International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-2, Issue-5, September-2014

Security In Inter Cloud Data Transfer

Prof. Rajesh Babu, Prof. Ananth Kumar

***Abstract*— Cloud computing has quickly become one of the most Networking software in the IT world due to its revolutionary model of computing as a utility. It promises increased flexibility, scalability, and reliability, while promising decreased operational and support costs. Cloud computing largely intended to deliver on-demand services. Cloud providers are able to offer customers the ability to change their levels of service in many ways without waiting for physical changes to occur. A major concern in the Cloud is security; some agree that the Cloud is a secure and trusted system, while others seem to think differently. 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 Security, Inter-Cloud security.**

I. INTRODUCTION

Cloud computing is an evolving term that describes the development of many existing Technologies and approaches to computing into something different. Cloud separates application and information resources from the underlying infrastructure, and the mechanisms used to deliver them. Cloud enhances collaboration, agility, scaling, and availability, and provides the potential for cost reduction through optimized and efficient computing. More specifically, cloud describes the use of a collection of services, applications, information, and infrastructure comprised of pools of compute, network, information, and storage resources.

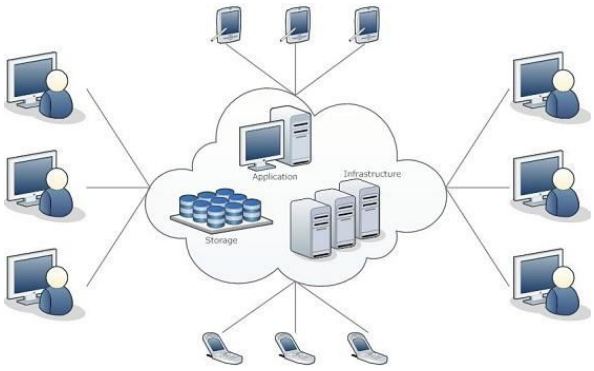

Fig 1: Cloud Computing

Manuscript received September 23, 2014

Prof.G.Rajesh Babu, Computer Science and Engineering , Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur, India, 8888866459.

Prof.Ananth Kumar, Computer Science and Engineering , Tulsiramji Gaikwad-Patil College of Engineering & Technology, Nagpur, India, 8554982311.

The three fundamental classifications are often referred to as the "SPI Model, "where 'SPI' refers to Software, Platform or Infrastructure (as a Service), respectively defined thus:

I. Cloud Software as a Service (SaaS):

The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser.The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings.

II. Cloud Platform as a Service (PaaS)

The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

III. Cloud Infrastructure as a Service (IaaS)

The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources .Where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

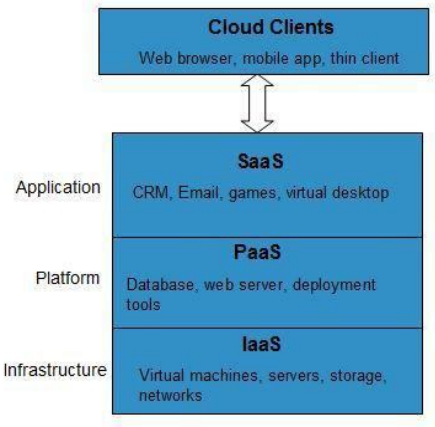

Fig 2: Service Models

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.

CLOUD DEPLOYMENT MODELS

A. 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.

B. Public Clouds:

Public Clouds are the original concept of cloud. This type of cloud , 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.

C. Community Cloud:

The cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, or compliance considerations). It may be managed by the organizations or a third party and may exist on-premises or off-premises.

D. 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).

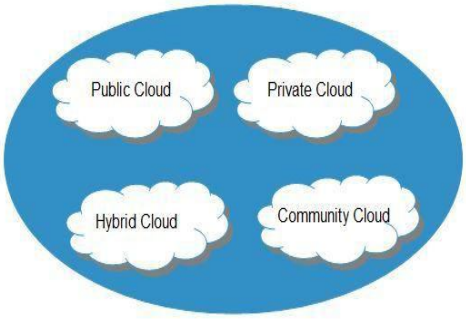

Fig 3: Cloud Deployment Models

II. 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.

III. 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.

A. 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 few minutes, but it take hours and day . 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.

Fig 4 Denial of Service Attacks in Cloud computing

B. 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 effect on the services.

C. Distributed Denial of Service (DDOS) Attacks:

This attack targets the networks and servers. It makes the network traffic and users being denied to access a certain Internet-based service in the cloud. In worst cases the attackers will use botnets to perform DDOS. In order to stop hackers of attacking the network, face blackmail is provided. DDOS attacks should be considered as threats for cloud providers such AWS, Google Apps, and Microsoft Cloud. These scenarios show us that cloud computing network is still not secure, and this will drive us to non-secure applications.

D. 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.

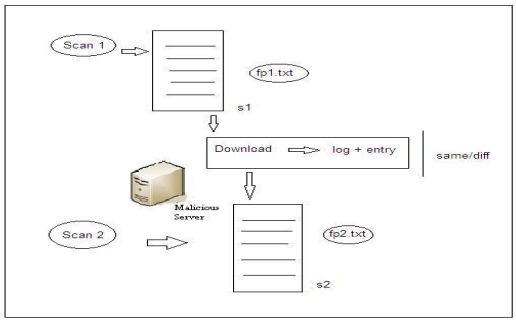

Fig 5 Detection of fingerprinting attack

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.

E. 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.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 is invalid, try through control server".

IV. CONCLUSION

Cloud computing security is still considered the major issue in the cloud computing environment. It is clear that although the use of cloud computing has rapidly increased. 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.

V. REFERENCES

[1] A.M. sharifi, S.K. Amirgholipour, M. Alirezanejad, B.S Aski,M Ghiami "Availability challenge of cloud system under DDOS attack" Indian J.Sci.Technol. pp: 2933-2937, 2012.

[2] D. Jamil and H .Zaki, "Security issues in cloud computing and countermeasures", IJEST, pp: 2672-2676, April 2011.

[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, pp. 1709-1716, 2009.

[4] B. Meena and K.A.Challa,, "cloud computing security issues with possible solutions", IJCST, pp: 340-344, March 2012.

[5] Michael Glenn, "A Summary of DoS/DDoS Prevention, Monitoring and Mitigation Techniques in a Service Provider Environment", SANS Institute 2003.

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

[7] Wikipedia, "window azure" 2012.

[8] K. Birman, G. Chockler and R. vanRenesse,"Toward a cloud computing research agenda", SIGACT News, 40, pp. 68-80, 2009.

[9] "Are security issues delaying adoption of cloud computing?" Networkworld.com.