ISSN:0975-9646

Integrity Verification in Multi-Cloud Storage by Efficient Cooperative Provable Data Possession

Trilok Singh Pardhi[1] , Dr. Rajeev Pandey[2], Prof.Uday Chourasia[3]

PG Scholar DoCSE[1], Asst. Prof. DoCSE[2] , Asst. Prof. DoCSE[3]
UIT-RGPV, Bhopal (India)[123]

Abstract- Provable data possession (PDP) is one of the procedure to make sure the integrity of data in storage outsourcing. Here in this paper, we talk to the creation of an efficient PDP method for distributed cloud storage to preserve the scalability of service and data migration. On the origin on homomorphic verifiable response and hash index hierarchy we anticipated a efficient cooperative PDP (ECPDP) method. We verify the security of our method founded on multi-prover zero-knowledge proof method, which can satisfy knowledge accuracy, fullness , and zero-knowledge assets. As well, we expressive performance optimization apparatus for our method, and in particular present an capable method for selecting finest parameter values to reduce the addition expenses of storage service bringers and client. Our experiment shows that our solution pioneers communication overheads and lower addition in evaluation with non-cooperative approachs.

***Keywords* – Scalability, Data Migration, Homomorphic, Multi-Prover.**

INTRODUCTION :

Cloud computing has become a more rapidly yield enlargement point in recent year by providing a comparabaly low-cast , scable , position-independent plateform for client's data. Although commercial cloud server have revolved approximately public clouds,the rising interest of edifice around private cloud on open-source cloud computing tools forces local user to have a flexible and agile private infra structure to run service workload within the administrative domain. Private cloud are not exclusive for being public cloud , and they can also support a multi cloud (Hybrid cloud) model by complementing a local transportation with computing capacity from an external public cloud. By using virtual infrastructure mamagement (VIM)[1] a multi cloud can allow remote access to its resource over the Internet via remote interface, such as the Web services interface that Amazon EC2 uses.

MODULE DESCRIPTION:

Multi cloud storage:

Multi cloud storage refer to any large cooperation in which many small cloud storage used to store large amount of data . In our system the each cloud server have data blocks. Data uploaded into multi cloud by cloud user. Cloud computing surroundings is constructed based on open architectures interfaces, that have the ability to add in multiple internal and/or external cloud services mutually to afford elevated interoperability. We call such a distributed cloud surroundings as a multi-Cloud . A multi-cloud permits clients to fluently access his/her possessions remotely throughout interfaces.

Efficient Cooperative PDP:

Cooperative PDP (CPDP) method is an efficient PDP method to verifying the availability and integrity in multi cloud storage. It contains three-layered index hierarchy and zero-knowledge property. Through this method computation cost of client and storage service providers would be reduced. This method based on modern cryptographic techniques without compromising data privacy. In this method us are using efficient RSA algorithm for key generation and MD5 algorithm for tag generation that is to be used forb integrity verification .

Data integrity:

Data Integrity is very key feature of cloud computing. The data should not obtain customized without intentionally. The data should remain intect unless it is customized by authorized person.

Third party auditor:

The Trusted Third Party (TTP) is an organization that's authorized by an another organization to manage or process identifiable data for a specific purpose . Trusted Third Party provide interaction between two parties and both trust the third party. In our system stored verification parameters and for these parameters provide public query services. The Trusted Third Party, observe the cloud user data and uploaded in the distributed cloud. In multi-cloud surroundings each cloud server have user data blocks. If any edition tried by cloud user a alert is sent to the Trusted Third Party.

***Cloud user*:**

In multiple cloud ,cloud user store a bulky amount of data and they have permissions to operate and access stored data. The User's data is rehabilitated into data blocks. In cloud server this data blocks are uploaded . The TPA examines the cloud data blocks and Uploaded in multi cloud. Only user can update the uploaded data. The data's in multi cloud is incorporated and downloaded by user's.

LITERATURE SURVEY

1) Ensuring Data Storage Security In Cloud Computing Environment

Cloud Computing has been predict as the next creation construction in IT Enterprise. In contrast to predictable solutions, where the IT services are in correct logical , physical and personnel controls, Cloud Computing moves on application software and databases to access the large

data centers, where the managing of the services and data may not be entirely reliable. This single attributes, on the other hand, posses many new security confronts that have not been well implied. In this article, we limelight on cloud data storage security, that has always been an vital facet of quality of service. To guarantee the correctness of cloud users' data in the cloud, we recommend an effective and flexible distributed method have two features, opposing to its ancestor. By utilizing the features, opposing to its predecessors. To obtain erasure-coded data we use of homomorphism token with distributed verification, our method achieves the combination of storage correctness, assurance and data error localization, i.e., the recognition of unruly server(s). Dissimilar most previous works, the new method further supports efficient dynamic operations safe and secure on data blocks, including: such operation like that data modification ,append and delete. Proposed method is vastly efficient supple against malicious data alteration attack, Byzantine collapse ,and even server colluding attacks prove based on general security and performance analysis.

Disadvantages:-

1. This method doesn't allow to automatic blocking the cloud server .
2. Less Security – None of the cryptographic techniques is used on the cloud data

2) **Privacy-Preserving Audit And Extraction Of Digital Contents**

A growing number of online services providers, such as Google, Yahoo!, and Amazon, are suppose to charge users for their storage. With the help of these service cloud user store our important data such as video, emails , document and file backups. On the day, a cloud user must totally trust such external services to preserve the integrity of data and return it undamaged. Unluckily, there are no service is to keep on the trust. To build storage services responsible for data failure, we proposed protocols that permit a third-party auditor to sporadically confirm the data stored by a assist and service in returning the same as usual data to the customer. That used protocols are privacy-preserving, in that they not at all divulge the data contents to the assessor. This solution eliminates the burden of verification from the customer, improves both the storage service's and customer's data dread of data leakage, and offers a method for free arbitration of data preservation contracts.

Disadvantages:-

1. There are no features to prove integrity based on public key or any other key while based on file name.
2. The details of attackers are notdynamic store but use the log file to store details and used data mining concepts to viewing it, that is time consuming job and less security.

3) Provable Data Possession At Untrusted Stores

Some method to provide data availability and integrity that follow traditional cryptographic technologies based on signature scheme and hash function. It cannot work on outsourced data. And did not suitable for a large size file. So Provable Data Possession method come on picture , to ensuring the integrity and availability of file and based on RSA scheme and reduced the communication cost. But PDP method are suitable only for single cloud storage not for multi cloud storage. The cloud user maintains a invariable quantity of metadata to confirm the proof. We have two provably-secure PDP mrthods that are further competent than earlier solutions, when compared with methods that get weaker guarantees.

Disadvantages:-

1. PDP method doesn't allow to automatic blocking the cloud server .
2. Owner's data will be stored in untrusted cloud servers.

4) Scalable and Efficient Provable Data Possession

To overcome the problem of Provable data Possession At Untrusted Store method they present the efficient new PDP method called The Scalable and Efficient Provable Data Possession . Which act as a powerfull deterrent to corrupt thus growing trust in the system . Recently proposed method are not capable for the large amount of data for that we use Scalable and Efficient Provable Data possession method . That method are based on an symmetric key cryptosystem and support to secure and efficient dynamic operation such as modification ,deletion ,append etc. That method gives probabilistic declaration of the untampered data which store in the server .That method are used for outsourcing of personal digital contact as a MAC, GMAIL, PICASA and OFOTO .

Disadvantages:-

1. By using the previous metadata orb response due to lack of randomness in the challenge server can deceive the owner .
2. The no of updates and challenges are limited .
3. Limitation of block insertion anywhere.

EXISTING SYSTEM

There survive different technologies and tools for multi cloud, like that Overt, VM Orchestrator and VMware vSphere. To create a distributed cloud storage podium for managing clients' data these tools provide help to cloud provider. However, if such a significant platform is helpless to security attacks, it would bring irreversible wounded to the clients. For example, the private data in any venture may be illegitimately accessed during a remote interface which supplied by a multi-cloud, or annals and relevant data and possibly will be vanished or tampered with when they are store into an doubtful storage pool exterior the venture. Therefore, it is requisite for cloud service providers. To present security techniques to handle their storage services. In the exixting system to generate keys for encryption and decription usein RSA public key scheme is based on the intractability of factoring the integer modulues which is the product of two large prime number.

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 massege attecks. 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 describe as:
Key generation algorithum :
To generate the key entity A have to do the following :

1. by chance and seceratly 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[14] used to calculate the single decryption key d, 1<d< ø(n) where e*d = 1mod ø(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 fron the cipher text c. Entity A must do the following :

1. Get the cipher text c from entity B
2. Convalesce 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 existing system doesn't have feature of automatic blocking the cloud server.
3. Existing system are less secure because of no modern cryptographic technique are used.
4. There are no feature to prove integrity based on public key or any other key while based on file name..
5. The details of attackers are not dynamic store but use the log file to store details and used data mining concepts to viewing it, that is time consuming job and less security.
6. Cloud user data store in untrusted cloud servers.

PROPOSED SYSTEM

To reduce these problem many algorithm have been designed and based on original RSA. Efficient RSA are the popular algorithm identified for improving the main algorithm. To verify the integrity an d availability of outsourced data in cloud storage we have two basic method that's called Provable data Possession method and Proof of Irretrievability. PDP method are used for a static case and based on RSA scheme .But in this method owner or anyone can challenge for possession. And no of updates are fixed previously and cloud user cannot insert block anywhere. So now we proposed a lightweight PDP for ensuring the availability and integrity of data in cloud server on the basis on homomorphic verifiable response and hash index hierarchy we projected a Efficient cooperative PDP (ECPDP) method. In these approach we use to Efficient RSA algorithm for key generation.
The RSA scheme to a scheme employs the general linear group of order of h*h matrix. The key range of efficient RSA is considerably momentous and can actually be used with hill cipher process . The difference of original RSA and efficient RSA is how to calculate ø(n) in key generation process . In Efficient RSA ø(n) was defined as
Assume that n= p * q is the product of two large prime number and suppose g is the general linear group of h*h matrices then g :

$$g = (ph - p0)*(ph - p1) \dots (ph - ph - 1) + (qh - q0)*(qh - q1) \dots (qh - qh - 1)$$

here g(n,h) determine as a ø(n,h) wher h is the rank of linear matices.

Key generation algorithm :
To gernerat the keys entity A have to do the following :

1. Randomly chose two large prime number p and q .
2. Compute the modulus n = p * q.
3. Compute g = (n , h).
4. Chose the random integer e where gcd(e , g)= 1
5. Compute the inverse d where ed = 1mod g
6. Determine the entity A private key and public key

The pair (d , g) is private key while the pair (e , n) is the public key

Public key encryption algorithm
Entity B encrypt a message m for entity A which entity A decrypts.
Encryption : entity B should do following :

1. Obtain entity A public key (n,e).
2. The message m as a h*h matrix X
3. Compute h*h matrix c = m^e mod n .
4. Send the encrypted message c to A.

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

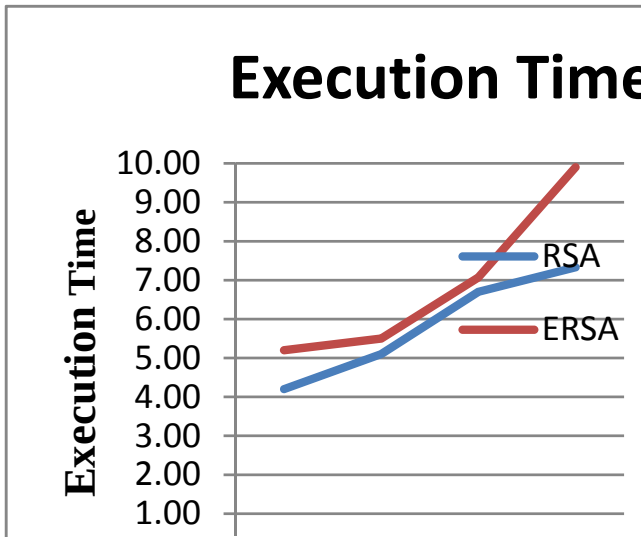
1. Get the cipher text c from entity B
2. Convalesce the message m = c^d mod n

Advantage of the proposed scheme

1. The key range of the proposed scheme is considerable. It means that it can be large enough to use by matices of high level of ranks. The key range of RSA algotithm is ø(n) = (p-1)(q-1). But in the suggested scheme the key range is length g(n).
2. The intractability of the integer factoring of the modulus n in the propose scheme stay as same as a in RSA scheme .
3. The proposed scheme can be used as a digital signature by inserted in the marix x as an item

ANALYSIS AND RESULT :

The result of proposed method and existing method was implemented in java and according to 2.40 Ghz Intel Core i3 CPU and 2.00 gb ram . The compare result between the existing scheme and proposed scheme were carrid out according to the different size of file and execution thie in m/s .



The total execution time compare of efficient RSA and original RSA was increased means to creak encrypted massage are difficult as compare then original RSA algorithm . Now the second approach to finding the tag we use to MD5 algorithm that's generate hash value for specific data of file block . This is unique value and generate one time another time it will be change ,so compare to old and new generated tag , if both tag are same so no modification in to the stored data of server .

CONCLUSION :

In this paper we proposed the construction of an efficient PDP method for distributed cloud storage. On the basis on hash index hierarchy and homomorphic verifiable response we projected a Efficient cooperative PDP (ECPDP) method, that's support to dynamic query such as insertion ,deletion append and modification etc on multiple storage servers. We also explained that our method offer all security assets follow to zero knowledge interactive proof system, therefore that it can resist different attacks which deployed in cloud as a public audit service. Moreover, we optimized the probabilistic uncertainty and intervallic verification to recover the audit performance. These experiments clearly established that our approaches only introduce a less amount of communication and computation outlay. These method are more suitable for storing the large amount of data in multi cloud server .

REFERENCE

1 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.

2 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.

3 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.

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

5 R. D. Pietro and G. Tsudik, G. Ateniese, L. V. Mancini, "Scalable and efficient provable data possession," Proceedings of the 4th international conference on Security and privacy in communication netowrks, SecureComm, 2008, pp. 1-10.

6 C. Papamanthou ,A. K¨upc¸ ¨u , C. C. Erway and R. Tamassia, "Dynamic provable data possession," in ACM Conference on Computer and Communications Security, E. Al-Shaer, S. Jha, and A. D. Keromytis, Eds. ACM, 2009, pp. 213-222.

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 H. Hu, and S. S. Yau, Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, "Dynamic audit services for integrity verification of outsourced storages in clouds," SAC, W. C. Chu, W. E. Wong, M. J. Palakal, and C.-C. Hung, Eds. ACM, 2011, pp. 1550-1557.

10 A. Oprea and A. Juels, K. D. Bowers, "Hail: a high-availability and integrity layer for cloud storage," ACM Conference on Computer and Communications Security. ACM, 2009, pp. 187-198.

11 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.

12 L. Fortnow, M. Sipser and J. Rompel "On the power of multiprover interactive protocols," Theoretical Computer Science, 1988, pp. 156-161.

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

14 Sattar Aboud, "Baghdad Method for Calculating Multiplicative Inverse", International Conference on Information Technology, Las Vegas, Nevada, USA. Pp: 816-819, 2004

15 A. Fox, R. Griffith,M. Armbrust ,A. D. Joseph, R. H. Katz, G. Lee, A. Konwinski, D. A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the clouds: A berkeley view of cloud computing," EECS Department, University of California, Berkeley, Tech. Rep., Feb 2009.

16 M. Franklin D. Boneh, "Identity-based encryption from the weil pairing," in *Advances in Cryptology (CRYPTO'2001)*, vol. 2139 of LNCS, 2001, pp. 213-229.

17 O. Goldreich, *Foundations of Cryptography: Basic Tools*. Cambridge University Press, 2001.