ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

Audit Service by Using TPA for Checking Data Integrity in Cloud System

Jagtap V. V., Aher S.M.,

M Tech Computer Science & Engineering & Asst. Professor, Vishwbharti Academy's College of Engineering, Ahmednagar/Pune University,Maharashtra,India.

M E Computer Science & Engineering & Asst.Professor, Vishwbharti Academy's College of Engineering, Ahmednagar/ Pune University, Maharashtra, India.

Abstract— Cloud computing is the vast computing utility, where users can remotely store their data into the cloud so to have the benefit of the on-demand availability of huge and different applications and services from a shared pool of configurable computing resources.Cloud-based outsourced storage space reduces the patron load of storage management. It also reduces the maintenance load of customer by providing a comparably low-cost, scalable, location-independent platform.This new model of data hosting service commence a new security challenges, which requires an independent auditing service which audit the data integrity of cloud. There are different existing auditing services available in cloud which audit data integrity remotely in static motion but these are not applicable whenever data is dynamically updated in cloud. Since it require efficient and secure dynamic auditing method for data owner. However in cloud, the clients no have direct physical possession of data. It shows client faces different formidable risk like missing or corruption of data. To keep away from the security and integrity risk of data, audit services are essential to ensure the integrity and availability of outsourced data and to achieve digital forensics and credibility on cloud computing.Provable data possession (PDP), 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. In this paper, profiting from the interactive proof system, we address the construction of an interactive PDP protocol to prevent the fraudulence of prove (soundness property) and the leakage of verified data (zero-knowledge property).

Keywords:Data integrity, Storage auditing, dynamic auditing, privacy-preserving auditing, cloud computing, zero knowledge.

I.INTRODUCTION

In recent years, the emerging cloud-computing is rapidly gaining thrust as an alternative to traditional computing system. 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. But By seeing the popularities of cloud computing services, it's fast development and advance technologies anyone can voted it as a future of computing world. Cloud stores the information that is locally stores in the computer, it contains spreadsheets, presentations, audio, photos, word processing documents, videos, records, photos. But for sensitive and confidential data there should be some security mechanism, so as to provide protection for private data .Conventionally, client can verify the data integrity based on two-party storage auditing protocols. But it is inefficient for auditing, because no one can give (i.e. client or cloud service provider) assurance to provide balance auditing.Therefore third-party auditing (TPA) is play important role for the storage auditing in cloud computing. It is very convenient for both side i.e. owner side and cloud service provider side.

One fundamental aspect of this paradigm shifting is that data are being centralized and outsourced into clouds. This kind of outsourced storage services in clouds have become a new profit growth point by providing a comparably low-cost, scalable, location-independent platform for managing clients' data.

The cloud storage service (CSS) relieves the burden of storage management and maintenance. However, if such an important service is susceptible to attacks or failures, it would bring irretrievable losses to users since their data or archives are stored into an uncertain storage pool outside the enterprises. These security risks come from the following reasons: the cloud infrastructures are much more powerful and reliable than personal computing devices. However, they are still susceptible to security threats both from outside and inside the cloud for the benefits of their possession,

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

there exist various motivations for cloud service providers (CSP) to behave unfaithfully toward the cloud users furthermore, the dispute occasionally suffers from the lack of trust on CSP .
Consequently, their behaviors may not be known by the cloud users, even if this dispute may result from the users' own improper operations. Therefore, it is necessary for cloud service providers to offer an efficient audit service to check the integrity and availability of the stored data. Traditional cryptographic technologies for data integrity and availability, based on hash functions and signature scheme, cannot work on the outsourced data without a local copy of data.
In addition, it is not a practical solution for data validation by downloading them due to the expensive transaction, especially for large-size files. Moreover, the solutions to audit the correctness of the data in a cloud environment can be formidable and expensive for the cloud users .
Therefore, it is crucial to realize public audit ability for CSS, so that data owners may resort to a third party auditor (TPA), who has expertise and capabilities that a common user does not have, for periodically auditing the outsourced data. This audit service is significantly important for digital forensics and data assurance in clouds.

II. EXISTING SYSTEM AND CHALLENGES

Ateniese et al. are the first to consider public audit ability in their "provable data possession" (PDP) model for ensuring possession of data files on untrusted storages. They utilize the RSA-based homomorphism linear authenticators for auditing outsourced data and suggest randomly sampling a few blocks of the file. However, among their two proposed schemes, the one with public audit ability exposes the linear combination of sampled blocks to external auditor. When used directly, their protocol is not provablyprivacy preserving, and thus may leak user data information to the external auditor.

III.PROPOSED SYSTEM AND IMPLEMENTATION

In this paper, we utilize the public Provable data possession (PDP), which is a cryptographic technique for verifying the integrity of data without retrieving it at an un trusted server; can be used to realize audit services. It with random masktechnique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind.
To support efficient Handling of multiple auditing tasks, we further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing tasks simultaneously. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We also show how to extent our main scheme to support batch auditing for TPA upon delegations from multi-users. We are integrating following modules in our proposed system.
Modules:
1.Audit Service System
2.Data Storage Service System
3.Audit Outsourcing Service System
4.Secure and Performance Analysis

1. Audit Service System:

In this module we provide an efficient and secure cryptographic interactive audit scheme for public audit ability. We provide an efficient and secure cryptographic interactive retains the soundness property and zero-knowledge property of proof systems. These two properties ensure that our scheme can not only prevent the deception and forgery of cloud storage providers, but also prevent the leakage of outsourced data in the process of verification.

2. Data Storage Service System:

In this module, we considered FOUR entities to store the data in secure manner:
1. Data owner (DO):
Who has a large amount of data to be stored in the cloud.
2. Cloud service provider (CSP):
Who provides data storage service and has enough storage spaces and computation resources.
3. Third party auditor (TPA):
Who has capabilities to manage or monitor – outsour ced data under the delegation of data owner.
4. Granted applications (GA):

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

Who have the right to access and manipulate stored data. These applications can be either inside clouds or outside clouds according to the specific requirements.

3. Audit Outsourcing Service System:

In this module the client (data owner) uses the secret key to preprocess the file, which consists of a collection of blocks, generates a set of public verification information that is stored in TPA, transmits the file and some verification tags to Cloud service provider CSP, and may delete its local copy.

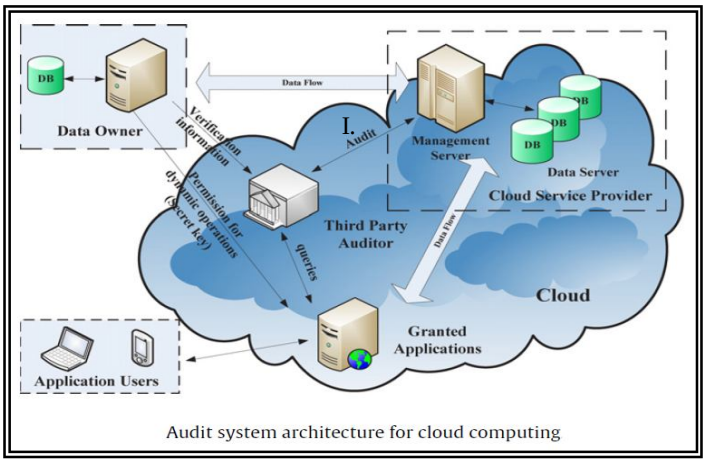
At a later time, using a protocol of proof of retrievability, TPA (as an audit agent of clients) issues a challenge to audit (or check) the integrity and availability of the outsourced data in terms of the public verification information. It is necessary to give an alarm for abnormal events.

4. Secure and Performance Analysis:

In this module, we considered to secure the data and give performance to the following:

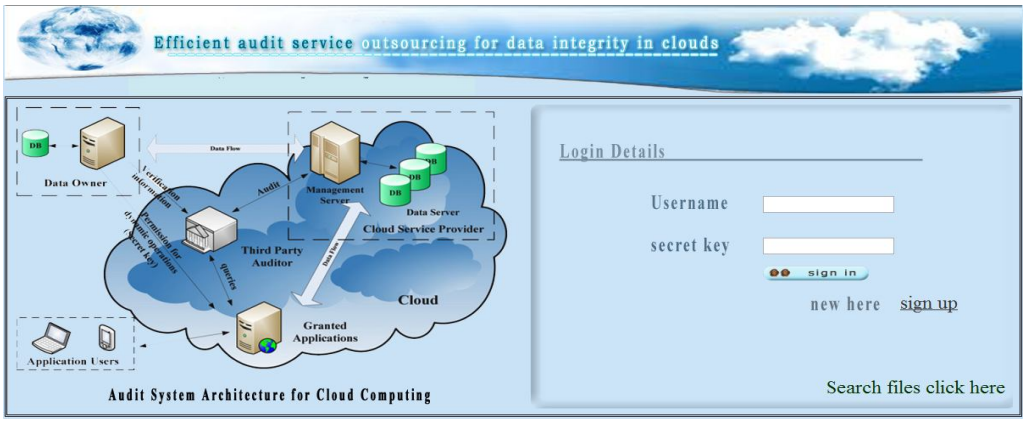
Audit-without-downloading:

To allow TPA (or other clients with the help of TPA) to verify the correctness of cloud data on demand.



Audit system architecture for cloud computing

IV.How The Proposed system Works:



I.User login page

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

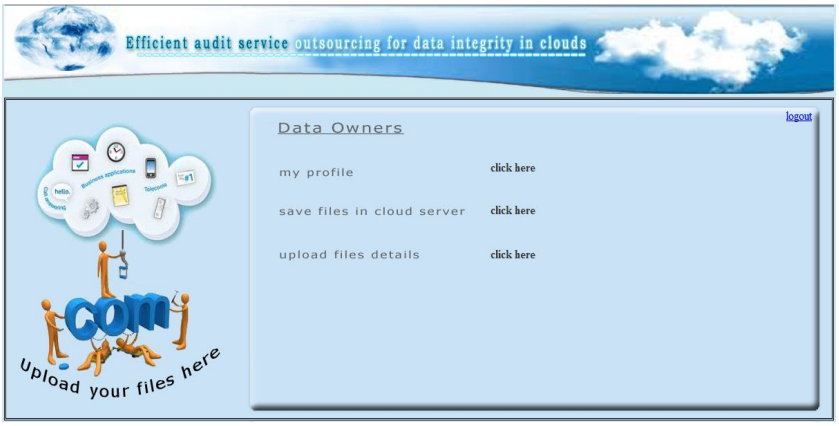
An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

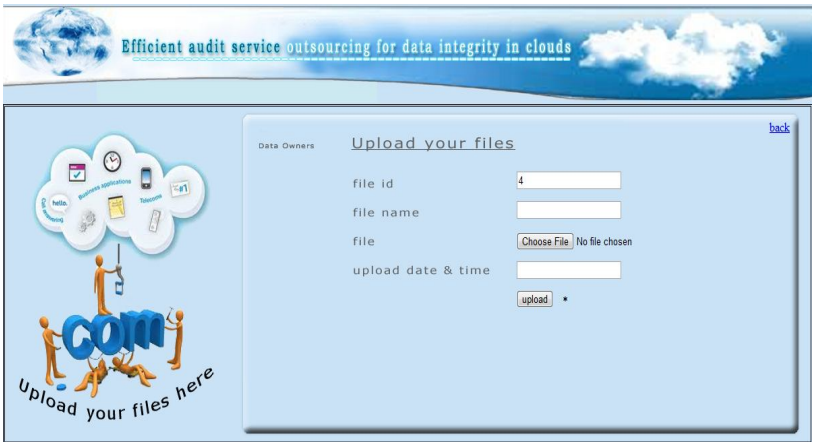
On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

II.User registration page



III.Data owner details



IV. Upload file

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

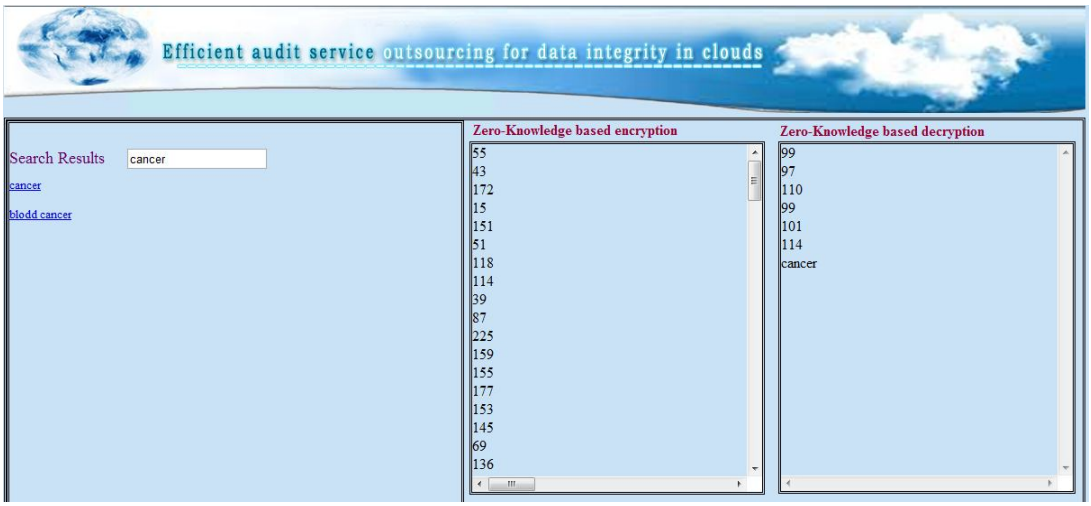
International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

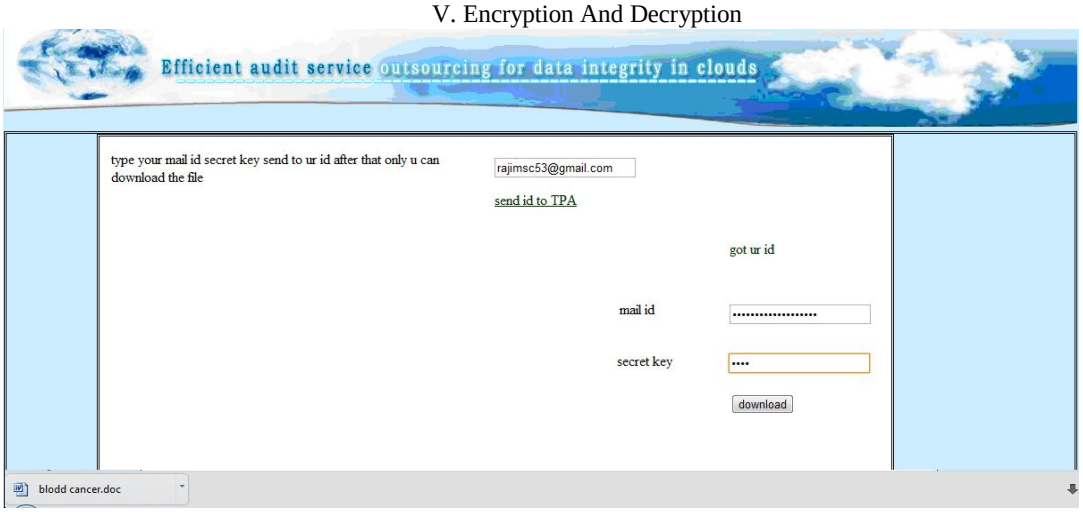
Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India



V. Encryption And Decryption



VI. Download file

IV. Conclusion

.

In this paper, we addressed the construction of an efficient audit service for data integrity in clouds. Profiting from the standard interactive proof system, we proposed an interactive audit protocol to implement the audit service based on a third party auditor. 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. To realize the audit model, we only need to maintain the security of the third party auditor and deploy a lightweight daemon to execute the verification protocol.

Hence, our technology can be easily adopted in a cloud computing environment to replace the traditional Hash-based solution. More importantly, we proposed and quantified a new audit approach based on probabilistic queries and periodic verification, as well as an optimization method of parameters of cloud audit services. This approach greatly

ISSN (Online) : 2319 – 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 3, Special Issue 4, April 2014

Two days National Conference – VISHWATECH 2014

On 21st & 22nd February, Organized by

Department of CIVIL, CE, ETC, MECHNICAL, MECHNICAL SAND, IT Engg. Of Vishwabharati Academy's College of engineering, Ahmednagar, Maharastra, India

reduces the workload on the storage servers, while still achieves the detection of servers' misbehaviour with a high probability. Our experiments clearly showed that our approach could minimize computation and communication overheads.

ACKNOWLEDGMENT

This paper is completed only because of the support from each and everyone of computer department faculties, colleagues,friends,and my students.

REFERENCES

[1]Yan Zhua,b, Hongxin Huc, Gail-Joon Ahnc, Stephen S. Yauc. "Efficient audit service outsourcing for data integ rity in clouds". In "The Journal of Systems and Software 85 (2012) 1083 – 1095".
[2]M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "A View of Cloud Computing," Comm. ACM, vo l. 53, no. 4,51,Secure Audit Service by Using TPA for Data Integrity in Cloud Systempp.50-58, 2010.
[3]T. Velte, A. Velte, and R. Elsenpeter, Cloud Computing: A Practical Approach, first ed., ch. 7. McGraw-Hill, 2010.
[4]A. Juels and B.S. Kaliski Jr., "PORs: Proofs o f Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Com m. Security (CCS '07), pp. 584-597, Oct. 2007.
[5]G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Se curity (CCS '07), pp. 598-609, Oct. 2007.
[6]M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, "Auditing to Keep Online Storage Services Honest," Proc. 11th US ENIX Workshop Hot Topics in Operating Systems (HotOS '07), pp. 1-6, 2007.
[7]G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Se curity (CCS '07), pp. 598-609, 2007.
[8]M.A. Shah, R. Swaminathan, and M. Baker, "Priv acy-Preserving Audit and Extraction of Digital Contents," Cryptolo gy ePrint Archive, Report 2008/186, 2008.
[9]A. Juels and J. Burton, S. Kaliski, "PORs: Pro ofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Se curity (CCS '07), pp. 584-597, Oct. 2007.

BIOGRAPHY

Author 1:Mrs. Jagtap V V ,M TECH Computer Science & Engineering, Asst.Professor, Vishwbharti Academy College of Engineering, Ahmednagar, currently working as a Asst professor in same college,I has 9-year experience.

Author2:Mrs. Aher S M , M E Computer Engineering ,Asst.Professor, Vishwbharti Academy College of Engineering, Ahmednagar ,currently working as a asst professor in same college,I has 5-year experience.