ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

Enhancement of Service and Data Security in Multi-Cloud Environment

M.Nivetha Mani[1], Dr.R.Murugan[2]

Assistant Professor, Dept. of CSE, CK College of Engineering and Technology, Cuddalore, India[1]

Professor, Dept. of CSE, CK College of Engineering and Technology, Cuddalore, India[2]

ABSTRACT: Cloud computing is the growth of a variety oftechnologies that have come together to modify an organization's approach to building out an IT infrastructure. There are numerous issues in cloud that need to resolve with respect to security and privacy. Single storage of data cannot efficiently manage the application.Consequently, clouds need to deploy multiple data storage in order to allow the applications to choose therelevant data. The proposed model is to securely store the information or data into the cloud using the various security storage methods and splitting data into several chunks and store it on multiple cloud providers (e.g. Google, Microsoft, Linux etc) In a manner that preserves data confidentiality, integrity and ensures availability. This approach preserves security and privacy of user's sensitive information by replicating data across multiple clouds, using a secret sharing and homomorphic encryption technique and also defining the new algorithm (CDSA) for secure storage The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Multi Cloud data storage has many advantages over the different types of data storage. In this project enhanced to security and service model for cloud computing.
.

KEYWORDS:Cloud Computing, Security, Data Storage, Multi-Cloud and Homomorphic Encryption.

I. INTRODUCTION

The Cloud computing offers dynamically scalable resources provisioned as a service over the Internet. The third party, on-demand, self-service, pay-per-use, and seamlessly scalable computing resources and services offered by the cloud paradigm promise to reduce capital as well as operational expenditures for hardware and software. Clouds can be categorized taking the physical location from the viewpoint of the user into account. A public cloud is offered by third-party service providers and involves resources outside the user's premises. In case the cloud system is installed on the user's premise—usually in the own data center this setup is called private cloud. A hybrid approach is denoted as hybrid cloud[1]. This project will concentrate on public clouds, because these services demand for the highest Security requirements but also—as this project will start arguing include high potential for security prospects. In public clouds, all of the three common cloud service layers (IaaS, Paas, SaaS) share the commonality that the end-users' digital assets are taken from an intra -organizational to an inter- organizational context[2]. This creates a number of issues, among which security aspects are regarded as the most critical factors when considering cloud computing adoption. Legislation and compliance frameworks raise further challenges on the outsourcing of data, applications, and processes. One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds. Several approaches employing this paradigm have been proposed recently. They differ in partitioning and distribution patterns, technologies, cryptographic methods, and targeted scenarios as well as security levels [3]. This project is an extension of and contains a survey on this different security by multi-cloud adoption approaches. 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 benefits.

An assessment of the different methods with regard to legal aspects and compliance implications is given in particular. Field measurements show that large-scale storage systems commonly experience disk/sector failures, some of which can result in permanent data loss. For example, the annualized replacement rate (ARR) for disks in production storage systems is around 2-4 percent [4]. Data loss events are also found in commercial cloud-storage services. With the exponential growth of archival data, a small failure rate can imply significant data loss in archival storage. This motivates us to explore high performance recovery so as to reduce the window of vulnerability [5]. Regenerating codes have recently been proposed to minimize repair traffic (i.e., the amount of data being read from surviving servers). In essence, they achieve this by not reading and reconstructing the whole file during repair as in traditional erasure codes,

DOI: 10.15680/IJIRCCE.2016. 0410012

but instead reading a set of chunks smaller than the original file from other surviving servers and reconstructing only the lost (or corrupted) data chunks [6]. In this project, we design and implement a practical data integrity protection (DIP) scheme for regenerating-coding based cloud storage. We augment the implementation of functional minimum-storage regenerating (FMSR) codes and construct FMSR-DIP codes, which allow clients to remotely verify the integrity of random subsets of long-term archival data under a multi-server setting. FMSR-DIP codes preserve fault tolerance and repair traffic saving as in FMSR codes. This adds to the portability of FMSRDIP codes and allows simple deployment in general types of storage services [7]. By combining integrity checking and efficient recovery, FMSR-DIP codes provide a low-cost solution for maintaining data availability in cloud storage. There are different types of clouds that you can subscribe to depending on your needs.

A. MULTI-CLOUD MODEL

1.

It is a more complex system than a hybrid cloud, which is typically a paired private and public cloud. Multi-cloud add more clouds to the mix (i.e. perhaps two or more public IaaS providers, a private PaaS, private use-based accounting, etc.) which aims at minimizing the risk of service availability failure, corruption of data, loss of privacy, and the possibility of malicious insiders in the single cloud. Known also as, “cloud-of-clouds”, this strategy can improve the enterprise overall performance by avoiding vendor lock-in (proprietary rights) and using different infrastructures to meet the needs of diverse partners and customers to avoid the service unavailability and security risks that can occur inside a single cloud infrastructure [8]. And assume that the main purpose of shifting towards inter-clouds is to improve what was offered in single cloud by distributing the reliability, trust and the security among multiple cloud providers. The main aim is to provide the high security and flexible service model for cloud consumers. When the cloud consumer’s use a single cloud system, there may be a chance to loss their own data and it may be corrupted .Once the users lost their data or information, it can’t be easy to retrieve that. But our proposed system defined for multi cloud storage for the consumer’s access and storing data into the secure manner [9].

II. RELATED WORK

In public clouds, all of the three common cloud service layers (IaaS, Paas, SaaS) share the data from the end-users. This creates a number of issues, among which security aspects are regarded as the most critical factors when considering cloud computing adoption. One idea on reducing the risk for data and applications in a public cloud is the simultaneous usage of multiple clouds[10]. Cloud computing creates a large number of security issues and challenges. The cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems. The main problem in cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. The user must be aware of the fact that all data given to the cloud provider leave the own control and protection sphere. A strong trust relationship between the cloud provider and the cloud user is considered a general prerequisite in cloud computing [11].

III. PROPOSED ALGORITHM

In a proposed model, multi- clouds are used to mitigate the risks of malicious data manipulation, disclosure, and process tampering. Integrating multi-clouds, the trust assumption can be lowered to an assumption of no collaborating cloud service providers. This setting makes it much harder for an external attacker to retrieve or tamper hosted data or applications of a specific cloud user. Multi cloud approaches are operating on different cloud service levels, are partly combined with cryptographic methods, and targeting different usage scenarios. This proposed model also defined by the new security algorithm for data storage process into the cloud server and using replication technique splitting the data and stored into several chunks of clouds or multi clouds. Multi cloud model overcoming the data loss, reduce the data corruption and increase the availability of cloud services [6]. The component present in proposed system is multi cloud model for cloud consumers and cloud broker and cloud providers. The cloud providers have ‘N’ number of datacentres for the consumers’ data storage.

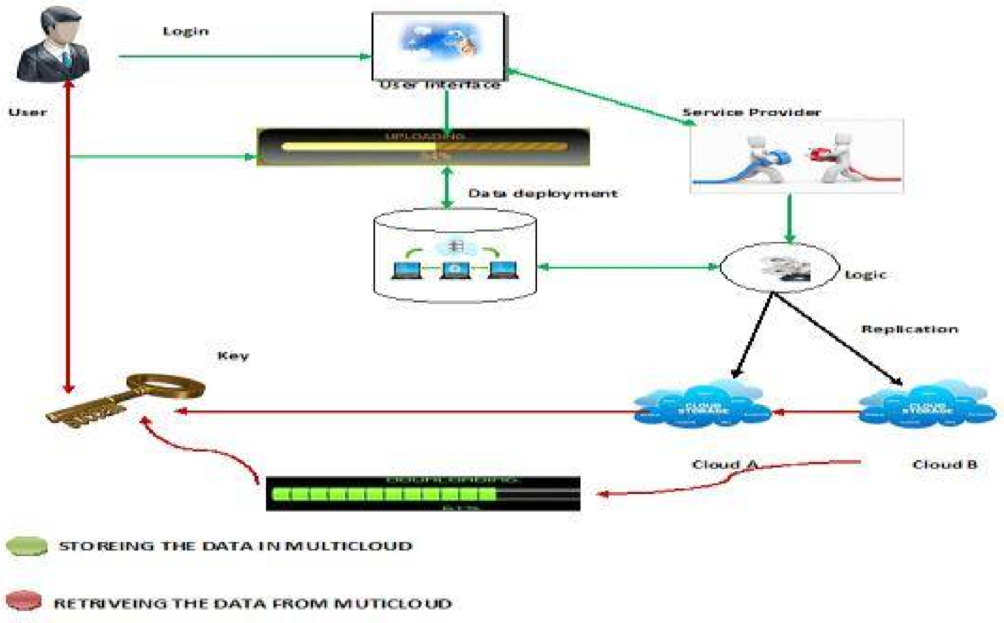

Fig.1. System Architecture

IV. PSEUDO CODE

```
MODULE M
Step 1:Begin
Step 2:Data is stored on cloud
Step 3:Data is encrypted
Step 4:Verification of data is done by CSP using AES
Step 5:If data is valid
Step 6:Go To Module T
 Step 7:Else
 Step 8:Invalid data
 Step 9:End
MODULE T
 Step 10:Begin
Step 11:Check the data stored.
 Step 12:If proof = direct then Report = direct access Else
 Step 13:Return {1, 0}
 Step 14: if integrity of data is verified as correct
 Step 15:  if integrity of data verified is incorrect End
```

V. SIMULATION RESULTS

Cloud consumers going to access the different type of clouds based on their needs the multi cloud setup for cloud storage .The multi –cloud environment has on many benefits for cloud users for the storage of data or applications. Here, two different types of cloud providers defined (i.e., cloud A and cloud B).User interface designed by the pre-processor for cloud users through the UI going to storage the data into cloud server .After the data storage into cloud server defined by the logic to store the data into two different clouds .Replication process used for the multi cloud data storage and secret sharing process for key generation. Key generation is used for encryption and decryption data uploading and downloading process

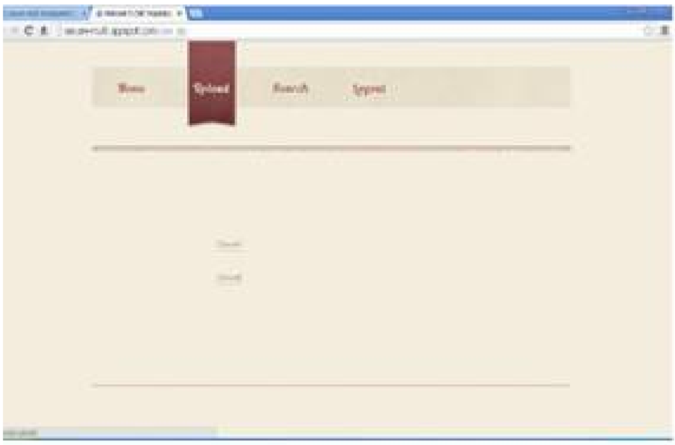

Fig.2. Uploading cloud

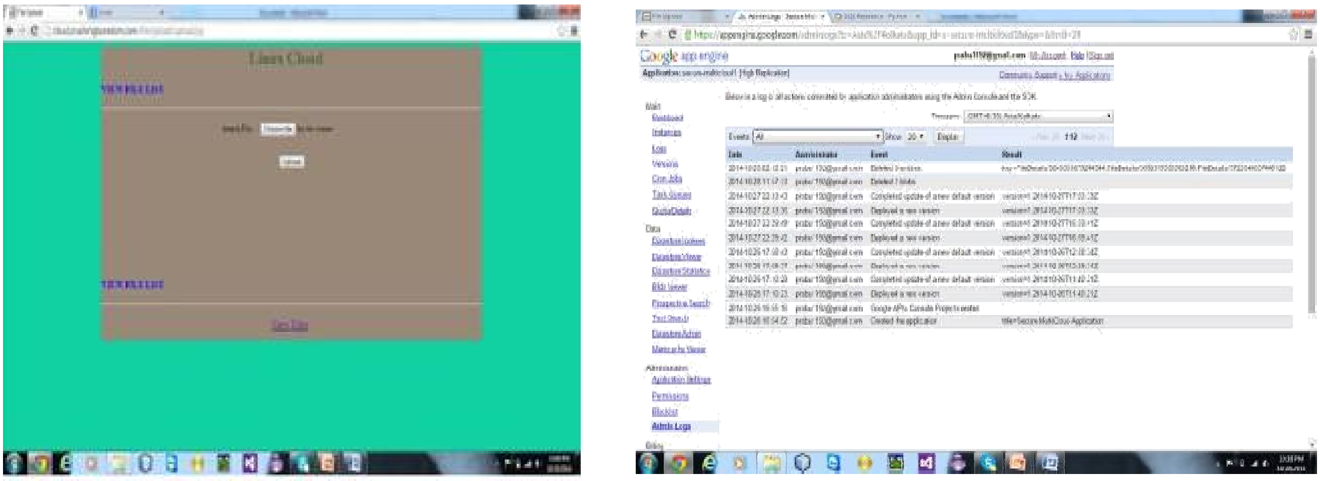

Fig.3.Cloud Storage-Linux cloud

VI. Conclusion and Future Work

The use of multiple cloud providers for gaining security and privacy benefits is nontrivial. The benefits of cloud computing are clear: minimizing the risk of physical infrastructure deployment, reducing cost of entry, reducing the execution and response time of applications, etc., To this end, this paper focuses on the issues related to the security aspects of cloud and aims at facilitating a new model which uses multiple cloud service providers (CSP) and Replication technique to prevent and overcome all the shortcomings of a single cloud model. The purpose of this model is to reduce the security risks which occur in cloud computing. Also, we address the issues related to data integrity, confidentiality and service availability arguing why the multi-clouds model is superior to single cloud by giving relevant scenarios where the single cloud approach fails. Therefore, it is clear that storing the data over multi-clouds is efficient, so with the tools and functionality available today, we strongly believe that there is no excuse for not going the multi-cloud route. In future develop Multi cloud computing into real time applications and enhancing the security aspects .We also concentrate the applied into high volume of data replication into multi-cloud system. We going to develop multiple applications into single login to control and access the cloud data's.

REFERENCES

[1] Vijay Varadharajan and UdayaTupakula."Security as a Service Model for Cloud Environment" IEEE Transactions on NetworkService Management, Vol. 11, No. 1, March 2014.

[2] Mohammed A. AlZain, Ben Soh and Eric Pardede ." MCDB: Using Multi-Clouds to Ensure Security in Cloud Computing" IEEE 25th International Conference on, 2013, pp. 1709-1716

[3] Jens-Matthias Bohli, NilsGruschka, MeikoJensen,Luigi Lo Iacono, and Ninja Marnau. "Security and Privacy-Enhancing Multi-cloud Architectures" IEEE Transactions on Dependable And Secure Computing, Vol. 10, No. 4, July/August 2013.

[4] Kan Yang, XiaohuaJia, KuiRen and Bo Zhang." DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems" Proceedings IEEEINFOCOM, 2013

[5] C. Yu, et al., "Protecting the security and privacy of the virtual machine through privilege separation," in Proc. Int. Conf. Computer. Sci Electron. Eng, 2013.

[6] Liu Hao, Dezhi Han, "*The study and design on secure-cloud storage system*", In IEEE society, 2011, page 5126-5129.

[7] DevHimel, SenTanmoy, BasakMadhusudan and Eunus Ali Mohammed, "*An Approach to Protect the Privacy ofCloud Data from Data Mining Based Attacks*", SCCompanion: High Performance Computing, Networking Storage and Analysis, 2012, page 1106-1115.

[8] Henry C. H. and Patrick P. C. Lee, "*Enabling DataIntegrity Protection in Regenerating-Coding-Based Cloud Storage*", 31st International Symposium onReliableDistributed Systems, 2012, page 51-60.

[9] Taeho Jung, Xiang-Yang, Zhiguo Wan, Meng Wan, "*Privacy Preserving Cloud Data Access With Multi-Authorities*", Proceedings IEEE INFOCOM, 2013, pp. 2625-2633.

[10] Gartner, "Gartner Says Cloud Adoption in Europe Will Trail U.S. by at Least Two Years," http://www.gartner.com/it/page.jsp?id=2032215, May 2012.

[11] Cong Wang,studentmember,ieee,QianWang,studentmember,ieee, KuiRen,member,ieee,NingCao,studentmember,ieee and WenjingLou,senior member,ieee,"Towared secure and dependable storage in cloud computing" 2012

[12] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *PKC'11*. Springer, 2011, pp. 53–70

BIOGRAPHY

Ms.M.Nivetha Mani has obtained UG and PG Degree in Anna University, Chennai. She has published 2 papers International conferences and 5 papers in International Journals. Presently working as Assistant Professor in CK College of engineering and technology, a unit of CavinKare, Cuddalore, Tamilnadu, India.

Dr. R. Muruganhas pursued his PhD Degree in Information and Communication Engineering faculty at Anna University, Chennai. He has more than 18 years of teaching and research experience. He has published more than 20 papers in International/National Journals and Conferences. Currently, he is working as a Professor and Head in the Department of Computer Science & Engineering at CK College of Engineering and Technology, Cuddalore.