International Journal of Advanced Science and Technology
Vol. 29, No. 12s, (2020), pp. 1058-1063

# Hypervisor based Intrusion Detection and Prevention System for Cloud Environment

Mr. Amarnath J L1, Dr. Sarika Malhotra2, Dr. Sharmila3, Dr. Vineeta Verma4

*1Research Scholar at VTU Belagavi, amar.rv2010@gmail.com,*

*2Associate Prof. JSPMs Imperial College of Engineering and Research, pune, sarika.malhotras19@gmail.com*

***Abstract***

*In recent days, the cloud computing technology has received the significant scope in the area of IT and networking services. But this technology is suffering with lack of sufficient development in terms of its security methods. Cloud computing basically provides the services like infrastructure, software, platform, etc. The cloud security is to be guaranteed and its monitoring services are carefully designed using necessary intrusion detection and prevention techniques. In a cloud environment, hypervisors and virtual machines (VMs) are more significant to protect the data from any attacker. A hypervisor or virtual machine monitor is a software, firmware or hardware that creates and runs VMs. A computer on which the hypervisor runs one or more VMs is called as a host machine whereas the VMs are called as guest machines. Cloud provider uses the virtualization method to share the sources that is available in two levels i.e. VM and hypervisor. In many infrastructures, the cloud virtual machines are shared with other organizations virtual machines as a service. In this paper, we have implemented a hypervisor-based Intrusion Detection and Prevention System for Cloud Environment. The hypervisor-based architecture is the most promising and greatly improved the user VM security. This method can detect and eradicate the rootkits and other type of attacks. Both linux and windows based rootkits, DoS attacks, file integrity verification tests were performed and they were successfully detected.*

***Index Terms—****Hypervisor, Cloud computing, Security, Intrusion Detection and Prevention.*

## INTRODUCTION

The enterprise network is the heart of the enterprise IT architecture [1]. Over the years [2] the way that the data was protected by deploying the network security. It is by using the firewalls that are put in the system. The work was carried out in the off-line process. In the recent days, people started using the applications on the cloud which is an online service. But this increasingly created the attacks and security related issues[3]. As an example, if a person creates a document in office365 application and he shares it with his partner on their office 365 which can be duplicated on drop-boxes and so on so forth. As another example, an employee can syncs his corporate emails from the cloud to the personal device. All

This traffic happens in the cloud that we are unaware because we do not operate across the network. So we were unable to protect our data in the cloud. So it is necessary to find the new ways to protect the cloud data of different cloud providers like office365, box, drop box, IaaS etc. [4]. All these cloud providers expose their API's and the cloud can embrace it's security model of the cloud service. And then it can build upon to create a layer of security that is called system across all the cloud services. This is the normal process that we deal with the cloud computing. But it is necessary to consider the following challenges to provide better services to the users.

Enable the employees and developers to use the cloud services to the maximum

We cannot relay on the traditional network controls.

We have to embrace the new cloud native way and API based controls.

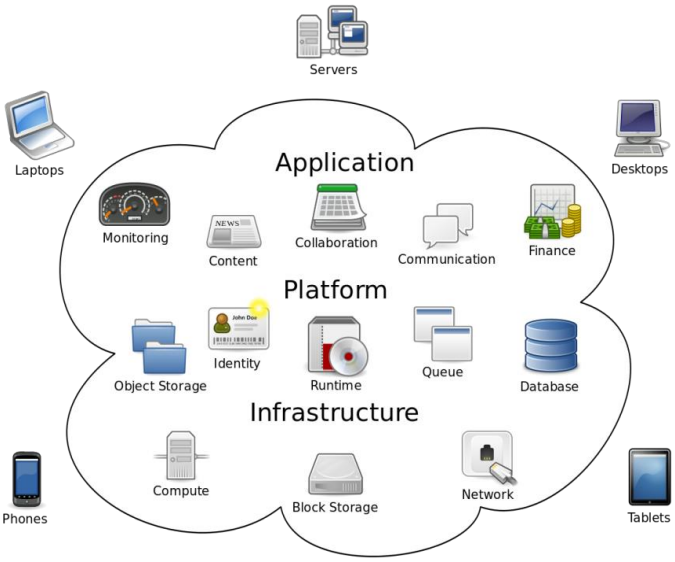


**Figure 1: A typical example of cloud computing environment**

Cloud computing [5-7] is the on demand computing resources, delivered to you over the internet. Here the cloud can provide an access to computing like an application that we need to run, a server of the company in most cases over the internet. It is also considered as a shared resource pool so that it transcends the responsibility of an organization. It can be a greater economy by renting its infrastructure rather than having it to be physically dedicated. A typical cloud computing environment is shown in figure 1.

The security implications [8-10] like the data privacy and confidentiality are the major concern while sharing the data. Sometimes we may not want to share some particular data. So understanding the classification and marking the data appropriately are to be considered. If it is shared or rented so that it should be guaranteed the availability of resources on the need. As our business relies on those resources, their availability is more important. We need to rely upon them as much as we do our current on premises data centre infrastructure system. And also, the geographical dissolving and the removal and virtualization of where the data is stored the legal jurisdiction for the geography of distributed resources becomes a concern.

Consider a two highly conceptualized virtual servers or server infrastructures as shown in figure 2. Now we have the virtual computers and instances of computers running as Virtual Machines (VM) [11 - 13]. This virtualization network consists of data centre and networking firewall. If we work on a virtualized network infrastructure that may include the data centre firewall, load balancing and other services. Its virtualized inside of these hosts and these are massive scale data centres that are servicing many tenants that are hosting the data, storage, compute and applications in the infrastructure. The cloud connects all of this and the data may be moving across and within. So it's difficult to physically determine where the data is and point to a server that might be running the particular application. And so we can see that with this introduction of network function virtualization the security of the hypervisor the virtual environment changes that how we design a network to be secure. These are really a choke point. Here, we have a very diverse set of components that we have to think about securing and so that changes our design.

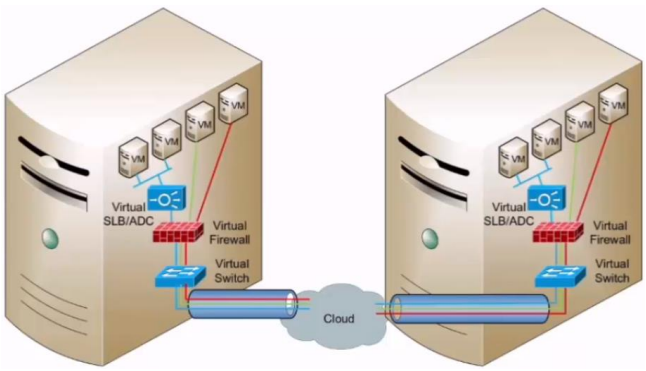

**Figure 2: Virtual server infrastructures connected through the cloud network**

The five characteristics of cloud are

On-demand self-service so that the user gets to provision of the resources as it seems to fit.

We have broad network access so we have reach-ability from the internet and many networks.

The resource pooling. Therefore, the service provider has pooled the large number of servers and storage systems that we can essentially have an inexhaustible supply and we rent what we need.

Rapid elasticity so that we can rent more or less on a moment's notice based on our mission, applications, needs, and nature of the business.

Measured service so that we only pay for what we use.

So, each of these characteristics has a corresponding security implication to it.

## Literature Survey

In the paper [14], the authors Jason N. and Y. Wang have proposed a hypervisor based cloud intrusion detection system. The proposed system uses hypervisors for leveraging the virtualization technologies in the cloud environment for intrusion detection and security.

In the paper [15], the authors Sylvie L., Marc L., Mohammed K., et. al, have proposed intrusion prevention techniques for an IaaS cloud using hypervisors. It has the advantages like the virtualization can be monitored by the hypervisor, improved security.

Proactive recovery approach [16] was proposed by Hans P. R. and Rudiger K. to build a fault and intrusion tolerant system which tolerates an arbitrary number of faults. The proactive recovery was implemented using virtualization-based replica of the infrastructure. In this design, the hypervisor initializes a replication in parallel to normal system execution to minimize the time.

Distributed intrusion detection architecture was proposed by S. Bharadwaja, Weiqing S., et. al. [17]. It was developed using Xen hypervisors which maintains cloud security using virtual networks. It can apply the dynamic filter operation for malicious hyper-calls in the virtual networks. It involves classification of hyper calls and to perform the integrity check on them.

A two-layer security set architecture was proposed by N. Sathyanarayanan, et. al, [18]. This architecture was designed using hypervisors. It can barricade, track and reciprocate as and when it senses hyper jacking. Prevention phase is the primary layer which is responsible for Authentication and Encryption/Decryption process. Detection Phase is the secondary layer which will perform the detection operation and responding operation using Honeyd. Layer1 uses the Challenge Handshake Authentication Protocol and Rijndael Ciphers as an advanced encryption technique. An additional security was provided by layer2 in case of failure of layer1. This layer is responsible to handle the external penetrations and malicious users. Hence, this system can provide the enhanced security using the two layer approach.

## SYSTEM ARCHITECTURE

The block diagram of our proposed system is shown in figure 3. It consists of Hypervisor as the main module. Virtual Machine Intrusion Detection and Prevention System (VM-IDPS) server and IDPS modules are the integral part of the hypervisor. Hypervisor has an access to performance data for the Virtual Machine (VM) that it hosts. The VM-IDPS module runs inside the hypervisor. This data provides insight into the activities occurring within a virtual machine without having direct knowledge of the actual operating system, applications or private data residing within the virtual machine. Every VM consists of a VM-IDPS client that can communicate with the server. The VM-IDPS client will scan the VM to certify for its robust and uninfected state. It is necessary to certify for system robustness so that the VM allows for function. Otherwise the VM-IDPS client raises a trigger alert for appropriate action so that the VM can be brought to the normal state. The VM-IDPS clients continuously monitor and analyze an every activity so that they detect and avert the malicious activity. The VM-IDPS client performs the different types of intrusion

detection techniques in order to detect an intrusion (like Rootkits, Virus, Worms, Ports scan, File alteration etc.). Those are like file integrity verification, signature and anomaly based intrusion detections. VM-IDPS clients continuously share the state information of VM with the server to detect an intrusion that was bypassed at VM level. VM-IDPS server utilizes cross-view analysis based intrusion detection techniques to spot an intrusion.

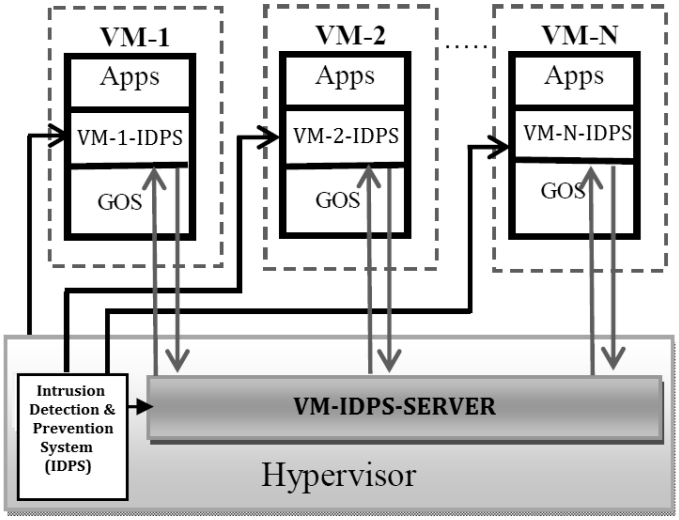


**Figure 3: Hypervisor based Intrusion Detection & Prevention System**

VM-IDPS clients continuously monitor the operating system files and all other critical files to ensure the file integrity. It can be done by computing and comparing their cryptographic hash digest with pre-computed values. If, any differences are found that will be considered as file content alteration. Then immediately VM-IDPS sends an alert message which tells the server that the file integrity violation was observed. Signature based intrusion detection is performed by comparing the obtained signature with its pre-defined signature. Anomaly based Intrusion Detection is performed by comparing observed activities with baseline profile. VM-IDPS server receives virtual machine's information from the client and it requests the hypervisor to supply actual low level information of that particular virtual machine. Hypervisor holds the complete control over the virtual machine, so it can supply the requested virtual machine information to VM-IDPS server. Then it compares these both the information's to identify the intrusion. It is called as the cross-view analysis.

## Results

This system implemented using the hypervisor (Oracle VirtualBox 4.03.18). It can send the low level (CPU & Memory) information to the VM-IDPS server. Hypervisor can automatically deploy VM-IDPS client onto every new VM. The server will be run on hypervisor. Here, it has been performed that the testing operation for the detection of Linux and windows rootkits, DoS attacks. They have been successfully detected.

Hacker Defender is considered as the windows rootkit. It can modify any API of windows. It allows the hackers to hide processes, files and registry keys. Also, it can check the open ports in any network connection. It has an executable file hxdef100.exe and the configuration file hxdef100.ini. The injected executable files can easily create a new process that hides the process. The hacker defender rootkit injection example was shown in figure 4. And the figure 5 shows that the alert message generated by our proposed system.

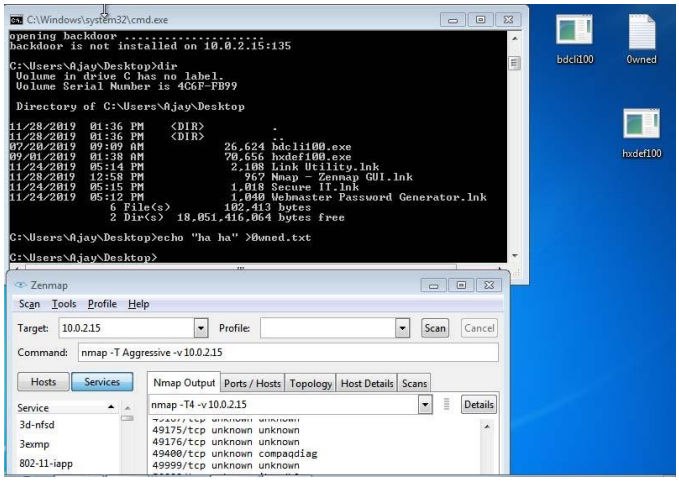


**Figure 4: Hacker Defender Rootkit Injection**

** Alert 1418200710.26154: mail - windows,
2019 Dec 10 14:08:30 (Laptop) 10.100.55.32>WinEvtLog Rule: 18147 (level 5) -> 'Application Installed.' User: ITDEPT 2019 Dec 10 14:08:28 WinEvtLog: Application: INFORMATION(11707): MsiInstaller: ITDEPT: ITDEPT-HP: Installation completed successfully.

**Figure 5: Alert message generated by our proposed system**

## Conclusion

Security is not a standstill activity and it is always evolving with time and technology upgradation. Here, we have implemented the hypervisor based intrusion detection and prevention system for cloud environment. It successfully detected the linux and windows rootkit and DoS attacks. These attacks are very hazardous for the system and cloud environment. File alternation identification is achieved by integrity checking algorithm. This system ensures the healthy state of every VM and cloud environment by detecting and eradicating intrusions in real time.

## References

[1]. C. Wang, S. S. M. Chow, Q. Wang, K. Ren and W. Lou, " Privacy-Preserving Public Auditing for Secure Cloud Storage," in IEEE Transactions on Computers, vol. 62, no. 2, p. p. 362 - 375, Feb. 2013.

[2]. Ajay Kumara M.A and Jaidhar C.D, " Hypervisor and virtual machine dependent Intrusion Detection and Prevention System for virtualized cloud environment," 2015 1st International Conference on Telematics and Future Generation Networks (TAFGEN), Kuala Lumpur, 2015, p. p. 28 - 33.

[3]. R. Moreno - Vozmediano, R. S. Montero and I. M. Llorente, " Key Challenges in Cloud Computing: Enabling the Future Internet of Services," in IEEE Internet Computing, vol. 17, no. 4, p. p. 18 - 25, July - Aug. 2013.

[4]. K. Salah, J. M. Alcaraz Calero, S. Zeadally, S. Al - Mulla and M. Alzaabi, " Using Cloud Computing to Implement a Security Overlay Network," in IEEE Security & Privacy, vol. 11, no. 1, p. p. 44 - 53, Jan. - Feb. 2013.

[5]. S. Meng and L. Liu, " Enhanced Monitoring - as - a - Service for Effective Cloud Management," in IEEE Transactions on Computers, vol. 62, no. 9, p. p. 1705 - 1720, Sept. 2013.

[6]. Z. Xiao and Y. Xiao, " Security and Privacy in Cloud Computing," in IEEE Communications Surveys & Tutorials, vol. 15, no. 2, p. p. 843 - 859, Second Quarter 2013.

[7]. J. Li, Y. Zhang, J. Ning, X. Huang, G. S. Poh and D. Wang, " Attribute Based Encryption with Privacy Protection and Accountability for CloudIoT," in IEEE Transactions on Cloud Computing.

[8]. K. Lee, " Comments on " Secure Data Sharing in Cloud Computing Using Revocable - Storage Identity - Based Encryption, " in IEEE Transactions on Cloud Computing.

[9]. X. Zhao and R. Jiang, " Distributed Machine Learning Oriented Data Integrity Verification Scheme in Cloud Computing Environment," in IEEE Access, vol. 8, p. p. 26372 - 26384, 2020.

[10]. Y. Liao, G. Zhang and H. Chen, " Cost - Efficient Outsourced Decryption of Attribute - Based Encryption Schemes for Both Users and Cloud Server in Green Cloud Computing," in IEEE Access, vol. 8, p. p. 20862 - 20869, 2020.

[11]. B. Wan, J. Dang, Z. Li, H. Gong, F. Zhang and S. Oh, " Modeling Analysis and Cost - Performance Ratio Optimization of Virtual Machine Scheduling in Cloud Computing," in IEEE Transactions on Parallel and Distributed Systems, vol. 31, no. 7, p. p. 1518 - 1532, 1 July 2020.

[12]. C. Gan, Q. Feng, X. Zhang, Z. Zhang and Q. Zhu, " Dynamical Propagation Model of Malware for Cloud Computing Security," in IEEE Access, vol. 8, p. p. 20325 - 20333, 2020.

[13]. P. Liu, " Public - Key Encryption Secure Against Related Randomness Attacks for Improved End - to - End Security of Cloud/Edge Computing," in IEEE Access, vol. 8, p. p. 16750 - 16759, 2020.

[14]. J. Nikolai and Yong Wang, " Hypervisor - based cloud intrusion detection system," 2014 International Conference on Computing, Networking and Communications (ICNC), Honolulu, HI, 2014, p. p. 989 - 993.

[15]. S. Laniepce, M. Lacoste, M. Kassi - Lahlou, F. Bignon, K. Lazri and A. Wailly, " Engineering Intrusion Prevention Services for IaaS Clouds: The Way of the Hypervisor," 2013 IEEE Seventh International Symposium on Service - Oriented System Engineering, Redwood City, 2013, p. p. 25 - 36.

[16]. H. P. Reiser and R. Kapitza, " Hypervisor - Based Efficient Proactive Recovery," 2007 26th IEEE International Symposium on Reliable Distributed Systems (SRDS 2007), Beijing, 2007, p. p. 83 - 92.

[17]. S. Bharadwaja, W. Sun, M. Niamat and F. Shen, " Collabra: A Xen Hypervisor Based Collaborative Intrusion Detection System," 2011 Eighth International Conference on Information Technology: New Generations, Las Vegas, NV, 2011, p. p. 695 - 700.

[18]. N. Sathyanarayanan and M. N. Nanda, " Two Layer Cloud Security Set Architecture On Hypervisor," 2018 Second International Conference on Advances in Electronics, Computers and Communications (ICAECC), Bangalore, 2018, p. p. 1 - 5.