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. 3, Issue 5, May 2015

Achieving Remote Data Integrity Verification and Eradicating Semihonest Attack in Multicloud Storage

P.Shanmugapriya[1], C.Kavitha[2]

P.G Scholar, Department of CSE, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Salem (Dt), India[1]

Assistant Professor, Department of CSE, Sri Shanmugha College of Engineering and Technology, Pullipalayam, Salem (Dt), India[2]

ABSTRACT: Data Storage outsourcing in cloud computing is a rising trend which prompts a number of interesting security issues. Provable data possession (PDP) is a method for ensuring the integrity of data in storage outsourcing. Remote integrity checking is crucial in cloud storage, here using multi cloud. It can help the clients to check their whole outsourced data by without downloading. This research addresses the construction of efficient PDP which called as RSA Based-PDP (RSA-PDP) mechanism for distributed cloud storage to support data migration and scalability of service. Uploading data are stored in different blocks in multicloud. The generation of tags with the length irrelevant to the size of data blocks. To reduce the memory space by using variable length block verification based on hashing algorithm. Cloud service provider is semi honest server so attacker can easily attack data. Here the data are secured from datamining attacker.

KEYWORDS: Multicloud, provable data possession, remote data integrity verification,variable length block, semi honest attack.

I. INTRODUCTION

Over the last years, cloud computing has develop an important theme in the computer field. Basically, it takes the data handling as a provision, such as storing, computing. It relieves of the load for storage management, universal data entree with independent geographical locations. Identically, it avoids of capital payments on hardware, software, and personnel maintenances, etc. Thus, cloud computing draws more intent from the enterprise. The foundations of cloud computing invention in the outsourcing of computing tasks to the third party. It needs the safety risks in terms of privacy, honesty and availability of data and service.

The issue to satisfy the cloud clients that their data are kept intact is especially dynamic since the clients do not store these data locally. Remote data integrity checking is an original to address this issue. For the common case, when the client stores his data on multicloud servers, the distributed storage and integrity checking are necessary. By the next side, the integrity checking protocol necessity be efficient in order to make it apposite for capacity limited end devices. Thus, created on distributed computation, this will study distributed remote data integrity checking model and present the corresponding concrete protocol in multicloud storage.

A. Motivation

It consider an ocean information service corporation Corin the cloud computing environment. Corcan offer the following services: ocean measurement data, ocean environment monitoring data, hydrological data, marine biological data, GIS information, etc. Apart from the above services, Corhas also some isolated information and some open information, such as the corporation's advertisement. Corwill stock these diverse ocean data on multiple cloud servers.

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. 3, Issue 5, May 2015

Different cloud service suppliers have different reputation and charging standard. Mainly, these cloud service providers need different charges according to the different security-levels. Generally, more protected and more costly. Thus, Corwill choice different cloud service providers to store its different data. For some sensitive ocean data, it will copy these data several times and store these copies on different cloud servers. For the private data, it will store them on the private cloud server. For the public advertisement data, it will store them on the reduced public cloud server. At last, Corstores its whole data on the different cloud servers according to their importance and sensitivity.

The storage selection will take account into the Cor's profits and losses. And so, the distributed cloud storage is spirited. In multi-cloud environment, distributed provable data possession is a significant element to secure the remote data. In PKI (public key infrastructure), provable data possession protocol requirements public key certificate distribution and management. It will suffer considerable overheads since the verifier will check the certificate when it checks the remote data integrity. Additionally with the heavy certificate verification, the system too hurts from the other difficult certificates management such as certificates generation, delivery, revocation, renewals, etc. In cloud computing, maximum verifiers only have low computation capacity. Identity-based public key cryptography can eliminate the difficult certificate management. In order to increase the efficiency, RSA based provable data possession is more gorgeous. Thus, it will be very meaningful to study the RSA-DPDP.

II. RELATED WORKS

Y.Dodis, S. Vadhan , D.wichs recommend an Meta scheduling systems play a crucial role in scheduling jobs that are submitted for execution and need special attention because an increasing number of jobs are being executed using a limited number of resources. The major problem of Meta scheduling is selecting the best resources (sites) to use to execute the underlying jobs while still achieving the following objectives: reducing the mean job turnaround time, guaranteeing site load balance, and considering job priorities.

The main objectives of meta-scheduling systems. The first objective is to reduce the MJTT by considering the job type and the quantity of jobs to be submitted in each batch. The second objective is to start a workload balance among the grid sites by accurately estimating the time that each job will wait in the grid site queue. The third objective is to prioritize jobs by considering the user and system priorities.

Ning Cao ; KuiRen ; Wenjing Lou propose an searchable encryption allows data owner to outsource his data in an encrypted manner while maintaining the selectively search capability over the encrypted data. Generally, searchable encryption can be achieved in its full functionality using an oblivious RAMs [16]. Although hiding everything during the search from a malicious server (including access pattern), utilizing oblivious RAM usually brings the cost of logarithmic number of interactions between the user and the server for each search request. Thus, in order to achieve more efficient solutions, almost all the existing works on searchable encryption literature resort to the weakened security guarantee, i.e., revealing the access pattern and search pattern but nothing else.

Before giving main result, first start with a straightforward however ideal scheme, where the security of this ranked searchable encryption is the similar as previous SSE schemes, It believe the analysis of these demerits will lead to our main result. Note that the basic scheme it discourse here is tightly pertained to recent work [10], though our focus is on secure result ranking. Actually, it can be considered as the most simplified version of searchable symmetric encryption that contents the nonadaptive security definition. This ranked searchable encryption system can be constructed from these four algorithms in two phases, Setup and Retrieval

Setup

The data owner initializes the public and secret parameters of the system by executing Key- Gen, and preprocesses the data file collection C by using Build Index to generate the searchable index from the unique words extracted from C. The owner then encrypts the data file collection C, and publishes the index including the keyword frequency-based relevance scores in certain encrypted form, together with the encrypted collection C to the Cloud. As part of Setup phase, the data owner also wants to distribute the necessary secret parameters (in our case, the trapdoor

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. 3, Issue 5, May 2015

generation key) to a group of authorized users by retaining off-the-shelf public key cryptography or more efficient unique such as broadcast encryption.

Retrieval

Provable data possession (PDP) [2] (or proofs of Retrievability (POR) [3]) is such a probabilistic proof technique for a storage provider to prove the integrity and ownership of clients' data without downloading data. The proof-checking without downloading makes it especially important for large-size files and folders (typically including many clients' files) to check whether these data have been tampered with or deleted without downloading the latest version of data. Therefore, it is able to exchange traditional hash and signature functions in storage outsourcing. Various PDP schemes have been recently proposed, such as Scalable PDP [4] and Dynamic PDP [5]. However, these schemes mainly focus on PDP issues at untrusted servers in a single cloud storage provider and are not suitable for a multi-cloud environment

It address the problem of provable data possession in distributed cloud environments from the following aspects:

- High security,
- Transparent verification
- High performance.

To achieve these goals, first propose a verification framework for multi-cloud storage along with two fundamental techniques: hash index hierarchy (HIH) and homomorphic verifiable response (HVR).

III. PROPOSED SYSTEM

A. *Architecture Diagram*

Multicloud server having more number of private clouds and multi clouds. User or ower can upload file to multicloud or download file from multicloud. TTP giving security to uploading and downloading files. After receiving request from user or owner, TTP only verify that file whether accept or not and having more challenges and response of mutlticloud storing files.

Combiner or divider is used to secure the file from semi honest attacker. Uploading and downloading files stored into more number of blocks in multicloud. While uploading divider concept id used and downloading combiner concept is used.Here deal with the construction of an well-organized PDP scheme for multicloud storage to support the scalability of service and data migration, in which here regard as the existence of multiple cloud service providers to cooperatively store and maintain the clients data.

The semi honest service provider can attack the owners data depend upon the single item identity and many items identity known as item based attacker and set baser attacker. Shared data flow process (uploading and downloading) performed between user or owner and multicloud.

This paper formalizes the RSA-PDP system model for remote data integrity checking and variable length block verification and security model for secure the data from data mining attacker.The generation of tags with the length irrelevant to the size of data blocks. To reduce the memory space by using variable length block verification based on hashing algorithm. Cloud service provider is semi honest server so attacker can easily attack data.

Here the data are secured from datamining attacker also can eliminate the difficult certificate management. In order to increase the efficiency, RSA based provable data possession is more gorgeous. Thus, it will be very meaningful of RSA-DPDP.

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. 3, Issue 5, May 2015

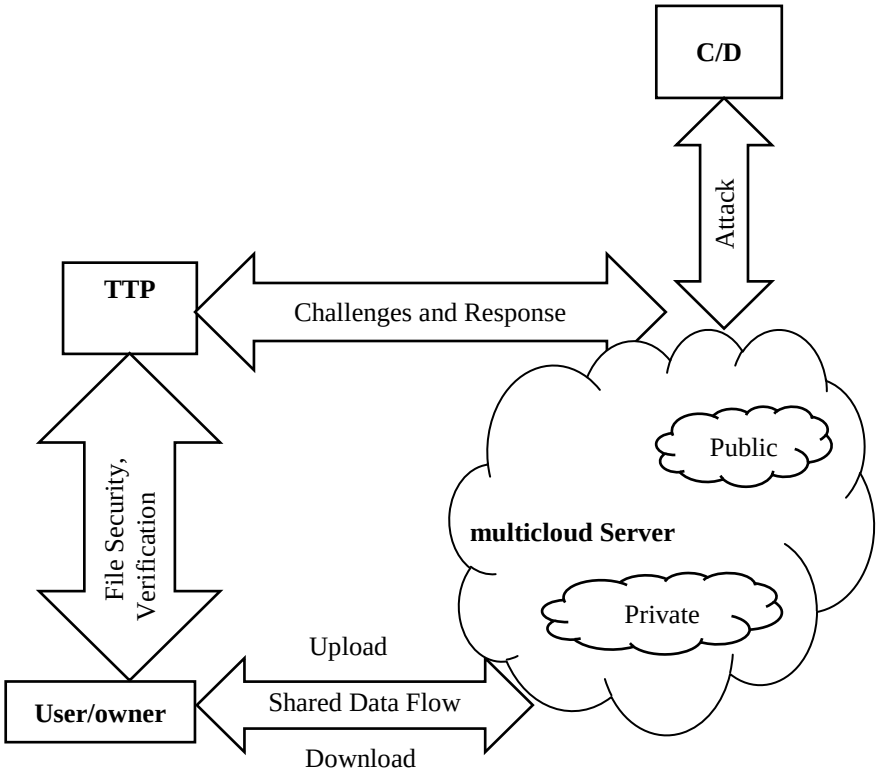

Fig: Architecture Diagram for Multicloud

B. Modules

a. User Module

Based on architecture, it consider a data storage service involving four entities: data owner (DO) the client (data owner) uses the 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 CSP, and may delete its local copy.

Registration

Each user register his user details for using records. Only registered user can able to login in cloud serve.

View Files

User view a block of uploaded files that is accepted by cloud servers and Verified by verifier in the multi cloud Server.

Download

User to download data from multi cloud server and that file verified by verifier file using his identity key to download the decrypted data.

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. 3, Issue 5, May 2015

b. Owner Module

Authorized Applications (AA), who have the right to access and manipulate stored data. Finally, application users can enjoy various cloud application services via these authorized applications.

Upload Files

Owner login into cloud server and upload their files into cloud.

Save To Cloud

After accepting uploaded files by verifier that all stored in multi-cloud.

c. Verifier Module

The construction of algorithms in this audit architecture. A more detailed descriptions of the can be found in Appendix A. Firstly, it present the definition of two algorithms for the tag generation process as follows:

- Key Gen: takes a security parameter as input, and returns a public/secret key pair.
- T agGen (sk, F): takes as inputs the secret key sk and a file F, and returns the triple, where denotes the secret used to generate the verification tags, is a set of public verification parameters u and index-hash and denotes the set of tags.

File Verification Module

The public verifier is able to correctly check the integrity of shared data. The public verifier can audit the integrity of shared data from multi cloud with entire Data and accept the file.

Accept Files

Public auditor can check all files integrity then accept the files to cloud.

d. Server Module

Cloud Service Provider (CSP), who provides data storage service and has enough storage space and computation resources. This kind of strong authorization-verification mechanism, neither assume that CSP is trust to guarantee the security of stored data, nor assume that a date owner has the capability to collect the evidence of CSP's faults after errors have been found.

To maximize the storage efficiency and audit performance, general fragment structure is introduced into audit system for outsourced storage. In an outsourced file F is split into n blocks, and each block mi is split into s sectors. The fragment framework consists of n block-tag pair, where i is a signature tag of block mi generated by some secrets. Finally, these block-tag pairs are stored in CSP and the encryption of the secrets (called as PVP) is in TTP.

View Files

Every server from multi-cloud verify the file block and accept the block of files to verify the verifier.

e. Attacker Module

The server or an intruder who gains access to it may possess some background knowledge using which they can on the encrypted database D∗. it generically refer to of these agents as an attacker and adopt a conservative model and assume that the attacker knows exactly the set of (plain) items I in the original transaction database D and their true supports.

Here assume the service provider (who can be an attacker) is semi-honestin the sense that although he does not know the details of our encryption algorithm, he can be enquiring and thus be able to use his background knowledge to make inferences on the encrypted transactions. It also assume that the attacker always returns (encrypted) item sets together with their exact support. The data owner (i.e., the corporate) considers the true identity of:

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. 3, Issue 5, May 2015

- Every cipher item,
- Every cipher transaction, and
- Every cipher frequent pattern as the intellectual property which should be protected.

It consider the following attackmodel:

Item-Based Attack

The semi honest service provider can attack the owners data depend upon the single item identity.

Set-Based Attack

The service provider attack the owners data depend upon the many item identities. The attacker can easily attacks the data correctly but they can't use that data because that data's are in cipertext form.

IV. RESULTS AND DISCUSSIONS

Uploading data are stored intonumber of blocks in multicloud. If the uploading data are larger thatsplitting into more number of blocks. While combining and dividing large data, the accuracy level more high. These combiner and divider is used to secure data from semi honest attacker.

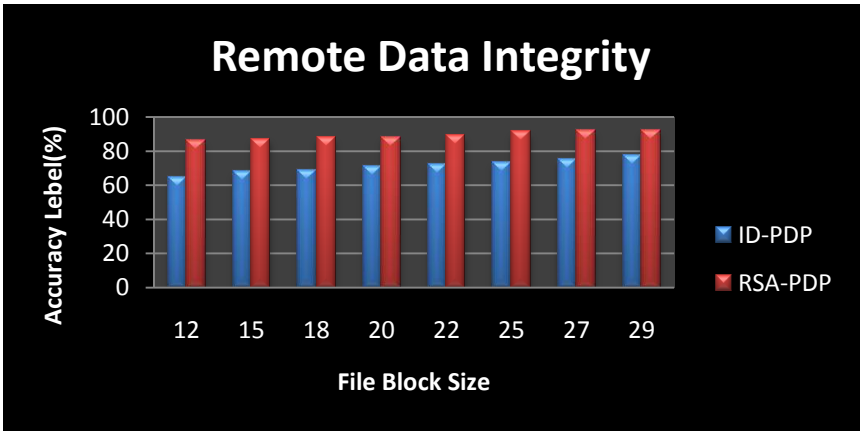

Fig: Result for RSA-PDP

V. CONCLUSION

The domain knowledge is collected and analysed in the introductory levels. A wide literature survey is conducted to analyse the techniques and concepts that proposed earlier. The literature survey is conducted in the area of remote data integrity checking and provable data possession. In multicloud storage, this paper formalizes the RSA-PDP system model for remote data integrity checking and variable length block verification and security model for secure the data from data mining attacker.

VI. FUTURE WORK

For further enhancement, data can be compressed and store in multicloud environment. Additionally, more security can be provided using algorithm which is efficient than RSA.

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. 3, Issue 5, May 2015

REFERENCES

[1]. Y. Zhu, H. Hu, G.J. Ahn, M. Yu, "Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage", IEEE Transactions on Parallel and Distributed Systems, 23(12), pp. 2231-2244, 2012.
[2]. H.Q. Wang, "Proxy Provable Data Possession in Public Clouds," IEEE Transactions on Services Computing, 2012.
[3]. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, "Zero-Knowledge Proofs of Retrievability", Sci China InfSci, 54(8), pp. 1608-1617, 2011.
[4]. A. F. Barsoum, M. A. Hasan, "Provable Possession and Replication of Data over Cloud Servers", CACR, University of Waterloo, Report2010/32, 2010.
[5]. Y. Zhu, H. Wang, Z. Hu, G. J. Ahn, H. Hu, S. S. Yau, "Efficient Provable Data Possession for Hybrid Clouds", CCS'10, pp. 756-758, 2010.
[6]. C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "Dynamic Provable Data Possession", CCS'09, pp. 213-222, 2009.
[7]. R. Curtmola, O. Khan, R. Burns, G. Ateniese, "MR-PDP: Multiple- Replica Provable Data Possession", ICDCS'08, pp. 411-420, 2008.
[8]. G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", SecureComm 2008, 2008.
[9]. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, D. Song, "Provable Data Possession at Untrusted Stores", CCS'07, pp. 598-609, 2007.
[10]. A. Juels, B. S. Kaliski Jr., "PORs: Proofs of Retrievability for Large Files", CCS'07, pp. 584-597, 2007