Data Security in Cloud Computing

Chandu Vaidya
Dept. of Computer Science and Engineering
RGCER
Nagpur, India
Chandu.nyss@gmail.com

Prashant Khobragade
Dept. of Computer Science and Engineering
RGCER
Nagpur, India
prashukhobragade@gmail.com

Abstract— Cloud computing is the computing model that allow for obtaining resources such as software on cloud, hardware and services over the internet. The clients stores their data on cloud for data security, for ease of accessing and integrity are prime related. In this paper, the problem of ensuring data integrity and security of data storage provided on cloud from the client while storing data over cloud. To ensuring correctness of data, it assumes that authentication required for uploading and retrieving of data over cloud and these task of allowing by a trusted party (TP) used for exposing risk of cloud storage services on behalf of the cloud client to verify data integrity stored in the cloud. This paper focuses on the data security, we proposed erasure correcting method in the file distribution to the cloud and the client authentication provides the redundancies and guarantees data dependability. By using RSA encryption technique and by calculating hash value with distributed verification of erasure coded data, our scheme achieves storage correctness as well as preserving privacy of data in cloud.

Keywords-*Cloud computing, Data integrity, Cloud Client.*

*****

I. INTRODUCTION

Cloud computing is computing paradigm in which task are assigned to a combination of connections software, hardware, services over the internet. Several trends are opening up the era of cloud computing which is use for computer technology. Conceptually, users get computing platform from computing clouds and then inside run their applications. Always cheaper and more powerful processors together with the software-as-a-service computing architecture. These are transforming data centers into of computing service on huge scale. The increasing network bandwidth and reliable yet flexible network connections make it even possible that users can now subscribe high quality service from data and software that reside solely on remote data centers.[15] Cloud offers great convenience to users, when transforming data into cloud since cloud client don't have to care about the complexities of direct hardware management. In cloud computing there are well example Amazon Elastic computer cloud (EC2) [3].

While this internet based online services do provide huge amount of storage space and customizable computing resources. This IT infrastructure shift however is eliminating the responsibility of local machines data in cloud computing vendor's maintenance at the same time. Result for users is at the mercy of their cloud service providers for the data availability and data integrity [6]. Data integrity defines accuracy and consistent data is stored is indicated by an modification in data between two updates of the data record. This data integrity refers the valid of data .In ensuring cloud data storage , the cloud data storage system ,cloud clients store their data in the cloud and it has no longer possess the data locally in cloud[10]. Recently, the importance of ensuring the remote data integrity [3] these techniques are, while can be used to ensure the storage correctness instead of having cloud clients possessing data It cannot address all the security threats in cloud data storage, so they are all focusing on individual's server scenario and most of them not consider dynamic data operations. To addressing this problem for ensuring cloud data storage correction chosen to reserve the RSA token properties, which can be perfectly integrated with the verification of erasure coded data in cloud [11].

II. RELATED WORK

The importance of ensuring the remote data integrity has been highlighted by the following research. This works under different security models and these can be useful to ensure the storage correctness without having users possessing local data are all focusing on single server scenario [1]. Provable data possession model for ensuring possession of file on untrusted storages [9].Although direct applying these techniques to multiple servers could be straightforward; the resulted verification would be linear to the number of servers.

- Jules et al.[5] defined a formal "proof of retrivabilty" (POR) model for ensuring the remote data integrity, their scheme combines spot-checking as well as error correcting code to ensure both possession and getting of files on archive service systems.
- Bowers et al.[4] extended "proof of retrivabilty" (POR) model to distributed systems, all these schemes are focusing on static data. The effectiveness of their scheme rests mainly on the proposing steps that the user conducts before outsourcing the data file. Any change to the contents of data file, even few bits must propagate through the error-correcting code and the corresponding random shuffling process, thus Introducing significant computation and communication complexity, However the token pre-computation of the tags imposes heavy computation overhead that can be expensive for an whole file.

III. RELATED METHOD

In this section shows system model in problem statement and adversary model.

A. System Model:

In this model shows representative network architecture of cloud services architecture. This is shown in Fig 1. In that there are three network entities are as follows:

- User: User stored their data in the cloud and relies on cloud for data storage and computation task.
- Cloud Server: Which is managed by cloud service provider (CSP) to provide data storage has significant storage space and computation resource.

Third Party Auditor: TPA, who is trusted and expose risk of cloud storage services on behalf of cloud client upon request.

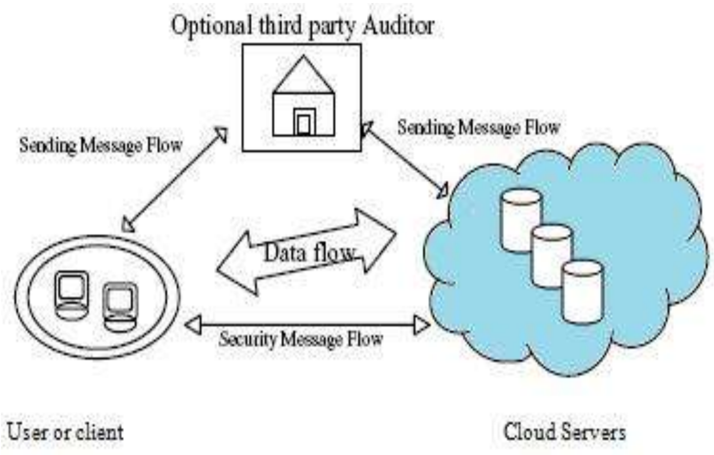

Figure 1: Cloud Storage Service Architecture.

In the cloud storage architecture, cloud make it possible to access our information from anywhere at any time. In that there are four cloud storages are as follows:

- **Public cloud storage:** in public cloud storage, it can access by any subscriber with an internet connection and access to the cloud space.
- **Private cloud storage:** In private cloud storage, it is established for a specific organizations and limits to access to those organizations.
- **Hybrid cloud storage**: In hybrid cloud storage, it is combination of the public and private cloud storage. It means where critical cloud data located in private cloud while other data is stored and accessed from public cloud.
- **Mobile cloud storage:** In mobile cloud storage, it stores the separate data in the cloud and access it from anywhere at any time.

Cloud client stores theirs data in cloud data storage through a cloud service provider into a set of cloud servers, which occurring at the same time and running in cooperated manner. Redundant of data can be employed with technique of erasure precisely code to further tolerate faults or server crash as users data grows in size. In this paper, this dynamic features makes also traditional integrity insurance techniques useless and requires new solutions[8].Therefore, data storage correctness assurance will be of most necessary in achieving a strong and safely cloud data storage system in the real world[7]. In other words, the cloud data we are assuming is unexpected to be rapidly changing in a relative short period. In this system model shows point to point communication between cloud service provider and cloud client.

B. Adversary Model

This model capture all kinds of data integrity threats and this cloud data not denoted at cloud client side but at the cloud service provide domain address. This can come from two attacks:

- Internal Attack: Cloud service provider can be untrusted.
- External Attack: This attack comes from outsiders and who are beyond control domain of cloud service providers.

IV. PROPOSED SYSTEM

This paper majorly focuses on cloud data storage security for client, which has always been an most aspect of quality of service. For ensuring the correctness of cloud clients data in the cloud, in this paper propose a encryption of client data with cryptographic algorithm, apposing to its predecessors. By using the RSA encryption technique with distributed verification of erasure coded data. In This paper proposed the client authentication for uploading and retrieving of data with integration of storage correctness insurance and data error localization most of works, the new scheme further supports secure and efficient dynamic operation on data block including operations. It relies on erasure-correcting code in the file distribution preparation to support redundancy parity vectors for verification of erasure coded data using the RSA authentication method; in this paper our scheme achieves data security for client and the integration of data error localization and storage correctness insurance. In this paper we achieve this goal by exploiting and uniquely combing encryption techniques and the cloud storage privacy for client.[15]

Encryption Algorithm:

The keys for the RSA algorithm are generated the following way:

1. Choose two different large random prime numbers p and q
2. Calculate $n = pq$

- n is the modulus for the public key and the private keys

3. Calculate the totient: $\phi(n) = (p-1)(q-1)$.

4. Choose an integer e such that 1 < e < $\phi(n)$, and e is coprime to $\phi(n)$ **ie:** e and $\phi(n)$ share no factors other than 1; gcd(e,$\phi(n)$) = 1.

- e is released as the public key exponent

5. Compute d to satisfy the congruence relation $de \equiv 1 \pmod{\phi(n)}$ **ie:** $de = 1 + k\phi(n)$ for some integer k.

- d is kept as the private key exponent

Hash Algorithm:

MD5 digests have been widely used in the software world to provide some assurance that a transferred file has arrived intact.

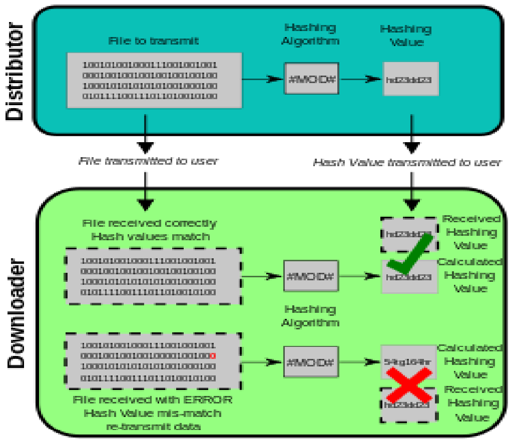

Figure 2: Hash value computing

For example, file servers often provide a pre-computed MD5 (known as Md5sum) checksum for the files, so that a user can compare the checksum of the downloaded file to it. Most unix-based operating systems include MD5 sum utilities in their distribution packages; Windows users may install a Microsoft utility, or use third-party applications. Android ROMs also utilize this type of checksum.

In the first reason cryptography services for the intention of data security protection could not be directly adopted due to the users‟ loss control of data under cloud computing. So, verification of correct data storage in the must be conducted without explicit knowledge of the entire data. Assuming various kinds of data for every cloud client stored in the cloud and requirements of long term continuous assurance of their data safely, the problem is that verifying exactness of data storage in the cloud becomes even more challenging. This construction drastically decreasing the communication and storage overhead as compared to the based file of replication in distribution techniques. Therefore correctness of data and availability of the data being stored on the distributed cloud servers may be guaranteed.[15] The key issue is to highly detect any unauthorized data alternation and corruption, possibly due to server compromise byzantine failure.

The secret key computation function we are considering belongs to a family of universal hash function, chosen to storage the RSA technique, which can be completely integrated with the verification of erasure-coded data. then, it is shown how to derive a challenge-response protocol for verifying the storage correctness as well as identifying misbehaving servers. Finally the process for file recovery and error resurgence based on removal- correcting code is also outlined. It is well known that erasure-correcting code may be used to stand multiple failures in distributed storage space systems. In cloud data storage, we relies on this technique to dissolve the data file F redundantly across a set of n = m+ k distributed servers.

V. Conclusion

In this paper, we examine the problem of data security problem stored the in cloud data storage, which is mostly a distributed storage system. Existing method rely on erasure-correcting code in the file distribution preparation to support redundancy parity vectors for verification of erasure coded data using the RSA encryption. In this paper our focus on the scheme which achieves the privacy of client data with security and integration of data error localization and storage correctness insurance. The security analysis shows that encryption techniques in cloud is highly required and resilient to Byzantine failure, malicious data change attack, and even server colluding attacks.

VI. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in cloud computing,”in Proc.of IWQoS‟09, July 2009, pp.1–9

[2] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik,“Scalable and Efficient Provable Data Possession,” Proc. Of SecureComm ‟08, pp. 1– 10, 2008.

[3] Amazon.com, “Amazon s3 availability event: July20,2008,”Onlineathttp://status.aws.amazon.com/s3-20080720.html, July 2008.

[4] K. D. Bowers, A. Juels, and A. Oprea, “Hail: A high-availability and integrity layer for cloud storage,” in Proc. of CCS‟09, 2009,pp. 187–198.

[5] A. Juels and J. Burton S. Kaliski, “Pors: Proofs of retrievability for large files,” in Proc. of CCS‟07, Alexandria, VA, October 2007, pp.584–597

[6] Sun Microsystems, Inc., “Building customer trust in cloud computing with transparent security,” Online at https://www.sun.com/offers/details/sun transparency.xml, November 2009.

[7] Q. Wang, K. Ren, W. Lou, and Y. Zhang, “Dependable and secure sensor data storage with dynamic integrity assurance,” in Proc. Of IEEE INFOCOM‟09, Rio de Janeiro, Brazil, April 2009.

[8] Q. Wang, K. Ren, W. Lou, and Y. Zhang, “Dependable and secure data storage with dynamic integrity assurance,” in Proc. Of IEEE INFOCOM‟09, Rio de Janeiro, Brazil, April 2009.

[9] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissinger, Z.Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ‟07), pp. 598-609, Oct. 2007.

[10] T. S. J. Schwarz and E. L. Miller, “Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage,” Proc.of ICDCS ’06, pp. 12–12, 2006.

[11] J. Hendricks, G. Ganger, and M. Reiter, “Verifying Distributed Erasurecoded Data,” Proc. 26th ACM Symposium on Principles of Distributed Computing, pp. 139–146, 2007.

[12] Prashant Khobragade, Latesh Malik, “Data generation and analysis for digital forensic application using data mining”, Fourth international conference on Communication systems and Network Technologies (CSNT), pp. 458-462, Bhopal, 2014.