*E-ISSN: 2321-9637* 

# Improved technique in Inter Cloud Data Transfer Security

Rajkumar R. Chalse<sup>1</sup>, Roshani Talmale<sup>2</sup>, Arun Katara<sup>3</sup> Department of WCC<sup>1</sup>, Department of CSE<sup>2</sup>, Department of Eletronics<sup>3</sup> TGPCET<sup>1</sup>, TGPCET<sup>2</sup>, DMIETR<sup>3</sup> Email: rajchalse@gmail.com<sup>1</sup>, roshanikambe@rediffmail.com<sup>2</sup>, arunkatara@gmail.com<sup>3</sup>

**Abstract-** The use of cloud computing has increased rapidly in many organizations. Cloud computing provides many benefits in terms of low cost and accessibility of data. Cloud computing provides an economical and efficient solution for sharing group resource among cloud users. It is an internet based service delivery model which provides internet based services, computing and storage for users in all market including financial, health care & government. In this paper we to provide Inter Cloud Data Transfer Security. Cloud security is becoming a key differentiator and competitive edge between cloud providers. This paper discusses the security issues arising in different type of clouds. This work aims to promote the use of multi-clouds due to its ability to reduce security risks that affect the cloud computing user.

**Index Terms-** Cloud, Security, Security challenges, Cloud computing, Data security, DMF, *Privacy-preserving*, Access Control, Dynamic groups.

## 1. INTRODUCTION

Cloud computing is a high-level computing mechanism and efficient way to use resources. Cloud allow user to use resources to their requirement and pay accordingly. The user can used the various cloud services such as software, which is in the cloud software as a service (SaaS). Eg. Google docs. A platform uses to build up applications is platform as a service (PaaS). Eg. Google App engine. At last, the scalable computing power, Infrastructure as a Service (IaaS), such as Amazon Ec2 [1].Though having many advantage of cloud computing, user still not assure on cloud services and put the Important Information in the cloud. The main issues of cloud computing are security, performance and availability. Security is Key issue in the cloud system.

If any kind of Failure occurs, it is not clear who is Responsible party. A failure can occur due to various reasons such hardware, which is in the Infrastructure as a Service (IaaS) layer of the cloud. Malware in software, which is in the software as a service (SaaS). And the customer's application running some kind of malicious code. Considering the above issues, the main focus on security of cloud computing. As another example, under the CLuE program, NSF joined with Google and IBM to offer academic institutions access to a large-scale distributed infrastructure [3].

In this paper focuses on the issues related to the data transfer security aspect of inter cloud. As data and information will be shared with a third party, cloud computing users want to avoid an entrusted cloud provider. The common type of Dos attack occurs when an attacker flood a network with excessive requests to the target server until the server is unable to provide services to normal user [2]. This paper describes data security and privacy protection issues in cloud. We detect some main security issues in cloud computation, try to identify the basic cause of the failure and propose some possible solution. The rest of the paper is ordered as follows. In the next section we describe cloud deployment models. In section III describe some related work. In section IV security issues and basic causes are elaborated, followed by some proposed method to solve the problems. In section V describe the experimental environment. In section VI shows the results of various attacks. Finally conclusion in section VII.

## 2. CLOUD DEPLOYMENT MODELS

## 2.1. Private Clouds:

Private clouds (aka, on-premises cloud) are cloud deployments inside the organization's premises, managed internally without the benefits of the economy of scale but with advantages in terms of security. This is becoming a new form of architecture for the Datacenter, sometimes mentioned as a Datacenter-in-a-box. VMware is pioneering this approach, delivering products that will help to implement this type of cloud through their products vCloud, vCenter, and vSphere. VMWare is also leading an effort to achieve standardization for the cloud through the DMFT (Distributed Management Task Force) organization.

## 2.2. Public Clouds:

Public Clouds are the original concept of cloud. This type of cloud provides all the benefits of the economy of scale, ease of management, and ever growing elasticity. The major concern about this style of deployment is security, and that is the only reason why the other types of cloud deployment have a say.

## 2.3. Hybrid Clouds:

Hybrid Clouds are a deployment type that sits between the private and the public clouds. Hybrid Clouds are usually a combination of private clouds and public clouds, usually, managed using the same administration and monitoring consoles (therefore, the importance of cloud standardization).

## 3. RELATED WORK

There is a huge number of publications on cloud security issues .In this section we concentrate on some attack on cloud computing. Meena et al. [4] describe the flooding attack in a cloud system. In this how adversary has achieved the authorization to make a request to the cloud, and create bogus data and pose this request to the cloud server. Result engaging the whole cloud system just by interrupting the usual processing of one server, in essence flooding the system. proposed approach is to organize the entire server in the cloud system as a group of fleet of servers. Hypervisor can be utilized for the Scheduling among fleets. PID can be appended in the messaging, which will justify the identity of the legitimate customers.

Glen [5] in the TCP SYN flood attack protocol violation attack that is used in several variations. Attacker sends the first packet (with the SYN bit set) of the well known TCP 3-way handshake. The possible solution for that in modern UNIX and Windows by implementations have fixed this issue by increasing the queue size rate limiting the number of TCP SYN Packets allowed. TCP SYN cookies are another way to mitigate this type of attack.

Herrmann et al. [6] present a novel method that applies common text mining to the normalized frequency distribution of observable IP packet sizes. In this, robust against small modifications of websites. Furthermore the packet size can be recorded with common networking monitoring tool by a passive, external observer with the several experiments. They demonstrated their method robust and succeed to detect almost all websites.

## 4. SECURITY ISSUES AND SOLUTION IN INTER CLOUD COMPUTING

Although cloud service providers can offer benefits to users, security risks play a major role in the cloud computing environment. We will focus on specific problems for various kinds of attack in the cloud: Denial of service (DOS) attack, fingerprinting attack, unauthorized user attack. We describe each of these security issues in cloud system and find out their basic causes. The propose method to mitigate such attacks to ensure the integrity and security of cloud systems.

## 4.1. Dos Attack:

The client access resources mean services available to them for a time being. The services might be unavailable or violated either by different ways such as hardware, software constraints and malicious attack from outside. If suppose client trying to use the cloud service the message "service not available" will appear not for a few seconds or minutes, but hours and day to take . This status might be as a result (Dos) attacks. In this, the detection of Dos attack based on the behavioral of threshold. This means that if the user request greater than the assigned range value, it should be considered that attack on cloud system and the cloud will hang. The number of user packets are over the threshold system blocked this user.

Determining Threshold: It is a simplest way for defining a threshold is to set the constant value however; it's not an optimal solution, because the possibility of false detection will be more. Assigning the constant value, because of that reduction in the false-incorrect detection.

The proposed method for defeating Dos is relatively simple and powerful techniques. In this technique, we track the no of source IP packet in the log's list of the server. Log file that are maintained the server. If the particular IP is observed for over n consecutive packets size of more than normal range within time period. Then it is consider as attacker and packets from this node are blocked thereafter. The above thresholds can be programmatically varied according to the various conditions such as network traffic patterns etc. in this way the cloud will not hang and does not affect on the services.

## 4.2. Fingerprinting Attack:

So many people would use cloud computing services, to access a service in a cloud user has to login, when user login to access a services his logs are maintained on the server. So the huge logs arise from transaction between systems, user information update and data processing and so on. Delete once the user logout.



is invalid, try through control server".

#### Fig 1 Detection of fingerprinting attack

The proposed methods to prevent such an attack we use dual file scan method. In this method, when user get logged in we scan the server compute the size of various logging files. And discontinue to accessing a cloud service send the logout request. After logout we scan the system yet again and compute the size of various logging file. If there is a distinction in the size found i.e. second scan is larger compare to the first one. It means that user is not entirely logged out and his logs are still not deleted. The proposed method deletes the logs and secures the user confidential data. If there is same in the size found i.e. second scan is similar to first one. It means user is entirely logged out.

#### 4.3. Unauthorized User Attack:

Authorized user can send request to the server through proper channel without neglecting the control server. But if the user send direct request to server bypassing control server and accessing cloud services, in this case the server in the cloud get vulnerable to easy attack, such an attack is referred as unauthorized user attack.



Fig 2 Unauthorized user attack

To overcome this type of an attack the method we proposed here is to use a token based strategy in which user send request to the control server which in turn forward request to any of the server in the cloud, along with a encrypted token. Server receiving the request decrypts the token and if valid it processes the request of the user. If user send request straight to the server, in that case, since there is no token with the request. Server responds with a message "your request

## 5. EXPERIMENTAL ENVIRONMENTS

Microsoft cloud computing platform used to build, deploy and manage application through a global network of Microsoft- managed datacenter. Window azure allows for applications to be built using many different languages, tools or frameworks and makes it possible for developers to integrate their public cloud application in their existing IT environment [7].

Azure framework is the finest available tool. This gives us to setup cloud environment on which we perform the various operations in different server. Because of azure we are not required to physically setup cloud. It creates different server with different ports for each server to avoid collision. Because of azure we setup cloud environment otherwise it's a complex job to physically setup cloud.

#### 6. RESULTS

From figure 3(a) we have to see that the main page of multi-cloud operation where client can easily access the one of the web servers in the cloud. In the next figure 3(b) shows that the registration for new user page if the user is new, in response request is being in process to create new user account. In figure 4(a) shows the user or admin login page, so user or admin can logon in this application, figure 4(b) show the admin login page after successful login by admin And figure 4(c) show the user verify page where all user available in this cloud. In the next figure 4(d) show the file verify page. In this page there are n number of files uploaded by user it verify by admin if the file is correctly uploaded by authorized user then it is added or it is rejected. In all figure shows the security against unauthorized user attack. If user send direct request to server accessing cloud services.



Fig 3(a): main page of multi-cloud.

## International Journal of Research in Advent Technology, Vol.2, No.2, February 2014 E-ISSN: 2321-9637











Fig. 4(d) File verify page

## 7. CONCLUSION

It is clear that although the use of cloud computing has rapidly increased; cloud computing security is still considered the major issue in the cloud computing environment. In this paper, we proposed a security frame work for inter cloud communication in cloud computing environment. Dos attack, fingerprinting attack, unauthorized user attack are detected and mitigate using methods which is implemented on window azure framework. These techniques securing servers and users from attackers. One great advantage of the development of security frame work is the communication between different servers and users are efficient in inter cloud system.

## REFERENCES

- A.M. sharifi, S.K. Amirgholipour, M. Alirezanejad, B.S Aski,M Ghiami (2012) "Availability challenge of cloud system under DDOS attack" Indian J.Sci.Technol. pp: 2933-2937.
- [2] D. Jamil and H .Zaki,(April 2011) "Security issues in cloud computing and countermeasures", IJEST, pp: 2672-2676.
- [3] D. Agrawal, A. El Abbadi, F. Emekci and A. Metwally, "Database Management as a Service: Challenges and Opportunities", ICDE'09:Proc.25thIntl. Conf. on Data Engineering, 2009, pp. 1709-1716.
- [4] B. Meena and K.A.Challa,(March 2012), "cloud computing security issues with possible solutions", IJCST, pp: 340-344.
- [5] Michael Glenn, "A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment", SANS Institute 2003.

## E-ISSN: 2321-9637

- [6] Dominik Herrmann, Rolf Wendolsky, Hannes Federrath (Nov 2009), "website fingerprinting: Attacking popular privacy enhancing technologies with the multinomial navi-byes classifier", CCSW'09.
- [7] Wikipedia, "window azure" 2012.