Defeating Attacks in Cloud Computing

Poonam Bobade, Seematai Wadekar, Nisha Pagare, K.S.Warke

***Abstract*— As vulnerabilities keep increasing exponentially every year, the need to efficiently classify, manage, and analyze them also increases. As more and more users, becomes very important to have proper vulnerability management in cloud. In this paper presentation of vulnerability management framework for cloud computing is represented. Cloud computing is a new environment in computer oriented services. It is not an easy task to securely maintain all essential data where it has the need in many applications for clients in cloud. To maintain our data in cloud, it may not be fully trustworthy because client doesn't have copy of all stored data. Therefore the security is the biggest problem of this system, because the services of cloud computing is based on the sharing. So, the preventive measures of, the different types of attacks in cloud computing services is described.**

***Keywords*— Cloud Computing, D-DOS, IP Spoofing, Malware, Security, Vulnerability.**

I. INTRODUCTION

Accessing security of software services on cloud is complex because the security depends on the vulnerability of infrastructure, platform and the software services. This system have some similarities to distributed system, according to this similarities cloud computing also uses the features of networking. Cloud computing is redefining the way computers are used. In many systems, the platform or the infrastructure on which the software will actually run may not be known or guaranteed. This implies that the security of the software services must be assured regardless of the underlying infrastructure or platform, requiring a large number of combinations. Another common and most used trend in cloud and service oriented architecture (SOA) environments is service composition, whereby new services can be created rapidly by composing existing services. Once again here the component services must be tested for security levels or purpose on a large number of platform and infrastructure combinations. Infrastructure as a Service(IaaS) as the bottom layer where resources are managed physically. Platform as a Service(PaaS) which provide service as the middle layer. Software as a Service(SaaS) as the top layer which offers software applications as a service.[1]. Cloud computing scenario can be modeled using various classes of participant: service user, service instance and cloud provider. Attacks in cloud takes place among these participants[10].

SQL Structured Query Language injection and Cross site Scripting attack are the common application layer attacks, which are the techniques used to defeat website by manipulating or deleting the data through inputting unwanted common strings[2].

II. PROPOSED SYSTEM

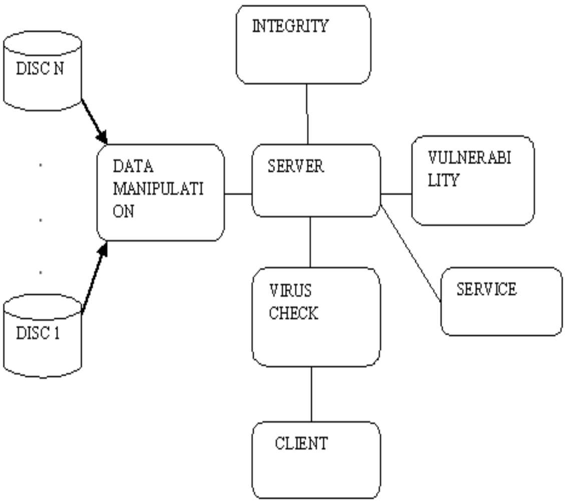

Fig.1 Proposed System Architecture

The "cloud" in cloud computing can be defined as the set of hardware, networks, storage, services, and interfaces that combine to deliver aspects of computing as a service. Cloud services include the delivery of software, infrastructure, and storage over the Internet (either as separate components or a complete platform) based on user demand. Cloud computing has four essential characteristics: elasticity and the ability to scale up and down, self-service provisioning and automatic deprovisioning, application programming interfaces (APIs), billing and metering of service usage in a pay-as-you-go model

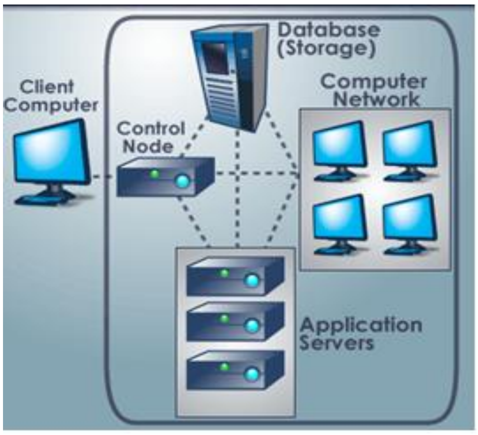

Fig 2.Working Of Cloud

Manuscript received January, 2014.

Miss. Poonam Bobade, Computer Engineering, Bharati Vidyapeeth's college of engineering for women, Pune, India.

Miss. Seematai Wadekar, , Computer Engineering, Bharati Vidyapeeth's college of engineering for women, Pune, India.

Miss. Nisha Pagare, Computer Engineering, Bharati Vidyapeeth's college of engineering for women, Pune, India.

Prof. K.S.Warke,Computer Engineering, Bharati Vidyapeeth's college of engineering for women, Pune, India .

In cloud, client access service from server so some authentication is required. Unknown user can inject malicious code in database, So we cannot write the dynamic query. Multiple client can access the service from the server. The data transfer is in packet form, hacker can get IP address of registered client and data get accessed to him. We can monitor packets using network-monitoring software. A packet on an external interface that has both its source and destination IP addresses in the local domain is an indication of IP spoofing. Some professionals said that cloud is Vulnerable to D-Dos attack. When Some user provide high request to access the service then sometime that particular service won't get available to other user then system will come to know that this will be D-Dos attack. We compare these request & time duration between the request with some threshold value If request time is greater than threshold value then that client will be blocked.

A.Vulnerability

Man in the middle of attack.

Vulnerability is the probability that an asset will be unable to resist the actions i.e., take preventive measures towards resisting force. In this topic, demonstration of various attacks through creation of a cloud and its prevention measures, through the client on the server.

B. Objectives

- Demonstrate solution for vulnerability.
- Implementation of the various kinds of attacks and overcoming issues are focused.
- Analyzing how system will behave for various kind of attacks.

III. APPLICATIONS

- This system can be used in college level for preventing attacks in network.
- This system can be used in organizational level.
- It can be useful for securing the private cloud.
- The system can be found in web application like firewall.

IV. ADVANTAGES

- Physical storage centre no longer required.
- It is convenient that is anyone can access from anywhere.

V. DISADVANTAGES

- If user enters weak user name then it can be hacked by attacker.
- If any new attack is generated then it will not be detected by the system.
- Risk of data loss**.**

VI. CONCLUSION

The various attacks and its defensive issues and overcoming them, is the prior concern and is done effectively and appropriately. In this system work the demonstration of the mentioned attacks regarding vulnerability and its demonstration of vulnerability management in cloud system is defined.

REFERENCES

1. Zhifeng Xiao and Yang Xiao, senior member, IEEE Security and privacy in cloud computing, 2012.
2. Amol Poman , Mahesh Gundras, Prashant Pujari ,"G Rahul Johari USIT, GGSIP University Sector 16-C Dwarka, India & Pankaj Sharma CERT -In Ministry of communication & IT Govt. of India.A survey on Web application vulnerabilities (SQLIA, XSS) Exploitation and security Engine for SQL injection, 2012
3. Farzad Sababhi ,Faculty of computer engineering Azad University Iran. Cloud computing Security Threats & Responses.2011
4. Fog Computing: Mitigating Insider Data Theft Attacks in the Cloud Salvatore J. Stolfo Computer Science Department Columbia University New York , NY, US, Malek Ben Salem Cyber Security Laboratory Accenture Technology Labs Reston, VA, USA Angelo's D. Keromytis Allure Security Technologies New York , NY, USA.
5. Data Integrity Proofs in Cloud Storage Sravan Kumar R Software Engineering and Technology labs Infosys Technologies Ltd Hyderabad, India.Ashutosh Saxena Software Engineering and Technology labs Infosys Technologies Ltd Hyderabad, India.
6. Prudent Practices for Designing Malware Experiments: Status Quoand outlook. Christian Rossow , Christian J. Dietrich, Chris Grier, Christian Kreibich, Vern Paxson , Norbert Pohlmann, Herbert Bos, Maarten van Steen.
7. Preventing IP Source Address Spoofing: A Two-Level, State Machine-Based Method BI Jun, LIU Bingyang, WU Jianping , SHEN Yan.
8. A unified approach for detection and prevention of DDOS attacks using enhanced support vector machins and filtering mechanisms T. Subbulakshmi, P. Parameswaran, C. Parthiban, M. Mariselvi, J. Adlene Anusha and G.Mahalakshmi bed.
9. Data Integrity Proofs in Cloud Storage.Sravan Kumar R, Ashutosh Saxena,978-1-4244-8953-4/11/$26.00c 2011 IEEE
10. N. Gruschka, M. Jensen, "Attack Surfaces: A Taxonomy for Attacks on Cloud Services," Cloud Computing, IEEE International Conference on, pp. 276-279, 2010 IEEE 3rd International Conference on Cloud Computing, 2010.
11. The Management of Security in Cloud Computing Ramgovind S, Eloff MM, Smith ESchool of Computing, University of South Africa, Pretoria, South Africa. 978-1-4244-5495-2/10/$26.00 ©2010 IEEE
12. Security and Privacy Challenges in Cloud Computing Environments, Hassan Takabi and James B.D.Joshi Gail-Joon Ahn 1540-7993/10/$26.00 © 2010 IEEE