IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-03, Issue-09 E-ISSN: 2347-2693

Secure Data Storage and Retrieval Using Adaptive Integrity Protocol Model in Cloud Environment

S.Sujitha[1*] and S. J. Mohana[2]

Erode Arts & Science College (Autonomous), Erode-638 009

www.ijcseonline.org

Received: Aug/12/2015 Revised: Aug/28/2015 Accepted: Sep/20/2015 Published: Sep/30/2015

Abstract— Cloud computing is provide a dynamically scalable resources provisioned as a service over the webpage. The third-party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud environment promise to reduce capital as well as operational expenditures for hardware and software. Various distinct architectures are introduced and discussed according to their security and privacy capabilities and prospects. It provides four distinct models in form of abstracted multi-cloud architectures. These developed multi cloud architectures allow to categorize the available schemes and to analyze them according to their security reimbursement. An assessment of the different methods replication of applications, partition of application system into tiers, partition of application logic into fragments and partition of application data into fragments is given in particular. In addition, enabling public audit ability for cloud storage is of critical importance so that users can resort to an Integrity third party auditor (ITPA) to check the integrity of outsourced data and be worry-free. This paper proposes a secure cloud storage system supporting Isolation-preserving public auditing. It further extends the result to enable the ITPA to perform audits for multiple cloud users simultaneously and efficiently.

Keywords— Cloud Computing, Multi-cloud, Integrity, Isolation Preserving Auditing, ITPA

I. INTRODUCTION

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [8]. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as critical data and processes. When considering using a cloud service, the user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. Hence, a strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing. Depending on the political context this trust may touch legal obligations. An attacker that has access to the cloud storage component is able to take snapshots or alter data in the storage. This might be done once, multiple times, or continuously. An attacker that also has access to the processing logic of the cloud can also modify the functions and their input and output data.

Replication of applications allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.

Partition of application System into tiers allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.

Partition of application logic into fragments allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.

Partition of application data into fragments allows distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

The existing system utilizes the technique of public key based homomorphism linear authenticator (or HLA for short), which enables Third Party Auditor to perform the auditing without demanding the local copy of data and thus drastically reduces the communication and computation overhead as compared to the straightforward data auditing approaches. By integrating the HLA with random masking, the protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process. The aggregation and algebraic properties of the authenticator further benefit our design for the batch auditing. Various prime numbers are assigned as tags for each segment of file which is stored in server. Each segment is having two prime numbers each of which belongs to a different prime order. The third party auditor knows the prime numbers in a random manner. During verification, the third party auditor sends the numbers as random challenge and if the numbers are matched with tags then the file integrity is said to be verified

The rest of this paper is organized as follows. Section 2 presents the related work followed by the main

contribution multi cloud security as well as the problem definition in Section 3. Section 4 gives a brief introduction to Isolation Preserving Auditing while and explains the proposed approach. Finally, Section 5 presents the evaluation of the algorithm followed by the conclusions and future work described in Section 6 and Section 7.

II. RELATED WORK

The cloud computing paradigm has been hailed for its promise of enormous cost-saving potential. In spite of this euphoria, the consequences regarding a migration to the cloud need to be thoroughly considered. Amongst many obstacles present, the highest weight is assigned to the issues arising within security. Cloud security is discussions to date mostly focus on the fact that customers must completely trust their cloud providers with respect to the confidentiality and integrity of their data, as well as computation faultlessness. However, another important area is often overlooked: if the Cloud control interface is compromised, the attacker gains immense potency over the customer's data. This attack vector is a novelty as the result of the control interface (alongside with virtualization techniques) being a new feature of the Cloud Computing paradigm, as NIST lists On-demand self-service and Broad network access as essential characteristics of Cloud Computing systems [1]. The main goal of this paper [2] is the investigation and evaluation of security and privacy threats caused by the unawareness of users in the cloud. Although the methods and techniques described in this paper are applicable to arbitrary IaaS providers, they focused on one of the major cloud providers

However, to actually agree on a specific SLA a user first has to assess his organizational risks related to security and resilience [3]. Current solutions that restrict the provision of sensible services to dedicated private, hybrid or so called national clouds do not go far enough as they reduce the user's flexibility when scaling in or out and still force him to trust the cloud provider. Furthermore, private clouds intensify the vendor lock-in problem. Last but not least, there is no support for deciding which services and data could be safely migrated to which cloud. Instead they demanded new methods and technical support to put the user in a position to benefit from the advantages of cloud computing without giving up the sovereignty over his data and applications. In their current work, they followed a system oriented approach focusing on technical means to achieve this goal.

They identified security as a major obstacle that prevents someone to transfer his resources into the cloud. In order to make sound business decisions and to maintain or obtain security certifications, cloud customers need assurance that providers are following sound security practices and behave according to agreed SLAs [4]. Thus, their overall goal is the development of a flexible open source cloud platform that integrates all necessary components for the development of user-controlled and -monitored secure cloud environments [5].

III. MAIN CONTRIBUTIONS

The proposed system includes all the existing system approach which covers multiple cloud service provider environments. In addition, size blocks of data are being processed with varying size nature in different cloud locations having same copy of data. The data blocks is stored and retrieved in different cloud locations based on the storage and computational capability. Thus the proposed system explores such issue to provide the support of variable-length block verification. Likewise, the privacy level for all cloud providers is analyzed by trusted authority and security degree and performance is quantified for encryption algorithms. The following main objective is proposed system.

- To replicate the applications that allows to receive multiple results from one operation performed in distinct clouds and to compare them within the own premise. This enables the user to get evidence on the integrity of the result.
- To partition the application System into tiers that allows separating the logic from the data. This gives additional protection against data leakage due to flaws in the application logic.
- To partition the application logic into fragments that allows distributing the application logic to distinct clouds. This has two benefits. First, no cloud provider learns the complete application logic. Second, no cloud provider learns the overall calculated result of the application. Thus, this leads to data and application confidentiality.
- To partition the application data into fragments that allows distributing fine-grained fragments of the data to distinct clouds. None of the involved cloud providers gains access to all the data, which safeguards the data's confidentiality.

IV. PROPOSED PROTOCOL

The proposed system includes all the existing system approach which covers multiple cloud service provider environments. In addition, size blocks of data are being processed with varying size nature in different cloud locations having same copy of data. The data blocks is stored and retrieved in different cloud locations based on the storage and computational capability. Thus the proposed system explores such issue to provide the support of variable-length block verification. Likewise, the privacy level for all cloud providers is analyzed by trusted authority and security degree and performance is quantified for encryption algorithms. The proposed system has following advantages.

- Partial data of files are taken from multiple mirror locations and send to selected client.
- Suitable for very large size files.
- Irrelevant size blocks of data are handled among the multiple cloud service providers based on their computational capabilities.

- Different trust level is set to different cloud providers and encryption/decryption is varied based on the clouds computational capability.

ITPA PROTOCOL PROCESS

1) MULTI-CLOUD SECURITY

In this first step process, the cloud node id and the cloud provider name is added. There are more cloud nodes for single cloud provider. From the trusted authority, the cloud node receives secret tags for file blocks so that the blocks can be processed/ verified by the cloud nodes. The next step, files are added to cloud nodes and executed based on a) Replication of applications from the random cloud node, b) Partition of application System into tiers such that even the web server does not know the location of record in database server, c) Partition of application logic into fragments such that half of the application login in one file stored in one cloud node and other half of the application logic in other file stored in other cloud node and d) Partition of application data into fragments such that partial records in one cloud database and remaining records in other cloud database.

2) PRIVACY PRESERVING AUDITING PROTOCOL

In this step, the file name is selected, the file content is split into various segments and each segment is given two prime numbers each of which belongs to two prime order. One is given to user; other is given to third party auditor. The combination of the two is kept in server. During auditing, third party auditor randomly picks the segment ids and send corresponding prime number vector to cloud server. If the credentials match, then the file integrity is said to be verified.

3) BATCH AUDITING PROTOCOL

In this step, during auditing, two processes of same third party auditor randomly pick the two set of segment ids and send corresponding prime number vectors to cloud server. If the credentials match, then the file integrity is said to be verified.

4) STORAGE AND COMPUTATIONAL CAPABILITY BASED FILE STORAGE

A) FILE SELECTION

In this step, the file content is selected from client files. The file data is saved in cache.

B) ENCRYPTION

In this step, either DES (Data Encryption Standard) or AES (Advanced Encryption Standard) encryption work is carried out and the selected file is encrypted.

Speed: The requirement of this level presents that no sensitive information in the data. Cloud location with low computational capability uses weak encryption composition (DES) and high computational capability uses more encryption (AES) to obtain more performance for using cloud services.

C) DECRYPTION

In this step, decryption work (DES and AES) is carried out.

V. EXPERIMENTAL RESULTS

Table 1.1 is describe the theoretical analysis for existing system and proposed system. The replication allocation and computation overhead details

METHOD	REPLICATION	COMPUTATION OVERHEAD
Resource Replication	Required	In client only
PIR based segmentation	Not required	Low in client tier/ More in database tier (stored
		procedure) and negligible in web tier
Segmentation of application logic and data	Not required	In client only
Third party auditing	Not required	High In client, Low in third party system and
		negligible in cloud node

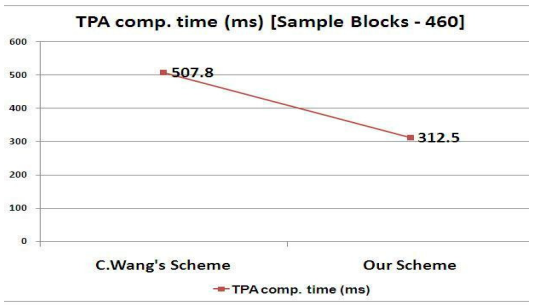

FIG 1.1 ITPA Computation Time Chart Comparisons

Fig 1.2 ITPA Computation Time in % Findings:

- The proposed system provides a safe cloud storage methodology which supports privacy-preserving

third party auditing better than existing system.

- This thesis suggests that the security can be increased if the architecture is changed from single cloud to multi cloud environment.
- Security mechanisms involved during third party auditing of outsourced data is discussed.
- The methods are studied to perform the auditing without demanding the local copy of data and thus drastically reduce the communication and computation overhead.
- Four schemes are presented that can be applied in multi cloud environment to increase the security aspects.
- Hiding resource usage statistics of a single resource for a single cloud provider is achieved if first method is applied.
- The computation and data transfer size is very low if the second method is applied.
- The third method provides the security such that a single provider may not be aware of the execution flow of the single application as well as the cloud provider could not know or access all the data.
- The fourth method provides the benefit of auditing with very low credential data to verify the file content.
- It is proved that the third party auditing computation time is better than existing approach.
- The future study should focus on security proof and enhancements in data retrieval of the proposed framework.

VI.CONCLUSION

It is believed that almost all the system objectives that have been planned at the commencement of the software development have been net with and the implementation process of the paper is completed. A trial run of the system has been made and is giving good results the procedures for processing is simple and regular order. The process of preparing plans been missed out which might be considered for further modification of the application. The paper effectively stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever necessary so that they are secure.

VII. FUTURE ENHANCEMENTS

The following enhancements are should be in future.

- The application if developed as web services, then many applications can make use of the records.
- The data integrity in cloud environment is not considered. The error situation can be recovered if there is any mismatch.
- The web site and database can be hosted in real cloud place during the implementation.

REFERENCES

[1] S. Bugiel, S. Nurnberger, T. Poppelmann, A.-R. Sadeghi, and T.Schneider, ―AmazonIA: When Elasticity Snaps Back,‖ Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 389-400, **2011**.

[2] Amazon Elastic Compute Cloud (Amazon EC2).http://aws.amazon.com/ec2/.

[3] D. Catteddu (Ed.): Security & Resilience in Governmental Clouds – Making an informed decision. ENISA Report, January **2011**.

[4] J. Somorovsky, M. Heiderich, M. Jensen, J. Schwenk, N. Gruschka, and L. Lo Iacono, ―All Your Clouds Are Belong to Us: Security Analysis of Cloud Management Interfaces,‖ Proc. Third ACM Workshop Cloud Computing Security Workshop (CCSW '11), pp. 3-14, **2011**.

[5] P. Mell and T. Grance: The NIST Definition of Cloud Computing (Draft). Recommendations of the National Institute of Standards and Technology (NIST), Special Publication 800—145 (Draft), available at http://csrc.nist.gov/publications/drafts/800-145/Draft-SP-800-145_cloud-definition.pdf, January **2011**.

[6] G. Danezis and B. Livshits, ―Towards Ensuring Client-Side Computational Integrity (Position Paper),‖ Proc. ACM Cloud Computing Security Workshop (CCSW '11), pp. 125-130, **2011**.