National Conference on Science, Engineering and Technology (NCSET – 2016) ISSN: 2321-8169
Volume: 4 Issue: 6 130 - 131

A Survey on Security Issues and Emerging Trends in Cloud Computing Security

Mr. Vinod Kokitkar
Asst. Professor
Department of MCA
Gogte Institute of Technology
Belagavi

Mr. Prashant Mithari
Asst. Professor
Department of MCA
Gogte Institute of Technology
Belagavi

Mr. Hrishikesh Mogare
Asst. Professor
Department of MCA
Gogte Institute of Technology
Belagavi

Abstract- Cloud computing is a dynamic environment for delivery of services to the clients on demand. Many organizations are in a dilemma, whether to cloudify or not to cloudify. The main reason for this dilemma is with respect to the security issues related to cloud computing. Removing this dilemma from the organization is a key factor. This paper provides a well defined approach to the several security threats that prevent organizations from adopting cloud computing techniques. This paper also provides a comprehensive survey of the emerging security solutions to protect the cloud environment

*****

I. INTRODUCTION

Cloud Computing is gaining more and more thrust due to technology related elements [1]. Cloud computing is graded into into two main parts Front End and Back End. Front end refers to the clients that access services from the cloud and back end refers to the network of servers that have programs and facility of data storage[2]. Proof shows that even though cloud computing provides a major boulevard for businesses, making a shift to the cloud computing is obstructed by several security issues. For example, financial institutions financial institutes are attracted by cloud computing but for security reasons they are still in the early stages of adoption. The cloud security is gauged by setting up and running Dionaea honeypots for a few months in the cloud provide networks.[3]. In order for cloud computing to be viewed as a potential alternative, it should provide the same level of security as traditional IT systems. Hence an awareness of the various security tools is needed.

II. CLOUD ARCHITECTURE

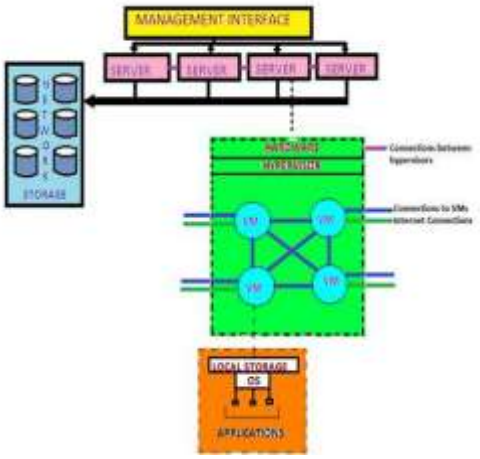

Fig 1: Architecture of Cloud Infrastructure

III. SECURITY ISSUES

1. Seizing control over services and accounts: Gaining control over others accounts is not new in today's world. It includes phishing, deleting and manipulating the user account and sensitive data. Such an individual can be termed as a hacker. [2]
2. Shared technologies threats: Attackers can utilize the weakness of the Virtual Machine Monitor(VMM) and can get entry into the physical host[4]
3. Data breach: A situation where sensitive data is accessed, controlled and manipulated by an unauthorized individual. [5]
4. Envious insiders: An employee who has appropriate privileges to gain access might manipulate sensitive data and misuse it. [6]

IV. ATTACK VECTORS

The aforestated issues are caused by 3 main lines of attack: Network, Hypervisor, and Computing Hardware. [1]

1. Network-based attacks: The network is one of the main ways in which cloud can be compromised. One of the most dangerous is the Distributed Denial of Service(DDoS). DDoS is classified into two types: net-work/transport level and application level attacks.[7]. Another type of threat is Code Injection where an attacker introduces a Script Injection, XML Injection or a Command Injection thereby changing the course of execution.
2. Hardware-based attacks: Attackers can take advantage of the multi-tenant environment to access physical resources such as memory bus,disk bus,and data and instruction caches(L1, L2,L3)in which they can find decrypted data and the cryptographic keys of well-known algorithms (AES, DES,RSA)and of other VMs instances. This is called Cache-Based Side-Channel attack.
3. Hypervisor-based attacks: The hypervisor is the software layer which guarantees the clouds multi-tenacy feature. The NIST guide to security and privacy of clouds says that if an attacker gains access to the guest O.S and hence the hypervisor, then it can have a severe impact on the whole infrastructure. [8]

V. EMERGING TRENDS IN SECURITY

In the following we identify some of the ways in which security can be provided to cloud computing environment so that it can be easily adopted by organizations.

1. Authentication and identity management: an authentication and identity management system can be used which allows users to access the cloud based on their credentials. Existing password-based authentication has an inherited limitation and poses significant risks.[9]. Hence another alternative is to use a One Time Password(OTP) to access the cloud services. This OTP can remain alive for a limited period and self destructs or becomes invalid after a specified time.
2. Provide Secure Interface: During authentication, most of the interfaces and API store user information in the form of cookies, password and transaction history. Such information can be easily accessed by intruders or attackers to hack the cloud environment. So its responsibility to cloud provider to invent an API and interface in such a way that they will need only important information of users to provide interaction with cloud services and do not store user personal information such as passwords, cookies, transaction history even user wishes to do it [2]
3. Cryptography Unit:Another way is to provide a cryptography unit which stores data in an encrypted form. The cloud will maintain the unique random key generator so every user on cloud will have unique key for data encryption and decryption purpose. Whenever user want to access the data then every time this user will get his decryption key via E-mail on his registered mail id registered at the time of creation of account on cloud.

VI. CONCLUSION

This paper gives an overview of the cloud computing attacks. The paper surveyed the different threats and also the emerging security techniques that are available for protecting the cloud environment. The paper also discusses the different attack vectors. And as we moving forward to the direction of cloud computing the security and privacy issues will generate day by day in the area of computation, storage management, infrastructure handling, input/output management, resource utilization and authorized user activities. Being a work-in-progress, we can continue with the collection and classification of cloud-based attacks and vulnerabilities in order to prove or controvert our attack taxonomys applicability and appropriateness.

VII. REFERENCES

[1] L. Coppolino et al., Cloud security: Emerging threats and current solutions, Computers and Electrical Engineering(2016).
[2] Mr. Anup Date, Mr. Dinesh Datar: A Multi-Level Security Framework for Cloud Computing, IJCSMC, Vol. 3, Issue. 4, April 2014.
[3] Awadhi E A, Salah K,Martin T.Assessing the security of the cloud environment.GC Cconference and exhibition(GCC), 20137th.Doha:IEEE; 2013
[4] Nanavati M, Colp P, Aiello B, Warfield A.2014. Cloud security: a gathering storm. Commun ACM May2014.
[5] searchsecurity.techtarget.com/definition/data-breach
[6] Kandias M,Virvilis N, Gritzalis D. The insider threat in cloud computing.
[7] Zargar ST, Joshi J, Tipper D. A survey of defense mechanisms against distributed denial of service flooding attacks IEEE Common Surveys Tutor Fourth Quarter 2013
[8] Grance T.,Jansen W..Guidelines on security and privacy in public cloud computing.NIST.
[9] Security and privacy issues in cloud computing, Jaydip Sen,Innovation Labs, Tata Consultancy Services Ltd., Kolkata, INDIA.