, Cloud Computing , Data Mining

I. SYSTEM ANALYSIS

1.1 EXISTING SYSTEM

As data generation is far outpacing data storage it proves costly for small firms to frequently update their hardware whenever additional data is created. Also maintaining the storages can be a difficult task. It transmitting the file across the network to the client can consume heavy bandwidths. The problem is further complicated by the fact that the owner of the data may be a small device, like a PDA (personal digital assist) or a mobile phone, which have limited CPU power, battery power and communication bandwidth.

1.1.1 DISADVANTAGE

- The main drawback of this scheme is the high resource costs it requires for the implementation.
- Also computing hash value for even a moderately large data files can be computationally burdensome for some clients (PDAs, mobile phones, etc).
- Data encryption is large so the disadvantage is small users with limited computational power (PDAs, mobile phones etc.).

1.2 PROPOSED SYSTEM

One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. It provide a scheme which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA). It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted.

ADVANTAGES:

Apart from reduction in storage costs data outsourcing to the cloud also helps in reducing the maintenance.

- Avoiding local storage of data.
- By reducing the costs of storage, maintenance and personnel.
- It reduces the chance of losing data by hardware failures.
- Not cheating the owner.

II. PROBLEM DEFINITION

The problem specification of the organization is developing an exclusive technique, which is useful for both sender and receiver. It will be developed over the internet.

2.1 DEVELOPING SOLUTION STRATEGIES

To provide high degree of correctness and effectiveness and to reduce the workload it is very important to computerize the system. System computerized is easy to handle and provide the high accuracy in its output.

2.2 ANTICIPATED ADVANTAGES

- It provides high security and reliability occurs.
- The authorization is highly provided.
- It gives assurance for the security of data.
- It facilitates faster information retrivel.
- Well efficiency designed forms.
- Easy management of client system.

III. MODULE DESCRIPTION

- Registration
- Upload File
- Admin Module
- TPA Module
- Download
- Key Generation

3.1 REGISTRATION

This module is used to store the Customer Registration Details. The Registration details includes user name, password, address, phone number, E-mail, etc.. The verification code will be send to the customer mail id for authentication purpose. When the customer wants to enter this system he must enter this code.

3.2 UPLOAD FILE

This module is used to upload files to the cloud server on any time. When uploading the file the secret will be generated by using keygen algorithm. Each uploaded files will have unique key and this key is forwarded to the user registered mail id.

3.3 ADMIN MODULE

The administrator is a primary user called as cloud owner. The Admin will manage the entire

application and storage device. Admin can monitor the entire files and users stored on the server at any time. But admin cannot download user files without user permission. Admin can view files and content at any time but he cannot download file without user acceptance. If Admin want to download the file he will send the request information to the user through this system. After the response from the user only he can download the file because of privacy.

3.4 THIRD PARTY AUDITOR MODULE

The third party auditor is a user who verify the users and files stored on the cloud. They can audit those things but they cannot view the content or download the files stored on the cloud.

The auditing is classified into two categories

1) Batch Auditing Module

With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

2) Data Dynamics Module:

Hence, supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now it show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. They can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

3.5 DOWNLOAD

It is used to download files But without secret key this system will not allow download the file.

3.6 KEY GENERATION

This module used to generate the secret key by using keygen algorithm and swill send to the personal mail is of the user. The secret key is must for uploading and download files on the cloud server.

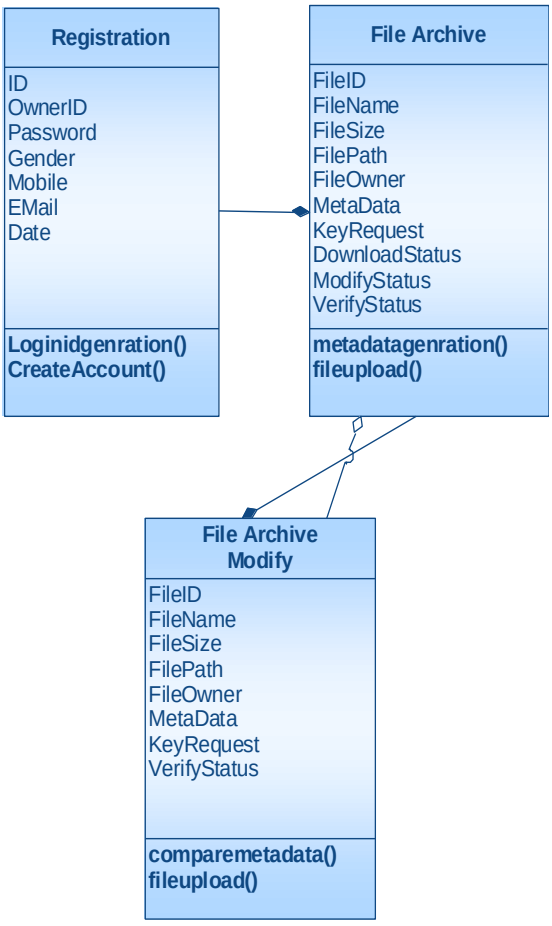

Figure 1. CLASS DIAGRAM

IV. SYSTEM IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

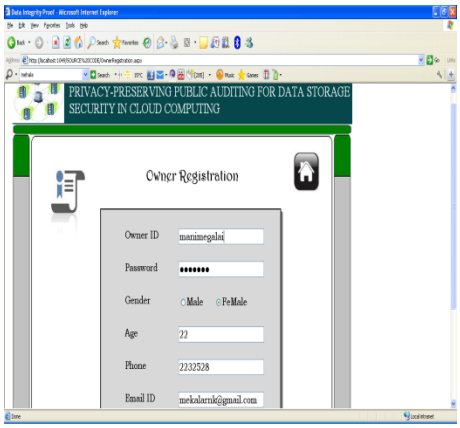

Figure 2. Owner Registration Form

V. ALGORITHM

META-DATA GENERATION

Let the verifier V wishes to the store the file F with the archive. Let this file F consist of n file blocks. Initially preprocess the file and create metadata to be appended to the file. Let each of the n data blocks have m bits in them. A typical data file F which the client wishes to store in the cloud. Each of the Meta data from the data blocks m_i is encrypted by using a suitable algorithm to give a new modified Meta data M_i. Without loss of generality it show this process by using a simple XOR operation. The encryption method can be improvised to provide still stronger protection for verifier's data.

All the Meta data bit blocks that are generated using the above procedure are to be concatenated together. This concatenated Meta data should be appended to the file F before storing it at the cloud server. The file F along with the appended Meta data e F is archived with the cloud.

VI. SYSTEM MAINTENANCE

CLOUD STORAGE

Data outsourcing to cloud storage servers is raising trend among many firms and users owing to its economic advantages. This essentially means that the owner (client) of the data moves its data to a third party cloud storage server.

SIMPLY ARCHIVES

This problem tries to obtain and verify a proof that the data that is stored by a user at remote data storage in the cloud is not modified by the archive and thereby the integrity of the data is assured. Cloud archive is not cheating the owner, if cheating, in this context, means that the storage archive might delete some of the data or may modify some of the data. While developing proofs for data possession at untrusted cloud storage servers they are often limited by the resources at the cloud server as well as at the client.

SENTINELS

In this scheme, unlike in the key-hash approach scheme, only a single key can be used irrespective of the size of the file or the number of files whose retrievability it wants to verify. Also the archive needs to access only a small portion of the file F unlike in the key-has scheme which required the archive to process the entire file F for each protocol verification. If the prover has modified or deleted a substantial portion of F, then with high probability it will also have suppressed a number of sentinels.

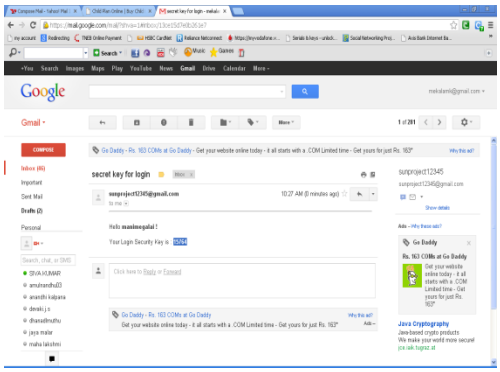

Figure 3. Owner Login Verification To Mail

VERIFICATION PHASE

The verifier before storing the file at the archive, preprocesses the file and appends some Meta data to

the file and stores at the archive. At the time of verification the verifier uses this Meta data to verify the integrity of the data. It is important to note that our proof of data integrity protocol just checks the integrity of data i.e. if the data has been illegally modified or deleted. It does not prevent the archive from modifying the data.

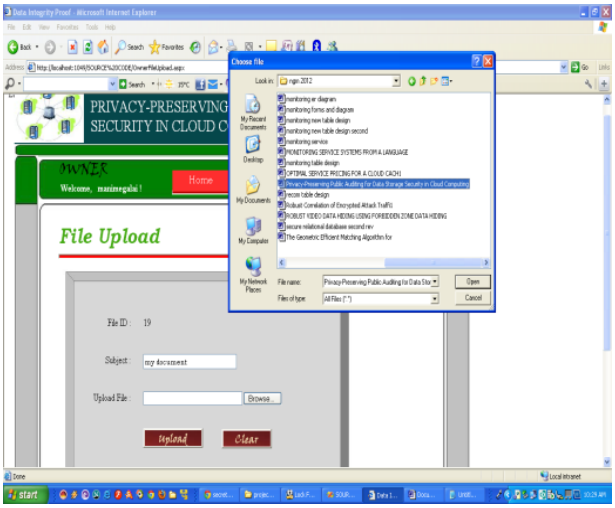

Figure 4. Owner Select The Document To Upload

VII. CONCLUSION

This project have worked to facilitate the client in getting a proof of integrity of the data which they wishes to store in the cloud storage servers with bare minimum costs and efforts. Our scheme was developed to reduce the computational and storage overhead of the client as well as to minimize the computational overhead of the cloud storage server. It also minimized the size of the proof of data integrity so as to reduce the network bandwidth consumption. Many of the schemes proposed earlier require the archive to perform tasks that need a lot of computational power to generate the proof of data integrity. But in our scheme the archive just need to fetch and send few bits of data to the client.

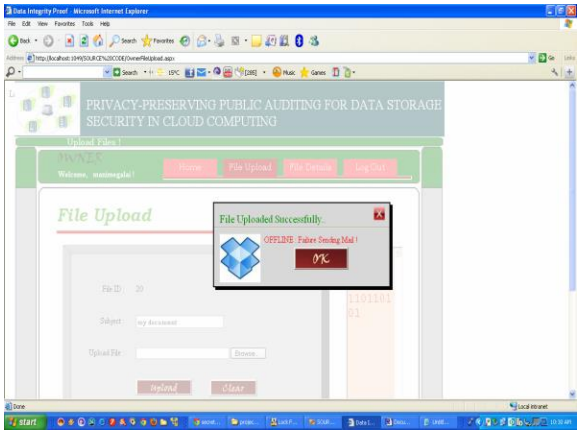

Figure 5. Owner File Status Successfully

Figure 6. View File Details by Administrator

VIII. FUTURE ENHANCEMENT

In future it is a possible one to add new web pages without any problem with enhanced. As the technology used is a good one it is flexible for future enhancement and it is also possible to alter the front-end and back-end without any problem.

This web-based one is created effectively in a user-friendly manner and any new system that is developed in future must be incorporated or updated without any problem. So this will support enhancements in future.

IX. REFERENCES

[1]. ArchanaJadhav, Vipul Oswal, Sagar Madane ,Harshal Zope,Vishal Hatmode "VNC ARCHITECTURE BASED REMOTE DESKTOP ACCESS THROUGH ANDROID MOBILE PHONES" International Journal of Advanced Research in Computer and

Communication Engineering Vol. 1, Issue 2, April 2012 .

[2]. Remote Control of Mobile Devices in Android Platform Angel, Gonzalez Villan , Student Member, IEEE and JosepJorbaEsteve,Member, IEEE.

[3]. Virtual Network Computing,Tristan Richardson, Quentin StaffordFraser,Kenneth R. Wood and Andy Hopper,Reprint from IEEE Internet Computing Volume 2, Number 1 January/February 1998.

[4]. T. Richardson, \The RFB Protocol", Tech. rep., RealVNC Ltd,2007 .

[5]. The RFB Protocol, Tristan Richardson, Real VNC Ltd(formerly of Olivetti Research Ltd / AT&T Labs Cambridge) ,Version 3.8,Last updated 26 November 2010.

[6]. R.Manikandasamy"Remote Desktop Connection Using Mobile Phone "International Journal of Science, Engineering and Technology Research (IJSETR) Volume 2, Issue 8, August 2013.

[7]. H.Kawashima, K. Koshiba, K. Tuchimochi, K. Futamura, M. Enomoto, and M. Watanabe, "Virtual PC-type thin client system," NEC TECHNICAL JOURNAL,(SEP- 2007).

[8]. P. Simoens, F. A. Ali, B. Vankeirsbilck, L. Deboosere, F. De Turck, B. Dhoedt, P. Demeester, and R. Torrea-Duran,"Cross-Layer Optimization of Radio Sleep Intervals to Increase Thin Client Energy Efficiency," IEEE COMMUNICATIONS LETTERS, (DEC- 2010).

[9]. V. Rivoira and F.Pascali, "HSDPA: High-speed internet over your mobile phone", IEC newsletter, (June -2007).

[10]. Michael Lloyd Lee, "J2ME VNC", codigofonte, (February-2005).

[11]. HarshitaTomar ,GunjeshSahney ,"Virtual Network Computing- A Prodigious Technology For Remote Desktop Sharing"HarshitaTomar et al Int. Journal of Engineering Research and Applications . www.ijera.com ISSN : 2248-9622, Vol. 3, Issue 6, Nov-Dec 2013.

[12]. Virtual Network Computing Tristan Richardson, Quentin Stafford-Fraser, Kenneth R. Wood and Andy Hopper Reprint from IEEE Internet Computing Volume 2, Number 1 AT&T Laboratories Cambridge (1999). "Xbased VNC server". Virtual Network Computing. Archived from the original on 2007-03-19. Retrieved 2007-03-24

[13]. IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661, ISBN: 22788727Volume 6, Issue 5 (Nov. - Dec. 2012), PP 16-20 Virtual Network Computing Based Droid desktop VaidehiMurarka, Sneha Mehta,DishantUpadhyay, AbhijitLal .

WEBSITES

[14]. http://www.asp.net.com

[15]. http://www.dotnetspider.com/

[16]. http://www.dotnetspark.com

[17]. http://www.almaden.ibm.com/software/quest/Resources/

[18]. http://www.computer.org/publications/dlib

[19]. http://www.developerfusion.com