SECURITY IN MULTI-CLOUD DATA STORAGE WITH SIC ARCHITECTURE

Kalyani.M.Borse[1], Ankita.G.Deshpande[2], Ashlesha.A.Deshpande[3], Ms.Juily.S.Hardas[4]

[1, 2, 3, 4]*Student, Computer Engineering Department, GES R.H.S.COE, Maharashtra, India*

Abstract

Cloud computing is becoming an important thing to deal with, in many organizations around the world. It provides many benefits like 1. cost, 2.Reliability and 3.Ease in retrieval of data. Security in cloud computing is gaining more and more importance as organizations often store sensitive data and important data on the cloud. Security of data in cloud is an issue which should be focused carefully. Customers do not want to lose their sensitive data due to malicious insiders and hackers in the cloud. In addition, the loss of service availability has caused many problems for a large number of recently. Data intrusion technique create many problems for the users of cloud computing. The other issues such as data theft, data lost should be overcome to provide better services to the customers. It is observed that the research into the use of intercloud providers to maintain security has received less attention from the research community than has the use of single clouds. Multi-cloud environment has ability to reduce the security risks as well as it can ensure the security and reliability. The system aim to provide a framework to deploy a secure cloud database that will guarantee to avoid security risks facing the cloud computing community This paper suggests new architecture for cloud environment which will help in reducing the security threats. The efficient and secure use of cloud computing will provide many benefit to the organizations in terms of money and ease in access to the data.

Keywords: *Cloud computing, single cloud, multi-clouds, cloud Storage, data integrity, data intrusion, service availability, Performance, cost-reduction.*

----------***----------

1. INTRODUCTION

Cloud Computing is a technology that uses the internet and remotely located servers to store the data of the users and for running the application programs. Cloud computing allows business organizations to use applications without access their personal files at any computer with internet access and installation Cloud computing can be defined as a pool of virtualized computing resources that allows users to gain access to applications and data in a web-based environment on demand.[10] . As use of cloud computing is growing rapidly in every for m of organization, to provide security to the data in cloud computing is the main issue to deal with.[1] Some security issues like data loss and malicious insiders are reasons to fear for customers using cloud computing services. In a cloud computing environment, individuals and businesses work with applications and data stored and/or maintained on shared machines in a internet environment rather than physically located in the home of a user or as corporate [1] environment. Vulnerabilities in a particular cloud service or cloud computing environment can potentially be exploited by criminals and actors with malicious intent [4].

Traditional approach of using single cloud server, may also lead in slowing down the retrieval of data. Dealing with single cloud providers is becoming less favorable with customers due to commonly occurring problems such as service availability failure and the possibility that there are malicious insiders or hackers in the single cloud. In recent years, there has been a move towards multi-clouds, intercloud or cloud-of-clouds. [1] This paper is focusing on using the multi cloud architecture to deal with the security issues raised while using the single cloud. In cloud computing organizations private data is given to the third party, they want to avoid an untrusted cloud provider.

2."SINGLE" CLOUD SERVICE PROVIDERS

Privacy preservation and data integrity are the two main issues faced by "single" Cloud service providers. In his/her own organization one can ensure strong security policies. But in case of cloud computing one has to trust completely on his service provider. [3] Also there is an overhead of managing huge amount of data on a single server. It is easier for malicious outsider to penetrate through security if the data is not actually stored by organization itself; instead they are trusting on third party for taking care of their data.

Disadvantage:

- Need High cost for cloud maintains process
- Data losses accrued.
- Can fail in ensuring the complete security from possible threats

3. OBJECTIVES OF MULTI-COULD ARCHITECTURE

3.1 Security

In multi cloud data Storage, Data and Information will be shared with external users, therefore cloud computing users want to avoid important information from attackers or malicious insider is of critical importance. In Iaas, users are responsible for protecting operating system and cloud providers must provide protection for users data. Resources in the cloud are accessed through the Internet, frequently even if the cloud provider concentrates on security in the cloud infrastructure; the data is still transmitted to the users through networks which may be insecure.
1. Data integrity 2. Data intrusion 3. Service availability these are the three Security factors.

3.1.1 Data Integrity

The data stored in the cloud may lost from damage while transferring from one place to another. Examples: Of the threats of attacks from both inside and outside the cloud provider.

3.1.2 Data Intrusion

Another security risk that may occur with cloud provider, such as the any particular cloud service is hacked password. If someone gains access to that cloud service password, they will be able to access all of the accounts instance and resources. Thus the stolen password permits the hacker to erase and to modify all the data inside any virtual machine instance for the stolen user account, or even disable its services. There is a possibility for the users email (Amazon user name) to be hacked for a discussion of the potential risks of email.

3.1.3 Service Availability

There is possibility that the service may be unavailable from time to time. If any users files break the cloud storage policy, the users web service may terminate for any reason at any time. . Therefore Cloud provider maintain the backup and data authentication which assures that returned data is same as stored data is extremely important.

3.2 Performance

In single architecture, there is one main cloud server which will process and response the request from the users. If more than expected no of clients will requested for data/service to the single server then the performance will slow down

Each user will have to wait more for accessing his/her data. In case of overload, the server may hang sometime. In multi cloud we have more than one cloud server to process the users request So this divides the responsibility of handling requests among several servers. So ultimately we can provide better solution to our providers.

3.3 Cost-Reduction

Secured storage and data availability can be provided to the customers in the market of economical distribution of information in all the available service providers. In model customer decide his data among their several SPs available in the market. Also we provide decision for the customer, to which SPs he must choose to access data and quality of service offered by service provider.

4. ARCHITECTURE OF MULTI-CLOUD SYSTEM

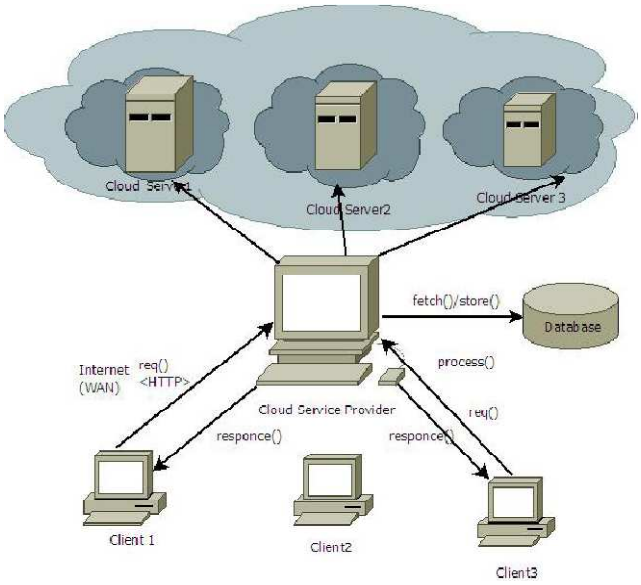

Fig 1: SIC Architecture

SIC - Secure Inter-Cloud Architecture. The proposed architecture is the 3 tier architecture. In our architecture, there is one CSP i.e. cloud service provider. This is the main central server which keeps the data about clients. Client in the diagram represents any cloud service user. Clients/users does not have any idea about where exactly the data/files has been stored. Data is stored in cloud server. The servers may reside in different physical locations. The CSP decides the servers to store the data depending upon available spaces. We can use load balancing algorithms for making the decision, on which server we should actually store the data. The CSP will also keep track about the files stored on each server. The cloud servers will only store the data, but they will not have any records about the user accounts, their passwords or encryption and decryption keys.

CSP is central server, it must be well configured. Care should be taken for protection of CSP. Cloud service provider acts as an effective bridge between the user and cloud server. Cloud

users, who have data to be stored in the cloud and rely on the cloud for data computation, consist of both individual consumers and organizations.

5. USE OF DATA ENCRYPTION TECHNIQUES

For ensuring more security in cloud environment, we can use data encryption. If the data is distributed in multi cloud environment as well as it is encrypted, we can protect our data in even better way. The data which is uploaded by the user, can be encrypted first and then we can store it on the cloud server. This will be helpful in providing two-way security to the customer's data. To store the data in multicloud environment The symmetric key or secret key algorithms are the best choice for such applications. Symmetric key algorithm is also known as the secret key encryption. It is a cryptographic technique in which both the sender and receiver of data use the same key for the purpose of encryption and decryption of data. Symmetric key algorithms are suitable for storing data in cloud multi cloud, as user should be able to access his data easily.

Secret-key encryption algorithms use a same secret key to encrypt and decrypt data. You must protect the key from access by unauthorized agents, because anyone that has the key can use it to decrypt your data or encrypt their own data, claiming it originated from you. Secret-key encryption is also referred to as symmetric encryption because the same key is used for encryption and decryption. Secret-key encryption algorithms are very fast (compared with public key algorithms) and are well suited for performing cryptographic transformations on large streams of data.[6]

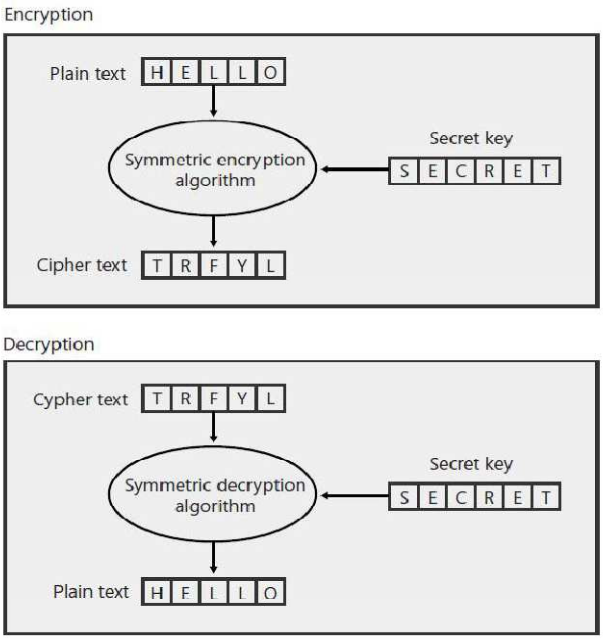

Fig 2: Symmetric Encryption

6. FUTURE WORKS

In future, we aim to provide more secure cloud environment to avoid the security risks. Cloud computing should not end with only single cloud. The new concepts like multi-cloud, sky computing should be adopted by the cloud service providers for ensuring better security to customer's data. Here the key factor to focus is to increase the performance and scalability of the cloud servers in multi-cloud environment. One should also try to increase the level of security by using new and better data encryption techniques. Also, the cloud service provider (CSP) in the above architecture should be more secure, as it stores the sensitive data like user accounts and encryption keys. Our aim is that Clients would be able to access their applications and data from anywhere at any time. They could access the cloud computing system using any computer linked to the Internet. Data wouldn't be confined to a hard drive on one user's computer or even a corporation's internal network. One more challenge is to successfully implement the load balancing algorithms for distributing the data among the cloud servers. Providing the extra layers of security may result into increase in the time to provide data access to the user. We should also take care that user should able to gain easy and timely access to his data, without any hurdle. Both the terms security and ease in access to the data should go hands in hands.

CONCLUSIONS

Even if the use of cloud computing have increased rapidly during last decade, the security in the cloud environment is the main issue to be focused on .it is the responsibility of a good cloud service provider to ensure secure storage of data on the cloud to his customer. In this paper, we proposed a secured multi-cloud architecture in cloud computing, which seeks to provide each customer secure environment to store his data and he should be able to access his data without any failure or delay. We are trying to provide two way security to the data, by encrypting the data and by storing data on the multiple servers. Also, the responsibility of storing the sensitive data about the user accounts is taken by different central server (CSP), which will help in securing the data from attacks. We support the migration to multi-clouds due to its ability to decrease security risks that affect the cloud computing user.

REFERENCES

[1]. Thom, "Cloud computing security: From Single to Multi-clouds", Department of Computer Science and Computer Engineering, La Trobe University, Bundoora 3086, Australia. Mohammed A. AlZain, Eric Pardede, Ben Soh, James A.

[2]. " Data integrity proofs in cloud storage", Infosys Technologies Ltd Hyderabad, India. Sravan Kumar R, Ashutosh Saxena,

[3]. ”Using Multi Shares for Ensuring Privacy in Database-as-a-Service”, 44th Hawaii Intl. Conf. on System Sciences (HICSS),2011, pp. 1-9. M.A. AlZain and E. Pardede
[4]. ”Towards Of Secured Cost Effective Multi Cloud Storage In Cloud Computing” , Communication Systems, Bannari Amman Institute of Technology. K.RAJASEKAR1 and C. KAMALANATHAN2
[5]. October3,2006. Amazon, Amazon Web Services. Web services licensing agreement,
[6]. Tony Northrup, Microsoft .NET Framework Application Development Fondation 2nd edition, Training Kit.
[7]. ”DepSky: dependable and secure storage in a cloud-of-clouds”, EuroSys’11:Proc. 6thConf. On Computer systems, 2011, pp. 31-46.] A. Bessani, M. Correia, B. Quaresma, F. Andr and P. Sousa,
[8]. ”Toward a cloud computing research agenda”, SIGACT News,40, 2009, pp. 68-80. K. Birman, G. Chockler and R. van Renesse
[9]. Pratap Reddy Institute of Technology Hyderabad, India ”Security for Effective Data Storage in Multi Clouds”. T.NEETHA Kommuri, CH.SUSHMA,Kommuri
[10]. Kim-Kwang Raymond Choo ”Cloud computing: Challenges and future directions”.

BIOGRAPHIES

Ms. Kalyani Manik Borse

Ms. Ankita Govind .Deshpande

Ms. Ashlesha Amrut .Deshpande

Ms. Juily Shripad Hardas