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

Key Generation for Outsourced Storages in Clouds

Sandeep.S[1], Vijayakumar.P[2], Anand.V[3]

M.Tech Student, Department of IT, Student IEEE Member, V.S.B Engineering College, Karur, Tamilnadu, India[1, 2]

H.O.D, Department of IT, V.S.B Engineering College, Karur, Tamilnadu, India[3]

ABSTRACT: In this paper we proposed a key generation and third party audit algorithm for verifying the integrity of untrusted and outsourced storage in cloud. Our audit service is developed according to these techniques, splitting and merging, random sampling, dynamic auditing, and index hash table, supporting provable updates to outsourced data and timely anomaly detection. In addition to that we proposed a method based on periodic verification for improving the audit service performance. Our experimental results not only validating the effectiveness approaches, but also show our audit system verifies the integrity with lower computation overhead and also requiring less storage for audit meta data.

KEYWORDS: Storage security, provable data possession, audit service, cloud storage

I. INTRODUCTION

Cloud computing has led to a shift in how people think about IT systems architecture. Many organizations today are either implementing cloud-based solutions, or evaluating which cloud-based solutions they will be implementing in the future. According to Gartner Inc. cloud computing is "no less influential than e-business". This shift in architecture from an enterprise-based traditional server-based system to a cloud-based system will have associated costs of entry and risks, but it can result in enormous benefits in savings and in IT and business agility.

While there is considerable pressure on organizations to consider moving to the cloud-based services, security issues continue to be one of the largest concerns that organizations have about this move. The different cloud-based deployment models, including private, public or hybrid cloud, bring with them a range of challenges, and security concerns cut across them all. Many organizations will need to apply best practice security standards that are far in excess of those that they currently implement with their on-premise systems. The migration or adoption of cloud services then can provide an advantage in that firms can design, from the ground up, their new cloud-based infrastructures with security "baked-in"; this is in contrast to the piecemeal and "after the fact" or "bolted-on" nature of security seen in most data centers today.

The cloud service model that an organization wants to implement influences security design and implementation. We will cover the three cloud computing service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). These models all have different security issues that need to be considered and more importantly, a determination of the balance of responsibilities between the customer and the cloud provider for each of the service models also needs to be made.

Data storage in the cloud also requires particular consideration. The regulatory environment within which many industries operate may generate particular issues with cloud-based data storage, such as legislation on data access, issues with where the data is stored and used, as well as the important issues around the management of cryptographic keys. Strong cryptographic protection and encryption of any stored data is essential, whether that information is at rest or in transit. This becomes even more important when considering the issue of data storage in jurisdictions where data privacy laws differ from that of the firm's host country. Cloud-based systems introduce new challenges in authentication and authorization, as organizations must be able to identify users with confidence without generating excessive overhead related to account provisioning. Authorization decisions must be well-defined and very granular, particularly in multi-tenant environments.

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

The relationship between customer and Cloud Service Provider (CSP) must also be explicitly stated in relation to who has administrative rights and consequent access to privileged customer information. Operational frameworks such as IT Infrastructure Library (ITIL) and Microsoft Operations Framework (MOF) help provide an effective project structure when architecting cloud-based solutions to business problems and scenarios. The cloud environment also provides the opportunity to redefine the monitoring and reporting environment and enable real-time access to management data to the right individuals through customized dashboards.Finally; we reviewed the effects of compliance on cloud-based operations and analyze the effects that regulatory compliance has on the options available to organizations that operate within those environments. We will look at the factors that the cloud security architect may need to consider and mechanisms for mitigating.

Service Models:

Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user- specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming .The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Essential Characteristics of cloud computing:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly Out ward and in ward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimize resource use by leveraging a metering capability 1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user Accounts).

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

Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Deployment Models
Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.
Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

II. OBJECTIVES

An aim of this project is to securely we can upload our files into the server using generation of secret keys. And also we can able to do all the dynamic operation for our files. When you are downloading your files that should be ask that secret key for your downloading file. if your giving correct key then only you can able to do all the modification. This is only aim of our services in cloud.

Algorithm used:-

- AES algorithm with periodic verification.
- File Splitting algorithm.
- Merging Algorithm.

Existing work:-
In Existing System remotely stored data might be not accessed by the clients to do a dynamic operation, for instance, through block operations such as modification, deletion and insertion. However, these operations may raise security issues in most of existing schemes. And also we cant create any secret key for uploading files.
Disadvantages:-

- No secret key.
- Very less security.
- Cloud service provider can able access the data.

III. PROPOSED WORK

In our scheme, each client holds a secret key, which can be used to generate the tags of many files. Each processed file produces a public verification parameter. Using that secret key only the client can do upload and download operation. And we are implementing probabilistic query and periodic verification for improving the performance of audit services. We shown our audit system verifies the integrity with lower computation overhead and requiring less extra storage for audit meta data. The strict audit and supervision for outsourced data, and offer efficient evidences for anomalies.
Advantages in new system:

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

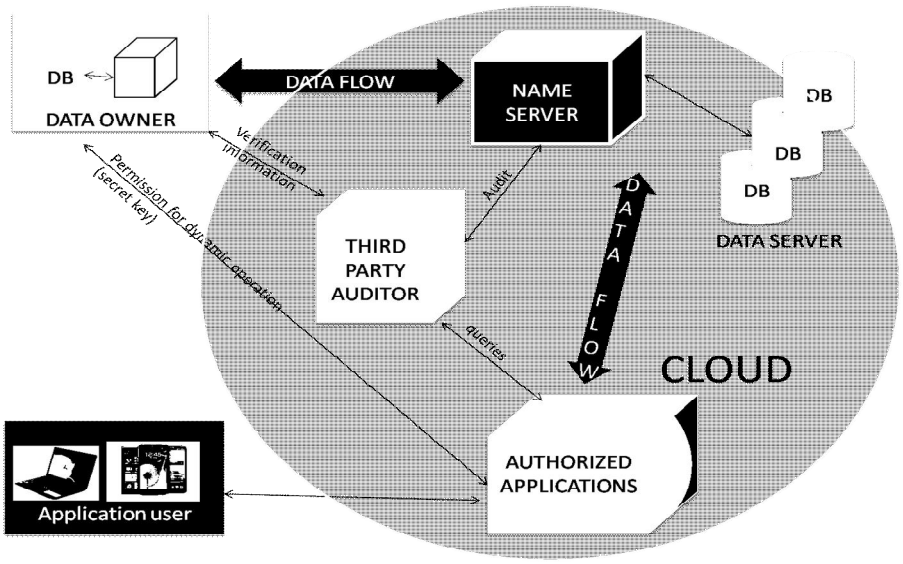
Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

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

- Secret key generation
- Securely uploaded files.
- Avoid anomalies
- Authorized user can able to do dynamic operations.

IV. SYSTEM ARCHITECTURE



Splitting and uploading files:-

File splitting is an approach to protecting sensitive data from unauthorized access by encrypting the data and storing different portions of a file on different servers.

When split data is accessed, the parts are retrieved, combined and decrypted. An unauthorized person would need to know the locations of the servers containing the parts, be able to get access to each server, know what data to combine, and how to decrypt it.

1) Tag generation:
The client (data owner) uses a secret key sk to pre-process a file, which consists of a collection of n blocks, generates a set of public verification parameters (PVP) and index-hash table (IHT) that are stored in TPA, transmits the file and some verification tags to Admin, and may delete its local copy (see Fig).

Fragment Structure and Secure Tags:
To maximize the storage efficiency and audit performance, our audit system introduces a general fragment structure for outsourced storages . We can use tags and corresponding data to construct a response in terms of the TPA's challenges in the verification protocol, such that this response can be verified without raw data. If a tag is unforgettable by anyone except the original signer, we call it a secure tag.

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

Although this fragment structure is simple and straightforward, but the file is split into n × s sectors and each block (s sectors) corresponds to a tag, so that the storage of signature tags can be reduced with the increase of s. Hence, this structure can reduce the extra storage for tags and improve the audit performance. There exist some schemes for the convergence of s blocks to generate a secure signature tag.

2) Periodic sampling audit:
By using an interactive proof protocol of irretrievability, TPA (or other applications) issues a "Random Sampling" challenge to audit the integrity and availability of the outsourced data in terms of verification information (involving PVP and IHT) stored in TPA (see Fig)
The ultimate goal of this audit infrastructure is to enhance the credibility of cloud storage services, but not to increase data owner's burden. Therefore, TPA should be constructed in clouds and maintained by a CSP. In order to ensure the trust and security, TPA must be secure enough to resist malicious attacks, and it should be strictly controlled to prevent unauthorized accesses even for internal members in clouds. A more practical way is that TPA in clouds should be mandated by a trusted third party (TTP).

In contrast with "whole" checking, random "sampling" checking greatly reduces the workload of audit services, while still achieves an effective detection of misbehaviors. Thus, a probabilistic audit on sampling checking is preferable to realize the anomaly detection in a timely manner, as well as to rationally allocate resources.
Since the single sampling checking may overlook a small number of data abnormalities, we propose a periodic sampling approach to audit outsourced data, which is named as Periodic Sampling Audit. With this approach, the audit activities are efficiently scheduled in an audit period, and a TPA merely needs to access small portions of files to perform audit in each activity. Therefore, this method can detect exceptions periodically, and reduce the sampling numbers in each audit.

Merging Files:-
Merging all split-ted files into single file.
All the files should be combined together. And get original files and then you can do all the dynamic operations and save it.

3) Audit for Dynamic Operations:
An authorized application, which holds a data owner's secret key sk, can manipulate the outsourced data and update the associated IHT stored in TPA.

4) Index-Hash Table:
In order to support dynamic data operations, we introduce a simple index-hash table to record the changes of file blocks, as well as generate the hash value of each block in the verification process. The structure of our index-hash table is similar to that of file block allocation table in file systems.
Although the index-hash table may increase the complexity of an audit system, it provides a higher assurance to monitor the behavior of an untrusted CSP, as well as valuable evidence for computer forensics, due to the reason that anyone cannot forge the valid without the secret key.
In practical applications, this architecture can be constructed into a virtualization infrastructure of cloud-based storage service .
Fig. An example of hash index hierarchy in Hadoop distributed file system (HDFS). In Fig. 4, we show an example of Hadoop distributed file system (HDFS) 2, which is a distributed, scalable, and portable file system.

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

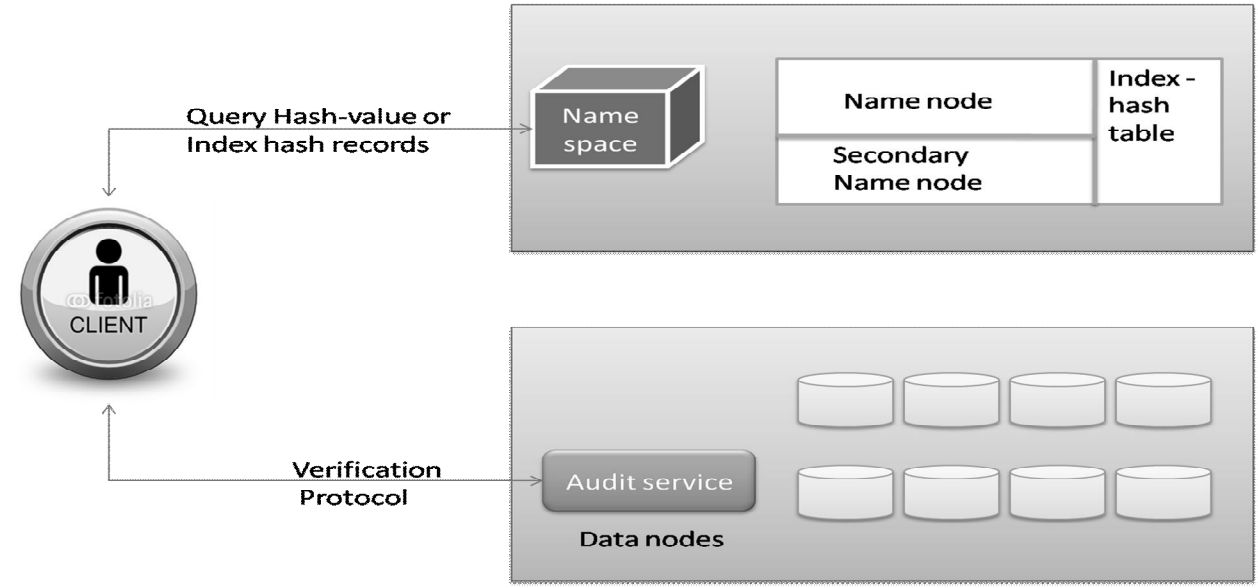
International Journal of Innovative Research in Computer and Communication Engineering

(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



HDFS' architecture is composed of Name Node and Data Node, where Name Node maps a file name to a set of indexes of blocks and Data Node indeed stores data blocks. To support dynamic audit, the index-hash table and the metadata of Name Node should be integrated together to provide an enquiry service for the hash value Based on these hash values, the clients or TPA can implement a verification protocol via audit services. Hence, it is easy to replace the common checksum algorithm with our scheme for anomaly detection without downloading data in current HDFS.

V. CONCLUSIONS

In this paper, we presented a construction of dynamic audit services for untrusted and outsourced storages. We also presented an efficient method for periodic sampling audit to enhance the performance of TPAs and storage service providers. Our experiments showed that our solution has a small, constant amount of overhead, which minimizes computation and communication costs. In future we can upgrade the techniques for splitting and merging algorithms. Then want to improve some third party auditor concept for secure outsourcing in cloud.

REFERENCES

[1] Amazon W eb Services, "Amazon S3 Availability Event: July 20, 2008," h ttp://st atus.aws.amazo n.com/s3-2008 0720.html, J uly 2008.
[2] A. Juels and B.S. Kaliski Jr., "PORs: Proofs of Retrievability for Larg e Fil es," Pr oc. ACM Conf . C o mpute r and Commu nic atio ns Security (CCS '07), pp. 584-597, 2007.
[3] M. Mowbray, "The Fog over the Grimpen Mire: Cloud Computing and the Law," Technical Report HPL-2009-99, HP Lab., 2009.
[4] A.A. Yavuz and P. Ning, "BAF: An Efficient Publicly Verifiable Secure Audit Logging Scheme for Distributed Systems," Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 219-228, 2009.
[5] G. Ateniese, R.C. Burns, R. Curtmola, J. Herring, L. Kissner, Z.N.J. Peterson, and D.X. Song, "Provable Data Possession at Untrusted Stores," Proc. 14th ACM Conf. Computer and Comm. Security, pp. 598-609, 2007.
[6] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, "Scalable and Efficient Provable Data Possession," Proc. Fourth Int'l Conf. Security and Privacy in Comm. Netowrks (SecureComm), pp. 1-10, 2008.
[7] B. Sotomayor, R.S. Montero, I.M. Llorente, and I.T. Foster, "Virtual Infrastructure Management in Private and Hybrid Clouds," IEEE Internet Computing, vol. 13, no. 5, pp. 14-22, Sept./Oct. 2009.

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

Mr.S.Sandeep Pursing the M.Tech (IT) in V.S.B Engineering College . He has received B.Tech(IT) degree from Angel College of Engineering and Technology. He has total number of 3 publications, 1 paper in International conference and 2 papers in national conferences and participated in various symposiums and workshops held at different places. His area of interest includes Security, Game development and Web Designing. Mailid: sssandeep34@gmail.com
PH: +91 7708843038

Mr.P.Vijayakumar Pursing the M.Tech (IT) in V.S.B Engineering College . He has received B.E (CSE) degree from Angel College of Engineering and Technology. He has total number of 4 publications, 1 paper in International conference and 3 papers in national conferences and participated in various symposiums and workshops held at different places. His area of interest includes Networking and Web Designing. Mailid: vijay248kumar@gmail.com

Mr.V.Anand has received M.Tech (IT) in Manonmanium Sundranar University. He is Currently working as Head of the Department of Information Technology in V.S.B Engineering College and he research Currently doing his Ph.D in Image mining. And his areas are Finger print, Image processing, Data mining and soft computing. He presented a paper in an International, National conference and attended workshops in various colleges. Mailid : itsanandmtech@gmail.com
Ph: +91 9442580690