Implementation of Artificial Intelligence for IDS in Cloud Data Centres: Using intrusion detection techniques in Cloud

B.Rajani
Shri Jagdish Prasad Jhabarmal Tibrewala (JJT) University
Department of Computer Sci. & Engg
E-mail: rajani.badi@gmail.com

R.Suhasini
Shri Jagdish Prasad Jhabarmal Tibrewala (JJT) University
Department of Computer Sci. & Engg
E-mail: hasini.r04@gmail.com

E.V.N.Jyothi
Shri Jagdish Prasad Jhabarmal Tibrewala (JJT) University
Department of Computer Sci. & Engg
E-mail: jyothiendluri@gmail.com

Venkateshwarla Rama Raju,
Senior member, IEEE
(JNTUH Affiliation): Computer Science & Eng
CMR College of Eng & Technology (Autonomous)
Hyderabad, India
E-mail:drvrr@cmrcet.org

ABSTRACT

Cloud computing provides large scale computing resource to each customers. Cloud systems can be threatened by numerous attacks as cloud provides services to no trustworthy system. We survey different intrusions affecting availability, confidentiality and integrity of Cloud resources and services. Proposals incorporating Intrusion Detection Systems (IDS) in Cloud are examined. We recommend IDS positioning in Cloud environment to achieve desired security in the next generation networks. As the speedy usage of personal computer system and computer network in business organization and government organization are Bringing up day by day, the computer network is the mass medium over which attacks are put together. It comes final result in completely destroyed, unauthorized utilization and modifies in private data and demeans the reliability of computer network. To providing protection in computer network Artificial intelligence has latterly contributed intrusion detection system. This paper presents intrusion detection system which automatically updates the suspicious activity of cloud users therefore whenever new user try to access the data or try to use cloud it will compare with the log database which is present at administrator side.

***KEYWORDS**: Cloud Computing; Cloud Security; Intrusion Detection System; Signature; Anomaly.*

INTRODUCTION

As Cloud Computing is the rapidly growing field of IT [1]. Cloud Computing is defined as an Internet based computing in which virtually shared servers that is data centers provide software, platform, infrastructure, policies and many resources [2]. A cloud data center can be defined from a different perspectives, and the most popular are categorized by IaaS, PaaS, and SaaS proposed by the NIST [3].

Cloud computing aims to provide convenient, on-demand, network access to a shared pool of configurable computing resources (e.g. networks, servers, storage, applications, and ser-vices), which can be rapidly provisioned and released with minimal management effort or service provider interactions (Mell and Grance, 2011).

Cloud provides services in various forms: Software as a Service-SaaS (e.g. Google apps, 2011), Plat-form as a Service-PaaS (e.g. Google app engine (2011)), Micro-soft's Azure (Azure services platform, 2011)) and Infrastructure as Service-IaaS (e.g. Amazon web services, 2011(AWS); Eucalyptus, 2011; Open Nebula
(Opennebula, 2011)).

As Cloud services are provisioned through the Internet; security and privacy of Cloud services are key issues to be looked upon. International Data Corporation (IDC) survey (Gens, 2009) showed that security is the greatest challenge of Cloud computing. The recent Cloud computing security white paper by Lockheed Martin Cyber Security division (Martin, 2010) shows that the major security concern after data security is intrusion detection and prevention in Cloud infrastructures. Cloud infrastructure makes use of virtualization techniques,

The author wish to thank the Secretary & Correspondent of CMRCET (Autonomous) Mr. Ch. Gopal Reddy. Thanks also for support of Department of Computer Science & Engineering (CSE).

integrated technologies and runs through standard Internet protocols. These may attract intruders due to many vulnerabilities involved in it.

Cloud computing also suffers from various traditional attacks such as IP spoofing, Address Resolution Protocol spoofing, Routing Information Protocol attack, DNS poisoning, Flooding, Denial of Service (DoS), Distributed Denial of Service (DDoS), etc. For e.g. DoS attack on the underlying Amazon Cloud infrastructure caused BitBucket.org, a site hosted on AWS to remain unavailable for few hours (Brooks, 2009). Computing-cost using current crypto-graphic techniques cannot be overlooked for Cloud (Chen and Sion, 2010). Firewall can be a good option to prevent outside attacks but does not work for insider attacks. Efficient intrusion detection systems (IDS) should be incorporated in Cloud infrastructure to mitigate these attacks.

IDS could be software, hardware or a combination of both. It captures the data from the network under examination and notify to the network manager by mailing or logging the intrusion event.

LITERATURE REVIEW

Over the past 3 decades, there has been a large increase in the number of real problems correlated to; Fault detection (Monitoring), Safety of multipart systems (Rockets, Airplanes, Cars), and Monitoring physiological variables in patient healthcare. More recently, anomaly detection in information technology settings is becoming vitally important and gaining momentum. This is due to the occurrence of exploding information and the model of cloud computing which has formed a demand for huge number of servers known as data centers. A data center is a very intricate operating environment and its smooth operation is dangerous to keep enterprise businesses running powerfully. While the complication and size of the data centers is constantly increasing, methods to monitor the numerous processes and metrics are still relatively undeveloped. Unnecessary to say, monitoring using dependable methods that are light weight, and scale with increasing number of servers and number of metrics is necessary for optimal and economical operations. Detection of immediate or fast changes, untimely prediction of imminent anomalies, and detection of anomalies in a relatively stable system typically constitute the taxonomy of change-point detection techniques [8]. IDS is split into two categories: misuse detection systems and anomaly detection systems [9]. Misuse detection is used to recognize intrusions that match known attack scenarios. However, anomaly detection is an attempt to explore for malicious behavior that deviates from recognized nor-mal patterns. In order to detect the intrusion, different approaches have been developed and proposed over the last decade. In the early stage, rule based expert systems and statistical approaches are two typical ways to detect intrusion. A rule-based expert IDS can detect some well-known intrusions with high detection rate, but it is difficult to detect new intrusions, and its signature database needs to be updated manually and frequently. This paper advances anomaly detection schemes by considering ranking of anomalies based on severity in conjunction with flagging anomalies.

INTRUSIONS TO CLOUD SYSTEMS

There are several common intrusions affecting availability, confidentiality and integrity of Cloud resources and services.

I. Insider attack

Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to others (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2) (Slaviero, 2009).

II. Flooding attack

In this attack, attacker tries to flood victim by sending huge number of packets from innocent host (zombie) in network. Packets can be of type TCP, UDP, ICMP or a mix of them. This kind of attack may be possible due to illegitimate network connections.

In case of Cloud, the requests for VMs are accessible by anyone through Internet, which may cause DoS (or DDoS) attack via zombies. Flooding attack affects the service's availability to authorized user. By attacking a single server providing a certain service, attacker can cause a loss of availability of the intended service. Such an attack is called direct DoS attack. If the server's hardware resources are completely exhausted by processing the flood requests, the other service instances on the same hardware machine are no longer able to perform their intended tasks. Such type of attack is called indirect DoS attack.

Flooding attack may raise the usage bills drastically as the Cloud would not be able to distinguish between the normal usage and fake usage.

III. User to root attacks

Here, an attacker gets an access to legitimate user's account by sniffing password. This makes him/her able to exploit vulnerabil-ities for gaining root level access to system. For example, Buffer overflows are used to generate root shells from a process running as root. It occurs when application program code overfills static buffer. The mechanisms used to secure the authentication process are a frequent target. There are no universal standard security mechanisms that can be used to prevent security risks like weak password recovery workflows, phishing attacks, keyloggers, etc.

In case of Cloud, attacker acquires access to valid user's instances which enables him/her for gaining root level access to VMs or host.

IV. Port scanning

Port scanning provides list of open ports, closed ports and filtered ports. Through port scanning, attackers can find open ports and attack on services running on these ports. Network related details such as IP address, MAC address, router, gateway filtering, firewall rules, etc. can be known through this attack. Various port scanning techniques are TCP scanning, UDP scan-ning, SYN scanning, FIN scanning, ACK scanning, Window scan-ning etc. In Cloud scenario, attacker can attack offered services through port scanning (by discovering open ports upon which these services are provided).

V. Attacks on virtual machine (VM) or hypervisor

By compromising the lower layer hypervisor, attacker can gain control over installed VMs. For e.g. BLUEPILL (Rutkowska, 2006), SubVir (King et al., 2006) and DKSM (Bahram et al., 2010) are some well-known attacks on virtual layer. Through these attacks, hackers can be able to compromise installed-hypervisor to gain control over the host.

New vulnerabilities, such as zero-day vulnerability, are found in Virtual Machines (VMs) (NIST: National vulnerability database, 2011) that attract an attacker to gain access to hypervisor or other installed VMs. Zero-day exploits are used by attackers before the developer of the target software knows about the vulnerability. A zero-day vulnerability was exploited in the HyperVM virtuali-zation application which resulted in destruction of many virtual server based websites (Goodin, 2009).

4 SYSTEM FLOW

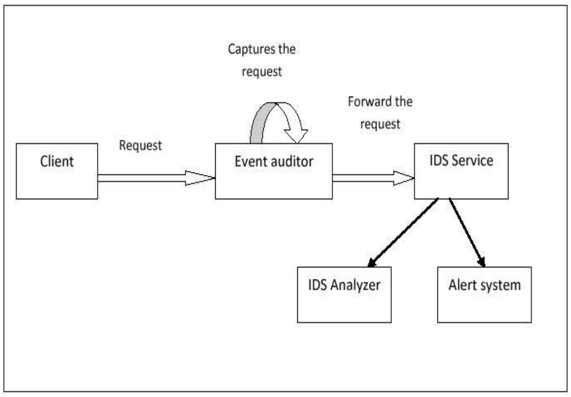


Figure 1: Client request with proposed system

The Intrusion Detection Service (IDS) [8] service enhances a clouds protection level by providing two methods of intrusion detection. First approach is performance approach which orders how recent user actions are compared to the normal behaviour. The second approach is information approach that marks cognized trails resulted by attacks or some sequences of actions from the user who represents an attack. The inspected data is sent to the IDS service core, which examines the conduct by using artificial intelligence to find deflections. This has two subsystems namely analyzer system and alert system. The analyzer uses the profile history database to find out the distance within a distinctive user behavior and the suspicious behavior and conveys this to the IDS service. The rules analyzer obtains audit packages and finds out if a rule in the database is worn out. It delivers the result to the IDS service core. With such responses, the IDS find out the intruder that the action comprises an attack and alarms the other nodes if the suspicious behaviour is high. This subsystem will work when intrusion is detected. If any node among the cloud system is affected by intrusion then this alert system will alert the remaining nodes about the intrusion.

The storage service is a database system which contains two types of services namely information based service and performance based service. Whenever a node gets requests or responses, the analyzer system compares the node information in the storage service. This paper used audit information from a log system as well the communication system to evaluate the information based system. The created a series of rules to illustrate security policies that the IDS should monitor. The information service is nothing but set of rules which is formed from previous attacks.

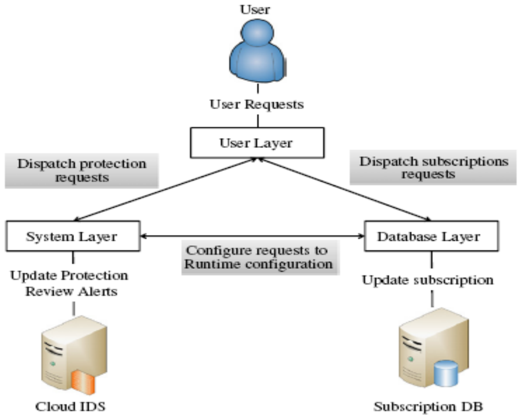

User
User Requests
User Layer
Dispatch protection requests
Dispatch subscriptions requests
System Layer
Configure requests to Runtime configuration
Database Layer
Update Protection Review Alerts
Update subscription
Cloud IDS
Subscription DB

Fig 2.Intrusion detection as a service in Cloud.

The system architecture consists of intrusion detection, alert clustering, threshold check, intrusion response and blocking and cooperative agent. In case of intrusion detection, it drops attacker packet, then sends alert message about the attack detected by itself to other region. Alert clustering module collects alert produced by other regions. The decision about alert (whether it is true or false) is identified after calculating severity of collected alerts. This approach is suitable for preventing Cloud system from single point of failure caused by DDoS attack.

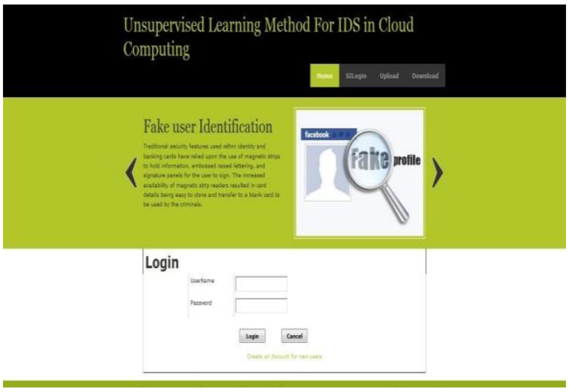
Dastjerdi and Bakar (2009) proposed scalable, flexible and cost effective method to detect intrusion for Cloud applications regardless of their locations using mobile agent. This method aims for protecting VMs that are outside the organization. Mobile agent collects evi-dences of an attack from all the attacked VM for further analysis and auditing. This approach is used to detect intrusion in VM migrated outside the organization. However, it produces more network load.

Ram (2012) proposed mutual agent based approach to detect DDoS attack in Cloud computing. In this approach, IDS module is deployed in each Cloud region, as presented by Lo et al. (2008). If any region finds intrusion, mutual agent at that region notifies other regions. Each region calculates severity of alerts generated from other regions. If new attack is found after calculating severity of intrusion, new blocking rule is added into block table at each region. In such a way, DDoS attack is detected in whole Cloud by using mutual cooperation among Cloud regions. For intrusion detection, Snort is used in this approach. Therefore, known attacks in network can be detected. However, it cannot detect unknown attack. Also, it requires high computation cost for exchanging alerts.

5 RESULTS AND DISCUSSIONS

5.1 I. Login Page:

In login page we provide userid and password so that any user who is an authenticated person is able to login in the system to enjoy the environment provided by the cloud for communication. The following screen shot gives the complete idea about the login page.


Unsupervised Learning Method For IDS in Cloud Computing

Fake user Identification

Traditional security features used within identity and banking cards have relied upon the use of magnetic strips to hold information, embossed raised lettering, and signature panels for the user to sign. The increased availability of magnetic strip readers resulted in card details being easy to clone and transfer to a blank card to be used by the criminals.

Login

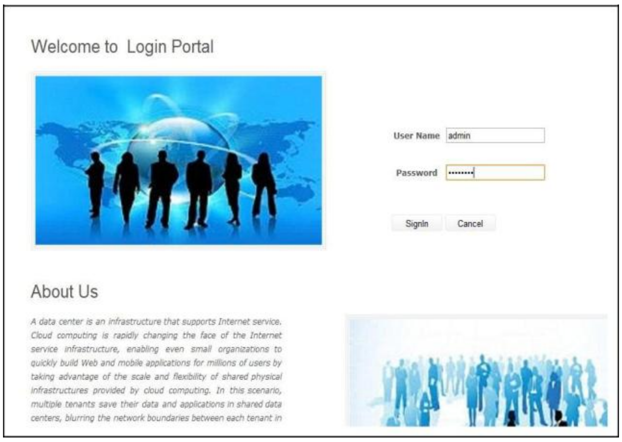
UserName

Password

Fig 3. Login page for end users

For the end users it is the easiest way to login with the cloud communication. There is link provided for the new users which are not registered with the cloud to register themselves with the cloud environment. After the registration of new user the request of registration is sent directly to the admin for activation of the user. The admin have to check the documents of new registered user physically. After verifying the documents the admin decide the activation of new user. Only after that the user is able to login.

II. Admin Login Page:


Welcome to Login Portal

User Name admin

Password ••••••••

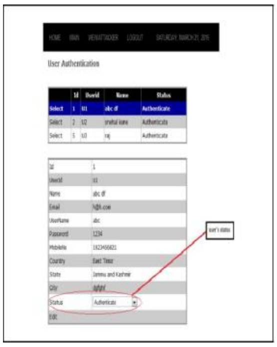
About Us

A data center is an infrastructure that supports Internet service. Cloud computing is rapidly changing the face of the Internet service infrastructure, enabling even small organizations to quickly build Web and mobile applications for millions of users by taking advantage of the scale and flexibility of shared physical infrastructures provided by cloud computing. In this scenario, multiple tenants save their data and applications in shared data centers, blurring the network boundaries between each tenant in

Fig 4: Admin login page

In admin login we provide the admin with some functions like main, view attacker and logout. Main contains two services user authentication and log maintenance. In user authentication admin would check the log and packet data of particular user and then provide the authentication to that user. View attacker provides the attackers view that make the attack on system.

III. User Authentication and Log Monitoring



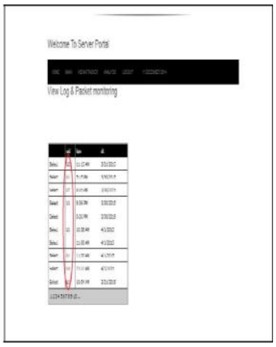
HOME MAIN VIEWATTACKER LOGOUT SATURDAY, MARCH 21, 2015

User Authentication

	Id	UserId	Name	Status
Select	1	U1	abc df	Authenticate
Select	2	U2	snehal kene	Authenticate
Select	5	U3	raj	Authenticate

Id	1
UserId	U1
Name	abc df
Email	h@h.com
UserName	abc
Password	1234
MobileNo	1823456821
Country	East Timor
State	Jammu and Kashmir
City	dgfdgf
Status	Authenticate
Edit	

Fig 5: User Authentication



Welcome To Server Portal

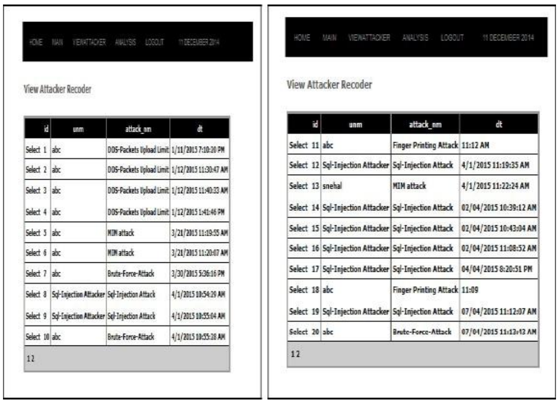
View Log & Packet monitoring

Fig 6: Log Monitoring and Packet Monitoring

In admin login page we provide user id and password so that any user who try to login to the system, an admin will analyze the user. Whether the user is authorized or not, if the user is genuine then admin change his states to authenticate otherwise keep it as new.

System provide log monitoring in which we keep the log maintenance of user. System provide unique id (such as U1, U2, and so on as shown in fig) to each user so that no one can get or hack the user log. Log and packet monitoring page contain unique user id, login time, date and log out time and the file which is uploaded and downloaded by the user.

IV. View Attacker Record:



HOME MAIN VIEWATTACKER ANALYSIS LOGOUT 11 DECEMBER 2014

View Attacker Recoder

	id	unm	attack_nm	dt
Select	1	abc	DOS-Packets Upload Limit	1/11/2015 7:10:20 PM
Select	2	abc	DOS-Packets Upload Limit	1/12/2015 11:30:47 AM
Select	3	abc	DOS-Packets Upload Limit	1/12/2015 11:40:33 AM
Select	4	abc	DOS-Packets Upload Limit	1/12/2015 1:41:46 PM
Select	5	abc	MIM attack	3/21/2015 11:19:55 AM
Select	6	abc	MIM attack	3/21/2015 11:20:07 AM
Select	7	abc	Brute-Force-Attack	3/30/2015 5:36:16 PM
Select	8	Sql-Injection Attacker	Sql-Injection Attack	4/1/2015 10:54:29 AM
Select	9	Sql-Injection Attacker	Sql-Injection Attack	4/1/2015 10:55:04 AM
Select	10	abc	Brute-Force-Attack	4/1/2015 10:55:28 AM
1 2				

HOME MAIN VIEWATTACKER ANALYSIS LOGOUT 11 DECEMBER 2014

View Attacker Recoder

	id	unm	attack_nm	dt
Select	11	abc	Finger Printing Attack	11:12 AM
Select	12	Sql-Injection Attacker	Sql-Injection Attack	4/1/2015 11:19:35 AM
Select	13	snehal	MIM attack	4/1/2015 11:22:24 AM
Select	14	Sql-Injection Attacker	Sql-Injection Attack	02/04/2015 10:39:12 AM
Select	15	Sql-Injection Attacker	Sql-Injection Attack	02/04/2015 10:43:04 AM
Select	16	Sql-Injection Attacker	Sql-Injection Attack	02/04/2015 11:08:52 AM
Select	17	Sql-Injection Attacker	Sql-Injection Attack	04/04/2015 8:20:51 PM
Select	18	abc	Finger Printing Attack	11:09
Select	19	Sql-Injection Attacker	Sql-Injection Attack	07/04/2015 11:12:07 AM
Select	20	abc	Brute-Force-Attack	07/04/2015 11:13:13 AM
1 2				

Fig 7: Attacker Record

The admin side shows the attacker view in which admin keep the record of previously occurred attacks. The proposed system detect some attacks like

DDos, Man-in-middle attack, fingerprinting attack, SQL injection and brute force attack . The attacker record contain user name, user id, attack type and date of occurrence.

CONCLUSION

As data centres grow in size and complexity, automated techniques to detect anomalous behavior in the data centres become important. We presented automated intrusion detection technique compares current user activities against previously loaded logs of users. This paper emphasized the usage of alternative options to incorporate intrusion detection into Cloud and explored locations in Cloud where IDS can be positioned for efficient detection. The adoption of soft computing techniques in IDS can improve the security. We have developed secure cloud storage system architecture and have shown that the system has several superior characteristics such as constant encryption and decryption of data. From our experiments, we observe that both encryption and decryption computations are efficient on the client side as well as server side.

REFERENCES

[1] Snehal G. Kene, Deepti P. Theng "A Review on Intrusion Detection Techniques for Cloud Computing and Security Challenges", IEEE sponsored 2nd international conference on electronics and communication systems icecs „2015.

[2] Shefali Singh, Krati Saxena, Zubair Khan "Intrusion Detection Based On Artificial Intelligence Techniques", International Conference Of Advance Research And Innovation (Icari-2014).

[3] Zhen Chen, Wenyu Dong, Hang Li, Peng Zhang, Xinming Chen, And Junwei Cao"Collaborative Network Security In Multi-Tenant Data Center For Cloud Computing", Tsinghua Science AndTechnology 1, February 2014.

[4] P. Praveen Kumar, K. Bhaskar Naik, "A Survey on Cloud Based Intrusion Detection System" International Journal of Software and Web Sciences (IJSWS) 2013.

[5] R. Quick, “5 reasons enterprises are frightened of the cloud”, http://thenextweb.com/insider/2013/09/11/5 reasons enterprises- are-frightened-of-the-cloud, 2013.

[6] R. Bace, P. Mell, “Intrusion Detection Systems”, National Institute of Standards and Technology (NIST), Technical Report, 800-31, 2001.

[7] U. Oktay, O. K. Sahingoz, “Proxy Network Intrusion Detection System for Cloud Computing”, ISBN: 978-1-4673-5613-8, 2013, IEEE, pp. 98-104.

[8] Krishnamurthy Viswanathan, Lakshminarayan Choudur, Vanish Talwar, Chengwei Wang*, Greg Macdonald, Wade Satterfield, “Ranking Anomalies In Data Centers” 2012 IEEE.

[9] A. Haeberlen,“ An Efficient Intrusion Detection Model Based on Fast Inductive Learning,” Sixth International Conference on Machine Learning and Cybernetics, Hong Kong, 19-22 August 2007. Tavel, P. 2007.

[10] Sanjay Ram M, Velmurugan N, Thirukumaran S, “Effective Analysis of Cloud Based Intrusion Detection System” International Journal of Computer Applications & Information Technology Vol. I, Issue II, September, 2012.

[11] Theng, D.; Hande, K.N., "VM Management for Cross-Cloud Computing Environment," Communication Systems and Network Technologies (CSNT), 2012 International Conference on , vol., no., pp.731,735, 11-13 May 2012.

[12] Azure services platform, Website, /http://www.microsoft.com/azureS; 2011.

[13] Amazon web services, Website, /http://aws.amazon.comS; 2011.

[14] Arshad J, Townend P, Xu J. An abstract model for integrated intrusion detection and severity analysis for clouds. International Journal of Cloud Applications and Computing 2011;1(1):1–17.