ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Secrecy Maintaining Public Inspecting For Secure Cloud Storage

K.Sangamithra[1], S.Tamilselvan[2]

M.E, M.P.Nachimuthu.M.Jaganathan Engineering College, Tamilnadu, India[1]

Asst. Professor, M.P.Nachimuthu.M.Jaganathan Engineering College, Tamilnadu, India [2]

ABSTRACT: A framework to supply a secure cloud database that will guarantee to prevent security risks and Secret key to pre-process the file. Multi-cloud will be implemented as hybrid cloud. This framework will apply the use of secret sharing algorithm, MAC algorithm, audit protocol for outsourced data to reduce the risks of data intrusion, loss of service availability and ensures data unity. Muti-cloud usage is implemented by distributing data into three different cloud providers. The public Demonstrable Data Ownership (**DDO**), which is a cryptographic technique for verifying the unity of data without retrieving it at an untrusted server; can be used to realize audit services. Random cover technique is used to achieve a secrecy-Maintaining public inspecting system for cloud data storage security.

KEYWORDS: Ownership, cryptographic, data intrusion.

I. INTRODUCTION

Cloud computing provides a scalability environment for growing amounts of data and processes that work on various applications and services by means of on-demand self-services. One basic view of this prototype changing is that data are being centralized and outsourced into clouds. This kind of outsourced storage services in clouds have become a new profit development point by providing a comparably low-cost, ascendable, position-independent structure for dealing clients' data. The cloud storage service (CSS) relieves the burden of storage management and sustainment. However, if such an important service is dangerous to attacks or failures, it would bring irretrievable losses to users since their data or archives are stored into an unsure storage pool outside the enterprises.

The security risks come from the following reasons: the cloud substructures are much more powerful and authentic than personal calculating devices. However, they are still capable to security threats both from outside and inside the cloud for the benefits of their ownership, there exist various needs for cloud service providers (CSP) to behave unreliably toward the cloud users furthermore, the challenge at a time suffers from the lack of hope on CSP. Their behaviors may not be known by the cloud users, even if this challenge may result from the users' own wrong operations. It is necessary for cloud service providers to offer an efficient audit service to check the unity and accessibility of the stored data. Conventional cryptology technologies for data unity and availability, based on hash functions and signature strategies cannot work on the outsourced data without a local copy of data. In addition, it is not a realistic solution for data establishment by downloading them due to the worthful transaction, especially for large-size files. The solutions to audit the correctness of the data in a cloud environment can be doubtful and expensive for the cloud users. This is essential to realize public audit ability for CSS, so that data owners may resort to a third party auditor (TPA), who has expertness and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is importantly important for digital forensics and data confidence in clouds. To implement public audit ability, the notions of proof of irretrievable and Demonstrable Data Ownership (DDO) have been proposed by some researchers.

II. RELATED WORKS

Yan Zhua – 2012 [10] says that Cloud-based outsourced storage saves the client's burden for storage management and maintenance by providing a comparably low-cost, ascendable, position-independent platform.The clients has no longer have physical possession of data indicates that they are facing a potentially formidable risk for missing or imperfect data. To avoid the protection risks, audit services are critical to ensure the unity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing. The authors proposed Demonstrable Data Ownership(DDO), which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server, can be used to realize audit services.

Armbrust – 2010 [1] says that Cloud computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services. The services themselves have long been referred to as Software as a Service (SaaS).Some vendors use terms such as IaaS (Infrastructure as a Service) and PaaS (Platform as a Service) to describe their products, but we eschew these because accepted definitions for them still vary widely. The line between "low-level" infrastructure and a higher-level "platform" is not crisp. We believe the two are more alike than different, and we consider them together. The data center hardware and software is what we will call a cloud. When a cloud is made available in a pay-as-user- go manner to the general public, we call it a public cloud; the service being sold is utility computing. The author use the term private cloudto refer to internal data centers of a business or other organization, not made available to the general public.

Ateniese – 2007 [2] says a model was created for Demonstrable Data Ownership(DDO) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically dilutes I/O prices. The client maintains a constant amount of metadata to verify the proof. The challenge/response rule carries a small, constant amount of data, which decrease network communication. Thus, the DDO model for remote data checking supports large data sets in widely-distributed storage systems.

III. THE PROPOSED SCHEMES

As data owners no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading the data for its integrity verification is not a practical solution due to the high cost of input/output (I/O) and transmission across the network. Besides, it is often insufficient to detect data corruption only when accessing the data, as it does not give correctness assurance for un accessed data and might be too late to recover the data loss or damage. Considering the large size of the outsourced data and the owner's constrained resource capability, the tasks of auditing the data correctness in a cloud environment can be formidable and expensive for data owners.

1. The public Demonstrable Data Ownership(DDO),which is a cryptographic technique for verifying the integrity of data without retrieving it at an untrusted server; can be used to realize audit services.
2. Random mask technique is used to achieve a privacy-preserving public auditing system for cloud data storage security to support efficient handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multi-user setting.

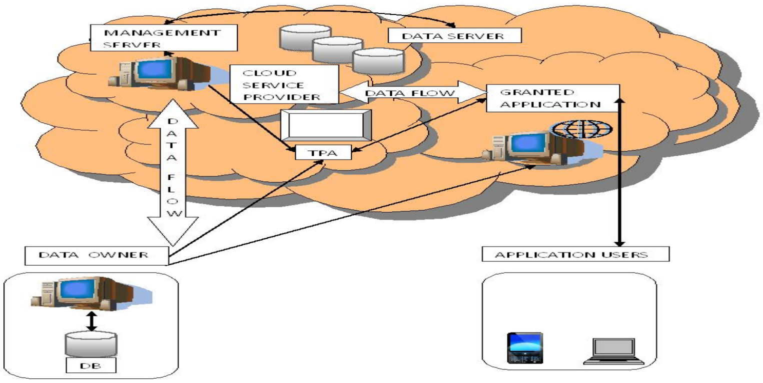


Figure 1 Architecture Diagram

3.1 Data Owner (DO)

Has a large amount of data to be stored. First owner can register in to application and then login. After Login the Owner Main Page is viewed, owner can browse the files in the extension (.txt,.java,.htm,.html,.xml) as a multiselection. Then owner can upload the file to server. Before uploading the file to server upload to TPA. TPA is generate an MAC address and security code for the files individually and sends back to Owner.

3.2 Cloud Service Provider (CSP)

Provides data storage service and have enough storage spaces and computation resources. The Data will be stored in the form of Owner Name, IP Address, Port number, file path, MAC Address and security code.

In Cloud Server There is a possibility for deleting the owner data without the owner knowledge.

3.3 Third Party Auditor (TPA)

Have capabilities to manage or monitor outsourced data under the delegation of data owner. If the file is deleted in Cloud Server information will be passed to TPA without the knowledge of Cloud Server. Mentioning this particular file is deleted or corrupted. Keeping this information TPA uploads a deleted copy of file to Cloud Server. Now Data Owner is worry free.

3.4 Granted Applications (GA)

The Data user after logging in to application can enter the owner name and port and request a file. If this request is accepted then owner is granted permission to access the files. Then list of files of the particular owner will be displayed with MAC and security code. Then Data user can enter the file name and security code and make a request to cloud server. The cloud Server verifies the MAC and then stores the files in the user's computer.

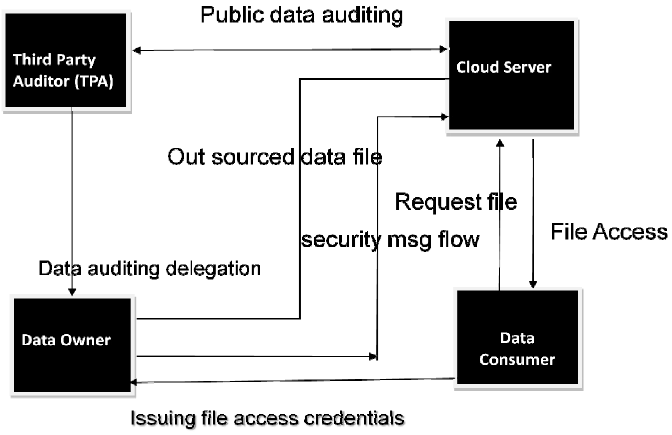
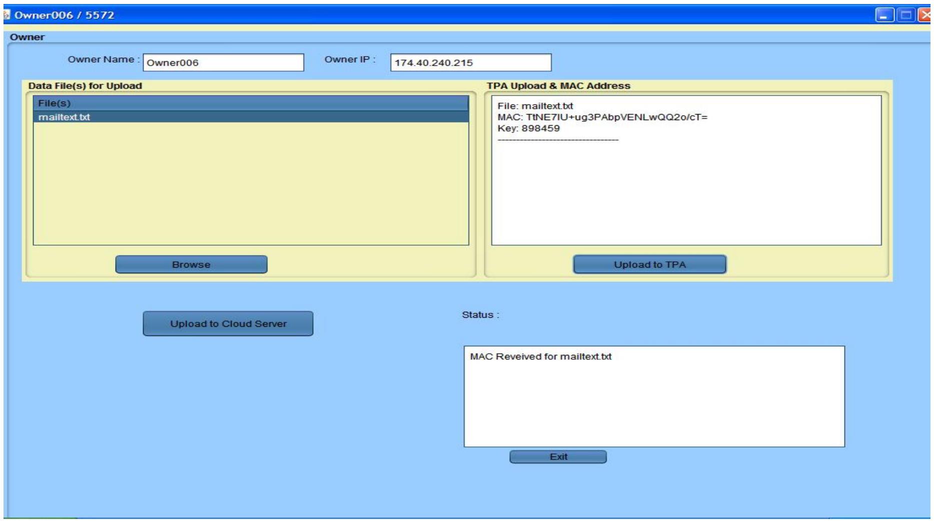


Figure 2 System Process

IV. SYSTEM IMPLEMENTATION

The project isimplemented with JAVA, Swing (JFC) as front end and the connectivity JDBC is used to connect the back end MS Access, the tool used for implementation is My Eclipse.The Data Owner after the registration can browse the files in the extension (.txt,.java,.htm,.html,.xml) and can also perform multi selection. Then the owner can upload the file to server. Before uploading the file to server the file is uploading to TPA. TPA will generate a MAC address and security code for the files individually and sends back to Owner. The data will be stored in the form of Owner Name, IP Address, port number, file path, MAC Address and security code in the Cloud Server. The cloud server lists out the details present in the data owner module and the user request and response module.


Owner006 / 5572

Owner

Owner Name : Owner006
Owner IP : 174.40.240.215

Data File(s) for Upload

File(s)
mailtext.txt

TPA Upload & MAC Address

```
File: mailtext.txt
MAC: TtNE7IU+ug3PAbpVENLwQQ2o/cT=
Key: 898459
-----------------------------------
```

Status :

MAC Reveived for mailtext.txt

Figure 3 MAC address verified by Data Owner

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

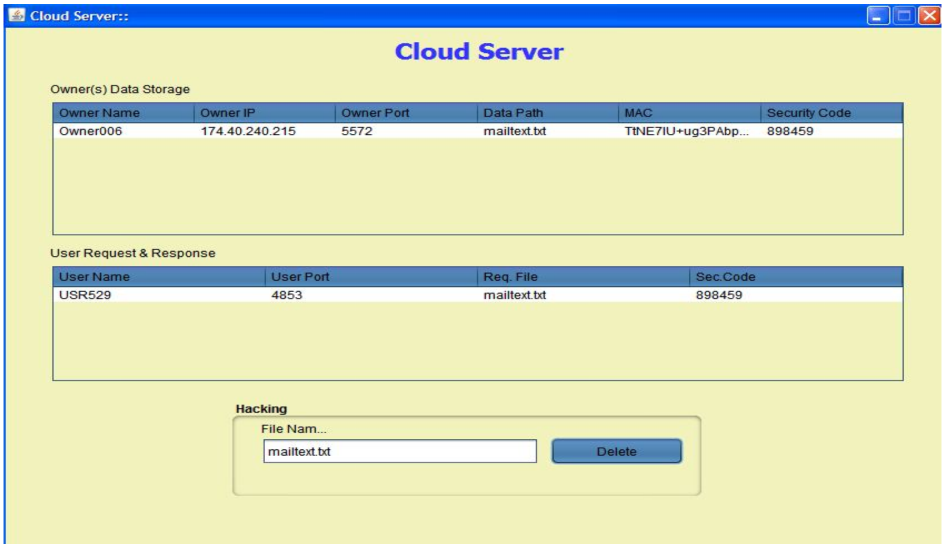
International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014



Cloud Server::

Cloud Server

Owner(s) Data Storage

Owner Name	Owner IP	Owner Port	Data Path	MAC	Security Code
Owner006	174.40.240.215	5572	mailtext.txt	TtNE7IU+ug3PAbp...	898459

User Request & Response

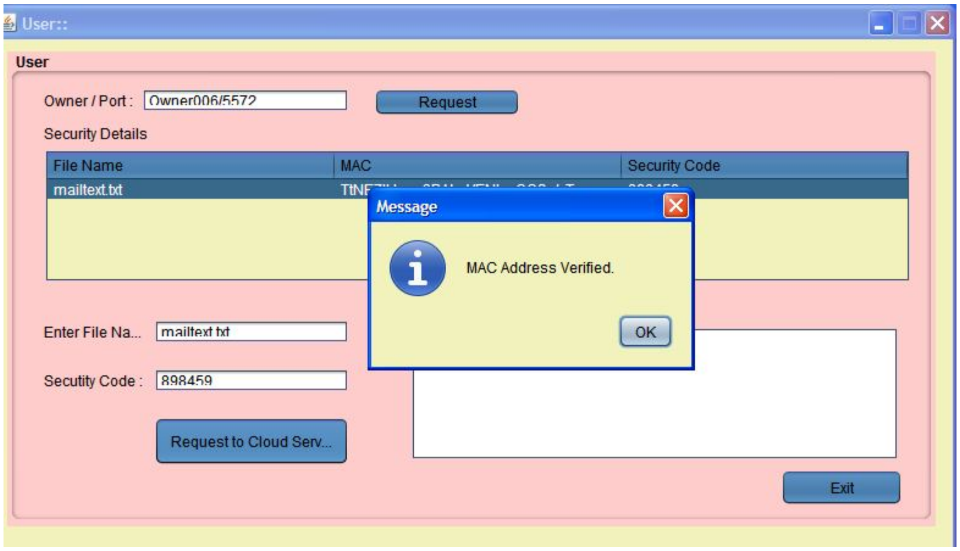
User Name	User Port	Req. File	Sec.Code
USR529	4853	mailtext.txt	898459

Hacking

File Nam... mailtext.txt

Figure 4 File Deleted in Cloud Server

Have capabilities to manage or monitor outsourced data under the delegation of data owner. If the file is deleted in Cloud Server information will be passed to TPA without the knowledge of Cloud Server. Mentioning this particular file is deleted or corrupted. Keeping this information TPA uploads a deleted copy of file to Cloud Server. Now Data Owner is worry free. The TPA uploads a deleted copy of file to Cloud Server. If the request is accepted then owner is granted permission to access the files. Then list of files of the particular owner will be displayed with MAC and security code.



User::

User

Owner / Port : Owner006/5572

Security Details

File Name	MAC	Security Code
mailtext.txt	TtNE	898459

Message

MAC Address Verified.

Enter File Na... mailtext.txt

Secutity Code : 898459

Figure 5 MAC Received

Then Data user can enter the file name and security code and make a request to cloud server. The cloud Server verifies the MAC and then stores the files in the user's computer. The user can now view the files in his folder created for him in his own PC.The requested file name and security code given by the user is successfully verified by the cloud server.

V. CONCLUSION

The construction of an efficient audit service for data integrity in clouds. In this audit service, the third party auditor, known as an agent of data owners, can issue a periodic verification to monitor the change of outsourced data by providing an optimized schedule. As data and information will be shared with a third party, cloud computing users want to avoid an untrusted cloud provider protects private and important information from attackers or malicious insiders. The migration from a single cloud to a multi-cloudenvironment and the use of special Audit protocolfor key generation is examined. It also overcomes the security issues, data availability failure, data integration and data intrusion. It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. The purpose of this work is to survey the recent research on single clouds and multi-clouds to address the security risks and solutions.

REFERENCES

[1] Armbrust, M . Fox, A. Griffith, R. Joseph, A.D , Katz, R.H. Konwinski, "View of Cloud Computing Communication", Proceedings of ACM Conference on Computer and Communications Security vol.53, no.4, pp.50–58, 2010.

[2] Ateniese, G , Burns, R.C , Curtmola, R . Herring, J.Kissner, L. Peterson, Z.N.J., "Provable data possession at untrusted stores", Proceedings of The ACMConference on Computer and Communications Security , pp. 598–609, 2007.

[3] Ateniese, G., Pietro, R. D , Mancini, L. V , Tsudik, G. "Scalable and efficient provable data possession", Proceedings of the 4th International Conference on Security and Privacy in Communication Networks, Secure Communication , pp.1–10,2008.

[4] Bowers, K.D. Juels, A. Oprea, "Hail: a high-availability and integrity layer for cloud storage", Proceedings of the ACM Conference on Computer and Communications Security, pp. 187–198,2009.

[5] Erway, C. A. Papamanthou, C. Tamassia, R. "Dynami provable data possession", Proceedings of the ACM Conference on Computer and Communications Security, pp. 213–222,2009.

[6] Pearson, R. K .L. Lee, "Towards achieving accountability, auditability and trust in cloud computing" , Proceedings of Advances in Computing and Communications in Computer and Information Science, pp. 432 – 444, 2011.

[7] Wang, C. Wang, Q. Ren, K. Lou, "Privacy - preserving public auditing for data storage security in cloud computing", Proceedings of INFOCOM, IEEE, vol. 193, pp. 14-19,2010.

[9] Xie, M. Wang, H. Yin, J. Meng, X. "Integrity auditing of outsourced data"Proceedings of the ACM Conference on Computer and Communications Security pp. 782–793,2007.

[10] Yan Zhua,b.HongxinHuc,Gail-JoonAhnc, Ganti Stephen S.Yauc"Efficient Audit service outsourcing for verifying data integrity in clouds"The Journal of Systems and Software vol. 85, pp.1083– 1095,2012.

[11] Tchifilionova, V. "Security and privacy implications of cloud computing Lost in the cloud", Proceedings of the Open Research Problems in Network Security of Lecture Notes in Computer Science. vol.6555pp. 149–158,2012.

[12] H.Waters," Compact proofs of retrievability", Proceedings of Advances in Cryptology – ASIACRY, , 14th International Conference on the Theory and Application of Cryptology and Information Security, pp. 90–107, 2008.