International Journals of Advanced Research in Computer Science and Software Engineering
ISSN: 2277-128X (Volume-9, Issue-8)

Research Article | **August 2019**

IDS with Honey Pot to Detect Man in Middle Attacks in Cloud Computing

Pasupuleti Satyavathi, Dharmaiah Devarapalli, Dr. K. Ganesh Reddy
Department of CSE, Shri Vishnu Engineering College for Women (A), Vishnupur, Bhimavaram, West Godavari District, Andhra Pradesh, India

Abstract— Providing security in cloud computing is challenging issue due to its distributed and multi OS environment. Cloud security mechanisms are deployed at (Virtual Machine Monitor) VMM layer to protect the multi tenant's privacy and integrity. VMM layer is still vulnerable to Attacks.The main objective of man-in-middle attack is to eavesdrop the user's privacy and masking their presence making it appear no third party is involving. Due to man-in-middle attack, The VMM gets affected in terms of integrity, confidentiality and availability. In proposed work, we develop IDS to address the security problems like Man-In-Middle Attack. The Intrusion Detection System is implemented is implemented with Honey pot technology to attract the attacker.The Honey pot intrusion detection system capable of detecting known and unknown attacks along with MITM attack in cloud environment.

Key Terms— Cloud Computing, Virtualization, Man-in-Middle Attack, Signature Based IDS, Honey Pot mechanism.

I. INTRODUCTION

Cloud computing is new technological domain in the IT industry.The cloud computing is becoming popular domain because it works efficiently under less cost. Virtualization is one of the key technologies in the cloud environment which enables the creation of VMM which manages virtual machines in efficient way. VMM hides the complexity of the underlying hardware or software and allows multiple TVMs to run on the same physical machine. The tenants have the flexibility to transfer information in same cloud and to other Clouds.The transformation should satisfy authentication,integrity and availability.Still Vmm has vulnerabilities to eavesdrop that information .Hence the security of the TVMs in the cloud environment is very important for the tenants and the cloud service provider.

In information security, The MIMA attack is relays secretly. Controls the information transferring between sender and receiver. The attacker mask his presence from sender and receiver communicating though private network.by identifying the vulnerabilities in the system attacker attacks the system.the attacker can get information that is confidential and either change that information or not. The attacker get succeed when all information of sender and receiver known then only he can control the transformation.

In cloud computing the security is less because multiple systems connected trough single network that is public to all users. Attacker can easily get the information all like sender, receiver and communication details. It is necessary to detect and prevent mima attack in cloud environment. We require more efficient method for detecting MIMA attack in less time.In our, proposed work the MIMA attack is detected by Intrusion detection system placed in Dom0.

This implementation done through two ways

1. Creating MIMA attack. 2. Placing the IDS in System. 3. Detecting attack trough ids

II. RELATED WORK

In this, we can refer well known IDS architectures and methods applied for detecting MIMA attack.from this knowledge we can get more clarity about proposed work.

Preethi mishra and Vijay varadharajan proposed vmguard-signature based security architecture for intrusion detection system. This ids works efficiently by intuducing bong of n-gram method integrated with TF-IDF method. Later random forest classifier is applied for searching the signature.

Muthu kumara and Praveen Kumar rajendran proposed intelligentintrusion detection system to detect the intrusions intelligently.

They implemented by using muthu-praveen algorithm of intelligent intrusion

1. Training the intrusion detection system
2. Testing the intrusion detection system
3. Implementing and updating of intelligent intrusion detection system.

Farouq Aliyua, Tarek Sheltamia, Elhadad M. Shakshukib proposed technique for intrusion detection system and intrusion prevention system for MIMA attack.The IDS consists of IDS nodes that periodically interrogate nodes one hop away. The IPS uses lightweight encryption to prevent Man in the Middle attack and its variants at fog level.

Montalba mostafavi and penman kabiri proposed detection of repetitive and irregular hyper call attacks from guest virtual machines to xen-hypervisor.in which the security is provided to hyper call interface i.ehypervisor to avoid malicious hypercallsby monitoring the hyper calls irregular sequence is identified and association rule algorithm is applied on collected data. The security is limited to hypervisor only.

Subramaniam.T.K1 and Deepa proposed solution for MITM attack through mitigation techniques. The solution they proposed is the encryption is used for sender's side and decryption is used for receiver side so The attacker cannot modify the encrypted data. The different encryption and decryption algorithm such as AES, DES, and Triple DES etc is used.

Priyanka chouhan and rajendran singh proposed solutions for cloud security issues. One of them is MITM attack. The Solution for MITM attack is by

1. one time password
2. foreinsic analysis of MITM attack
3. mutual authentication.

By these we can prevent authentication security related issues over cloud environment. proposed technique for preventing MITM attack public key encrypted with digital signature called lock-box approach. the lock-box the contains actual keys. to access the lock-box public key is required with digital signature.

III. IMPLEMENTATION

To implement the proposed work we require two components are

1. Creating MITM attack in cloud environment.
2. Placing the efficient IDS in the cloud environment.

The MITM attack is created in cloud environment through virtual box once the attack is created then it is to be detected.The attack is detected by Intrusion detection system. The IDS is placed in Cloud environment.

CREATION OF MITM ATTACK:

To create the MITM attack it is necessary to set three machines or tenants'attacker, victim server .victim and server can be any system with different operating system. it is better to choose system with kali linux operating system which provides more attacking tools.

1). Virtual machines interface configuration: to create MITM attack the port numbers and ip addresses are required for each of server, attacker and victim. Following are the ip addresses for machines.
   a. Set the Server (ifconfig) ip address as 198.168.2.5
   b. Set Attacker (ifconfig) IP address as 198.168.2.6
   c. Set Victim (ifconfig)IP address is198.168.2.7
2) Create any folder in "server" and name it as folder1 which is to be transmitting through network.
3) Create a file named "file" with content "hi hello MITM Attack"
4) After creation of directory Change directory to Folder1 and simpleHTTPserver with command " python –m simpleHTTPserver"
5) Open the victim virtual machine and open browser and type URL as bellow
   http://<server_ip>:8000/File.html .
6) Open victim virtual machines and type bellow iptable commands in victim virtual machine's terminal
   a. iptables -t nat -A OUTPUT -p tcp --dport 80 -j DNAT --to-destination 198.168.2.7
   b. iptables -t nat -A OUTPUT -p tcp--dport 443 -j DNAT --to-destination 198.168.2.7
   c. iptables -t nat -A OUTPUT -p tcp --dport 8000 -j DNAT --to-destination 198.168.2.7
7) Open attacker virtual machine and execute the following commands.
   a. sudosysctl -w net.ipv4.ip_forward=1
   b. sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 198.168.2.7
   c. sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 198.168.2.7
   d. sudo iptables -t nat -A PREROUTING -p tcp --dport 8000 -j DNAT --to-destination 198.168.2.7
   e. iptables -t nat -A POSTROUTING -j MASQUERADE.
8) Select eth0 in attacker and capture the communication between sender and receiver in cloud environment. This attack scenario is depicted on figure 1.

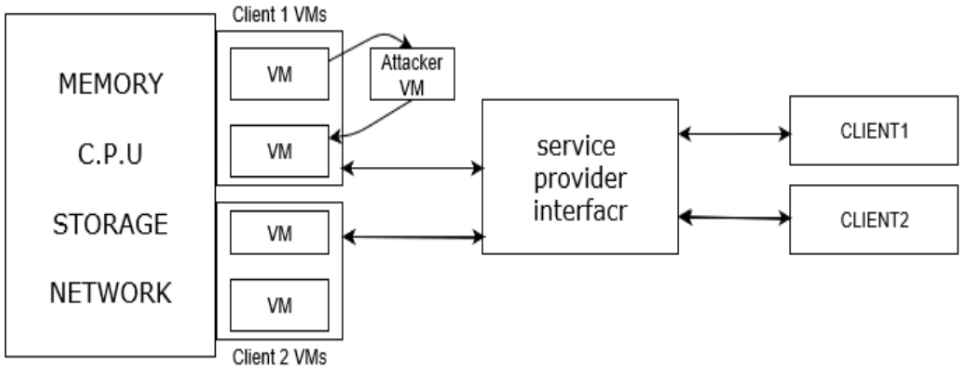

Figure1: Attack Scenario

IV. IDS WITH HONEYPOT TECHNIQUE

Cloud computing environment runs VMs communicate each other to perform the tasks over the distributed environment. Many VM communications are vulnerable to various types of attacks due to lack of security in cloud computing. To strengthen our data communication between VMs, we proposed IDS with Honeypot technique. To identify the known attacks we use signature based ids and to identify the man in middle attack we use Honeypot technique.

SIGNATURE- BASED INTRUSION DETECTION SYSTEM (SIDS):

SIDS maintains the known attack signatures database and it contains

1. Communication Latency of VMs
2. Number of Authentication failures
3. Number of Control packets per unit time
4. Number of Invalid packets per unit time
5. Number of data Integrity failures

All VMs requests are processed in SIDS, these request are verified by know signatures to find whether the received request is genuine request or fake request. For example, if the fifty packets is the maximum number of control packets can be sent per unit time, if any VM is generate more than fifty packets then the VM behavior is considered as abnormal behavior. If any VM abnormal behavior is more than the threshold abnormal behavior, then the VM is treated as an attacker and delete the attacker VM from the Cloud environment.

HONEY POT TECHNIQUE:

SIDS only verifies the known attacks like signature mismatching and fake packet flooding etc. To identify the unknown attacks, we use honeypot technique along with SIDS, and honeypot is an intelligent device to attract the attacker VMs. We mainly develop the fake VMs it can perform same operations as genuine VM on Cloud environment to attract the attacker VMs. In which, all legitimate VMs have hidden information which will be used for their secure VMs data communication, the hidden information contains down time VMs time intervals, during this time VMs won't perform any data communication with other VMs. This hidden information is among the legitimate VMs, so any attacker which masquerade the VMs in cloud environment does not have hidden information. There is more possibility attacker VM respond to other legitimate VMs during the actual VM down time. Thus, the attacker can easily identify by the legitimate VM when it receives the packets of a legitimate VM when it is down (not functioning based on hidden information). Any VMs detects the attacker VM then it immediately inform to Cloud service provider then this provider takes an action on the attacker VM. The figure 2.depicts the above honeypot technique procedure.

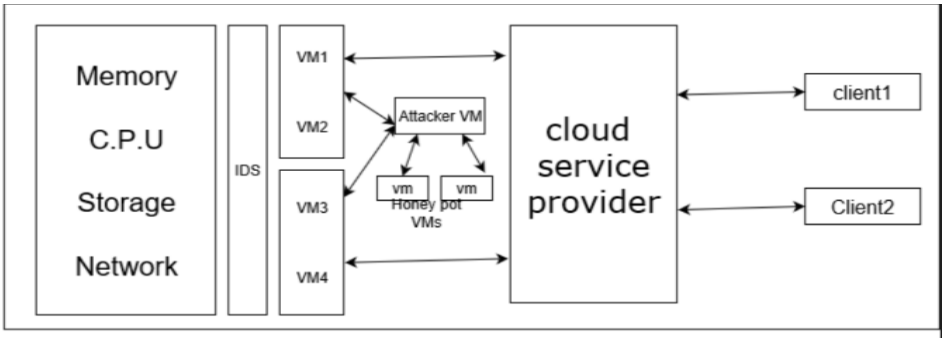

Figure 2: IDS with Honeypot

V. ALGORITHM: IDS WITH HONEY POT

step 1: //VM ←Virtual Machine
step 2: //VM' ←attacker Virtual Machine
step 3: //VM''←Honeypot Virtual Machine
step 4: //Req←VM Request
step 5: //Res← VM Response
step 6: //DRes← Data Response
step 7: While(ture)
step 8: Do
step 9: **Send Req** // for data communication
step 10: **If (Req= Legitimate)** //if IP and MAC is valid then Req is Legitimate
step 11: Send Res
step 12: Else
step 13: Res is fake and inform to CSP(cloud service provider)
step 14: **If(Res= Legitimate)** //if IP and MAC is valid then Res is Legitimate
step 15: Accept the Response
step 16: If (VM DRes time= VM down time)
step 17: DRes is fake and inform to CSP
step 18: Else
step 19: Process DRes
step 20: End-While

The above algorithm detect the man in middle attackers when the attacker uses masquerade technique to attack, then victim inform this information to Cloud service provider to take an action on attacker VM.

VI. RESULTS

IDS WITH HONEY POT IMPLEMENTATION:

To create the MITM attack it is necessary to set three machines or tenants attacker , victim server .victim and server can be any system with different operating system. It is better to choose system with kali linux operating system which provides more attacking tools.

1). Virtual machines interface configuration: to create MITM attack the port numbers and ip addresses are required for each of server, attacker and victim. Following are the ip addresses for machines.
   a. Set the Server(ifconfig) ip address as 198.168.2.5
   b. set Attacker(ifconfig) IP address as 198.168.2.6
   c. set Victim(ifconfig)IP address is198.168.2.7
   d. set Honeypot(ifconfig) IP address is 198.168.2.8
   e. set Honeypot is down at 7:45:00 to 7:45:10 sec
2) Create any folder in "Honeypot VM " and name it as folder1 which is to be transmit through network.
3) Create a file named "passords" with content "hi hello MITM Attack"
4) After creation of directory Change directory to Folder1 and simpleHTTPServer with command "python –m simpleHTTPserver"
5) Open the victim virtual machine and open browser and type URL as bellow
   http://<server_ip>:8000/Passwords.html .
6) Open victim virtual machines and type bellow iptable commands in victim virtual machine's terminal
   a. iptables -t nat -A OUTPUT -p tcp--dport 80 -j DNAT --to-destination 198.168.2.7
   b. iptables -t nat -A OUTPUT -p tcp--dport 443 -j DNAT --to-destination 198.168.2.7
   c. iptables -t nat -A OUTPUT -p tcp --dport 8000 -j DNAT --to-destination 198.168.2.7
7) Open attacker virtual machine and execute the following commands.
   a. Sudosysctl -w net.ipv4.ip_forward=1
   b. Sudo iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT --to-destination 198.168.2.7
   c. sudo iptables -t nat -A PREROUTING -p tcp --dport 443 -j DNAT --to-destination 198.168.2.7
   d. sudo iptables -t nat -A PREROUTING -p tcp --dport 8000 -j DNAT --to-destination 198.168.2.7
   e. iptables -t nat -A POSTROUTING -j MASQUERADE.
8) Victim 198.168.2.7 receives the data 7:45:04 sec.
9) Victim detects the that received data from the man in middle attacker and not from the actual server.
10) Victim 198.168.2.7 sends this information to server 198.168.2.5

VII. CONCLUSIONS

In this paper, we have addressed the various cloud computing attacks along with man in middle attack. We have proposed IDS with Honey pot to detect both known attacks and unknown attacks. To detect the man in middle attack we deploy Honey pot VMs to attract the attacker VMs. Our results proved that proposed approach detects the man in middle attackers and takes the proper action by the service provider.

BIBLIOGRAPHY

[1] Thu, A. A. (2013). Integrated intrusion detection and prevention system with Honey pot on cloud computing environment. International Journal of Computer Applications, 67(4).

[2] Bakshi, A., &Dujodwala, Y. B. (2010, February). Securing cloud from DDOS attacks using intrusion detection system in virtual machine. In 2010 Second International Conference on Communication Software and Networks (pp. 260-264). IEEE.

[3] Marcinkowski, S.J.; Stanton, J.M., "Motivational aspects of information security policies", IEEE International Conference on Systems, Man and Cybernetics, vol.3, pp.2527-2532 vol.3, 5-8 Oct. 2003.

[4] Campbell, S., "Supporting digital signatures in mobile environments," Twelfth IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2003. WET ICE 2003. Proceedings. , vol., no., pp.238-242, 9-11 June 2003.

[5] Karaarslan, E., Teke A., Şengonca H., "BilgisayarAğlarındaGüvenlikPolitikalarınınUygulanması."AkademikBilişimKonferansı, ÇukurovaÜniversitesi, 1s, 2003.

[6] Can, O.; Sahingoz, O.K., "A survey of intrusion detection systems in wireless sensor networks", 6th International Conference on in Modeling, Simulation, and Applied Optimization (ICMSAO), pp.1-6, 27-29 May 2015.

[7] Bashir, U.; Chachoo, M., "Intrusion detection and prevention system: Challenges & opportunities", International Conference on Computing for Sustainable Global Development (INDIA Com), pp.806-809, 5-7 March 2014.

[8] Benmoussa, H.; El Kalam, A.A.; Ouahman, A.A., "Towards a new intelligent generation of intrusion detection system", Proceedings of the 4th Edition of National Security Days (JNS4), pp.1-5, 12-13 May 2014.

[9] Malanik D., Kouril L., "Honeypot as the Intruder Detection System", In Proceedings of the 17th WSEAS International Conference on Computer, Kos(GR), pp. 96-101, 2013.

[10] Gökırmak Y., Bektaş O., Soysal M., Yiğit S., "Sanal IPv6 BalküpüAğıAltyapısı: Kovan", Ulusal IPv6 Konferansı, 2011.

[11] Gökırmak Y., Yüce E., Bektaş O., Soysal M., Orcan S., "IPv6 BalküpüTasarımı", TübitakUlakbim, Ankara, 2011.

[12] RiboldiJordaoda Silva Vargas, I.; Kleinschmidt, J.H., "Capture and Analysis of Malicious Traffic in VoIP Environments Using a Low Interaction Honeypot," Latin America Transactions, IEEE (Revista IEEE America Latina), vol.13, no.3, pp.777-783, March 2015.

[13] Shukla, R.; Singh, M., "PythonHoneyMonkey: Detecting malicious web URLs on client side honeypot systems," 3rd International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), vol., no., pp.1-5, 8-10 Oct. 2014.

