International Journal Of Core Engineering & Management
Volume-4, Issue-1, April-2017, ISSN No: 2348-9510

VERIFYING INTEGRITY IN MULTI-CLOUD STORAGE USING EFFICIENT COOPERATIVE PROVABLE DATA POSSESSION – A REVIEW

Roshanee Bopche
Research Scholer M.Tech ,Department of Computer Science & Engineering
Shri Ram Group Of Institution, Jabalpur (M.P), INDIA
rsbopche@gmail.com

Sapna Choudhary
Assistant Professor, Head of the Department, Department of Computer Science & Engineering
Shri Ram Group of Institution, Jabalpur(M.P.),INDIA
choudharysapnajain@gmail.com

Abstract

The term 'Cloud' is a network of remote servers hosted on the internet and used to Store, Manage, and Process data in place of local server or personal computer. Multi cloud storage is an tremendous technique using a collection of cloud to provide data storage and data sharing for clients cooperatively. Provable data possession(PDP) is a technique for ensuring the integrity of data in storage outsourcing. Construction of an efficient PDP scheme for distributed cloud storage to support the scalability of service and data migration .We present an efficient method for selecting optimal parameter values to minimize the computation costs of clients and storage service providers. We use Cooperative provable data possession scheme for based on interactive proof system(IPS). This Cooperative PDP scheme adopting Layered Index Hash Hierarchy(IHH).
Keywords:-Cloud Storage, Data Integrity,RSA,HMAC, CPDP.

I. INTRODUCTION

The term cloud is used as a metaphor for the Internet, based on the cloud design used to represent the Internet in computer network diagrams as an abstraction of the underlying infrastructure it represents. Typical cloud computing vendors offer current business applications online, accessible via a web browser, while the software and data are stored on the server.

II. CLOUD COMPUTING

Cloud computing has become one of the most discussed computer IT paradigms in recent years. With the rapid development of processing and storage technologies and the success of the Internet, computing resources are cheaper, more powerful and ubiquitous than ever. This technological trend made possible the realization of a new computing model called cloud computing, in which resources (eg CPU and memory) are provided as general utility available that can be leased and released by users through the Internet in an on-demand fashion.

Cloud computing provides an infrastructure, platform and software, services that are provided a

International Journal Of Core Engineering & Management
Volume-4, Issue-1, April-2017, ISSN No: 2348-9510

subscription service for the consumer. These services include Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) Amazon Elastic Compute Cloud (EC2), Google App Engine and Force.com Are examples of IaaS, PaaS and SaaS respectively. IaaS is a very flexible option and the best choice to move applications to the cloud when there is no time to revise the application code for a cloud environment.

III. RELATED WORK

A) Collaborative Integrity Verification In Hybrid Clouds:

A hybrid cloud is a cloud computing environment in which an organization provides and manages some internal resources and the others provided externally. However, this new environment could cause irreparable losses to the customer due to the lack of a verification mechanism for the integrity of distributed data outsourcing. In this paper address the construction of a collaborative integrity verification mechanism in hybrid clouds to support the scalable service and data migration, in which consider the existence of multiple cloud service providers to collaboratively store and maintain the clients' data. A hybrid cloud is a cloud computing environment in which an organization provides internal and external resources and manage it.
Architecture considers a data storage service involving three different entities: Granted clients, a large amount of data to be stored in hybrid clouds and have the permissions to access and manipulate the stored data.

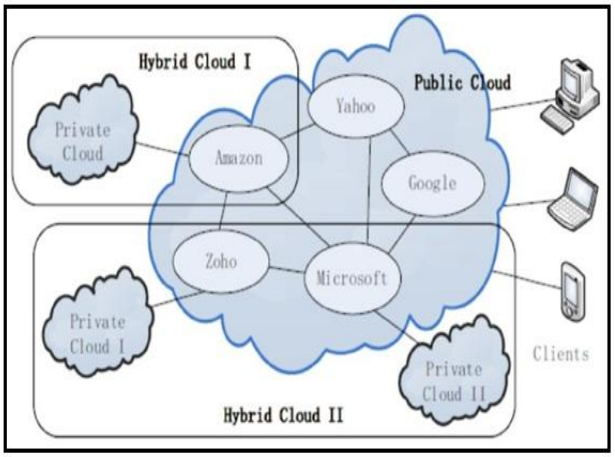

Figure: A1 Hybrid Cloud Diagram I[12]

Cloud Service Providers (CSPs), work together to provide data storage services and have enough storage spaces and computation resources; and Trusted Third Parties (TTPs), Trusted to store the verification parameters and offer the query services for these parameters.

International Journal Of Core Engineering & Management
Volume-4, Issue-1, April-2017, ISSN No: 2348-9510

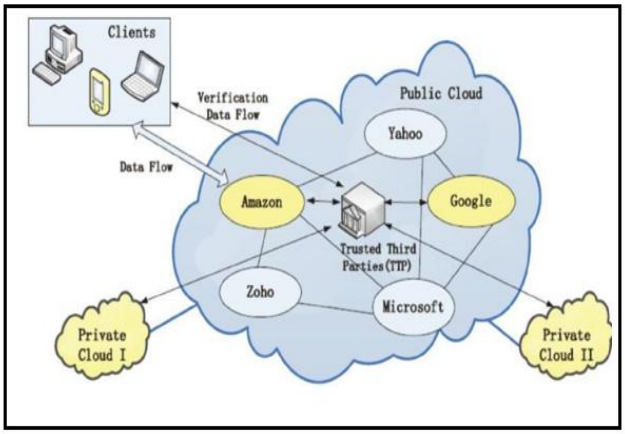

Figure: A2 Hybrid Cloud Diagram II[12]

B) Scalable and Efficient Provable Data Possession:
Storage Outsourcing is an upward trend that requires a number of interesting integrity issues, many of which have been extensively studied in the past. However Provable Data Possession (PDP) scheme that has recently appeared in the research literature. The main problem is the frequency, efficiently and safely verifies that a storage server stores its customers (very large potential) reliably the outsourced data. It is assumed that the storage server in terms of integrity and reliability is not reliable. The problem is the customer of a small computer device is exacerbated with limited resources. The work has dealt with this problem above either public-key cryptography or requires the client to outsource its data in encrypted form. Build a very effective and proven PDP security technology, which relies exclusively on symmetric key cryptography, as you do not need bulk encryption.

C) Ensuring Data Storage Integrity in Cloud Computing
Cloud computing was introduced as the next generation of enterprise computing architecture. Unlike traditional solutions whose IT services are under the physical, logical and personnel controls, cloud computing moves application software and databases into large data centers where data management and services Are not quite trustworthy.

D) Privacy-Preserving Audit and Extraction of Digital Contents:
A growing number of online services such as Google, Yahoo! and Amazon are beginning to charge users for their storage. Clients often use these services to store important data such as email, family photos and videos, and disk backups. A customer/client must have complete confidence in maintaining the integrity of the hosted data and in bringing these external services intact. Unfortunately, no service is infallible. To make storage services responsible for data loss, we present protocols that allow a third party verifier to examine the data stored by a regular service and support the client when returning data. More importantly, that our protocols are privacy-preserving by never betraying the contents of the data to the auditor. Our solution removes the burden of verification by the customer, the customer and the banking service alleviates the fear of data leaks and provides an arbitration method independent of data storage contracts.

E) Dynamic Provable Data Possession:

As outsourced storage services and resource sharing networks have become popular, the problem of effectively testing the integrity of data stored on unsecured servers, more attention received. The Provable Data Possession (PDP) model, the client processes the data and then sends it to an unsecured server for storage, while maintaining a small amount of metadata. The client asks the server to later on that the stored data has not been altered or deleted (without downloading actual data). However, the original PDP system only applies to static files (or only during). They present a framework of definition and efficient structures for DPDP that extends the PDP model to support detectable updates for the stored data, using a recent version of authenticated dictionaries based on the information of ranking. They provide a framework for defining and efficient structures for DPDP that extends the PDP model to support detectable updates on stored data. When an F file is composed of n blocks, the definition of an update is either the insertion of a new module (anywhere in the file, not only attach) or a change in an existing block, An arbitrary block. Therefore, our update process describes the most common form of changes that wants to run a client in a file.

F) Space-Efficient Block Storage Integrity:

The new method of providing block-level integrity in encrypted storage systems, namely, so that a client detects the modification of the data blocks by a non-secure storage server. It shows the encryption definitions for this parameter and develops solutions that do not change the size of the block or the number of sectors mentioned, an important consideration for modern storage systems.

G) Compact Proofs of Retrievability:

Proof of the Retrievability of the system, a data storage center must proves to verifier that it is to save all the clients data. The main challenge is to build systems that are both safe and demonstrable which is it should be possible to extract customer data from any prover who passes a check. Enter the first systems of validation of accessibility to the integrity of proofs Full Arbitrary Opposition in the strongest model. Our first program, built by the BLS signatures and secured in the random oracle model, has the shortest request and response of any proof of accessibility with public verifiability. Our second schema, are functions that constructs stylish pseudo-random (PRF) and is safe in the standard version has the shortest response of any proof of accessibility control with its own testability (destination along the query). Both systems rely on homomorphic properties to aggregate into a small proof has an Authenticator value. Current visions of cloud computing "and \ Software as a Service" call for information, both personal and professional, by a third party being rescued aim to use is delayed. Outsourced memory users are at the mercy of their storage providers for the continued availability of their data.

H) Proofs of Retrievability via Hardness Amplification:

Proofs of Retrievability (PoR), which were introduced by Juel and Kaliski, allowing the client to save an file on an unsafe server and later conduct an efficient audit log in which the server proves that (For now) has customer data. Constructions of PoR schemes attempt to minimize client and server storage, the complexity of audit communication, and even the number of blocks of files that the server accesses during verification. Identify the different variants of the problem(such as bounded-use vs. unbounded-use, knowledge-soundness vs. information-soundness), and enter

each of these variants near optimal ROP regimes.

I) Proofs Of Retrievability:

A problem with remote storage is liability. If data occasionally accessed, how users can be sure that they are honestly stored. For example, if a hardware failure of the remote storage provider suffers and loses some data, it could establish that there is no need to inform its customers because there is a good chance that the data will never be Accessible, and consequently the customer would never know! Otherwise, one of the smart storage providers may even choose to delete rarely used files to save money. For such concerns how to set a simple auditing process for customers to check if their data is stored properly. These audits called the Proofs of Retrievability.

IV. PROBLEM STATEMENT

A) Problem description:

Provable Data Possession (PDP) schemes evolved around public and single clouds offer a publicly accessible remote interface to check and manage the tremendous amount of data. The majority of existing PDP schemes is incapable of satisfying such an inherent requirement of hybrid clouds in terms of bandwidth and time. Although existing schemes can make a false or true decision for data possession without downloading data at untrusted stores, they are not suitable for a distributed cloud storage environment. In existing PDP scheme didn't have auto blocking mechanism to user data which stored in to cloud server and did not useful for the large amount of data. In existing PDP scheme server can generate tag for multiple file blocks in term of single response value on client side, but the response from multiple cloud can be combined into single response value . For lack of homomorpic response the PDP protocol to check the integrity of file block stored in multi cloud server. Also client need to known exact position of file block stored into multi cloud so verification process in case will lead to high communication overhead and computation cost. Existing scheme RSA algorithm is used for key generation.

- **RSA Scheme:**

The RSA relies on the fact that it is easy to multiply two large prime number together but extremely hard to factor them back from the result. RSA is a block cipher in which the plain text and cipher text are integer between 0 ang n-1. The RSA is public key cryptosystem that is based on the intricacy of integer factoring . The RSA public key encryption method is the first instance of a provably secure public key encryption method against preferred message attacks. Assuming that the factoring trouble is computationally obstinate and it is rigid to uncover the prime factor of n = p * q. The RSA method is described as:

Key generation algorithm:

To generate the key entity A have to do the following:

1.by chance and secretly choose two large prime number p and q .
2.Compute the modulus p*q.
3.Compute ø(n) = (p-1) * (q-1).
4.Select chance integer e, 1 <e <n where gcd(e, ø) = 1.
5. Baghdad method[16] used to calculate the single decryption key d, 1<d< ø(n) where e*d = 1modø(n)

6.Determine public key and private key for entity A , the pair (e,n) as a public key (d,n) as private key .

Public key encryption algorithm:

Message m encrypt by entity B for entity A which entity A decrypts to it.

Encryption: entity B should do following:

1. Obtain entity A public key (e,n).
2. Message m as an integer in the interval {0….n-1}.
3. Calculate c = m^e mod n .
4. Send the encrypted message c to A.

Decryption: To recover the message m from the cipher text c. Entity A must do the following:

1. Get the cipher text c from entity B
2. recover the message m = c^d mod n

Disadvantages:

1) This algorithm has some limitation alongside certain attacks (i.e. Brute force , Mathematical attack ,Timing attacks and Chiper-text attacks) .
2) In the current system has no function to automatically block the cloud server.
3) The current system is less secure because no modern cryptographic technique.
4) There is no function to prove integrity based on a public key or any other key based on the file name.
5) The details of the attackers are not stored dynamically, but use the log file to store the details and data mining used to examine the concepts, which is time-staking and less secure..
6) Cloud user data store in untrusted cloud servers.
7) The data integrity is proving only based on the file name and not on the public key or any Other key.
8) For lack of homomorphic responses, the verification process in such a case will lead to high Communication overheads and computation costs at client sides as well.

V. CONCLUSION

We proposed the implementation of an efficient method for distributed cloud PDP. Based on the hash index hierarchy and the verifiable homomorphic response we have projected an efficient cooperative PDP (ECPDP) method, supporting the dynamic query as insertion, deletion and modification Append, etc. On the storage servers. We also said that our method all security assets to track the interactive evidence system to zero knowledge so that it can withstand various attacks that used in the clouds as a public audit service. In addition, we optimized the probabilistic uncertainty and interval verification to restore audit performance. These experiments have clearly established that our approaches to present only a small amount of communication and calculation/computation. This method is more suitable for storing large amounts of data in the multi-cloud server. An Efficient Cooperative provable Data Possession scheme to support dynamically scalability on multiple storage server.

VI. Future Work

In our Efficient CPDP scheme Efficient RSA algorithm are used to key generation and MD5 algorithm for tag generation. Some one used to more effective algorithm to improve it. Trusted Third Party are used to monitoring all this process it should be able to make regular check on the integrity and availability of these delegated data at appropriate interval and should be able to organize , manage and maintain the outsourcing data.

REFERENCES

1. Rajkumar Buyya, Christian Vecchiola and S. Thamarai Selvi " Mastering Cloud Computing".

2. G. Joon Ahn, Y.Zun, H. Hu, "Cooprative provable data possession for Intrigrity verification in multi cloud storage," IEEE Transaction on parallel and distributed system , vol: PP, issue 99, 14-02-2012.

3. I. M. Llorente, I. T. Foster, R. S. Montero, B. Sotomayor, "Virtual infrastructure management in private and hybrid clouds," IEEE Internet Computing, vol.13, no. 5, pp. 14-22- 2009.

4. J. Herring, L. Kissner, Z. N. J. Peterson, G. Ateniese, R. C. Burns, R. Curtmola, and D. X. Song, "Provable data possession at untrusted stores," ACM Conference on Computer and Communications Security, P. Ning, S.D.C. di Vimercati, and P. F. Syverson, Eds. ACM, 2007, pp. 598-609.

5. P. Ning, S. D. C. di Vimercati, A. Juels and B. S. K. Jr., "Proofs of retrievability for large files," ACMConference on Computer and CommunicationsSecurity P. F. Syverson, Eds. ACM, 2007, pp. 584-597.

6. Pankaj Sareen " Cloud Computing: Types, Architecture, Applications, Concerns and Virtualization and Role of IT Governance in cloud", IJACCSSE, Volume-03, issue-03 pp. 533-538, March 2013.
7. B. Waters, H. Shacham "Compact proofs of retrievability," ASIACRYPT, ser. Lecture Notes in Computer Science, J. Pieprzyk, Ed., vol. 5350. Springer, 2008, pp. 90-107.

8. C.Wang and W. Lou, Q. Wang, J. Li, K. Ren, "Enabling public verifiability and data dynamics for storage security in cloud computing," ESORICS, ser. Lecture Notes in Computer Science, M. Backes and P. Ning, Eds., vol. 5789. Springer, 2009, pp. 355-370.

9. S. P. Vadhan, and D. Wichs, Y. Dodis, "Proofs of retrievability via hardness amplification," TCC, ser. Lecture Notes in Computer Science, O. Reingold, Ed., vol. 5444. Springer, 2009, pp. 109-127.

10. Trilok Singh Pardhi, Dr. Rajeev Pandey and Prof. Uday Chourasia " Survey of Integrity Verification in Multi-Cloud Storage by Efficient Cooperative Provable Data Possession",

International Journal of Computer Application *(0975 – 8887) Volume 102– No.8, September 2014.*

11. G.-J. Ahn, Y. Zhu, H. Hu, Y. Han, and S. Chen, "Collaborative integrity verification in hybrid clouds," in IEEE Conference onthe 7th International Conference on Collaborative Computing*: October 15-18*, 2011, pp. 197-206.

12. https://www.google.co.in/image.