Towards Secure and Dependable Storage Services in Cloud Computing

P. Joseph Charles [1], S.Mathiyalagan [2]
[1]Assistant professor- IT
[2]M.Sc., Comp science
[1, 2] St.joseph'scollege,Trichy

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 investigates the problem of data security in cloud data storage. To achieve the availability and quality of cloud data storage service for users, I propose in this paper a flexible distributed storage integrity auditing mechanism, utilizing the homomorphism token and distributed erasure-coded data. The homomorphic token with distributed verification of erasure coded data, which achieves the integration of storage. Considering the cloud data are dynamic in nature, the proposed design further supports secure and efficient dynamic operations on outsourced data, including block modification, deletion, and append. Analysis shows the proposed scheme is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks.*

I. INTRODUCTION

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 tenders 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 attempt to provide better services and performance on end-user computers.

Three different network entities can be identified as follows:

• **User**: an individual, who has data to be stored in the cloud and relies on the cloud for data storage and computation, can be either enterprise or individual clients.

• **Cloud Server (CS)**: an individual, which is managed by **cloud service provider**(CSP) to provide data storage service and has substantial storage space and computation resources

• **Third Party Auditor (TPA)**: an elective TPA, who has knowledge and facilities that users may not have, is confidential to assess and expose risk of cloud storage services on behalf of the users upon application. In cloud data storage, a user stores his data through a CSP into a set of cloud servers, which are running in a synchronized, cooperated and distributed manner. Data redundancy can be engaged with technique of erasure correcting code to further tolerate faults or server crash as handler's data grows in size and importance. Thereafter, for application purposes, the user interacts with the cloud servers via CSP to access or recover his data .In some cases, the customer may need to perform block level operations on his data.

Cloud computing and storage provides users with capabilities to store and process their data in third-party data centres. Organizations use the cloud in a variety of different service models (with acronyms such as SaaS, PaaS, and IaaS) and deployment models (private, public, hybrid, and community). Security concerns associated with cloud computing fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the cloud). The responsibility is shared, however. The provider must ensure that their infrastructure is secure and that their clients' data and applications are protected, while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially sensitive data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the sixth biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data centre. Additionally, data centres must be frequently monitored for suspicious activity.

In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result, there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured.[6] Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole data Centre to go down or be reconfigured to an attacker's liking.

III. PROPOSED SYSTEM

In cloud data storage system, user stores their data in the cloud. The accuracy and convenience of the data files stored on the distributed cloud servers must be assured. The key issue is to successfully detect unauthorized data modification and corruption. In order to strike a good poise 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 interconnected online burden of customer 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 may be used to tolerate several failures in distributed data storage systems. In order to accomplish the guarantee of data storage correctness and also data error localization instantaneously, our scheme relies on the precomputed verification tokens. The main idea is that before data file distribution, the user pre computes certain number of confirmation 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 significance to identify potential threats from external attacks. The system also make available the extension of the proposed main scheme is to support the third-party auditing, where customers can safely delegate the data integrity checking tasks to third party auditors and be worry-free to use the cloud storage services.

3.1 ENSURING CLOUD DATA STORAGE

In cloud data storage system, users store their data in the cloud and no extended possess the data locally. Thus, the perfection and convenience of the data files being stored on the distributed cloud servers must be assured. One of the key issues is to effectively detect any unauthorized data modification and corruption, probably due to server negotiation and/or random Byzantine failures.

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

In this segment we use erasure-correcting code to accept multiple failures in distributed storage systems. The data file F redundantly across a set of n = r + d distributed servers. An (r; d) Reed-Solomon erasure-correcting code is used to create d redundancy parity vectors from r data vectors in such a way that the original r data vectors can be rebuilt from any r out of the r + d data and parity vectors. By placing each of the r + d vectors on a server, where the original file can survive the failure of any d of the r + d servers without any loss of data , with a space overhead of d = r. For support of effective original file, our file layout is systematic where the unmodified m data file vectors together with d parity vectors is distributed across r + d different servers. After the file distribution operation pre-computation of the token is executed. Token pre-computation is the procedure for guaranteeing the data storage correctness and data error localization instantaneously. Our pattern entirely trusts on the authentication token that is pre-computed. The main idea is of this paper is to pre-computes a certain number of short authentication tokens on individual customer before file distribution the user random subset of data blocks is covered by each token.

3.3. Implementation of Correctness Verification and Error Localization

Many previous schemes do not explicitly consider the delinquent of data error localization. In this module, the system integrates the exactness authentication 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 detecting the misbehaving server from among all other servers we need to recover those files. The customer can always ask servers to send back blocks of the b rows

specified in the challenge and stimulate the correct blocks by erasure correction, shown in Algorithm, as long as the number of identified misbehaving servers is less than d. 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 we provide the dynamic data operation provision to customer. Normally there are four groupings of operation available Update operation, delete operation, append and insert operation. In update operation we have to update the current 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 adjust. We use the master key to execute that action to update the existing file. In Delete operation first we define the data blocks that are need to eliminate from the data server and after eliminate such file from the server we have to relocate the left behind 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 inserting the data for already existing data. Master key is the basic need for all dynamic data support operations performing in data servers.

IV. CONCLUSION

To achieve the of cloud data reliability, accessibility and enforce the quality of dependable cloud storage service for users, we propose an actual and elastic distributed scheme with clear dynamic data support. By using the homomorphic token with distributed authentication of erasure-coded data, our scheme achieves the integration of storage correctness insurance and data error localization. Considering the time, computation resources, and even the correlated online burden of customers, we also offer the extension of the proposed main scheme to support third-party auditing, where customers can safely representative the integrity checking tasks to third-party auditors and be worry-free to use the cloud storage services. The system attains the guarantees of cloud data integrity and convenience and enforces the worth of dependable cloud storage service for customers, by an effective and flexible distributed scheme with explicit dynamic data support.

REFERENCES

[1] CH.Venkatalakshmi et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (6), 2012,5374-5377

[2] A paper was presented at the 17th IEEE International Workshop on Quality of Service (IWQoS'09).

[3] Amazon.com, "Amazon web services (aws)," Online at http://aws.amazon.com/, 2009.