Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 357 – 362

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Preserving Data Confidentiality using Multi-Cloud Architecture

M Sulochana[1] ,Ojaswani Dubey[2]

[1]*SRM university,chennai 603203,india*
[2]*SRM university,chennai 603203,india*

Abstract

Cloud Computing offers resources as services that are dynamically provisioned over the internet. The security of cloud computing has always been an important aspect of the quality of service from cloud service providers. The main problem that the cloud computing paradigm implicitly contains is that of secure outsourcing of sensitive as well as business-critical data and processes. One central concern in cloud computing is privacy and integrity of data processes in cloud. By using two or more distinct clouds, risks such as manipulation of data, and other threats associated with process tampering can be reduced. By integrating distinct clouds, the trust assumption can be lowered. Therefore, to provide integrity and confidentiality, the application logic and the data logic is split into two distinct clouds so that no cloud provider will gain the complete knowledge of the user data. The administrator resides in a private cloud, allows only the authenticated users to access the cloud storage. The administrator performs encryption and segmentation of the data to provide data confidentiality.

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Keywords: Multi cloud; Encryption; Decryption; Segmentation; De-segmentation.

1. Introduction

Customers are provided with a set of IT services over a network. These services are provided for lease with the option of scaling up or down the service requirements of customers. This process is referred to as cloud computing. There are several advantages associated with cloud computing. These benefits primarily arise from the process's ability to reduce expenses associated with computing while increasing flexibility and scalability for computers. Clouds are categorized into public, private and hybrid clouds. A public cloud is one in which a service provider involves resources outside the user's premises, thereby providing applications and storage as resources available to the public over the Internet and involves resources outside the user's premises. A private cloud refers to a cloud

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.035

system that is installed on the user's premise, usually in the own data center. A hybrid approach is denoted as hybrid cloud. We will focus on public clouds. The public cloud services demand for the highest security. In public clouds, all of the three common cloud service layers (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)) share the commonality that the end-users digital assets are taken from an intra organizational to an inter-organizational context. This leads to several issues, such as those associated with security aspects of cloud computing.

One central concern in cloud computing is the privacy and integrity of data processed at the cloud. To solve the data security problems in public environment, we propose an effective model for security and integrity of data stored using multi cloud strategy. The system proposed in this paper offers a robust and secure architecture which allows data security of user as well as protects the system against other external agents.

2. Related Works

In Cloud computing, there are set of important policies, which include issues of privacy, anonymity, security, liability and reliability [1]. Cloud computing offers software applications and computing services to the users, which might be stored off-site at locations rather than at local data centre or the user's computer [2]. Usually cloud computing services are delivered by a third party provider who owns the infrastructure [3]. Any information is valuable as long as it has related data. The information is useless if related data is not available. The relation of database is fragmented and stored at various locations by service providers who provide database as a service. Theses fragments are cloned at more than one service provider to ensure accessibility thus reducing data transfer costs. In [4] it is explained that the use of cloud computing has increased rapidly in many organizations. In Cloud computing, there are many problems like security of data, files system, backups, network traffic, and host security. In [5] it is proposed that use of digital signature with RSA algorithm in cloud computing model, thereby encrypting the data while it is being transferred over the network which provides security to the user data. Cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. This unique attribute, however, poses many new security challenges which have not been well understood [6]. Therefore it is necessary to provide cloud data storage security, which has always been an important aspect of quality of service. In the cloud, breach in the security of any component can lead to both disaster for the organization (the customer) and defacing for the provider. [7] explores the security issues related to the cloud also discusses the existing security approaches to secure the cloud infrastructure and applications and their drawbacks.

3. Challenges

Cloud computing has evolved as an important solution for many enterprises by providing reliable, efficient and cost effective resources as service. The service provider offers resources to the user based on either pay and use or pay as you need. Cloud computing offers many benefits to the user by providing dynamic scalability, flexibility, reduced IT costs and by minimizing the time for implementation. Cloud computing offers on-demand, self service, pay-per-use and scalable computing resources and services, thereby reducing the capital and operational expenditures for hardware and software as well. Despite the potential benefits of the cloud computing, the enterprises are slow in adopting it due to security issues and challenges associated with it. Security and privacy are the major concerns in adopting cloud. Since the cloud provider offers Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS), storage as a service and other services, the idea of handing of user data to the service provider is worrisome. The major challenges that are preventing the enterprises from adopting cloud computing are as follows:

3.1. Confidentiality

Once the user host data to the cloud there should be some guarantee that data accessibility will be given only to the authorized user. Inappropriate access to customer sensitive data by cloud personnel can pose potential threat to cloud data. The user should be assured that the data hosted on the cloud will be confidential. The assurances for the

data security can be provided to the clients through proper practices and privacy policies. Also procedures should be in place to prevent data leakage and to provide data safety. Preserving confidentiality is one of the major issues faced by cloud systems, since the user data is stored at a remote location that the Service Provider has full access to. There have been some methods of preserving the confidentiality of data stored in the cloud such as data encryption. The cloud seeker should be assured that data hosted on the cloud will be confidential.

3.2. Availability

In cloud computing, the services offered by the cloud provider must be available to the user. Consider a scenario where the user wants to store the data in cloud for future use. Once the data is stored in cloud, the stored data must be made available to the user without any interruption in retrieving the data. Users may also need to assure themselves that cloud applications are adequately secured for their specific purposes. Single cloud environment is affected with service unavailability, data loss, improper access of data and data integrity challenges which can be solved by the use of multiple clouds. Sometimes, due to limited resources or because of some intruder attack, the required data may not reach the user on time. Such occurrence is known as service unavailability. In single cloud, service unavailability is a major threat. Multi cloud computing is a better solution for service availability concern.

3.3. Integrity

Integrity is the guarantee that the data stored in the cloud is the data retrieved without altering intentionally or unintentionally. The data correctness, legality and security are the most fields that influence on the cloud and rely on the service provider. Cloud computing is a promising computing model that enables convenient and on-demand network access to a shared pool of configurable computing resources. Using cloud storage service is moving the data into the cloud server. Integrity must be provided so that the client let cloud service providers host their data on cloud servers and the client can access data from the cloud servers without loss of data.

4. Multi cloud strategy

Multi-cloud strategy is the use of two or more clouds to minimize the risk of service availability failure, loss of data, and loss of privacy. The simultaneous usage of multiple clouds may reduce the risk for data and applications in a public cloud. The standard barriers to cloud adoption such as security, reliability, cost and loss of control remain. Therefore by deploying multi-cloud environments, organizations gain more flexibility with the ability to determine what workloads to run where and more control over the services they use.

5. Proposed work

In this proposed multi cloud architecture, the application logic layer and the data persistence layer are separated with the assignment to two distinct public clouds, whereas the admin resides in another private cloud.

5.1. Authentication and uploading

The user enters the username and password through the cloud A and requests the administrator for accessing the cloud B. Only the authorized users are allowed to access the cloud storage. A user can only access the data after proper authentication is met. This is done only by the administrator. The administrator allocates some space to the user based on the requests. The administrator is the most integral part of this architecture as it is responsible for the efficient functioning of the primary and the secondary clouds.

The authenticated user is allowed to upload the data. The administrator receives the data uploaded by the user from the cloud A and performs security mechanisms to minimize the risk.

5.2. Encryption and segmentation

The data gathered from cloud A is encrypted using the RSA data encryption algorithm to maintain the security of data. Also, the encrypted data is segmented into chunks of data and stored at different locations in cloud B.
Each chunk is in an unreadable format to ensure high level data security. Thus, encryption reduces the loss of data by application logic flaws.

5.3. Downloading

Whenever the user requests for a file, the file is retrieved from cloud B. The data retrieved from cloud B is sent to the administrator for de-segmentation and decryption of data.

5.4. De-segmentation and decryption

The data received by the administrator is de-segmented. However, the data would be in an unreadable encrypted format. For the file to be back in its original form, data decryption takes place. The administrator performs decryption code to get the data in its original form. The data is then sent to the user.

The data sent is user specific and can only be sent to authenticated users. User authentication is performed by the administrator to maintain integrity of data.

6. Procedure

In the proposed system the application logic layer and the data layer are segregated into two different clouds, cloud A & cloud B as shown in Figure 1. The administrator resides in private cloud and allows only the authenticated users to access the data storage. In order to provide security to the user data, the administrator performs encryption of the uploaded data. So that the intruder will not able to read the encrypted data that is in unreadable format. After the encryption, the administrator segments the encrypted data and stores at different locations, so that the storage provider even cannot misuse the data. This provides more confidentiality to the user data. Also the flaws in the application logic will not lead to the data leakage. Step –by –step procedure involved in proposed system is given below:

1. The user login to access the cloud storage.
2. The administrator performs the authentication verification
3. User requests to upload the data.
4. When the user uploads the data, the administrator encrypts the data using RSA data encryption algorithm.

   The encrypted data is then partitioned into chunks of data using segmentation algorithm and stored at different locations in cloud 2.
5. If the user wants to download the data, the user requests the administrator to download the file.
6. The segmented and encrypted data is sent to the administrator.

   The administrator performs de-segmentation and decryption before sending the data to the user.
7. The data in its original form is sent to user.

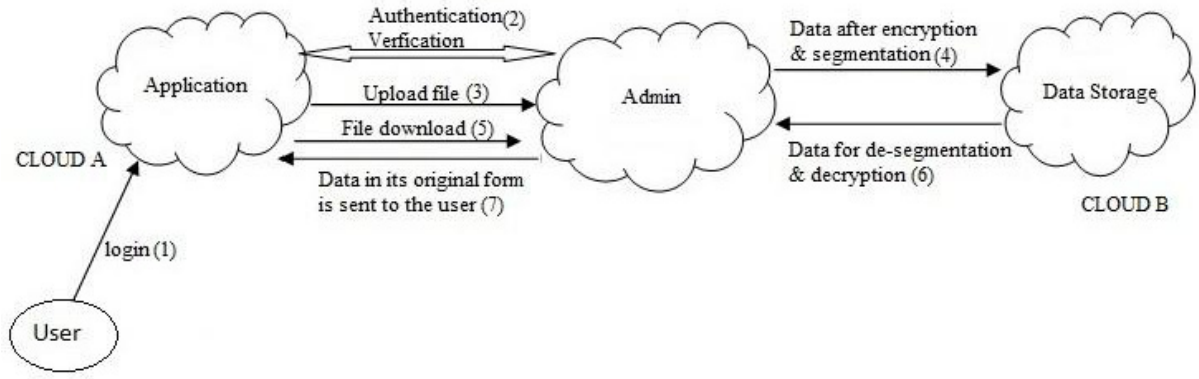

Figure 1 Architecture Diagram

7. Proposed Results

This proposed architecture reduces the data leakage risk in the presence of application logic flaws. Also ensures security and integrity to the data saved in the cloud. The following table depicts the comparison of proposed and existing system

Table: 1 Comparison of existing system with proposed system

Regular system	Proposed System
Encryption is not available.	Encryption of data takes place to provide data security
Less reliable	High level of reliability is ensured
Data is available but security is not maintained	Data is available with security and integrity
Either integrity or confidentiality is provided	Here both integrity and confidentiality is provided using multi cloud system

References

[1] Farzad Sabahi. Cloud Computing Security Threats and Responses, Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference.

[2] Ashutosh Kumar Dubey, Animesh Kumar Dubey, Mayank Namdev, Shiv Shakti Shrivastava. Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment. Software Engineering (CONSEG), *CSI Sixth International Conference*, Sept. 2012.

[3] Kuyoro S O, Ibikunle Frank, Awodele O, Cloud Computing Security Issues and Challenges, *IJCN*, volume (3): Issue (5): 2011,p 247 - 255

[4] Behl, A., Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," *Information and Communication Technologies (WICT), 2011 World Congress on*, vol., no., p.217, 222, 11-14 Dec. 2011.
[5] Manpreet Kaur , Rajbir Singh, Implementing Encryption Algorithms to Enhance Data Security of Cloud in Cloud Computing, *IJCA* , Volume 70 , 2013 - Number 18
[6] Cong Wang; Qian Wang; Kui Ren; Wenjing Lou, Ensuring data storage security in Cloud computing," *QualityofService, 2009. IWQoS. 17th International Workshop on* , vol., no., p 1,9, 13-15 July 2009
[7] Behl, A., Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation," *Information and Communication Technologies (WICT), 2011 World Congress on*, vol., no., p.217, 222, 11-14 Dec. 2011.
[8] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Security and Privacy-Enhancing using Multi-cloud Architectures" *IEEE Transactions on dependable and secure computing,* Vol. 10, No. 4, July/August 2013
[9] P.Kalpana, "Cloud Computing – Wave of the Future", *International Journal of Electronics Communication and Computer Engineering*, Vol 3, Issue 3, ISSN 2249–071X, June 2012.
[10] Subedari Mithila, P. Pradeep Kumar, "Data Security through Confidentiality in Cloud Computing Environment", Subedari Mithila et al, *IJCSIT* Vol. 2 , 1836-1840, 2011.
[11] Simarjeet Kaur, "Cryptography and Encryption in Cloud Computing", VSRD *International Journal of Computer Science and Information Technology*, Vol.2 (3), 242-249, 2012.
[12] Vidyanand Ukey et al, / Dataset Segmentation for Cloud Computing and Securing Data Using ECC *(IJCSIT) International Journal of Computer Science and Information Technologies*, Vol. 5 (3) , 2014, 4210-4213.