ISSN:2320-0790

An International Journal of Advanced Computer Technology

Virtual Machine Introspection

S C Rachana[1], Dr. H S Guruprasad[2]
[1] PG Scholar, Dept. of ISE, BMSCE, Bangalore
[2] Professor and Head, Dept. of CSE, BMSCE, Bangalore

Abstract: Cloud computing is an Internet-based computing solution which provides the resources in an effective manner. A very serious issue in cloud computing is security which is a major obstacle for the adoption of cloud. The most important threats of cloud computing are Multitenancy, Availability, Loss of control, Loss of Data, outside attacks, DOS attacks, malicious insiders, etc. Among many security issues in cloud, the Virtual Machine Security is one of the very serious issues. Thus, monitoring of virtual machine is essential. The paper proposes a Virtual Network Introspection [VMI] System to secure the Virtual machines from Distributed Denial of Service [DDOS] and Zombie attacks.

Keywords: Virtual Machine (VM), Virtual Machine Introspection (VMI), Intrusion Detection System (IDS), Virtual Machine Monitor (VMM), Hypervisor, Infrastructure-as-a-Service (IaaS), Botnet.

I INTRODUCTION

Cloud computing delivers the software (IT) as a service. In the cloud, many computers are configured to work together where the resources are allocated on demand. Cloud computing allows the customers to access resources through the internet from anywhere at any time without thinking about the management and maintenance issues of the resources. Resources of cloud computing can be provided dynamically. One of the important attribute of cloud computing is scalability which can be achieved through server virtualization. The best example of Cloud computing is Google Apps. The services can be accessed using Google Apps through the browser over the Internet. Cloud computing is cheaper than any other computing models. In cloud, the maintenance cost is zero as the clients are free from maintenance and management issues. Thus, cloud computing is also called “Utility Computing”or “IT on demand”.

Security issues in cloud are a major obstacle for its adoption. Security issues can be grouped into sensitive data access, data segregation, privacy, bug exploitation, recovery, accountability, malicious insiders, management console security, account control, and multi-tenancy issues. There are many other challenges and risks in cloud computing that leads to loss of security which has to be taken care in order to build trust in customers about cloud computing technology. The main focus of the paper is on Virtual Machine Security among many other issues.

A virtual machine mimics the physical machine as software. Many operating systems and software’s can be installed in virtual machine. Virtual machines are accompanied with the virtualization layer called hypervisor which runs on client or server operating system. Virtual machine attacks include VM-to-VM attacks, Hypervisor attacks, Denial-Of-Service attacks, Isolation breakage, Remote management vulnerabilities etc. Thus, virtual machine monitors are used to monitor the virtual machines. The existing popular virtual machine monitors are Xen, VMware ESX Server etc.

VMI is another technique used for monitoring the state of virtual machines in real time. The focus of the paper is on the DOS/DDOS attacks to virtual machines. DOS attacks leads to delayed response for a request, no response to the legitimate traffic and resource management problems. Thus, DOS/DDOS attacks overload the server. As a solution to mitigate the DOS/DDOS attacks,architecture of VMI is proposed in this paper.

The paper gives the related work in the section II. The proposed VMI is being explained along with architecture and flowchart in the section III. The implementation details of the proposed architecture are given in section IV. The proposed VMI is experimented and the results of it are presented in the section V. The conclusion for the paper is given in the section VI.

II RELATED WORK

Akhil Behl [1] describes very common and critical security challenges. There are many security threats which come from inside or outside of cloud providers/consumers environment is classified into insider threats, outsider malicious attacks, data loss, issues related to multi-tenancy, loss of control, service disruption. The security feature in a cloud environment has to be adopted to protect cloud virtual infrastructure. Availability and Performance, outside attacks, Malicious Insiders, Multitenancy, Loss of Control, and Service Disruptions are the kind of attacks which has to be mainly addressed. FaraziSabhai. [2] describes the well-known Gartner's seven security issues. The basic security issues such as Data leakage, DoS (Denial of Service) attacks are addressed. Some of the solutions for cloud security such as Access Control, Incident Counter measure and Response are proposed.Tal Garfinkelet. al. [3] introduces IDS for virtual machines and explains VMM and VMI. The paper proposes architecture for Virtual Machine Monitor implementation. The Virtual Machine Introspection (VMI) system possesses three properties such as Isolation, Inspection, and Interposition. The prototype is experimented for security and performance overhead and it has the ability to detect real time attacks with high performance. Anthony Roberts et. al. [4] proposes a framework called Pathogen for analysis and monitoring of real time systems which use VMI for monitoring a system without the use of local agents. Pathogen is used to monitor multiple Virtual Machines within an organization and it creates a light weight Virtual Machine Introspection and fills in the semantic gap. Pathogen is implemented and analyzed for the results.

Anaset. al. [5] describes two ways to implement Virtual Machine Introspection (VMI) tools and techniques. A proposed system is implemented using one of the two ways and its system design is given. The system involves Log File, ZFS File System, Backup Spooler, Virtual Machine recovery etc. The system is tested for its behavior. Ying Wang et. al. [6] gives the importance of VM Detector along with some related work. A VM Detector design is proposed to detect hidden process by multi-view comparison and its goals are mentioned. A VM Detector is used to obtain views of kernel level, VMM level and also detects hidden suspicious process. The proposed approach is implemented and experimented for testing the function and performance.Li Ruanet. al. [7] introduces Cloud Distributed Virtual Machine Monitor (Cloud DVMM) by comparing with some existing VMM's. The theoretical model of DVMM, its attributes and operations are specified briefly. The system architecture of DVMM is given with brief explanation and DVMM is implemented, evaluated for analysis. AmaniS et. al. [8] describes the key security problems in IaaS environment. To overcome the security challenges in IaaS, a high level CloudSec architecture is proposed which has VMI Layer with the two components such as Front-end and Back-end component. CloudSec is implemented using VMSafe API's on a VMware hypervisor.

III PROPOSED SYSTEM

The proposed system introduces the VMI architecture as depicted in Figure.1.The VMI effectively detects the DOS/DDOS attacks for the virtual machines based on predefined threshold access count values. The architecture consists of three servers such as Gateway Server and two cloud servers. The virtual applications are running in two cloud servers along with separate VMI agent running in these two servers. The application is accessible to two different types of users such as admin and end users. The user's requests are received by the cloud servers via the gateway server. The network controller consists of various VM profiles and controls various network activities.Admin can login to monitor the status of the machines connected, state of servers and applications, and admin can also change the password.End user can access any application on the cloud server using a common user interface. This architecture comprises of three modules such as VMI Agent, Attack Analyzer, and Network Controller.

The VMI agentmonitors the connection activities in the network, alerts the attack analyzer about the threats for further detection. Each VMI agent running on two cloud servers is assigned a predefined threshold access value. When cloud server receives a request by an IP address the agent obtains the details of that IP addresses from the log file and increments its count. If that particular IP has accessed the applications more than VMI agent's threshold access count value then, an alert notification is sent to the attack analyzer module as depicted in Figure.2.

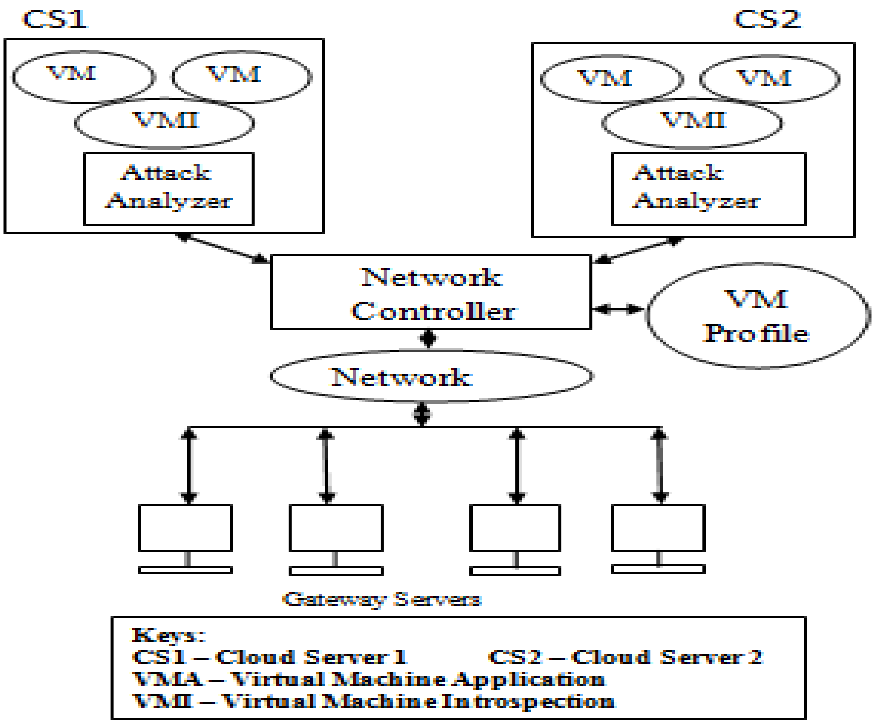


Figure.1. Virtual Machine Introspection Architecture

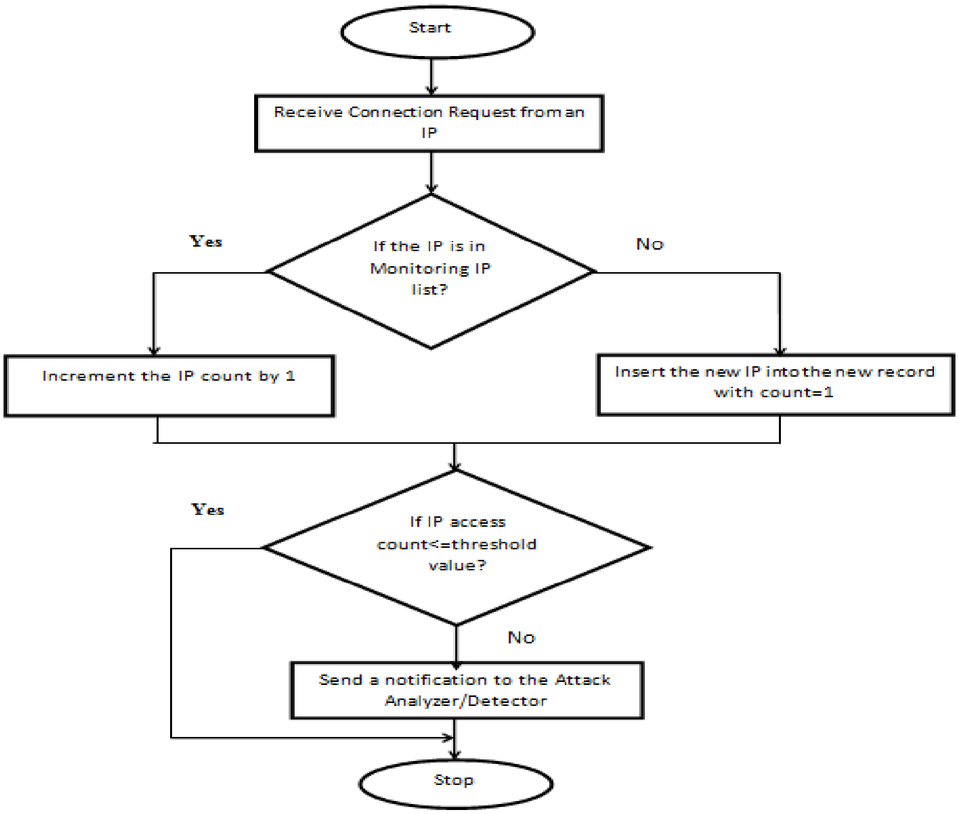

Start
Receive Connection Request from an IP
If the IP is in Monitoring IP list?
Yes
No
Increment the IP count by 1
Insert the new IP into the new record with count=1
If IP access count<=threshold value?
Yes
No
Send a notification to the Attack Analyzer/Detector
Stop

Figure.2.Flowchart for VMI agent

The Attack analyzer receives the IP address from VMI agent and monitors that IP for further analysis. If user from that particular IP accesses more than the threshold access count value of the attack analyzer, then the IP is suspected to be an attacker. Thus, the IP is sent to the scenario attacker present within attack analyzer as depicted in Figure.3.

The scenario attacker will check in its databases such as local_db, global_db for the suspected IP address. If the IP is found in any of the databases to be misbehaved then it is being displayed to the admin. If that IP address is not found in the two databases, then it is being added to the network analyzer database (nw_analyzer_db). A notification is given to the admin by the scenario attacker that the IP has misbehaved and is being blocked from further access.

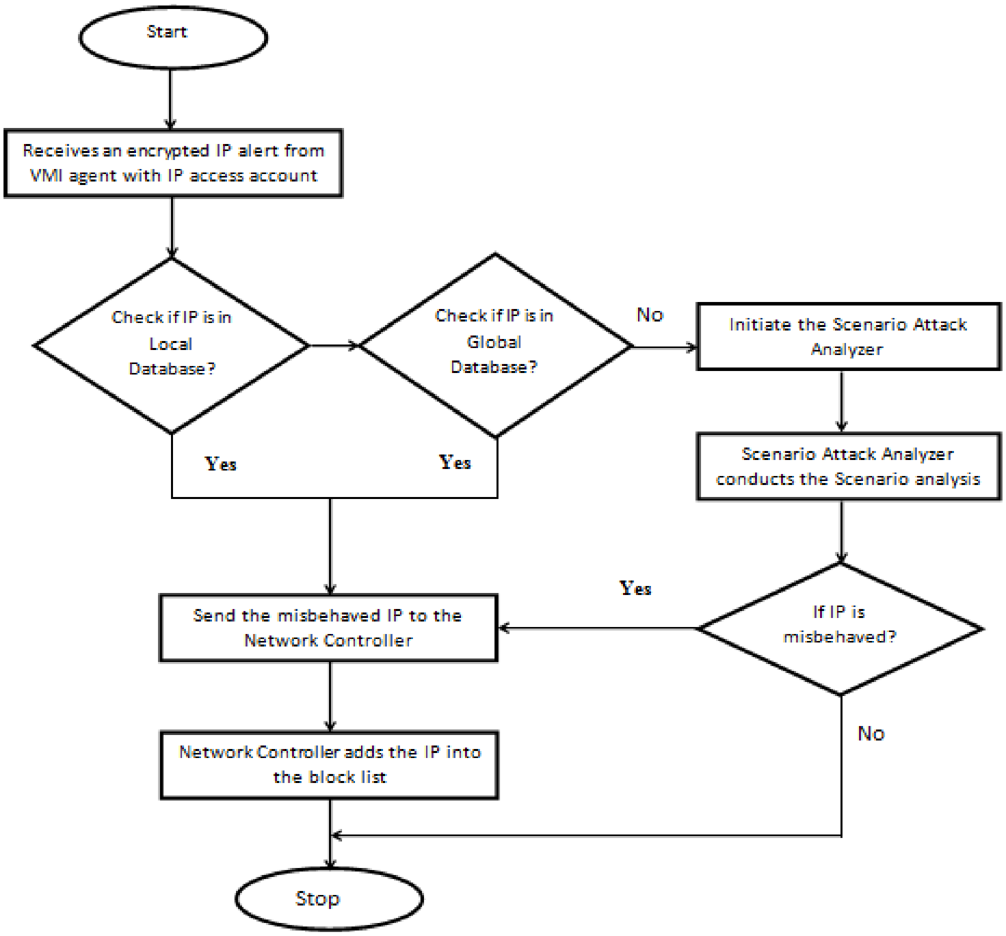

Start
Receives an encrypted IP alert from VMI agent with IP access account
Check if IP is in Local Database?
Check if IP is in Global Database?
No
Initiate the Scenario Attack Analyzer
Scenario Attack Analyzer conducts the Scenario analysis
Yes
Yes
Yes
Send the misbehaved IP to the Network Controller
If IP is misbehaved?
No
Network Controller adds the IP into the block list
Stop

Figure.3. Flowchart for Attack Analyzer

The Network controller collects the network information such as the number of the devices connected, status of each VM and their connections etc. and stores it in VM profiles. Various VM profile records are stored in Network Controller database. As depicted in Figure.3,VMI agent sends an alert in the form of IP address to the Attack Analyzer. Attack analyzer checks for the IP address in the local and global database. If IP is found, then it is added to the Network Controller's VM profiles.If the IP is not found in the two databases, then scenario analysis is initiated and the suspected IP is sent to the Network Controller.

IV IMPLEMENTATION

The proposed architecture is implemented using Java platform. The three modulesdiscussed in section III has been deployed on a single Windows machine and access to the sample applications present on this machine is being granted to the users connected to the network. The end users can access the cloud server applications with the aid of Wi-Fi hotspot.

Virtual Machine Introspection [VMI] agent:

VMI agent monitors the users in the network by obtaining the users information from the log file in a given timer value. Another timer is used during which this agent must detect the IP address which has accessed more than the VMI agents threshold access count value. If the agent suspects any IP address that has crossed the threshold, then this IP is obtained using DAO [Data Access Object] and stored into the database table usingResultSet.getObject(). This IP address is encrypted and sent to the Attack Analyzer as a threat notification. The encryption is achieved using Advanced Encryption Standard [AES] algorithm. This Algorithm is implemented using encrypt(), decrypt() and generatekey() methods of Java.

Attack Analyzer/Detector:

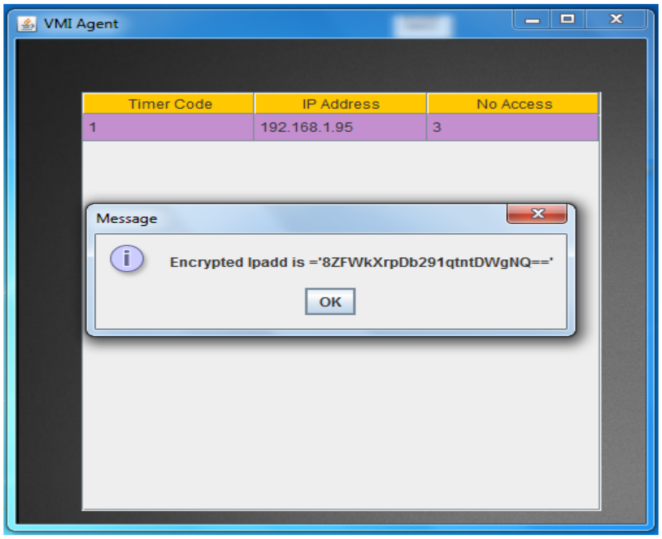
The encrypted form of IP address is received and decrypted using decrypt() method. The Attack analyzer checks if the decrypted IP is in local_db or global_db by calling a method Network_DAO.checkBlockIp() and Resultset(). Then, the attack analyzer obtains the IP using Network_DAO()and checkAccess() which is used to check the access count of the IP. If the access limit of the IP is crossed, then it is added into the block IP table using addObject() and is sent to network controller using updateBlockIp().

V EXPERIMENTS AND RESULTS

In this paper, a prototype system of VMI is designed and implemented using Java. The experiment is conducted to protect VM's from DOS/DDOS attacks. The experimental environment consists of three PC's among which one is gateway server and other two cloud servers. The Web Server used is the Tomcat and Database Server used is MySql. The three PC's are connected together using Wi-Fi Hotspot. The proposed system provides a common user interface for all the users using SQLyog 5.19. Java program runs in Eclipse IDE.

VMI agent:

VMI agent detection is displayed in a window which shows the Timer Code, IP address which is accessing the virtual applications and the access count of the IP address. In Figure.4, the IP 192.168.1.95 has accessed the virtual application more than VMI agent's threshold access count value. Therefore, that particular IP is encrypted and sent to Attack Analyzer as an alert notification which is as shown in a sub window in Figure.4



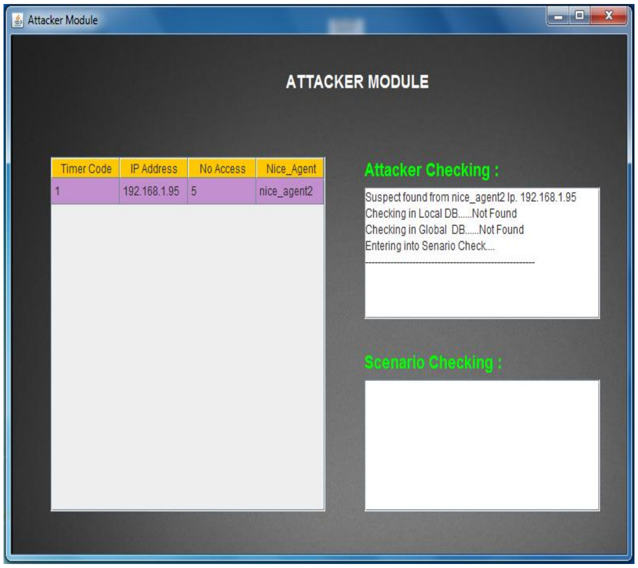
Timer Code	IP Address	No Access
1	192.168.1.95	3

Encrypted Ipadd is ='8ZFWkXrpDb291qtntDWgNQ=='

Figure.4. VMI agent sends the suspected IP in the encrypted form to Attack Analyzer

Attack Analyzer:

The Attack analyzer decrypts the received alert to obtain the IP and monitors the IP which is received as an alert by the VMI agent.The Attack Analyzer then checks for that IP in Local_db, Global_db as in Figure.5.

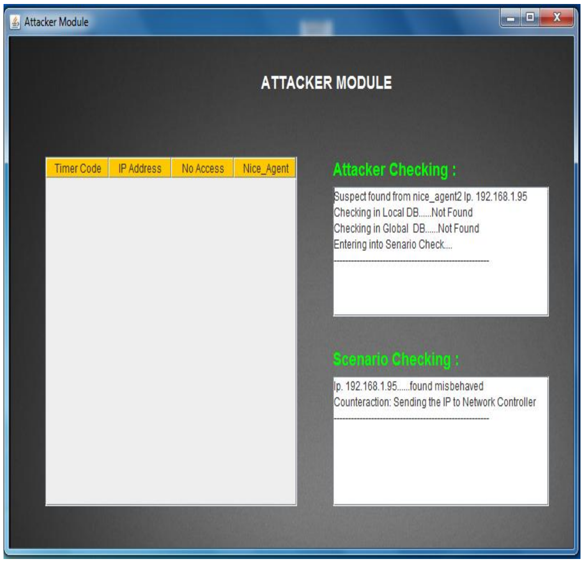


Timer Code	IP Address	No Access	Nice_Agent
1	192.168.1.95	5	nice_agent2

```
Suspect found from nice_agent2 Ip. 192.168.1.95
Checking in Local DB......Not Found
Checking in Global  DB......Not Found
Entering into Senario Check....
----------------------------------------------------------
```

Figure.5. Attack Analyzer checking for the suspected IP in Local_db and Global_db.

If IP is found in any of the two databases to be misbehaved then it is sent to network controller. If IP is not found in the two databases, then it initiates the Scenario Attack Analyzer as in Figure.5. The Scenario Attack Analyzer checks if IP's access count is greater than Attack Analyzers threshold. If yes, then, Scenario Attacker decides that IP has misbehaved and sends IP to the Network Controller as in Figure.6. Network controller in turn stores the IP into its database and necessary countermeasuresuch as blocking the misbehaved IP is taken.

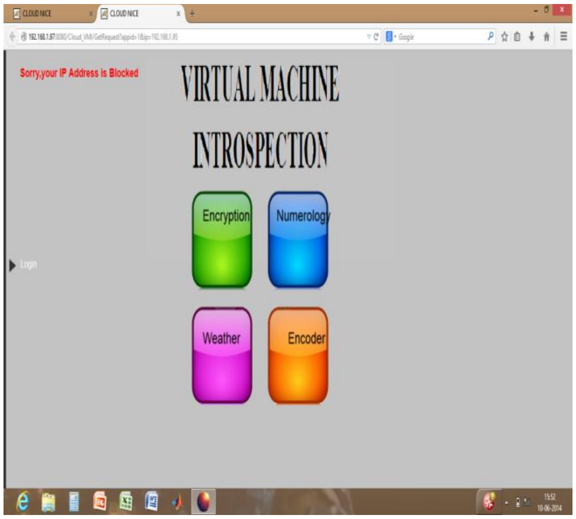


```
Suspect found from nice_agent2 Ip. 192.168.1.95
Checking in Local DB......Not Found
Checking in Global  DB......Not Found
Entering into Senario Check....
-----------------------------------------------------------
```

```
Ip. 192.168.1.95......found misbehaved
Counteraction: Sending the IP to Network Controller
-----------------------------------------------------------
```

Figure.6. Attack Analyzer Module detects IP to be misbehaved

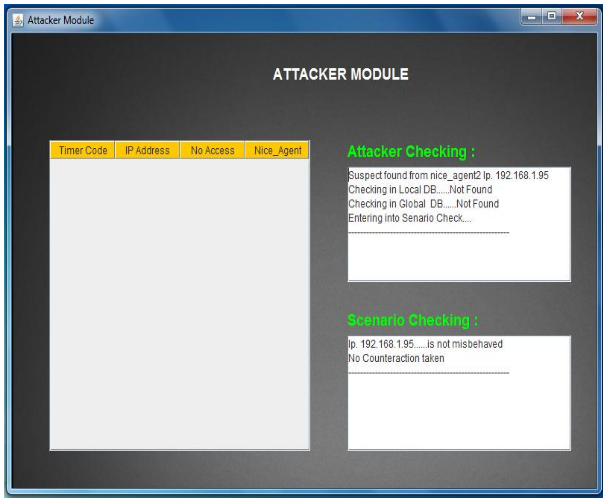
If next request arrives from the same misbehaved IP then the misbehaved IP is being blocked from further accessesas in Figure.7.



Sorry,your IP Address is Blocked

Figure.7. Blocking of the misbehaved IP

If IP's access count has not crossed Attack Analyzer's threshold access count value, then no countermeasure is taken as in Figure.8.



```
Suspect found from nice_agent2 Ip. 192.168.1.95
Checking in Local DB......Not Found
Checking in Global  DB......Not Found
Entering into Senario Check....
-----------------------------------------------------------
```

```
Ip. 192.168.1.95......is not misbehaved
No Counteraction taken
-----------------------------------------------------------
```

Figure.8. Attack Analyzer Module detects IP has not misbehaved

VI CONCLUSION

The proposed VMI architecture effectively detects the DOS/DDOS attacks. The misbehaved users are successfully blocked at the gateway level using theVMI agent and the attacker module. Thus, the VMI can reduce the risk of cloud system from being attacked and misused by the internal and external attackers. As future work, a Host based IDS can be incorporated into the implemented system to increase the accuracy of attack detection.

Acknowledgement

The authors would like to acknowledge and thank Technical Education Quality Improvement Program [TEQIP] Phase 2, BMS College of Engineering and SPFU [State Project Facilitation Unit], Karnataka for supporting the research work.

REFERENCES

[1] AkhilBhel, "Emerging Security Challenges in Cloud Computing", Information and Communication Technologies, 2011 World Congress on, Mumbai, 11th - 14th Dec 2011, pp 217 - 222, Print ISBN: 978-1-4673-0127-5, DOI: 10.1109/WICT.2011.6141247.

[2] FarzadSabahi, "Cloud Computing Security Threats and Responses", IEEE 3rd International Conference on Communication software and Networks(ICCSN), 27-29 May 2011, pp 245-249, Print ISBN: 978-1-61284-485-5, DOI: 10.1109/ICCSN.2011.6014715.

[3] Tal Garfinkel, Mendel Rosenblum, “A Virtual Machine Introspection Based Architecture for Intrusion Detection”, Network and Distributed Systems Security Symposium, 2003, pp 191-206, DOI: 10.1.1.11.8367.

[4] Anthony Roberts, Richard McClatchey, SaadLiaquat, Nigel Edwards, Mike Wray, “Introducing Pathogen: A Real Time Virtual Machine Introspection Framework”, conference on Computer & communications security, New York, NY, USA, November 2013, ISBN: 978-1-4503-2477-9, DOI: 10.1145/2508859.2512518.

[5] AnasAyad, UweDippel, “Agent Based Monitoring Of Virtual Machines”, International Symposium on Information Technology, Kuala Lumpur, 15-17 June 2010, pp1-6, Print ISBN: 978-1-4244-6715-0, DOI:10.1109/ITSIM.2010.5561375.

[6] Ying Wang, Chunming Hu, Bo Li, “VMDetector: A VMM-based Platform to Detect Hidden Process by Multi-viewComparison”,IEEE 13th International Symposium on High-Assurance Systems Engineering, Boca Raton, FL, 10-12 Nov. 2011, pp307-312, Print ISBN:978-1-4673-0107-7, DOI: 10.1109/HASE.2011.41.

[7] Li Ruan, JinbinPeng, Limin Xiao, Xiang Wang, “CloudDVMM: Distributed Virtual Machine Monitor for Cloud Computing”, IEEE International Conference on GreenCom and CPSCom, Beijing, 20-23 Aug. 2013, pp 1853-1858, DOI: 10.1109/GreenCom-iThings-CPSCom.2013.344.

[8] Amani S. Ibrahim, James Hamlyn-Harris, John Grundy, Mohamed Almorsy, “CloudSec: A Security Monitoring Appliance for Virtual Machines in the IaaS Cloud Model”, 5th International Conference on Network and System Security, Milan, 6-8 Sept. 2011, pp 113-120,Print ISBN:978-1-4577-0458-1,DOI:10.1109/ICNSS.2011.6059967.

[9] MiikaKomu, MohitSethi, RamasivakarthikMallavarapu, HeikkiOirola, Rasib Khan, SasuTarkoma, “Secure Networking for Virtual Machines in the Cloud”,IEEE International Conference on Cluster Computing Workshops, 24-28 Sept. 2012, Beijing, pp 88-96, Print ISBN: 978-1-4673-2893-7, DOI 10.1109/ClusterW.2012.29.

[10] SiFan Liu Jie Wu, ZhiHui Lu HuiXiong, “VMRaS: A Novel Virtual Machine Risk Assessment Scheme in the CloudEnvironment”,IEEE 10th International Conference on Services Computing, Santa Clara, CA, June 28-July 3, 2013, pp384-391, Print ISBN: 978-0-7695-5026-8, DOI:10.1109/SCC.2013.12.

[11] Roland Schwarzkopf, Matthias Schmidt, Christian Strack, Simon Martin, Bernd Freisleben, “Increasing virtual machine security in cloud environments”, Journal of Cloud Computing: Advances, Systems and Applications, July 2012, pp 1-12, Online ISSN: 2192-113X, DOI: 10.1186/2192-113X-1-12.

[12] Bryan D. Payne, Martim D. P. de A. Carbone, Wenke Lee, “Secure and Flexible Monitoring of Virtual Machines”, 23rd Annual Computer Security Applications Conference, 10-14 Dec. 2007, Miami Beach, FL, pp 385-397, Print ISBN:978-0-7695-3060-4, DOI 10.1109/ACSAC.2007.10.

[13] Manabu Hirano, Takahiro Shinagawa, Hideki Eiraku, Shoichi Hasegawa, KazumasaOmote, “Introducing Role-based Access Control to a Secure Virtual Machine Monitor: Security Policy Enforcement Mechanism for Distributed Computers”, IEEE Asia-Pacific Services Computing Conference, Yilan, 9-12 Dec. 2008,pp 1225-1230, Print ISBN: 978-0-7695-3473-2/08, DOI: 10.1109/APSCC.2008.14.

[14] Asit More, ShashikalaTapaswi, “Dynamic malware detection and recording using virtual machine introspection”, Best Practices Meet, Chennai, 12 July 2013, pp 1-6, Print ISBN: 978-1-4799-0637-6, DOI:10.1109/BPM.2013.6615011.

[15] Hanqian Wu, Yi Ding, Chuck Winer, Li Yao, “Network Security for Virtual Machine in Cloud Computing”,5th International Conference on Computer Sciences and Convergence Information Technology, Seoul, Nov. 30 2010-Dec. 2 2010, pp 18-21,Print-ISBN:978-1-4244-8567-3,DOI:10.1109/ICCIT.2010.571102.

[16] Martin Crawford, Gilbert Peterson, “Insider Threat Detection using Virtual Machine Introspection”, 46th Hawaii International Conference on System Sciences,Wailea, HI, USA 7-10 Jan. 2013, pp 1821-1830, Print ISBN: 978-1-4673-5933-7, DOI: 10.1109/HICSS.2013.278.

[17] Manabu Hirano, Takahiro Shinagawa, Hideki Eiraku, Shoichi Hasegawa, KazumasaOmote, “Introducing Role-based Access Control to a Secure Virtual Machine Monitor: Security Policy

Enforcement Mechanism for Distributed Computers", IEEE Asia-Pacific Services Computing Conference, Yilan, 9-12 Dec. 2008,pp 1225-1230, Print ISBN: 978-0-7695-3473-2/08, DOI: 10.1109/APSCC.2008.14.

[18] BingyuZou, Huanguo Zhang, "Integrity Protection and Attestation of Security Critical Executions on Virtualized Platform in Cloud Computing Environment", IEEE International Conference on GreenCom and CPSCom, Beijing, 20-23 Aug. 2013, pp 2071-2075, DOI:10.1109/GreenCom-iThings-CPSCom.2013.388.

[19] Kenichi Kourai, Takeshi Azumi, Shigeru Chiba, "A Self-protection Mechanism against Stepping-stone Attacks for IaaS Clouds", 9th International Conference on Ubiquitous Intelligence and Computing/Autonomic and Trusted Computing, Fukuoka, 4-7 Sept. 2012, pp 539-546, Print ISBN: 978-1-4673-3084-8, DOI: 10.1109/UIC-ATC.2012.139.

[20] Paul A. Karger, "Is Your Virtual Machine Monitor Secure?" , Third Asia-Pacific Trusted Infrastructure Technologies Conference, Hubei, 14-17 Oct. 2008, pp 5, Print ISBN:978-0-7695-3363-6, DOI:10.1109/APTC.2008.18.

[21] Sylvie Laniepce, Marc Lacoste, Mohammed Kassi-Lahlou, Fabien Bignon, KahinaLazri, AurelienWailly, "Engineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor", IEEE International Symposium On Service Oriented System Engineering, Redwood City, 25-28 March 2013, pp 25-36, Print ISBN:978-1-4673-5659-6, DOI:10.1109/SOSE.2013.27.

[22] Shun-Wen Hsiaoy, Yi-Ning Chen, Yeali S. Sun, Meng Chang Chen, "A Cooperative Botnet Profiling and Detection in Virtualized Environment", IEEE Conference on Communication and Network Security, National Harbor, MD, 14-16 Oct. 2013, pp 154-162, DOI: 10.1109/CNS.2013.6682703.

[23] Kara Nance and Brian Hay, Matt Bishop, "Investigating the Implications of Virtual Machine Introspection for Digital Forensics", International Conference on Availability, Reliability and Security, Fukuoka, 16-19 March 2009, pp 1024-1029, Print ISBN: 978-1-4244-3572-2, DOI:10.1109/ARES.2009.173.

[24] FabrizioBaiardi, Daniele Sgandurra, "Building Trustworthy Intrusion Detection through VM Introspection", Third International Symposium onInformation Assurance and Security, Manchester, 29-31 Aug. 2007, pp 209-214, Print ISBN: 0-7695-2876-7, DOI: 10.1109/IAS.2007.36.

[25] Bryan D. Payne, Martim Carbone, Monirul Sharif, Wenke Lee, "Lares: An Architecture for Secure Active Monitoring Using Virtualization", IEEE Symposium on Security and Privacy, 2008, Washington, DC, USA, pp 233-247, ISBN: 978-0-7695-3168-7, DOI:10.1109/SP.2008.24.

AUTHOR BIOGRAPHY

Ms. S C Rachana is a PG Scholar in Computer Networks and Engineering at B.M.S College Of Engineering, Bangalore. My research areas are Cloud Computing, Cloud Computing Security, Computer network.

Dr. H S Guruprasad is working as Professor and Head, Information Science Department at BMS College of Engineering, Bangalore. He has twenty four years of teaching experience. He has been awarded with Rashtriya Gaurav award in 2012. His research areas are Network Communications, algorithms, Cloud Computing and Sensor Networks.