ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

ENHANCED MULTIDIVISION AND REPLICATION OF DATA IN MULTICLOUD FOR SECURITY FRAMEWORK PROTOCOL

[1]R.Maheswari, [2]S.Udhaya Kumar, [3]V.Sathish Kumar
[1]Assistant Professor, [2,3]UG Scholar,
Department Of Computer Science and Engineering,
Nandha College of Technology, Erode.

Abstract— Cloud computing is give a dynamically scalable possessions provisioned as a service in excess of the webpage. The third-party, on-demand, self-service, pay-per-use, and flawlessly scalable computing resources and services obtainable by the cloud environment assure to decrease resources as well as operational expenditures for hardware and software. Various separate architectures are developed and discussed according to their security and privacy capabilities and forecast. It provides four dissimilar models in form of abstracted multi-cloud architectures. These developed multi cloud architectures allow to classify the accessible schemes and to examine them according to their security settlement. An assessment of the diverse methods duplication of applications, division of application system into tiers, division 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 significance so that users are able to 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 behind Isolation-preserving public auditing. It further extends the result to enable the ITPA to carry out audits for multiple cloud users concurrently and proficiently.

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

I. INTRODUCTION

Cloud computing creates a huge number of security issues and challenges. A record of security threats to cloud computing is offered in [8]. These issues collection from the required trust in the cloud provider and attacks on cloud interfaces to use wrongly the cloud services for attacks on other systems. The main trouble that the cloud computing paradigm utterly includes is that of secure outsourcing of sensitive as well as significant data and processes. When considering using a cloud service, the user must be awake of the fact that all data provide to the cloud provider leave the own control and protection sphere. Hence, a sturdy trust relationship between the cloud provider and the cloud user is considered a common prerequisite in cloud computing. Depending on the supporting context this trust may touch permissible obligations. An attacker that has access to the cloud storage element is able to take snapshots or modify data in the storage.

This may be done once, several times, or continuously. An attacker that also has access to the processing logic of the cloud be capable of altering the functions and their input and output data.

- Replication of applications permits to receive many results from one operation performed in separate clouds and to evaluate them within the own premise. This enables the user to get evidence on the reliability of the result.
- Partition of application System into tiers allows distancing the logic from the data. This provides extra protection against data outflow due to flaws in the application logic.
- Partition of application logic into fragments permits distributing the application logic to separate clouds. This has two benefits. First, no cloud provider understands the total application logic. Second, no cloud provider understands the overall calculated result of the application. Thus, this leads to data and application privacy.
- Partition of application data into fragments permits distributing fine-grained fragments of the data to different clouds. Nothing of the involved cloud provider's additions access to all the data, which safeguards the data's privacy.

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

The existing system employs the technique of public key based homomorphism linear authenticator (or HLA for short), which enables Third Party Auditor to achieve the auditing without challenging the local copy of data and thus radically decreases the communication and computation overhead equally compared to the straightforward data auditing methods. By integrating the HLA with arbitrary masking, the protocol assurances that the TPA could not understands any knowledge about the data content kept in the cloud server through the efficient auditing process. The combination and algebraic properties of the authenticator additionally use our design for the batch auditing. Various prime numbers are allocated as tags for every segment of file which is stored in server. Every segment have two prime numbers each of which goes to a unlike prime order. The third party auditor recognizes the prime numbers in a random method. During verification, the third party auditor leads the numbers as casual challenge and if the numbers are coordinated with tags formerly the file integrity is said to be checked

The rest of this paper is prepared as follows. Section 2 offerings the related work tracked by the main contribution multi cloud security as well as the difficult definition in Section 3. Section 4 yields a brief introduction to Isolation Preserving Auditing while and describes the proposed method. In conclusion, Section 5 offerings the calculation of the algorithm followed by the conclusions and future work explained in Section 6 and Section 7.

II. RELATED WORK

The cloud computing paradigm has been greeted for its promise of huge cost-saving potential. In spite of this ecstasy, the consequences regarding a immigration to the cloud need to be carefully measured. Amongst many obstacles present, the highest weight is allotted to the subjects rising within security. Cloud security is deliberations to date mostly focus on the detail that customers must completely trust their cloud providers with respect to the secrecy and integrity of their data, as well as computation impeccability.

However, another significant area is often ignored: if the Cloud control interface is compromised, the attacker gains huge potency over the customer's data. This attack vector is a newness as the result of the control interface (alongside with virtualization techniques) existence a new feature of the Cloud Computing paradigm, as NIST shows On-demand self-service and Broad network access as critical characteristics of Cloud Computing systems [1]. The main target of this paper [2] is the investigation and evaluation of security and privacy threats affected of the unawareness of users in the cloud. Although the methods and techniques explained in this paper are appropriate to arbitrary IaaS providers, they dedicated on one of the main cloud providers

However, to actually decide on an exact SLA a user first has to weigh his organizational risks associated to security and elasticity [3]. Present solutions that check the delivery of sensible services to dedicated private, hybrid or so called national clouds do not go far sufficient as they decrease the user's elasticity when climbing in or out and still vigor him to trust the cloud provider. Additionally, private clouds intensify the vendor lock-in problem. Last but not least, there is no provision for deciding which services and data could be securely voyaged to which cloud. Instead they required new methods and technical provision to put the user in a position to lead from the advantages of cloud computing without giving up the dominion over his data and applications. In their present work, they tracked a system oriented method concentrating on technical means to attain this goal.

They recognized security as a main obstacle that stops someone to transfer his possessions into the cloud. In order to make sound business decisions and to keep or obtain security certifications, cloud customers requisite guarantee that providers are following sound security performs and behave according to decided SLAs [4]. Thus, their overall goal is the development of a elastic open source cloud platform that integrates all necessary constituents for the development of user-controlled and -monitored secure cloud environments [5].

III. MAIN CONTRIBUTIONS

The proposed system contains all the existing system methods which covers multiple cloud service provider environments. Additionally, size blocks of data are being processed with varying size nature in different cloud locations having equal copy of data. The data blocks is stored and gathered in different cloud locations based on the storage and computational capability. Thus the proposed system provides such issue to provide the support of variable-length block verification. similarly, the privacy level for all cloud

providers is analyzed by trusted authority and security grade and performance is measured for encryption algorithms. The following major objective is proposed system.

- To duplicate the applications that permits to receive many results from one operation performed in different clouds and to compare them inside the own premise. This enables the user to grow suggestion on the integrity of the result.
- To partition the application System into tiers that permits separating the logic from the data. This offers additional protection beside data leakage due to faults in the application logic.
- To partition the application logic into fragments that permits distributing the application logic to different clouds. This has two benefits. First, no cloud provider understands the whole application logic. Second, no cloud provider understands the overall evaluated result of the application. Thus, it leads to data and application privacy.
- To partition the application data into remains that permits dispensing fine-grained fragments of the data to different clouds. None of the concerned cloud providers improves access to all the data, which safeguards the data's privacy.

IV. PROPOSED PROTOCOL

The proposed system contains all the existing system method which covers many cloud service provider environments. In addition, size blocks of data are presence processed with varying size nature in changed cloud locations having equal copy of data. The data blocks is stored and regained in different cloud locations created on the storage and computational capability. Thus the proposed system includes such issue to provide the care of variable-length block verification. Likewise, the privacy level for all cloud providers is scrutinized by trusted authority and security degree and performance is measured for encryption algorithms. The proposed system has following advantages.

- Limited data of files are taken from many mirror locations and send to selected client.
- Particular for very large size files.
- Irrelevant size blocks of data are touched among the multiple cloud service breadwinners based on their computational abilities.
- Different trust level is set to different cloud workers and encryption/decryption is varied founded on the exhausts computational capability.

ITPA PROTOCOL PROCESS

1) MULTI-CLOUD SECURITY

In this step process, the cloud node id and the cloud provider name is included. There are more cloud nodes for single cloud provider. From the trusted expert, the cloud node receives underground tags for file blocks so that the blocks can be processed/ confirmed by the cloud nodes. The next step, files are added to cloud nodes and executed based on a) Duplication of applications from the random cloud node, b) Wall of application System into levels such that even the web server does not understand the location of record in database server, c) Divider of application logic into remains such that half of the application login in one folder stored in one cloud node and other half of the application logic in other file stored in another cloud node and d) Partition of application data into remains such that partial records in each cloud database and remaining records in other cloud database.

2) PRIVACY PRESERVING AUDITING PROTOCOL

In this method, the file name is chosen, the file content is divided into various parts and each segment is given two main numbers each of which belongs to two prime order. One is given to user's other is given to third festivity auditor. The combination of the two is kept in server.

During reviewing, third party auditor randomly picks the segment ids and send consistent prime number course to cloud server. If the permits match, then the file truth is said to be verified.

3) BATCH AUDITING PROTOCOL

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

In this step, during checking, two processes of same third party auditor casually pick the two set of part ids and send agreeing prime number vectors to cloud waiter. If the permits match, then the file truth is said to be verified.

4) STORAGE AND COMPUTATIONAL CAPABILITY BASED FILE STORAGE

A) FILE SELECTION

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

B) ENCRYPTION

In this step, whether DES (Data Encryption Standard) or AES (Advanced Encryption Standard) encryption work is accepted out and the particular sleeve is encrypted.

Speed: The requirement of this close presents that no delicate information in the data. Cloud place with low computational skill uses weak encryption composition (DES) and high computational skill uses more encryption (AES) to obtain more act for using cloud services.

C) DECRYPTION

In this step, decryption effort (DES and AES) is passed out.

V. EXPERIMENTAL RESULTS

Table 1.1 is describe the academic analysis for current system and future system. The duplication distribution and totaling 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

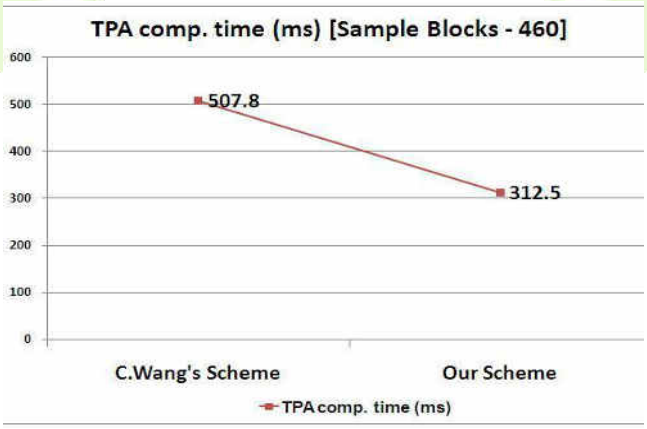

FIG 1.1 ITPA Computation Time Chart Comparisons

ISSN 2395-695X (Print)
ISSN 2395-695X (Online)

International Journal of Advanced Research in Biology Engineering Science and Technology (IJARBEST)

Vol. 2, Special Issue 10, March 2016

Fig 1.2 ITPA Computation Time In %

Findings:

- The future system provides a safe cloud storage methodology which capitals privacy-preserving third party auditing better than current system.
- This thesis recommends that the security can be increased if the architecture is changed from single cloud to multi cloud environment.
- Security methods difficult during third party auditing of outsourced data is conversed.
- The approaches are studied to perform the auditing without difficult the local copy of data and thus drastically reduce the communication and computation overhead.
- Four schemes are offered 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 gained if first method is applied.
- The computation and data transfer size is very low if the second technique is applied.
- The third method delivers the security such that a single provider may not be alert of the implementation flow of the single application as well as the cloud provider could not know or admittance all the data.
- The fourth technique provides the turnover of auditing with very low credential data to prove the file content.
- It is proved that the third party auditing computation time is improved than existing method.
- The future study should focus on security resistant and improvements in data recovery of the proposed framework.

VI.CONCLUSION

It is supposed that almost all the system objects that have been intentional at the commencement of the software development have been net with and the application 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 change of the application. The paper efficiently stores and retrieves the records from the cloud space database server. The records are encrypted and decrypted whenever needed so that they are secure.

VII. FUTURE ENHANCEMENTS

The following enhancements are should be in future.

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

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.

1. S. Groß and A. Schill, ―Towards User Centric Data Governance and Control in the Cloud,‖ Proc. IFIP WG 11.4 Int'l Conf. Open Problems in Network Security (iNetSeC), pp. 132-144, 2011.
2. M. Burkhart,M. Strasser, D. Many, and X. Dimitropoulos, ―SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics,‖ Proc. USENIX Security Symp., pp. 223-240, 2010.