International Journal of Advance Engineering and Research Development (IJAERD)
Volume 1,Issue 3, April 2014, e-ISSN: 2348 - 4470 , print-ISSN:2348-6406

Customizable Virtual Machine security Analyzer in Cloud Computing Environment

Patel Deepkumar A.[1],Prof.Upen Nathwani[2]

[1,2]Computer Engineering, Noble Engineering College -Junagadh,deeppatel1989@hotmail.com

Abstract—Cloud Computing is a new model that provides on-demand network access of the computing. Virtualization technology is for data centers and cloud architectures. It has many security issues that must be point out before cloud computing technology is affected by them. Many companies are starting to utilize the infrastructure-as-a-service (IaaS) sometime called Haas-Hardware as service. Attackers can explore vulnerabilities of a cloud system. in Iaas, detection of zombie exploration attacks is extremely difficult for distributed servers in which various virtual machine operating. To prevent vulnerable virtual machines from being compromise in the cloud, we depict multiphase distributed liability detection, measurement. Proposed work customizes Framework for virtual machine attack detection and compromise virtual machine.

Keywords-Cloud Computing; Iaas ; Virtual Machine; Virtualization; Security

I. INTRODUCTION

Cloud computing providers deliver applications via the internet, which are accessed from web browsers and desktop and mobile apps, while the business software and data are stored on servers at a remote location. Clouds are popular because they provide a simple, seamless approach to provisioning applications and information services. Network-based services, which appear to be provided by real server hardware, and are in fact served up by virtual hardware, simulated by software running on one or more real machines are often called cloud computing [1].

II. SERVICE PROVIDED BY CLOUD COMPUTING

Cloud services may be offered in various forms from the bottom layer to top layer

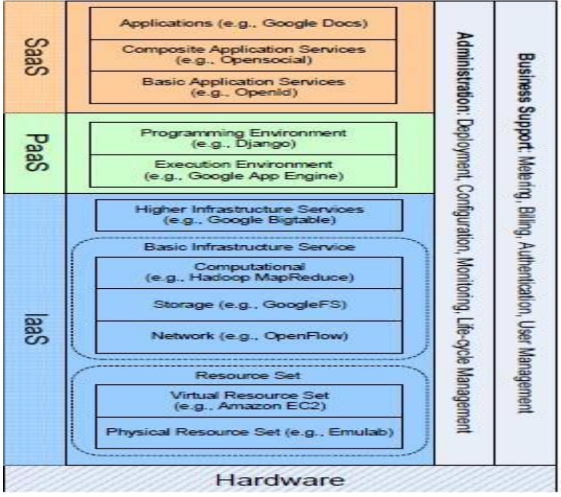
SaaS
Applications (e.g., Google Docs)
Composite Application Services (e.g., Opensocial)
Basic Application Services (e.g., Openid)
PaaS
Programming Environment (e.g., Django)
Execution Environment (e.g., Google App Engine)
IaaS
Higher Infrastructure Services (e.g., Google Bigtable)
Basic Infrastructure Service
Computational (e.g., Hadoop MapReduce)
Storage (e.g., GoogleFS)
Network (e.g., OpenFlow)
Resource Set
Virtual Resource Set (e.g., Amazon EC2)
Physical Resource Set (e.g., Emulab)
Administration: Deployment, Configuration, Monitoring, Life-cycle Management
Business Support: Metering, Billing, Authentication, User Management
Hardware

Fig 1: Architecture of Cloud Computing [2]

A. Software as a service (SaaS)

It is software delivery model in which software and its associated data hosted centrally and accessed by using client web browser over internet.

B. Platform as a service (PaaS)

Offer deployment of application without cost and complexity of buying and managing underlying hardware and software provisioning hosting capabilities.

C. Infrastructure as a service (IaaS)

Iaas means computer infrastructure. Virtualization environment. Iaas provides set of APIs –application programming interface. It allows management and other forms of interaction with the infrastructure by consumers.

III. DEPLOYMENT MODELS

Three model Public clouds, Private clouds, Hybrid clouds

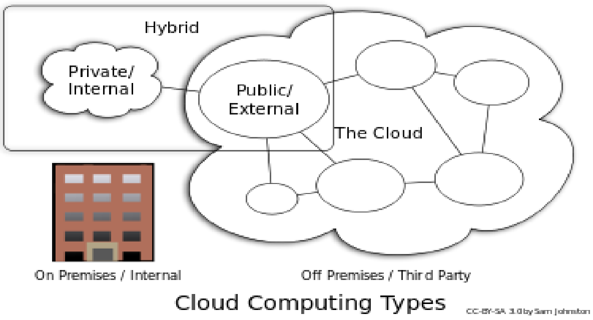

Fig. 2: Cloud computing types [1]

A. Private Cloud

Private cloud is cloud infrastructure operated solely for a single organization, whether managed internally or by a third-party and hosted internally or externally [1].

Example: Eucalyptus,Ubuntu Enterprise Cloud - UEC (powered by Eucalyptus) ,Amazon VPC (Virtual Private Cloud) ,VMware Cloud Infrastructure Suite ,Microsoft ECI data center

B. Public Cloud

A cloud is called a "public cloud" when the services are rendered over a network that is open for public use [1].

Example: Google App Engine, Microsoft Windows Azure, IBM Smart Cloud, Amazon EC2

C. Hybrid Cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models.[1]

Examples: Windows Azure (capable of Hybrid Cloud), VMware vCloud (Hybrid Cloud Services)

D. Community Cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns. [1]

Examples: Google Apps for Government, Microsoft Government Community Cloud

IV. CLOUD COMPUTING SECURITY THREATS

A. Data Breach

It is a security incident in which unauthorized user do copied, transmitted, sensitive, protected or confidential data. Vulnerabilities include Loss of Personally identifiable information (PII), Loss of Encryption keys, and Brute Force attack [3].

B. Account Or Service Traffic Hijacking

Attacker gain access to user's data. Vulnerabilities include Session Hijacking, SQL Injections, Cross-site scripting, Man in the middle attack, wrapping attack Problem, Malware injection attack, Social Engineering attack, Phishing attack [3].

C. Data Loss

Attacker gain access to Information and delete data. Vulnerabilities include Loss of Encryption keys, Cloud service termination, and Hardware or Software failure, Natural Disaster, Human Error [3].

D. Denial of Service [3][4]

Denial-of-service attacks are attacks meant to prevent users of a cloud service from being able to access their data or their applications. By forcing the victim cloud service to consume in ordinate amounts of finite system resources such as process or power, memory, disk space or network bandwidth, the attacker causes an intolerable system slowdown and leaves all of the legitimate service users confused and angry as to why the service isn't responding[3].

1) Vulnerabilities:

A. Zombie attack [7]

Through Internet, an attacker tries to flood the victim by sending requests from innocent hosts in the network. These types of hosts are called zombies. In the Cloud, the requests for Virtual Machines (VMs) are accessible by each user through the Internet. An attacker can flood the large number of requests via zombies. Such an attack interrupts the expected behavior of Cloud affecting availability of Cloud services [3].

B.HX-DOS attack

It is combination of HTTP and XML messages that are intentionally sent to flood and destroy the communication channel of the cloud service provider.

C. Detection of DDOS [3]

DIDS (Distributed Intrusion Detection System) Signature based, open source network analyzer, snort is proposed to generate logs.

Hidden Markova Model [3]

SQL server 2005 is used to collect all the details of all the clients and check the browsing behavior of the users by hidden Markova Model. If Anomaly is detected then it denies the access of the users.

Entropy [3]

Entropy is a measure of randomness. Each incoming request sessions' entropy is calculated and is compared to predefined value in a system if greater deviation is found then user request of that session is declared as anomalous.

Semantic rule based approach [3]

It is used to detect anomaly in cloud application layer. A deterministic finite automaton is used to represent different malicious characteristics.

Dempster Shafer Theory [3]

It is applied to detect DDOS threat in cloud environment. It is an approach for combining evidence in attack conditions.

E. Insecure Interfaces and API's [3]

It provide set of API to interact with cloud service Vulnerabilities include Malicious or unidentified access, API dependencies, limited monitoring/logging capabilities, inflexible access controls, anonymous access, reusable tokens/passwords and improper authorizations[3].

F. Malicious insiders [3]

A malicious insider threat that misuse access Vulnerabilities include Rogue Administrator, Exploit Weaknesses Introduced by Use of the Cloud, Using the Cloud to Conduct Nefarious Activity, Lack of transparency in management process[3].

G. Abuse of cloud services

It includes Use of cloud computing for criminal activities, Illegal activity by cloud service provider [3].

H. Insufficient Due Diligence

Without understanding cloud service provider environment user push application in cloud environment. Vulnerabilities include insufficient skills and knowledge [3].

I. Shared Technology vulnerabilities

Infra structure as service (Iaas) vendor delivers their services to users. Vulnerabilities include VM Hopping, VM Escape, VM Escape, Cross-VM side-channel attack [3].

V. RELATED WORK

Paper Title & Approach

1) An Analysis of Intrusion Detection System in Cloud Environment

Ambikavathi C , S.K.Srivatsa [5] defines Cloud computing being a distributed model, need of secure usage is a major issue. The goal of cloud IDS is to analyze events happening on the cloud network and identify attacks.

2) LiteGreen: Saving Energy in Networked Desktops Using Virtualization

Tathagata Das, Pradeep Padala, Venkata N. Padmanabhan, Ramachandran Ramjee, Kang G. Shin [6] define The basic idea is to virtualized the user's desktop computing environment, by encapsulating it in a virtual machine (VM), and then migrating it between the user's physical desktop machine and a VM server, depending on whether the desktop computing environment is actively used or idle.

3) A survey on security issues and solutions at different layers of Cloud computing

Chirag Modi,Dhiren Patel,Bhavesh Borisaniya,Avi Patel,Muttukrishnan Rajarajan[7] defines the factors affecting Cloud computing adoption, vulnerabilities and attacks, and identify relevant solution directives to strengthen security and privacy in the Cloud environment

4) Network Security Platform, Denial-of-Service [DoS] Prevention Techniques

McAfe 18-December-2013[8] defines an overview of the types of Denial-of-Service (DoS)/Distributed Denial-of-Service (DDoS) attacks that Network Security Platform can detect and to know the response action (s) that can be taken against each type of DoS/DDoS attack.

5) Security and Privacy in Cloud Computing

Zhifeng Xiao and Yang Xiao, Senior Member, IEEE [2] defines we have identified the most representative security/privacy attributes (e.g., confidentiality, integrity, availability, accountability, and privacy-preservability), as well as discussing the vulnerabilities, which may be exploited by adversaries in order to perform various attacks. Defense strategies and suggestions were discussed as well.

6) Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts

Lingyu Wang , Anyi Liu, Sushil Jajodia [11] proposed To defend against multi-step intrusions in high-speed networks, efficient algorithms are needed to correlate isolated alerts into attack scenarios ,it propose a compact representation for the result of alert correlation

VI. PROPOSED WORK

Following Figure Shows the design of architecture and steps involved in achieving customized virtual machine security analyzer based on attack graph that store in database.

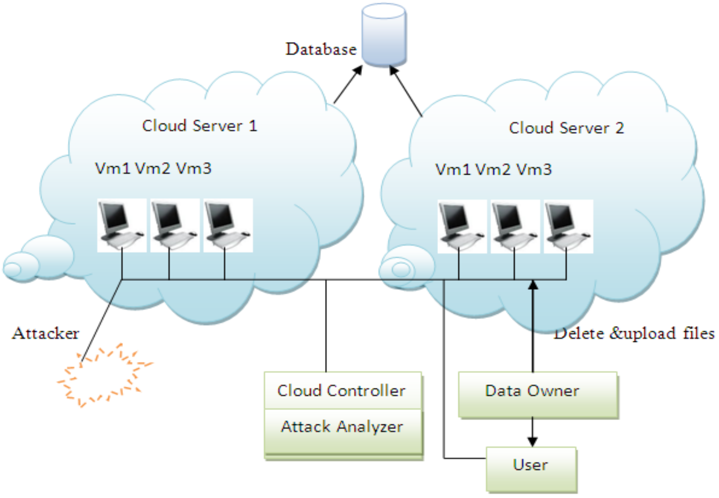

Fig. 3: Proposed Architecture

A. Sequence of Steps

Step 1. Create virtual machine on server (enter Name, Memory size, Threshold).
Step 2. Repeat step 1 for n virtual machine Active all virtual machine.
Step 3. Data owner upload the files.
Step 4. If file is null then display Threshold level Violated.
Step 5. If larger than display Virtual machine does not have enough space.
Step 6. Else file upload success
Step 7. Run Attacker Module, if A is new attack
Step 8. Then update a memory value in database, Check vulnerability, and stable, exploited.
Step 9. Run user module, request for file for access, generate secrete key (data owner issue file access information, file name, secrete key)
Step 10.if key is ok, file download.

B. Implementation Methodology

The Java programming language is Simple ,Architecture neutral, Object oriented, Portable, Distributed, High performance, Interpreted, Multithreaded, Robust for that we implement proposed architecture in java language.

C. Advantage of Proposed System Architecture

Now a days many people are using Cloud computing services, attacker also misuse the cloud service by always update with hacking tools. It review the concept of attack analyzer for cloud computing. It always beneficial for cloud service provider for providing better service to user.

VII. CONCLUSION

As we discussed before Cloud Computing now a days widely used. Threat must detect before it put its action in server or system. Various threat related cloud computing is reviewed in this paper. Attacker always updated with attacking tools to misuse the services

VIII. FUTURE WORK

We present framework for detect attacks in the distributed cloud computing environment. It utilizes the attack graph model that represented in database to conduct attack detection and prediction.

The proposed system shows how to detect accuracy and defeat victim exploitation phases of collaborative attacks. It defines the approach to analyze zombie explorative attacks comes in cloud environment. Attacker comes in many ways to cloud computing environment for that to improve the detection accuracy, need to investigated more in the future work. Implementation aspect we should implement with cloud simulator in future.

REFERENCES

[1] en.wikipedia.org/wiki/Cloud_computing

[2] Zhifeng Xiao and Yang Xiao, Senior Member, IEEE "Security and Privacy in Cloud Computing" IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 15, NO. 2, SECOND QUARTER 2013

[3] Harshal Mahajan, Dr.Nupur Giri "Threats to Cloud Computing Security" VESIT,International Technological Conference-2014 (I-TechCON),Jan.03- 04, 2014

[4] Muhammad Zakarya & Ayaz Ali Khan, "Cloud QoS, High Availability & Service Security Issues with Solutions", IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.7, July 2012

[5] Ambikavathi C , S.K.Srivatsa"Analysis of Intrusion Detection System in Cloud Environment" International Journal Of Research In Advance Technology In Engineering (IJRATE) Volume 1, Special Issue, October 2013

[6] Tathagata Das, Pradeep Padala, Venkata N. Padmanabhan, Ramachandran Ramjee, Kang G. Shin "LiteGreen: Saving Energy in Networked Desktops Using Virtualization" USENIX ATC, 2010

[7] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. & Rajarajan, M., "A survey of intrusion detection techniques in Cloud", Journal of Network and Computer Applications

[8] McAfe "Network Security Platform, Denial-of-Service [DoS] Prevention Techniques" 18-December-2013

[9] http://en.wikipedia.org/wiki/Cloud_computing_security

[10] http://earthnet.net/cloud.html#.UyQHdtKnCmg

[11] Lingyu Wang , Anyi Liu, Sushil Jajodia, Elsevier," Using attack graphs for correlating, hypothesizing, and predicting intrusion alerts" Computer Communications 29 (2006).