ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

Improving security issues and security attacks in cloud computing

Dr.V.Venkatesa Kumar[1], M.Nithya[2]

Assistant Professor, Department of Computer Science, Anna University Regional Centre, Coimbatore, India [1]

M.E. Full Time PG Scholar, Department of Computer Science, Anna University Regional Centre, Coimbatore, India[2]

Abstract:At present, cloud computing is the fastest growing technology in today's world. Cloud computing is a model that provides the services based on as-needed and when-needed basis. Cloud computing provides online information storage, infrastructure and application. Many organizations shift towards cloud computing due to its benefits of less hardware maintenance and reduced expenditure start-up cost and at the same time, cloud computing offers many hazards. In this paper, the solution for various security issues and security attacks are analyzed to secure cloud.

Keywords: Security issues, Security attacks, Cloud Security Alliance, Op5 monitor.

I. INTRODUCTION

The term cloud refers to the web or internet. Cloud computing is a metaphor for transferring the information services from the internet. With the help of web-based tools and application's, information is transmitted to the internet [1]. Cloud computing is a compilation of existing approaches and technologies, Prepacked among a brand infrastructure paradigm that provides improved measurability, elasticity, business process, quicker start-up time, reduced management prices and just-in-time accessibility of resources. Resources include database, software, service and server and so on [2].

In cloud computing, cloud actors play a major role. Cloud actors are referred as cloud agents. Two cloud actors are used. They are cloud provider and cloud consumer. A cloud provider is an organization responsible for providing cloud services to cloud consumers based on service level agreement (SLA). Cloud provider is also referred as data owner. Examples of cloud providers are Google, Amazon Web Service, IBM, Microsoft, eBay, Salesforce.com and so on. Cloud provider offers the owned IT resources to the cloud consumers for lease. Cloud consumer is an organization that uses IT resources based on the contract with a cloud provider. Cloud consumer is also referred as a client.

The following Fig1. illustrates the diagrammatic representation of cloud computing. Referring the diagram, cloud provider hosts the services in the cloud storage. Cloud consumer can use the services that have been stored in the cloud storage. With the help of internet, cloud users can access theresources through mobilephone,laptop and other devices.

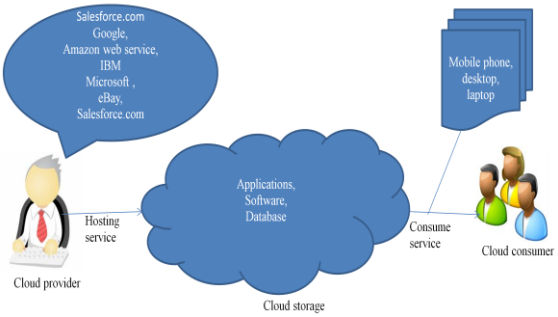

Fig 1. Diagrammatic representation of cloud computing

II. CHARACTERISTICS OF CLOUD COMPUTING

The important features of cloud computing involve [3]:

A. On-demand self service

Cloud computing provides the resources to the end users in a simple and flexible way. Initially, users use the limited resources and based on the need, users utilize more resources. Based on the resources used, users need to pay money. This on-demand self service is also called as a utility service.

B. A broad network access

The ability of the cloud users to use the cloud services that can be widely available. This characteristic is referred as ubiquitous access. Ubiquitous access requires a support for the particular devices, interfaces, protocols and technologies. To enable this access, cloud services should satisfy the needs of the cloud users.

C. Rapid elasticity

Ability of cloud computing that can be transparently extend the IT resources based on the request that has been given by cloud consumers or cloud providers. Wide range of scalability is achieved by the cloud providers with the vast range of IT resources.

D. Resource pooling

Cloud provider stores the IT resources in the cloud. Based on the needs of the end users, resources can be dynamically assigned and reassigned. Multiple cloud consumers can use a large amount of IT resources that has been stored by the cloud provider. Multi-tenancy achieves resource pooling.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

E. Measured service

The cloud platform maintains the use of IT resources that has been used by cloud consumers. This feature is closely related to the on-demand service characteristic. According to the resources used by the cloud consumers, cloud providers charge the cloud consumers.

III. CLOUD SECURITY AND ITS ISSUES

The main objective of cloud computing is data sharing. Since all users can share the data that have been stored in the cloud at that time there is a possibility of breaching information. In order to prevent the information leakage, cloud security is used. Cloud security is an approach of protecting the data in the cloud computing environment.

A. Parameters that influence cloud security

Cloud security is influenced by the following parameters [2].

- Networks
- Databases
- Operating system
- Virtualization
- Resource scheduling
- Transaction management
- Load balancing
- Concurrency control and
- Memory management

B. Security problems with cloud computing

Security is one of the biggest challenges in the cloud computing. There is also a chance for the attacker to steal the information in the cloud by acting as a legitimate user. This causes a number of problems when multiple users sharing the data in the cloud. The following Fig 2. represents the security issues in cloud.

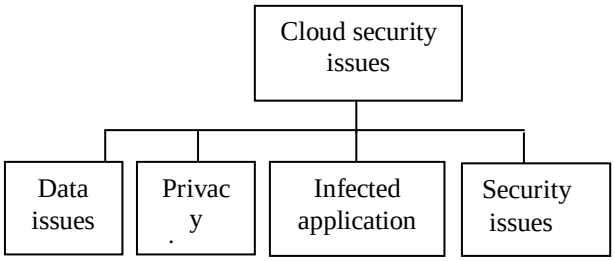

Fig2. Cloud security issues

The number of security problems that are faced by cloud computing [2] are

- Data issues
- Privacy issues
- Infected application
- Security issues.

A. Data issues

Sensitive data is stored in the cloud. At anytime, anyone from anywhere can access the data in the cloud. Two issues are faced by data security. They are data integrity and data loss [2][4].

1) Data integrity

In cloud, at the same time, many cloud providers and consumers can access and modify the data. So, there is a loss of data integrity in the cloud computing.

2) Data loss

Sensitive information is disclosed to the unauthorized users that are not authorized to see the data. At that time, there was a possibility of data breaches.

B. Privacy issues

There is no assurance to maintain the confidential data to be protected. Since anyone can access the data in the cloud. So, there is a possibility of breaching the privacy in the cloud [2][4].

C. Infected application

Cloud provider is responsible for monitoring the server [2][4]. So, this will protect against the malicious user from attaching the infectedapplication in the cloud. This will severely influence the cloud users.

D. Security Issues

In cloud computing, security must happen on two levels [4][5]. The one is on provider level and another is on customer level.

1) Security on provider level

Provider need to check that the server is secured from the external threats [5]. A cloud is good if there is a security offered by the provider to the customers.

2) Security on user level

User needs to check that the data received by the provider are without any loss [5].

IV. SOLUTION TO THE SECURITY PROBLEMS

The Cloud Security Alliance (CSA) is a non-profit organization that has developed a set of rules and frameworks for implementing the security within a cloud computing environment. It provides four important framework layers for cloud security. They are virtual network monitor layer, cloud data layer, cloud storage layer and virtual machine layer [2]. The following figure2 represents the framework layers for cloud security.

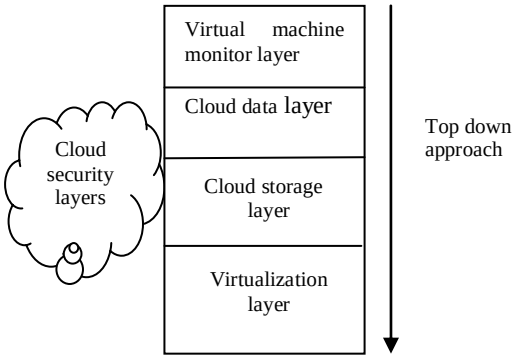

Fig 3. Framework layers of cloud security

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

First layer in the cloud security is the virtual network monitor layer. It is the top most layers in cloud security layers. The virtual network monitor layer provides end to end visibility for highly virtualized infrastructure. Virtualization platforms such as VMware, KVM and XEN. It keeps monitoring the response time and also validating the availability of network components. In this, op5 monitor is used to monitor all levels in virtual infrastructure, including servers and network device that provides a complete solution for virtual infrastructure. Op5 monitor is a best solution for monitoring the virtual infrastructure. Second layer in the cloud security is the cloud data layer [2]. It is the major layer that has been used in the cloud.Third layer in the cloud security is the cloud storage layer. This layer provides flexible data storage and runs the applications with fast changing data paradigm. Last layer in cloud security is virtual machine layer [2]. The virtual machine is a software application in which the operating system or programs can be run in the cloud computing infrastructure.It is constructed within the virtualization layer includes Hypervisor. Virtualization layer is used to construct many separate Virtual machines.

V. SECURITY ATTACKS AND ITS POSSIBLE SOLUTIONS

At present, many of the organizations uses cloud computing to share the confidential data. Many hackers trying to violate the security to use the cloud resources. Security attack is an intelligent act that attempts to violate the services in the cloud. Different types of

attacks are used by the hackers to prevent the cloud users to access the data in the cloud.

A. Denial of Service (DOS) attack

In DoS attack, the attacker tries to prevent the legitimate users to access the resources in the cloud. In this attack, bulk messages are sent by the attacker querying the server to verify the requests. While verifying the requests, it has returned invalid addresses. The attackerreturn address has not been able to find by the network or server. While verifying requests, attackers make the server to pause before ending the connection [6]. When the connection is closed by the server, the hacker sends more valid messages with invalid addresses. This makes the network or server in a busy state. This attack causes the network traffic and services are not accessible by users.

B. Denial of Service attack solution

DOS attack is prevented by using prior automatic switches that provide the packet rate analysis. DOS attack is mainly used to protect the network traffic against authorized and unauthorized users [6].

C. Malware injection Attack

In a malware injection attack, an attacker tries to insert mischievous code or service which emerges like the existing services executing in the cloud. This attack is also known as driven-by downloading or meta-data spoofing attack [6]. Attackers steal the information from Internet by forcing the users to download the malicious software automatically without the knowledge of users. By doing this, reliability of the service is not verified.

D. Malware-Injection attack solution

The malware-injection attack is prevented by allowing the cloud users to create an account in the cloud and provider create the copy of cloud user's VM image in the cloud image storage system [6]. In this file allocation table is used to determine the current code that is being run by the client. Integrity is checked by using File Allocation Table (FAT) from the user's virtual machine. Virtual machine image repositories such as VMware's Virtual Appliance Market Place and Amazon EC2 [7].

E. Wrapping attack

The attack uses a method known as XML signature wrapping and shows vulnerabilities while executing the web service request. In wrapping attack, the attacker tries to insert the malicious element in the SOAP(Simple Object Access Protocol) message structure in Transport Layer Service(TLS) and after inserting the malicious code, fake content of the message is copied into the server and while executing, cloud server working is interrupted by the attacker [6].

F. Wrapping attack solution

The Wrapping attack is prevented by increasing the security while sending the message from a web server to a web browser by using SOAP messages. An extra bit called STAMP bit [7] is added to the signature value and is included in the SOAP header. This extra bit prevents the attacker by changing the signature value. uses a method known as XML signature wrapping and shows vulnerabilities while executing the web service request. In wrapping attack, the attacker tries to insert the malicious element in the SOAP(Simple Object Access Protocol) message structure in Transport Layer Service(TLS) and after inserting the malicious code, fake content of the message is copied into the server and while executing, cloud server working is interrupted by the attacker [6].

G. Flooding attack

In flooding attack, an adversary can easily create fake data and whenever the server is overloaded,it allocates the job to the nearest server and specific server is itself offload [7]. While allocating, it offers more capable and quicker processing request. While processing the requests, the server first validates the legitimacy of the requested requests and also invalid requests must be validated to verify the authenticity and also checks the consumption of CPU utilization and memory allocation and causes the flooding of a system.

H. Flooding attack solution

Flooding attack is prevented by challenger to add fake data by allocating each server to perform a specific job and all the servers are internally communicating with each other quickly through message passing [7]. When the server is overloaded, a new server is employed with the

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 10, October 2014

destination of the requests of the overloaded server. In this PID is appended to the message to identify the requests of the valid customer and PID is encrypted by using RSA or hash value implementation [6].

I. Data stealing attack

Data stealing attack is the most widely used traditional approach to verify the user account. In this attack, attacker steals the information of user account and password. In this attack, confidential information about the user is lost by the activity of the challenger.

J. Data stealing attack solution

The data stealing attack is prevented from generating a unique number to the customer while login every time to use the system [7]. When the session is expired, PID generator is used to commit the task and PID generator is present inside the hypervisor.

VI. CONCLUSION

In this paper, the various solutions for security issues and security attacks in the cloud are discussed. In the near future, the security matrix concept is used based on a multidimensional approach to analyze further threats in the cloud and that ensures the cloud more secure.

REFERENCES

[1] Kalyani Kadam, Rahul Paikrao, Ambika Pawar, "Survey on Cloud Computing Security", IJETAE, Volume 3, Issue 12, December 2013.
[2] AbhinayB. Angadi, Akshata B. Angadi, Karuna C. Gull, "Security Issues with Possible Solutions in Cloud Computing-A Survey", IJARCET, Volume 2, Issue 2, February 2013.
[3] A. N. Suresh, Ch. Sailaja, G. Gayatri, D.V.S. Deepak, "Security Challenges In Cloud Computing", IJERT, Vol. 2 Issue 2, February-2013.
[4] Dr.Nedhal A. Al-Saiyd, Nada Sail, "Data Integrity in Cloud Computing Security", Journal of Theoretical and Applied Information Technology, 31st December 2013. Vol. 58 No.3
[5] Rushikesh Vilas Belamkar, "Challenges and Security Issues in Cloud Computing", ISRJ, ISSN 2230-7850, Volume-4, Issue-2, March-2014.
[6] Apurva Shitoot, Sanjay Sahu, Rahul Chawda, "Security Aspects in Cloud Computing", IJETT, Volume 6 number 3 - Dec 2013.
[7] Kazi Zunnurhain and Susan V. Vrbsky, "Security Attacks and Solutions in Clouds".

BIOGRAPHIES

Dr. V. Venkatesakumar is currently working as Assistant Professor in Anna University Regional centre Coimbatore, India. He received his Bachelor and Master Degree, B.E from Bharathiar University, M.E and Ph.D., from Anna University Chennai.. He has more than 11 years of experience in Teaching and Industry. His research area includes Cloud Computing, Operating System, Software Engineering, Security and Web Technologies.

M.Nithya received her B.E degree in Computer Science Engineering from Sri Krishna College of Engineering and Technology, Coimbatore in 2013. . She is currently pursuing M.E degree in Computer Science and Engineering from Anna University Regional Centre, Coimbatore. Her area of interest is cloud computing, Networks, Database.