Volume 5, Issue 10, October-2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Implementation of Secured Architecture for Multi Cloud Computing Using Encryption Technique

Suruchi Narote*, Prof. S. B. Jadhav
Computer Engineering Department, Dr. VBKCOE, Malkapur,
Maharashtra, India

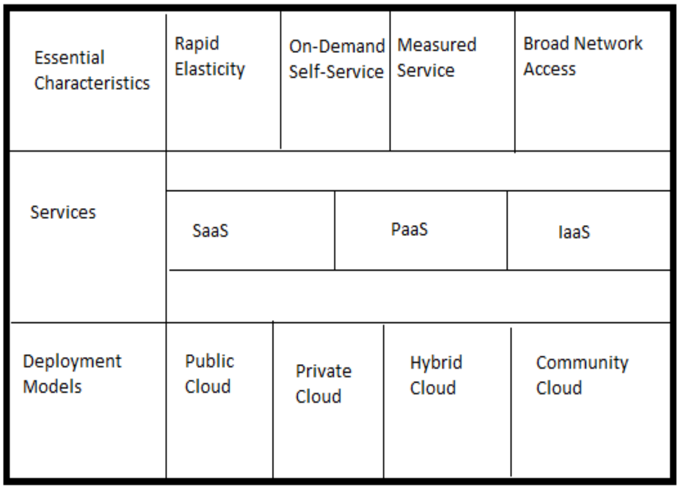
Abstract: In this paper we are implementing a secured architecutre for multi cloud computing using encryption technique. Now a days cloud computing is playing an important role for storing and sharing dada but it have some some disadvantages like data can be hacked by some malicious users and data is stored at remote servers so it can be used by unkown users who can do any changes in the data easily and can access our private data. So for the security purpose of data in cloud computing we are implementing two encryption techniques these are key aggregate encryption technique and identity based encryption technique. This application uses two clouds one for storing the data and other for storing the application. This two encyrption techniques providing a securd architecture for storing the client's data.

Keywords- Cloud, security, multicloud, Key aggregate cryptosystem (KAC), Identity based encryption (IBE)

I. INTRODUCTION

Cloud computing is a technique for accessing and sharing computing resources asper the requirements of the user.Cloud computing provides a solution to user and the organization for storing and accessing their data at the thied party data centers. The cloud aims to cut costs, and helps the users focus on their core business instead of being impeded by IT obstacles.[3]

Cloud model composed of 5 essential characteristics, 3 services and four deployment models:



Essential Characteristics	Rapid Elasticity	On-Demand Self-Service	Measured Service	Broad Network Access
Services	SaaS	PaaS	IaaS	
Deployment Models	Public Cloud	Private Cloud	Hybrid Cloud	Community Cloud

Characteristics of the clouds are as follows:

1) Rapid Elasticity: Elasticity is the characteristics which allow cloud providers to add and releese the resources as per the need of their client's. Elasticity aims at matching the amount of resources allocated to a service with the amount of resources it actually requires, avoiding over- or under-provisioning.

2) On-Demand-Self-Service: Services of cloud are on-demand, it means the customer or client can request the services as per their requirements without human interaction with the cloud service provider.

3) Measured Service: Measured service is a term which allows cloud service providers to compute and measure the services used by their clients for various reasons, including billing, effective use of resources etc.

4) Broad Network Access: Broad network access refers to resources hosted in a private cloud network (operated within a company's firewall) that are available for access from a wide range of devices, such as tablets, PCs, Macs and smartphones. These resources are also accessible from a wide range of locations that offer online access.

Services of clouds are as follows:

1)SaaS(Software as a Service): Software as a Service is the most popular service in cloud market and is still growing rapidly. SaaS uses the internet to deliver the applications that are managed by the third -party and whose interface is accessed on the client's side.Most SaaS applications can be run directly by the web browser without any installations and downloads required. In SaaS everything is managed by the service provider so it is easy for the enterprises to streamline their maintainance and support.

2)PaaS(Platform as a Service): Platform as a Srevice provides a platform to applications and other development. PaaS allows the developers to develop their own applications.PaaS makes the development , testing and development of applications easily,quickly and in cost effective manner. PaaS allows third party vendors that they can manage OSes,srever, networking, storage and PaaS software itself, as developers manages the applications.

3)IaaS(Infrastructure as a Service): Cloud infrastructure services, known as Infrastructure as a Service (IaaS), are self-service models for accessing, monitoring, and managing remote datacenter infrastructures, such as compute , storage, networking, and networking services (e.g. firewalls). Instead of purchasing our own hardware, users can purchase IaaS based on consumption, similar to electricity or other utility billing.

II. LITERATURE REVIEW

In 2013 Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Lacono and Ninja Marnau, “Security and PrivacyEnhancing Multicloud Architectures”, 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 this paper provides a servey on different security by multicloud adoption approaches. It provides four distinct models in form of abstracted multicloud architectures. These developed multicloud architectures allow to categorize the available schemes and to analyze them according to their security benefits.[1]

In 2014 Cheng-Kang Chu, Sherman S. M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng,” KeyAggregate Cryptosystem for Scalable Data Sharing in Cloud Storage” In this paper, we study how to make a decryption key more powerful in the sense that it allows decryption of multiple cipher texts, without increasing its size.

“To design an efficient public-key encryption scheme which supports flexible delegation in the sense that any subset of the ciphertexts (produced by the encryption scheme) is decryptable by a constant-size decryption key (generated by the owner of the master-secret key)?” [2]

III. RELATED WORK

1) "Design and implementation of a secure multi-cloud data storage using encryption" by Chukkala Varsha Sampath and Pothabathula Srikanth :

In this paper we describe the design and development of a cloud computing based secure multi cloud data storage using encryption. This application uses multiple cloud storages, to cooperatively store and maintain the client’s data. We use two mechanisms - Multi Agent system (MAS) and Data Encoding technique. These are combined together to give a new mechanism to provide data integrity and security for client’s data in cloud storages.

2)"Secure Multi-Cloud data sharing using Key Aggregate Cryptosystem for scalable data sharing" by Suhas Bachhav, Chetan Chaudhari, Nikhilesh Shinde and Poonam Kaloge:

In this paper they describe a system with an efficient public-key encryption. In this any number of subsection of the cipher text can be decrypted by using the decryption key. The problem is solved by the overview of key aggregate cryptosystem.

3)"Cloud computing security using encryption technique "by Sanjoli Singla and Jasmeet Singh :

In this paper the authors deal with the issue of data security during transmission of data. The main concern here is to encrypt the data so that confidentiality and privacy can be achieved. The algorithm used here is Rijndael Encryption Algorithm along with EAPCHAP.

4)"Cloud Computing Security and encryption "by Varsha Alangar :

In this paper the author has tried to attract analyst attention towards the problem of data security and as firmly believe that data encryption can help to solve this issue. The author has provided a list of various encryption techniques such as RSA, DES, etc.

IV. PROPOSED WORK

We propose a secured architecture for multi cloud computing using encryption techniques for providing security. The main reason to use multi cloud is the security of confidential data and storage of application.We had implement a banking application for loan processing.This application uses multiple clouds one for storing the application and the second one for storing the database. In this application we implemented two encryption techniques these are Key aggregate encyption and identity based encryption for securing the data from unauthorized access. In this admin plays an important rolefor uploading the data submitted by the customer and downloads the users data when requested.Admin encypts the data using encryption key before uploading the data and decrypt the data using decryption key before downloading the data. Data is stored on the database in encrypted form so that no unauthorized user can access the private data of others. For more security purpose we also encrypted the algorithm used for encryption and decryption of data. This will be useful if anyone hacked the encryption key. The two different techniques are implemented for securing the data:

1) Key aggregate encryption: In KAC, users not only encrypt a message under public key, but also under an identifier of ciphertext called as class. Ciphertext are divided into different classes. To extract the corresponding secret key for different classes, a master secret key is used which is hold by the key owner. More importantly the extracted key is the aggregate key which is as compact as the secret key for a single class, but combining the power of many keys to decrypt the subset of any ciphertext classes. In KAC the size of all the keys (public key, master secret key and aggregate key) and ciphertext are all constant.

2) Identity based encryption: Identity-based encryption (IBE), is an important primitive of ID-based cryptography. As such it is a type of publickey encryption in which the public key of a user is some unique information about the identity of the user (e.g. a user's email address). This can use the text-value of the name or domain name as a key or the physical IP address it translates to.

The conceptual advantages of this application is:

1) It provides security to the confidential data.
2) It provides us servises and storage on demand and as per the need.

V. CONCLUSION

In cloud computing data security is the important issue .In the adoption of cloud computing services data security and privacy are the major concerns fromthe client's perspective.So in this application we focused on the security.In our proposed system ,only authorized user can access the data,no other user can access the data of another user.From security perspective we encrypt the data before uploading and decrypt the data before downloading.

REFERENCES

[1] Jens-Matthias Bohli, Nils Gruschka, Meiko Jensen, Luigi Lo Lacono and Ninja Marnau, “Security and PrivacyEnhancing Multicloud Architectures”, IEEE Transactions on Dependable and Secure Computing, VOL. 10, NO. 4, JULY?AUG 2013

[2] Cheng-Kang Chu ,Chow, S.S.M, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng , “Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage”, IEEE Transactions on Parallel and Distributed Systems. Volume: 25, Issue: 2. Year :2014.

[3] MOHAMMAD HAMDAQA AND LADAN TAHVILDAR "'Software Technologies Applied Research (STAR) Group", University of Waterloo, Waterloo, Ontario, Canada