A Survey on Cloud Security: Infrastructure as a Service

Mahesh M. Baradkar[#1], Dr.Bandu B. Meshram[*2],

[#1]*Veermata Jijabai Technological Institute(VJTI), Student, Department of Computer Engineering*

[#2]*Veermata Jijabai Technological Institute(VJTI), Professor,Department of Computer Engineering*

Abstract *- Cloud Service Provider more popular topic that has drastically changed the way of working with the complex, time consuming, and costly solution. CSP provides computer infrastructure to enterprises with some SLA. SLA consists of some promises like providing simplicity, utilities with virtualization. After utilizing some of the resources provided by the CSP, most of the organizations are looking for the fastest way of accessing available resources anywhere any time with less cost.[16]*

Three important services delivered for cloud computing are Software as a Service, Platform as a Service, and Infrastructure as a Service. Users have accessibility to these services using Internet. Users can pay to the cloud service provider as per their use of resources for specific time, eg. Web hosting. Cloud service providers generally price according to Quality of Service requirements. Private, Public, and Hybrid clouds are types of cloud deployment models. [2][19]

Keywords - *SLA, IaaS,Components of IaaS, Virtual Machine.*

I. INTRODUCTION

The organization itself decides which cloud deployment model will be best suitable for current and future business requirements. Private cloud infrastructure is not accessible to the general public, while public cloud services are available to everyone.

This paper discuss about tools to implement Infrastructure for cloud, Cloud security, various Attacks on Infrastructure. In this paper we are reviewing various tools to investigate the attacker which is harmful for the infrastructure, various log files of different Cloud service providers, as well as how we can generate our own log files in simple web application.[14]

Examples Amazon Elastic Cloud Computing1, Microsoft Azure2, and Google App Engine3.

Every organization is moving towards the cloud platform because of its various advantages like without investing much more utilize massive capacities just with few clicks, no need to train staff, or purchase new license of software.

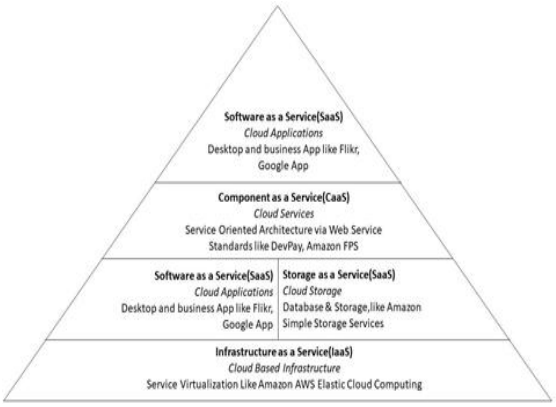

Fig. 1 Cloud Delivery model

Small and medium organizations are also moving their business towards the outsourcing infrastructure. Cloud Computing offers the virtualization of technology to organization with a high security, massive scalability, shared resources, and manageable environmental components. Cloud computing of virtualization technology involved in dependency and designing purposes which might intersect with component as a services like SOA via Web service standards.

To get involved in the outstanding business workflow SOA among cloud service provider and clients (users) followed independently. The most important and base layer for all in cloud computing is IaaS layer which provides cheap and PAYG processing capabilities, data storage with other useful resources. This paper briefly introduces study of security and privacy of IaaS components such as Database, Operating system (instance of cloud operating system), firewalls, switches, virtual machine etc. [15]

II. IAAS COMPONENTS

From past few years the development in cloud services have drastically improved and carried new challenges to the user. The most impeding challenge in using cloud computing is Security and Privacy.[6] Breaking the security of cloud single component ascendency the any others security, results in collapse of entire cloud security. In the following subsections we discuss the security matter of every element with some solution & recommendations.[16]

A. Service Level Agreement (SLA)

A service-level agreement (SLA) is a activity of a service giver and a service user (client). Most common agreement is that services provided to the customer as per the agreed contract, eg. Internet Service Provider and telephone companies. Similarly cloud service provider and customer are responsible to give and take Quality of Services with acceptable level of quality.[1]

SLA consists of goals and objectives, stakeholders, customer requirement, service provider requirements, SLA monitoring, service agreement, service scope, service assumptions, service management, negotiation.

To workout the responsibility & benefits of every troops SLA contract and negotiation is most important phase. The misunderstanding can cause breaching the security of system.

The QoS attributes must be carefully and continuously monitored for the enforcement of SLA in dynamic environment.[13][16]

B. Utility Computing

To make computing resources and infrastructure component available, utility computing is used as service provisioning model. Like other computing services (eg. grid computing) utility computing model minimizes the associated total costs and maximises the overall efficiency of needed resources. Utility computing package consists of computation, storage & services as metered services.

C. Cloud Software

To implement cloud infrastructure plenty of software's are used like OpenStack, CloudStack, Eucalyptus, Synnefo, FOSS-Cloud, openQRM, OpenShift, Cloud Foundry, Docker, Salt Stack etc. These software's used to integrate, facilitate and maintain various factors of SOA between CSP and Client.

Each cloud service provider serves different services which are different from each other. And cannot be agreed to certain features are strictly followed to client. Among these services security is the main and important aspect of cloud computing, i.e we cannot guarantee that certain vulnerability and bugs cannot be breached by anyone.[11]

Various commonly used attacks must be prevented from unauthorized access. Which can be done by using signature based authentication or protection to the web services consequently affecting cloud services. There are many security standards added by the CSP which can prevent unauthorized access to the cloud computing services.[12]

D. Platform Virtualization

There is huge demand in the market of data centers and cloud computing resources with high performance and data storage capacity.

Multiple standalone systems are combined by virtualizing resources to form single computing resource platform (example network, storage, CPUs and Memory). These virtualization hides complex part of managing physical platform. VM simplifies scalability of computing resources as well as multi tenancy and scalability.[7]

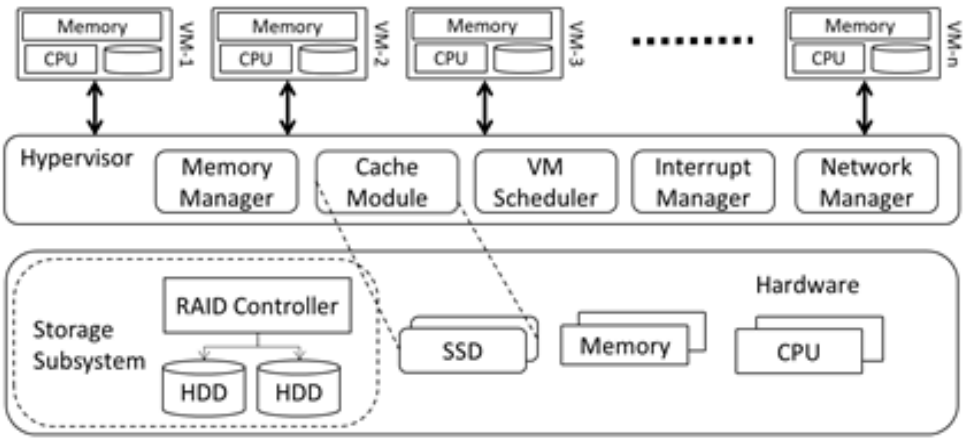

Fig 2 Interaction between Host and VMs

It is not allowed to connect to Virtual disks, memory or applications on the same node, due to separation of VMs by hypervisor. IaaS requires accurately a shared environment; need to be accurately configured to maintain strong separation. Cloud

service providers takes utmost care of their customers to reduce the threats generated from monitoring, transmission, migration, DOS and modification. In the following section, we brief about vulnerabilities and virtualization that prone to delivery model of IaaS from the point of privacy, data integrity and security of the IaaS.[10][16]

1) Security threats sourced from host

Enterprises are now days more involved in a cloud virtual world. Various threats are generated form the host due to monitoring, modification or communication with the virtual machines. These threats are monitored i.e. considered as a most valuable step included in control actions like start, pause, shutdown, restart the virtual machine and its resources. Xenaccses tool is used to run processes from user level, to access customers virtual machine at run time. Xen is used by various service providers like Amazon EC2 and citrix are Xen based.[16]

2) VMs Security threats

Security threats that are from other virtual machine which are generated because of communication, modification and monitoring of virtual machines from other VM or external machine.

VM Monitors other multiple VMs: Latest architecture of CPUs with integrated memory protection features, may prevent violation of security and privacy policy. Hypervisor is the only who prevents monitoring the other memory resources, disk allocated of other virtual machines.[7] [16]

VM to VM Communication: It is totally depend on how those machines are configured like sharing physical machine with other with multiple enterprises.

This makes security of every VM, instances visible. A Secure virtual machine (SVM) analyses all network traffic virtually by using Intrusion Prevention System. IPS is having capability to detect and prevent virtual network known and unknown attacks.

Denial of Service (DoS)

Due to misconfiguration of virtual machine, DoS attacks become more powerful and acquires all available resources. This leads to the starvation of VM and function inappropriately. However Hypervisor is intelligent enough to avoid 100% gaining of shared resources like CPU, RAM, network bandwidth, and graphics memory of machine.

If in any case allocation of any resources is done then hypervisor is so configured to handle such situation by taking appropriate solution, like restart VM automatically. It is better option to restart virtual machine.[9]

E. Networks & Internet Connectivity

Cloud infrastructure is explored in multiple geographical areas to reduce damage of non-predictive disasters and latency. Each site is connected logically as local area network with high speed internet.

IaaS model is vulnerable to various attacks like Distributed DoS, Man in the middle (MITM), IP Spoofing as well as Port scanning.[5] In some cases web based deployment service uses EC2 and Amazon's EBS.

Due to privileges of system admin internal attacks are more severe as compared to the external attack which allows installing and running any malicious code.

However there are some practical solutions and techniques to mitigate these attacks.[16]

Impact of attacks impacts on various Logical network segmentation, Firewalls implementing, Traffic encryption, Network monitoring.

F. Computer Hardware

Physical resources like CPUs, Network devices and storage devices pool is distributed by IaaS interface by serving multiple consumers to deliver shared business model.[7]

Due to virtualization it is possible to keep security of shared resources and control communication with multiple shared resources. Shared physical resources consist of computing resources, network components and storage devices.[8][16]

III. IAAS SECURITY MODEL

Following graph shows IaaS components vs security model with security policies and restriction levels. Each component has its security policy restrictions. Restriction levels start with loose to tight which are provided by the CSP, client and services needed. Diagram shows the relationship among various IaaS components and client requirements on security. As we move from client to CSP security restrictions get tighter.

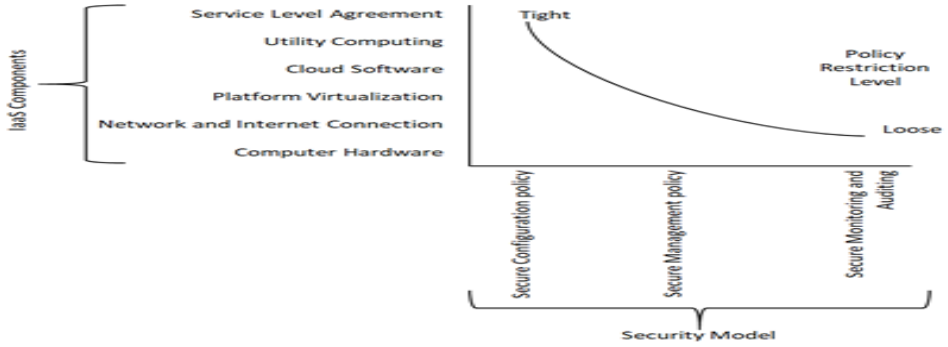

Fig.3 Security Model for IaaS

IV. OPENSTACK AND ITS COMPONENTS

As discussed earlier there are no of cloud operating and or management software's out of which OpenStack is also cloud operating system which controls large pools of resources like storage, compute and networking resources entire datacenter, and are managed through APIs which uses common authentication system.[3]

Horizon is a dashboard gives admin control while improving their users to provision resources through ought a web interface.

Reading Log files and location

A "log file" is a file which records events occurred in software like operating system, instances, or communication among software's and resources during the running state. Logging is the act by keeping a log of relevant actions. Logs can be of any type like event log, communication log, reading logs, login logs, and transaction logs.[3][11][15]

Each component of OpenStack maintains its own log records in different path /var/log/ and with subsequent component name example system log will be in /var/log/syslog.

Reading Log files:

Every cloud service provider uses its own log generation techniques and formats.

OpenStack services uses standard logging levels, to trace its security: TRACE, DEBUG, INFO, AUDIT, WARNING, ERROR, and CRITICAL.[15][18] i.e. messages will be recorded in comparison with log level.

Example: if stack trace is available then TRACE is logged, and information is provided with INFO for every message.[4]

We can disable logging at DEBUG-level, edit /etc/nova/nova.conf file as:

debug=false

Keystone component handles differently.

To make changes at the logging level, we can edit the /etc/keystone/logging.conf file and find the logger_root and handler_file sections.

To make changes in the horizon, it is configured in /etc/openstack_dashboard/local_settings.py.

Horizon uses Django web application.

To find the location of error need to search in particular log file for CRITICAL, or ERROR message from start to end of log file.[4] Screenshot shows log message with its related ERROR from which trace back can be done.

Fig 4: Reading Log file

Attack Name	Category
Cloud Malware Injection	Infrastructure
Flooding Attack	Infrastructure
Denial of Service	Network, Infrastructure
Port Scanning	Network
Attack on Virtual Machine or hypervisor	Infrastructure
Cross VM side Channel	Infrastructure
Phishing	Infrastructure, Network

Table 6: Common Attacks on Cloud Infrastructure

Fig 4 shows log file error message while messaging and its corresponding path that is recorded in various interrelated log files.

Various common Attacks on cloud infrastructure are shown in table 6.

V. CONCLUSION

The favourable clearness and virtualization technology Cloud computing on the basis of which the utility has been delivered has changed the vision towards providing IT infrastructure to the organization. Thus very few of the organizations don't know about the fast access of best business applications provided by cloud. Currently the systems are generating their own log files using which one can trace the security threats whereas the OpenStack services uses standard logging levels to trace their security using various commands and through which the messages are recorded in comparison with log files.

Also OpenStack, CloudStack, Eucalyptus, Synnefo, FOSS-Cloud, openQRM, OpenShift, Cloud Foundry, Docker, SaltStack are other such softwares using I was able to achieve the integration of various factors of SOA between CSP and client. Thus I have studied various methods to analyse the security traces and threats in cloud.

REFERENCES

[1] Ruan, Keyun&Carthy, Joe &Kechadi, Tahar&Crosbie, Mark. (2011). Cloud forensics: An overview. Researchgate

[2] Oliver, Gillian & Knight, Steve. (2015). Storage is a Strategic Issue: Digital Preservation in the Cloud. D-Lib Magazine. 21. 10.1045/march2015-oliver. Researchgate

[3] V. Agrawal, D. Kotia, K. Moshirian and M. Kim, "Log-Based Cloud Monitoring System for OpenStack," 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService), Bamberg, 2018, pp. 276-281. doi: 10.1109/BigDataService.2018.00049

[4] J. Tong, L. Ying, T. Hongyan and W. Zhonghai, "An Approach to Pinpointing Bug-Induced Failure in Logs of Open Cloud Platforms," 2016 IEEE 9th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2016, pp. 294-302. doi: 10.1109/CLOUD.2016.0047

[5] Mohamed Jabir, Raja &Khanji, Salam &Abdallah Ahmad, Liza &Alfandi, Omar & Said, Huwida. (2016). Analysis of cloud computing attacks and countermeasures. 1-1. 10.1109/ICACT.2016.7423295. Researchgate

[6] O'Shaughnessy, Stephen & Keane, Anthony. (2013). Impact of Cloud Computing on Digital Forensic Investigations. IFIP Advances in Information and Communication Technology. 410. 291-303. 10.1007/978-3-642-41148-9_20. Researchgate

[7] Saad Alqahtany1 · Nathan Clarke1 · Steven Furnell1 · Christoph "A forensic acquisition and analysis system for IaaS" Published on 25 November 2015 in Springer DOI 10.1007/s10586-015-0509-x

[8] Luis M. Vaquero · Luis Rodero-Merino · Daniel Morán "Locking the sky: a survey on IaaS cloud security" Received: 12 August 2010 / Accepted: 2 November 2010 / Published online: 24 November 2010 © Springer-Verlag 2010

[9] Sheik Khadar Ahmad Manoj*, D.LalithaBhaskari Cloud Forensics-A Framework for Investigating Cyber Attacks in Cloud Environment 1877-0509 © 2016 The Authors. Published by Elsevier B.V. in ScienceDirectdoi: 10.1016/j.procs.2016.05.202

[10] AHAD AKBARABADI, MAZDAK ZAMANI, SARAH FARAHMANDIAN, JOOBIN MOGHIMI ZADEH, SEYED MOSTAFA MIRHOSSEINI "An Overview on Methods to Detect Port Scanning Attacks in Cloud Computing"

[11] Raffael Marty "Cloud Application Logging for Forensics" March 21-25, 2011, TaiChung, Taiwan

[12] Chales P. Fpleeger, Shari Lawrence Fpleeger, Jonathan Margulies "Security in Computing" Fifth Edition Published by Prentice Hall – 2015 https://ahsanghazi.files.wordpress.com/2017/03/263973122-security-in-computing-5-e-charles-p-pfleeger-pdf1.pdf

[13] Issa M. Khalil 1,*, AbdallahKhreishah 2 and Muhammad Azeem "Cloud Computing Security: A Survey" Computers 2014, Third Edition, 1-35; doi:10.3390/computers3010001 ISSN 2073-431X https://www.researchgate.net/publication/269516029_Cloud_Computing_Security_A_Survey

[14] Fangfei, Z.; Goel, M.; Desnoyers, P.; Sundaram, R. Scheduler vulnerabilities and coordinated attacks in cloud computing. In Proceedings of the 2011 10th IEEE International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 25–27 August 2011;pp. 123–130

[15] https://docs.openstack.org

[16] Dawoud, Wesam&Takouna, Ibrahim &Meinel, C. (2010). Infrastructure as a service security: Challenges and solutions. 1 - 8.

[17] Dr.AliAwais Adnan, Computer Science, Bradford, UK, "Cloud Computing Challenges"

[18] https://docs.openstack.org/operations-guide/

[19] https://www.ibm.com/developerworks/community/groups/service/html/communitystart?communityUuid=e3ec7365-1b09-44f2-906f-19826275860f