ijecs open access www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 5 Issue -03 March, 2016 Page No. 16047-16049

Analysis of Security threats in ad hoc cloud.

[1]Mrs. Salini Suresh, [2]Dr.L.Manjunath Rao

[1]Research scholar Bharathiar University, Coimbotore.
151,12th cross, 5th main NGEF layout, Nagarbhavi, Bangalore, 9663363201
pnsalinisuresh@gmail.com
[2]Head, MCA department, Dr. Ambedkar Institute of Technology, Bangalore,
manjuarjun2004@yahoo.com

Abstract

The cloud is redefining the IT architectures of various business domains. Organizations have clearly recognized the unlimited benefits of cloud like dynamic payloads on the technical side and elastic financial models on the commercial side which guarantees in greater than before efficiency. The benefits of cloud computing can be maximized fully by applying novel technologies in security and risk management processes. The risk factors in terms of security is much more in public cloud computing compared to traditional computing which are bases on datacenter . In a highly shared ad hoc cloud environment which is in the control of instance-to-instance network connectivity security of the applications and sensitive data is a big challenge faced by the cloud providers. As the entire stack of applications, platform, infrastructure of the cloud is designed and managed by service providers the cloud users are uncertain about the security. This paper studies the generic security challenges in an ad hoc cloud environment .the security challenges and mitigations are discussed in section I. A survey was conducted with users of cloud from domains like health care, education and retail business. Analysis of survey data and the results are also discussed in section II.

Introduction

Ad hoc clouds rely on scalable virtualization technology which gives its user access to set of non-dedicated computing resources. The users of an ad hoc cloud are in a highly shared environment where resources are dynamically provisioned and organizations share the same remotely located physical hardware with strangers. Security and privacy has been the biggest challenges for organizations who are already using cloud as end to end solution for their IT needs and who are still considering moving into cloud. In a SPI model of cloud SaaS demands security at all levels of user identity and data access and maintain integrity and continuity of the applications. In IaaS secure networking and trusted computing should be the prime concern, and whereas at PaaS demands protection at the resource-management level.[1]

Section I
Security challenges in Ad hoc cloud model.

1) *Identity and Access Management (IAM*): The service provider in responsible for security of applications and users have less control over the security. In an ad hoc cloud environment where highly mobile users and multiple end devices, identity and access management is a key issue. IAM has to be addressed by proactive and reactive security tools .Implementing a strong IAM can be done through protocols like security assertion markup language (SAML) [2].

2) *Data leakage and protection* : sensitive organizational data is stored as plain text in cloud environments are more prone to breaches. Secure data processing and storage is usually the responsibility the service provider [3].Data protection can be achieved giving the access rights to the users at multiple levels. Encryption is an effective way to provide the control over their confidential data. Users have exclusive control of the encryption keys, and therefore control of their own data with in their environment[4] .There are no clear standards on how to the cloud service provider should do a recycling of storage resources like memory or disk space. When these resources are not properly recycled there are high chances of data remanence . Solution for data remanence can be established through service level agreements which should clearly state the strategies for data deletion once a tenant vacates the storage space [5].

The other persistent threats faced in ad hoc cloud environment can be:

3) *Hypervisor attacks*: In a multitenant ad hoc cloud users highly share physical resources with others through common software virtualization layers. With an added risk to user's resource stack, the cloud user consumer is completely ignorant of another tenants identity and intentions. The virtual machine could be malicious and prone to hypervisor attacks or sniff communications. Vulnerability of side-channel attack in a cloud environment where a virtual machine sharing the same resource induce a arbitrary code into another virtual machine [6]. using TCCP (trusted cloud computing platform) secured Infrastructure as a service

provide a closed box execution environment where virtual machines can execute confidentially and allows users to attest to infrastructure service provider before virtual machines are launched .[7]

4) Network security: Due to resource pooling feature of ad hoc clouds network components like IP, Ethernet, bandwidth, firewalls are shared among tenants who can cause cross tenant attacks. Users can demand from the service provider isolation in terms of network components.[8] .Flooding based denial of service(DOS) attack is another issue in multitenant shared cloud model . Unauthorized users can create denial of service by flooding the network port with unwanted packets.[9]. The above discussed security concerns also can be controlled through SDN by creating a secure tunnel between the Virtual Machines. Granularity and security management using SDN is better in Virtual machine level, application level and platform and infrastructure level. In this attack the invader sends the request for resources on the cloud rapidly so that the cloud gets flooded with the ample requests.

5) VM hopping: When bare metal is provided to an user as service, users create virtual machines. Creation of without policies and process can cause VM hopping and escape. In VM escape, the hackers escape from the virtual machine and start interacting with the hardware directly. Using VM hopping attackers hop between virtual servers gain access to physical hardware [10] .VM hopping is thus a critical concern for IaaS and PaaS layers of cloud. Tightly coupled process and policies on user rights at virtual machine manager level should be implemented. Using right IAM techniques can reduce VM hopping and escape.

6) *Man in the middle Cryptographic attack*: Untrusted user place between two trusted users of the cloud and interrupt the data. Wrapping Attack is an MITM attack similar to XML Signature wrapping attack where cloud users access cloud through web services. Login credentials are duplicated here.[12][13].Browser attack which causes data stealing is done damaging the signature and encryption during the translation of SOAP messages in between the web browser and web server. This can be regulated using encryption of data, digital certificates and security tokens and role based access.

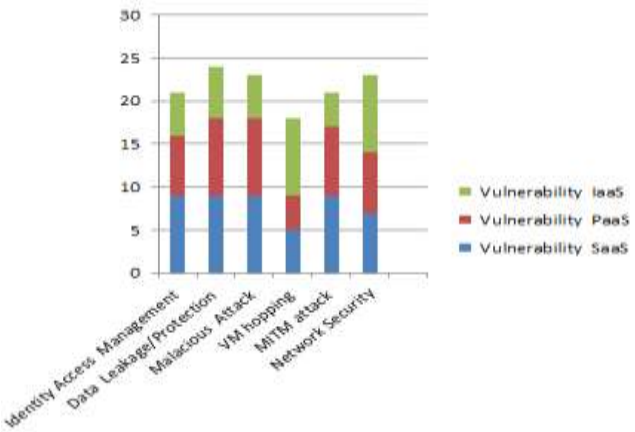


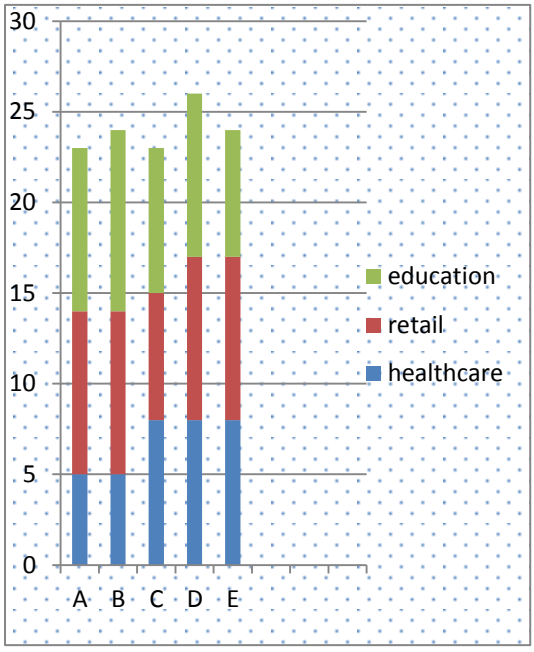
Figure1: Vulnerabilities in SaaS ,PaaS, IaaS

Section II

A survey was Conducted in fifteen Organizations from healthcare /Retail /Manufacturing and educational domains who moved their application to Private/public cloud in last 1 year . Thirty people Participated in the discussions who are the decision makers for the process of moving the application to cloud.

Questions asked to the respondents were:

1) Why did you move to cloud and which attributes of cloud are important for you?



- A indicates ad hoc scalability
- B indicates pay per use
- C indicates security
- D indicates mobile user/clients
- E indicates increasing application
- robustness

Figure2: cloud attributes in business

2) What do you think is the severity of the below written security threats in your cloud environment?

a) Identity and Access Management (IAM)

b) Data Leakage/Protection

c) Denial Of Service attack.

d) Hacking

e) Network security

The organizations were using on premise applications for their business needs which they moved to cloud recently. The analysis shows even though efficiency has improved

technically and economically after migrating to cloud, the security concerns still prevail.

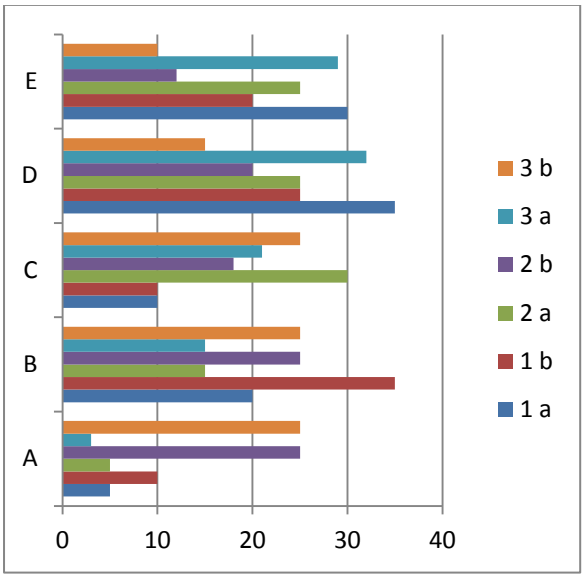


Figure3: security threats, on premise vs cloud

- A indicates Identity and Access Management (IAM)
- B indicates Data Leakage/Protection
- C indicates Denial Of Service attack.
- D indicates Hacking
- E indicates Network security
- 1a indicates health care on premise
- 1b indicates health care on cloud
- 2a indicates retail/manufacturing on premise
- 2b indicates retail/manufacturing on cloud
- 3a indicates education on premise
- 3b indicates education on cloud

References

[1 [. Kai Hwang University of Southern California Deyi Li Tsinghua University, China "Trusted Cloud Computing with Secure Resources and Data Coloring", ieee internet computing, september/october 2010,pno:15-22

[2]. Cloud Security Alliance (2012) SecaaS implementation guidance, category 1: identity and Access managament. Available: https://downloads.cloudsecurityalliance.org /initiatives/secaas/ SecaaS_Cat_1_IAM_ Implementation_ Guidance.pdf.

[3].Ju J, Wang Y, Fu J, Wu J, Lin Z (2010) "Research on Key Technology in SaaS. ": International Conference on Intelligent Computing and Cognitive Informatics (ICICCI), Hangzhou, China. IEEE Computer Society, Washington, DC, USA, pp 384–387

4)Harnik D, Pinkas B, Shulman-Peleg A (2010) "Side channels in Cloud services: deduplication in Cloud Storage". IEEE Security Privacy 8(6):40–47

[5]. ENISA (2009) Cloud Computing: benefits, risks and recommendations for information Security. Available: files/deliverables/cloud-computing-risk-assessment.

[6] "Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party ComputeClouds," . November 2009 by MIT and UCSD

[7]Towards Trusted Cloud Computing Nuno Santos Krishna P. Gummadi Rodrigo Rodrigues,MPI-SWS.

[8] http://people.csail.mit.edu/tromer/papers/cloudsec.pdf

[9]Detecting flooding based DOS attack in cloud computing environment using covariance matrix approach , ICUIMC '13 Proceedings of the 7th International Conference on Ubiquitous proposes an approach for detecting and fixing floodind based DOS.

[10] Pouring Cloud Virtualization Security Inside Out Yasir Shoaib, Olivia Das Department of Electrical and Computer Engineering, Ryerson University, Toronto, ON M5B 2K3.

[11]A. Singh and M. Shrivastava, "Overview of attacks on cloud computing," International Journal of Engineering and Innovative Technology (IJEIT), vol. 1, no. 4, 2012.pno-321-323

[12]A Survey of Cloud Authentication Attacks and Solution Approaches B.Sumitra*1, C.R. Pethuru2, M.Misbahuddin3 pno6246-6253

[13] B.Meena and K.A. Challa , "Cloud Computing Security Issues with possible solutions," Int, Journal of Computerr Science and Technology, vol.2, Issue: 1, Jan–March, 2012

Author profile

Salini Suresh is currently working as assistant professor in Department of Computer science at Shesharipuram academy for business studies,Bangalore.she is a research scholar in Bharathiar university.