OPEN ACCESS

International
Journal
Of Modern Engineering Research (IJMER)

Towards Secure and Dependable Storage Services in Cloud Computing

Aarthi T.[1], Mrs. Rathi G.[2], Prabakaran R. S.[3]
PG Scholar (CSE)[1], Assistant professor UG(CSE)[2], PG Scholar(CSE)[3]
Sri Ramakrishna Engineering College Coimbatore

ABSTRACT: *Cloud Computing has emerged as one of the most influential paradigms in the IT industry for last few years. In such computing the data confidentiality, flexibility and access control are the main parameters to be considered in the research area. The proposed system investigate the problem of data security in cloud data storage.To achieve the availability and quality of cloud data storage service for users, the proposed system designs an distributed scheme with explicit dynamic data support, that includes block update, delete, and append. It also rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. The homomorphic token with distributed verification of erasure coded data, which achieves the integration of storage. The system ensures the security and dependability for cloud data storage under the aforementioned adversary model. Analysis shows that this scheme is highly efficient and resilient against byzantine failure, severals data modification attack and colliding attacks.*

Keywords: *user, cloud server, third party auditor, public auditing*

I. INTRODUCTION TO CLOUD COMPUTING

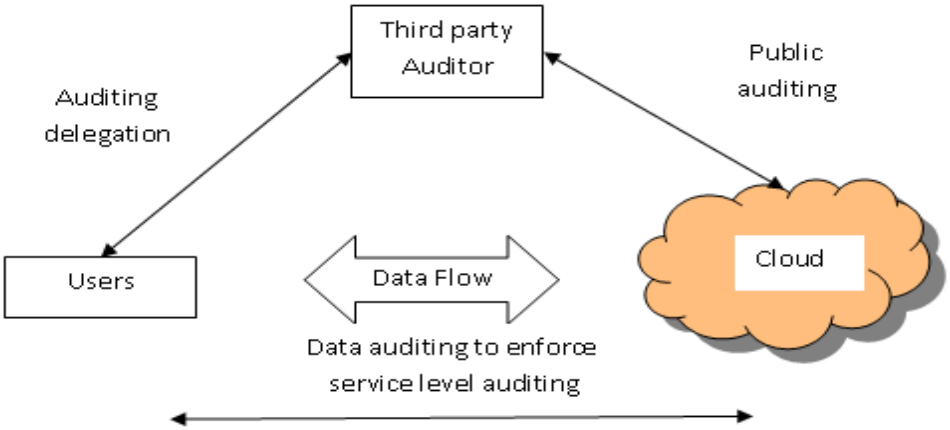
Cloud computing is the delivery information as a service, which shares data resources, software, and data information that are provided to computers as a metered service over a network .

Cloud computing provides data access and data storage resources without requiring cloud users.End users access cloud based applications through a web browser or a light weight desktop or mobile app while the data are stored on servers at a remote location. Cloud application providers strive to provide better service and performance on end-user computers.

II. PROPOSED SYSTEM

In cloud data storage system, user store their data in the cloud. The correctness and availability of the data files [1], [2] stored on the distributed cloud servers must be guaranteed. The key issues is to effectively detect unauthorized data modification and corruption. In order to strike a good balance between error resilience and data dynamics, system explore the algebraic property of our token computation and erasure-coded data, that efficiently support dynamic operation on data blocks. the time, computation data resources, and even the related online burden of users data are saved ,by providing the extension of the proposed main scheme to support third-party auditing. It is well known that erasure-correcting code[4], [6] may be used to tolerate multiple failures in distributed data storage systems. In order to achieve the assurance of data storage correctness and also data error localization simultaneously, our scheme relies on the precomputed verification tokens. The main idea is that before data file distribution, the user pre computes certain number of verification tokens on individual vector. The proposed scheme achieves the integration of storage correctness insurance and data error localization. Error localization is key prerequisite for eliminating errors in storage systems. It is also of critical importance to identify potential threats from external attacks. The system also provide the extension of the proposed main scheme is to support the third-party auditing, where users can safely delegate the data integrity checking tasks to third party auditors and be worry-free to use the cloud storage services.

III. ARCHITECHTURE DIAGRAM



3.1. Developing an Cloud model

Initially the basic network model for the cloud data storage is developed in this module. Three different entities can be identified as follows: User: user is the one who stores data in the cloud and relies on the cloud for data storage and data computation, can be either enterprise or individual customers. Cloud Server (CS):is the one, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources. Third-Party Auditor: who are expertise and have the capabilities that users wont have, who is trusted to assess and expose risk of cloud storage services on behalf of the users upon request.

3.2. Implementing the file distribution and the token pre-computation

In this module we use erasure-correcting code to tolerate multiple failures in distributed storage systems. The data file F redundantly across a set of n = m + k distributed servers. An (m; k) Reed-Solomon erasure-correcting code is used to create k redundancy parity vectors from m data vectors in such a way that the original m data vectors can be reconstructed from any m out of the m + k data and parity vectors. By placing each of the m + k vectors on a server, where the original file can survive the failure of any k of the m + k servers without any loss of data , with a space overhead of k = m. For support of efficient original file, our file layout is systematic ,where the unmodified m data file vectors together with k parity vectors is distributed across m + k different servers. After the file distribution operation precompution of the token is performed. Token precomputation is the process for assuring the data storage correctness and data error localization simultaneously, our scheme entirely relies on the verification tokens that is precomputed. The main idea is of this project is to precomputes a certain number of short verification tokens on individual vector before file distribution the user $G^{(j)}$ ($j \in \{1; \ldots ; n\}$), random subset of data blocks is covered by each token.

3.3. Implementation of Correctness Verification and Error Localization

Many previous scheme [3], [5] do not explicitly consider the problem of data error localization. In this module, the system integrate the correctness verification and error localization (misbehaving server identification) . The response values from servers for each challenge contain information to locate potential data error(s).

3.4. Implementation of Error Recovery and Third party auditor

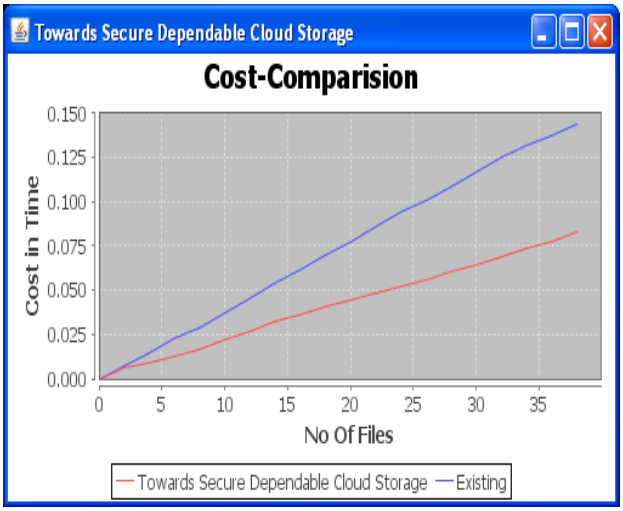
After identifying the misbehaving server from among all other servers we need to recover those files. The user can always ask servers to send back blocks of the r rows specified in the challenge and regenerate the correct blocks by erasure correction, shown in Algorithm, as long as the number of identified misbehaving servers is less than k. The newly recovered blocks can then be redistributed to the misbehaving servers to maintain the correctness of storage.

3.5. Providing dynamic data operation support

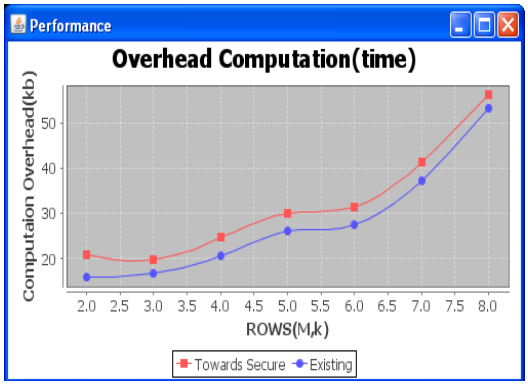
In this module we provide the dynamic data operation support to user [7], [8], [9]. Normally there are four categories of operation available Update operation, delete operation, append and insert operation. In update operation we have to update the existing or already available blocks of data in servers in this operation the user must priory know about the data block which is going to modify or alter. We use the master key to perform that action to update the existing file. In Delete operation first we define the data blocks that are need to remove

from the data server and after remove such file from the server we have to rearrange the remaining data blocks in the storage. The Append and the Insert are the same operation but in append we add new data's to already existing server and the insert operation is we embedding the data for already existing data. Master key is the basic need for all dynamic data support operations performing in data servers.

IV. EVALUATION



The following graph shown in Fig.1 is cost comparison graph in which, number of files ranging from 0 to 35 are taken along x-axis and cost time taken for upload file ranging from 0 to 0.15 minutes are taken along y-axis. It can be inferred from the graph that as like Encryption; Decryption time taken by Reed Solomon Erasure Code is lesser than existing System which indicates proposed system works faster than the existing system.



The following graph shown in Fig.2 is overhead compuation graph in which, number of files ranging from 0 to 8 are taken along x-axis and overhead taken for distribute the file ranging from 10 to 50 kb are taken along y-axis. It can be inferred from the graph that as like Encryption; Decryption time taken by Reed Solomon Erasure Code is higher than existing System which indicates proposed system works faster than the existing system.

V. CONCLUSION AND FUTURE WORK

Thus the system investigates the problem of data security in cloud storage of data, which is essentially a distributed data storage system. The system achieve the assurances of cloud data integrity and availability and enforce the quality of dependable cloud storage service for users , by an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. The system rely on erasure-correcting code in the file distribution preparation to provide redundancy parity vectors and guarantee the data dependability. By utilizing the homomorphic token with distributed verification of erasure code, this scheme achieves the integration of data storage correctness insurance and data error localization, when data corruption has detected during the data storage correctness verification across the distributed servers, it can

almost guarantee the simultaneous identification of the misbehaving server. Considering the time, computation of data resources, and even the related online burden of users, the system also provide the extension of the proposed main scheme to support third-party auditing, where users can safely delegate the integrity checking tasks to thirdparty auditors and be worry-free to use the cloud data storage . by detailed security and extensive results, the system show that proposed scheme is highly efficient and resilient to Byzantine failure, malicious data file modification attack, and even server attacks.

The system ensures the security and dependability for cloud data storage under the aforementioned model. The Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure; malicious data file modification attack, and even server attacks. The system can enhance work by using Raptor codes is a additional pre-coding on an appropriate LT-Code. In asymptotic settings,a universal Raptor Codes with linear encode/decode time for which the failure probability converges to 1 polynomial fast in input size.

REFERENCES

[1] Ateniese.G, Burns.R, Curtmola.R, Herring.J, Kissner.L, Peterson.Z, and Song.D, "Provable Data Possession at UntrustedStores," Proc. 14th ACM Conf. Computer and Comm. Security (CCS'07), pp. 598-609, Oct. 2007.

[2] Bowers.K.D, Juels.A, and Oprea.A, "HAIL: A High-Availability and Integrity Layer for Cloud Storage," Proc. ACM Conf. Computer and Comm. Security (CCS '09), pp. 187-198, 2009.

[3] Erway.C, Kupcu.A, Papamanthou.C, and Tamassia.R, "Dynamic Provable Data Possession," Proc. 16th ACM.

[4] Hendricks.J, Ganger.G, and Reiter.M, "Verifying Distributed Erasure-Coded Data," Proc. 26th ACM Symp. Principles of Distributed Computing, pp. 139-146, 2007.

[5] Juels.A and Kaliski.B.S Jr., "PORs: Proofs of Retrievability for Large Files," Proc. 14th ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

[6] Plank.J.S and Ding.Y, "Note: Correction to the 1997 Tutorial on Reed-Solomon Coding," Technical Report CS-03-504, Univ. of Tennessee, Apr. 2003.

[7] Schwarz.T and Miller.E.L, "Store, Forget, and Check: Using Algebraic Signatures to Check Remotely Administered Storage," Proc. IEEE Int'l Conf. Distributed Computing Systems (ICDCS '06), pp. 12-12, 2006.

[8] Wang.Q, Wang.C, Li.J, Ren.K, and Lou.W, "Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security (ESORICS '09), pp. 355-370, 2009.WANG ET AL.: TOWARD SECURE AND DEPENDABLE STORAGE SERVICES IN CLOUD COMPUTING 231

[9] Wang.C, Wang.Q, Ren.K, and Lou.W, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM, Mar. 2010. [10] Wang.C, Ren.K, Lou.W, and Li.J, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.