DESIGN OF ADAPTIVE DISTRIBUTED INTRUSION DETECTION SYSTEM FOR CLOUD COMPUTING

***Hidam Rameshwar Singh**
****Dr. Rajeswari Mukhesh**
**Hindustan University, Chennai*
***HOD, Department Of CSE*
Hindustan University, Chennai

ABSTRACT

In the process of cloud deployment, the security issues cannot be underestimated. Due to their distributed nature, cloud computing environment are easy targets for intruders looking for possible vulnerabilities to exploit. There are various ways for an intruder to exploit and use the cloud resources maliciously. To combat attackers, intrusion detection system (IDS) offer additional security measure for cloud computing environment by investigating configuration, logs, network traffic and user action to identify typical attack behaviour.. The traditional IDSs can't appropriately identify suspicious activities due to the limitation of HIDS and NIDS. Thus, in this paper a hybrid based IDS has been proposed where Hypervisor Based Intrusion detection System (HyIDS) will work together with HIDS to give an adaptive, distributive intrusion detection system. The combination of HyIDS and HIDS will have more detecting power.

Keywords: *cloud computing, Intrusion detection system, hypervisor, virtual machine monitor introspection*

INTRODUCTION

Cloud computing has rapidly emerged as a widely accepted paradigm in computing systems, in which an end-user can request some computing capabilities and services when he needs it, and he can reach these resources across networks anytime, anywhere. While moving from traditional local computing paradigm to the cloud computing paradigm, new security and privacy challenges emerge because of the distributed nature of cloud computing. Some of these security vulnerabilities leave open doors, which stem from the existing computing models; and some of them, inherent from cloud-based models. As a result, malicious users force these doors to attack the system, and they attack on end-users' private data; processing power, bandwidth or storage capacity of the cloud network. Cloud computing organizations have to provide a high quality service and protect the users' sensitive data. To prevent these attackers, firewall mechanism and/or Intrusion Detection System (IDS) are effective solutions to resist them. They can provide additional protection mechanisms on the cloud distributed environments. IDS can identify suspicious activities by monitoring network traffic changes, configuration of the system, logs files, and actions of end-users. When such a suspicious

event is detected, IDS sends an alert message to user or monitoring console to trigger some actions for preventing these attacks.

Security in Cloud:

While moving from traditional computing paradigm to cloud computing paradigm new security and privacy challenges has emerged. Security of the cloud computing system can be thought in two dimensions: physical security and cyber security.

Physical security concerns the physical properties of the system. For example, a data centre, which is owned by provider infrastructure, has to realize security standards and hold security certifications globally; supervision and manageability on security preventions, incombustibility, uninterrupted power supplies, precautions for natural disasters (earthquake, flood, fire etc.) are indispensable. However twenty four hours and seven days monitoring for heat, humidity and air condition systems and also some biometric entrance systems may help for the business continuity.

On the other hand, cyber security defines the prevention of system from cyber world. There is a risk of cyber security attacks on services of cloud computing system. These attack can use huge amounts of computing resources, disables their usage by consumer efficiently. The following are the intrusions, which cause availability, confidentiality and integrity issues to Cloud resources and services.

Insider Attack: Employee, entrepreneur and associates which are still or former attended who can or could access the whole information system with privileged authority are defined as insider. Insider attacks are organized and run by these individuals to harm or temper knowledge about consumers or providers and include every kind of attacks which can be executed from inside.

Flooding Attack: In this type of attack, attackers can send very large amounts of packets from exploited information resources, and they are called as zombie. Packets can be either one of TCP, UDP, ICMP or a combination of these protocols. These kinds of attacks are mostly realized over unauthorized network connections. Because of cloud computing distributed nature, connections to the virtual machines are established over Internet. For this reason, exposition of cloud users with Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks are inevitable. Flooding attacks affect the availability of serviced for authorized users. An attack that is realized to a server which serves one kind of service can prevent a vast of scale accessibility to this served service. These kinds of attacks are called DoS attacks. If servers' resources are slogged after flooding attacks and it prevents the execution of other services, which run on the server, this kind of attacks are called indirect DoS attacks.

User to Root Attacks: In this type of attack, an intruder seizes the account and password information of an authorized user, and he can acquire limitless access to the whole system. Buffer overflows are used for establish console connection for authorized processes. This

type of intrusion can be realized with writing an excessive amount of data to a statically defined buffers' capacity, and the information is captured by intruders from this overflowed data. An attacker who owned the account and password information of an authorized user can hold the access privilege to servers and also to virtual machines.

Port Scanning: An attack that identifies open, closed and filtered ports on a system. In port scanning, intruders can seize information with the help of open ports like services that run on a system, IP and MAC addresses which belong to a connection, and router, gateway and firewall rules. TCP, UDP, SYN/FIN/ACK and Window scanning are the most common scanning attacks. Port scanning is not used by its own, an intruder realize the actual attack after getting information about open ports and running services.

Attacks on Virtualization: After compromising hypervisor, control of the virtual machines in the virtual environment will be captured. Zero day attacks are one of the methods that attack virtual machines and use hypervisor or other virtual machines to attack other virtual machines. Zero day attacks use known vulnerabilities before system or software developers apply patches or updates.

Intrusion Detection In Cloud

Intrusions Detection System are used to detect any anomaly or attack in a systems. In cloud environment, four types of IDS are applied: Host based intrusion detection system (HIDS), Network based intrusion detection system (NIDS), Hypervisor based intrusion detection system and Distributed intrusion detection system (DIDS).

Host based Intrusion Detection Systems (HIDS):

A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the information collected from a specific host machine. HIDS running on a host machine detects intrusion for the machine by collecting information such as file system used, network events, system calls etc. HIDS observes modification in host kernel, host file system and behaviour of the program. Upon detection of deviation from expected behaviour, it reports the existence of attack. The efficiency of HIDS depends on chosen system characteristics to monitor. With respect to Cloud computing, HIDS can be placed on a host machine, VM or hypervisor to detect intrusive behaviour through monitoring and analyzing log file, security access control policies, and user login information. If installed on VM, HIDS should be monitored by Cloud user whereas in case of installing it on Hypervisor, Cloud provider should monitor it.

Network based Intrusion Detection System (NIDS):

A Network based Intrusion Detection System (NIDS) is an intrusion detection system that tries to detect malicious activity such as DoS attacks, port scans or even attempts to crack into computers by monitoring network traffic. The information collected from network is compared with known attacks for intrusion detection. NIDS has stronger detection

mechanism to detect network intruders by comparing current behaviour with already observed behaviour in real time. NIDS mostly monitors IP and transport layer headers of individual packet and detects intrusion activity. NIDS uses signature based and anomaly based intrusion detection techniques. NIDS has very limited visibility inside the host machines. If the network traffic is encrypted, there is really no effective way for the NIDS to decrypt the traffic for analysis. NIDS placed between firewall and various hosts of the network NIDS can be deployed on Cloud server interacting with external network, for detecting network attacks on the VMs and hypervisor. However, it has several limitations. It cannot help when it comes to attack within a virtual network that runs entirely inside the hypervisor. In Cloud environment, installing NIDS is the responsibility of Cloud provider.

Distributed Intrusion Detection System (DIDS):

A Distributed IDS (DIDS) consists of several IDS (E.g. HIDS, NIDS etc.) over a large network, all of which communicate with each other, or with a central server that enables network monitoring. The intrusion detection components collect the system information and convert it into a standardized form to be passed to central analyzer. Central analyzer is machine that aggregates information from multiple IDS and analyzes the same. Combination of anomaly and signature based detection approaches are used for the analysis purpose. DIDS can be used for detecting known and unknown attacks since it takes advantages of both the NIDS and HIDS, which are complement of each other. In Cloud environment, DIDS can be placed at host machine or at the processing server in backend.

Hypervisor-based Intrusion Detection Systems:

Hypervisor-based intrusion detection system is an intrusion detection system specifically designed for hypervisors. Hypervisor is a platform to run VMs. Running at hypervisor layer, this type of IDS allows user to monitor and analyze communications between VMs, between hypervisor and VM and within the hypervisor based virtual network. Availability of information is one of the benefits of hypervisor based IDS. Novelty in the technology and lack of experience are the few of its challenges. VM introspection based IDS is one of the examples of hypervisor based intrusion detection system. Recently IBM Research is pursuing virtual machine introspection approach used to create a layered set of security services inside protected VM running on same physical machine as the guest VMs running in the Cloud system . As Cloud computing is defined as a pool of virtualized computer resources and to manage various virtual machines hypervisor (also known as virtual machine manager) is used. Hypervisor based IDS is one of the important techniques, specifically in Cloud computing, to detect intrusion in virtual environment

RELATED WORKS

Numerous works to detects intrusion in cloud computing were done by different researchers but most of the prior work fails to detect all the intrusion types and also to adapt with the dynamic environment.

Cloud and Grid computing are the most vulnerable targets for intruder's attacks due to their distributed environment. For such environments, Intrusion Detection System (IDS) can be used to enhance the security measures by a systematic examination of logs, configurations and network traffic. Traditional IDSs are not suitable for cloud environment as network based IDSs (NIDS) cannot detect encrypted node communication, also host based IDSs (HIDS) are not able to find the hidden attack trail. Kleber et al. [3] have proposed an IDS service at cloud middleware layer, which has an audit system designed to cover attacks that NIDS and HIDS cannot detect. The architecture of IDS service includes the node, service, event auditor and storage. The node contains resources that are accessed through middleware which defines access-control policies. The service facilitates communication through middleware. The event auditor monitors and captures the network data, also analyzes which rule / policy is broken. The storage holds behaviour-based (comparison of recent user actions to usual behaviour) and knowledge-based (known trails of previous attacks) databases. The audited data is sent to IDS service core, which analyzes the data and alarm to be an intrusion. The authors have tested their IDS prototype with the help of simulation and found its performance satisfactory for real-time implementation in a cloud environment. Although they have not discussed the security policies compliance check for cloud service provider and their reporting procedures to cloud users.

Nguyen Doan Man and Eui-Nam Huh [7] proposed a Collaborative IDS framework, which launches an idea of federation defence in the cloud computing. Based on this concept, IDSs are deployed in each Cloud computing region belonging to each cloud provider (CP).These IDSs cooperate with each other by exchanging alerts about recognized intrusions to prevent from further damages. Furthermore, this IDS framework also supports to synthesize information extracted from alerts for detecting large-scale coordinated attacks such as DDoS, stealthy scan, worms, etc. Also, the work allows Cloud users to configure all their own IDSs distributed on different Cloud regions via a unique user interface, which help to simplify management of Cloud users' IDSs

Parag K. Shelke, et al. [6] works on multi thread NIDS model for distributed cloud environment is based on three modules: capture & queuing module, analysis/ processing module and reporting module. The capture module, receives the in-bound and out-bound (ICMP, TCP, IP, UDP) data packets. The captured data packets are sent to the shared queue for analysis. The analysis and process module receives data packets from the shared queue and analyze it against signature base and a pre-defined rule set. Each process in a shared queue can have multiple threads which work in a collaborative fashion to improve the system performance. This work involve third party monitoring and service which make the system more complex and the used of single node NIDS will bottleneck the system and it is used for detecting only network intrusion hence fail to detect intrusion in host system or VM.

Shaohua Teng et al.[10] proposed a system to cope with malicious attacks, where a collaborative intrusion detection architecture is proposed and the E-CARGO model is used to model this system. According to CIDF (Common Intrusion Detection Frame), the components of the intrusion detection system are defined. Furthermore, it design and clearly

describe the behaviours of Agent and their interrelationship. Intrusion detection modelling can be taken as a software engineering problem, and E-CARGO model for Role-Based Collaboration is a promising approach to analyze collaborative systems. Therefore, this model is be used to describe the architecture of the detection model, the components and the relationships among the components.

Deepa Krishnan and Madhumita Chatterjee [1] used a Distributed approach in intrusion detection combining a knowledge based system and behavioral based scheme. This is supplemented by a surveillance agent which help in the adaptive nature of IDS functionality, by continuously monitoring the node behaviours so that an adaptive line in done. The behaviour based approach facilitates improved detection in the dynamic cloud environment and the knowledge based approach supports the detection scheme with its definitive rule base. The functionality of both these approaches has been improved by the addition of an adaptive approach which helps to significantly assist in lowering the false positives. In addition to this, another novel and the striking advantage of the proposed detection scheme is the alert clustering and analyzing facility thereby helping all cooperating nodes in detecting false alarms from any malicious nodes. DOS attacks in one node can be sent as alerts to help other cooperating nodes in updating themselves about new attack patterns leading to early detection and prevention of attacks. This scheme collectively helps to make the underlying cloud infrastructure more immune to attacks and continue to provide services to users.

Tal Garfinkel et al [13] propose an architecture and approach for leveraging the virtualization technology at the core of cloud computing to perform intrusion detection security using hypervisor performance metrics. Through the use of virtual machine performance metrics gathered from hypervisors, such as packets transmitted/received, block device read/write requests, and CPU utilization, the system demonstrates and verifies that suspicious activities can be profiled without detailed knowledge of the operating system running within the virtual machines[8][11][12]. The proposed hypervisor-based cloud intrusion detection system does not require additional software installed in virtual machines and has many advantages compared to host-based and network based intrusion detection systems which can complement these traditional approaches to intrusion detection.

PROPOSED SYSTEM

The proposed system is a hybrid IDS of HIDS and Hypervisor Based IDS(HyIDS). In this paper, HyIDS works by virtual machine monitor instropective[13]. This allow the system to detect an attact in the virtual environment from outside the system. The HyIDS is integrated with Hypervisor which will monitor the VMs by inspecting the event and other parameters. The proposed system will describe the deployment of IDS units in the cloud environment and their management. The architecture contains the different IDS units, storage module, and IDS controller.

(IJRST) 2016, Vol. No. 6, Issue No. II, Apr-Jun e-ISSN: 2249-0604; p-ISSN: 2454-180X

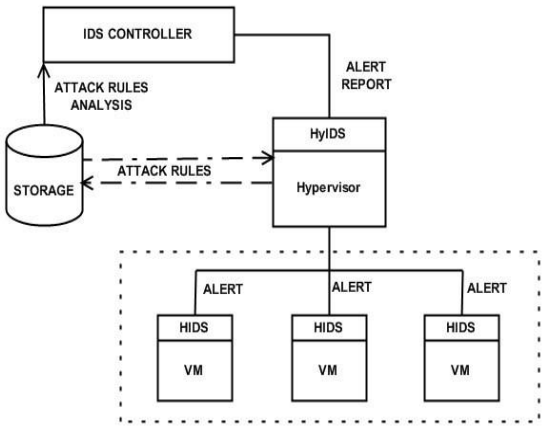

fig.1 System Architecture

IDS CONTROLLER

This is the central management component which control and monitors all IDS instances. The alerts generated by the IDS units (HyIDS and HIDS) will be transfer to this controller for further process and analysis. Then it will generate alert notifications and send to users or system admin about the attacks. It maintains logs of request and services of all VM nodes.

It contains the following components:

Notification module: - It directly with users to notify detected intrusion which affect their resources. It queries to database to get new alerts which are stored in the database. It collects all the entries related to a user from the database, parses and audit all alerts stored before creating the statistical reports and detailed reports if the user demand

Configuration module: It configure the IDS and there deployment in the VM. It also configures the notification mechanism to the users. For this a single web based user interface can be used to specify the monitoring functions, alert settings and threshold parameters for the intrusion detectors.

Alert Collector: It receives alerts from the VMs and hypervisor and update to the database. It will gather all the alerts from all the IDS units and extract important information from these alerts and then send this information to the alert processor for further processing task.

Alert Processor: It process the alerts from the IDSs and analyze and extract information and make a log of compromised VM, identification of suspicious attackers and details of recognized attacks. This information is then updated to the Database to prepare the policies and other counter measures against the compromised host or attackers.

IDS Units

The IDS contains the different intrusion detection system.

A. HYPERVISOR BASED IDS (HyIDS):

HyIDS is integrated to the hypervisor. Hypervisor can monitors all the VMs by Virtual Machine Introspection(VMI) of all the matrices of the VM system states like message packet transmitted/received, system event logs, CPU utilization, etc. It monitors the kernel of guest OS for the intrusion. It detects event that occur due to an attack rather than detecting the attacks.

The HyIDS has the following Sub-components :-

Local Database: It contains the information about implementation of Guest OS to interpret VM's State.

System Analyzer: It interprets system states and events from Hypervisor interface and OS interface library and decides whether the system has been compromised or not.

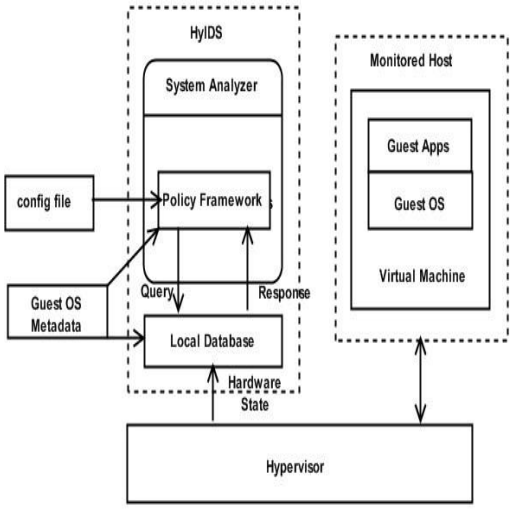

Fig.2 HyIDS

B. HOST BASED IDS(HIDS):

HIDS will be installed in each instance of VM. The proposed of HIDS is to monitor the respective VM to detect any attacks that the hypervisor fails to detect. Since HIDS is installed in the host it offers high visibility and can detect direct attacks in the host.

Intrusion Detector: It will monitor all the host VM for any intrusion by collecting data about network traffic, memory, file systems, logs, etc. to find potential threat. The alerts generated by the intrusion detector are raw alert and sent to the data analyzer for further processing.

Data analyzer: This will analyzed the detected data or intrusion and then analyze by comparing the behavior and signature from the database. The raw alerts sent by the intrusion

detector are compared with policy rules available in the database and identified the data for any threat.

Alert Generator: This is responsible for generating alerts based on the analyzed data. If there is any anomaly in the analysis then it will generate an alert and send it to the IDS Controller.

Database: This will store the knowledge based and behavior based attack rules. This is updated when a new alert are found

C. STORAGE UNITS:

This unit contains the attack rules that the IDS must analyze. It is formed by combining both knowledge based and behavior based. Any new attack are updated and stored in this module to form
new rule.

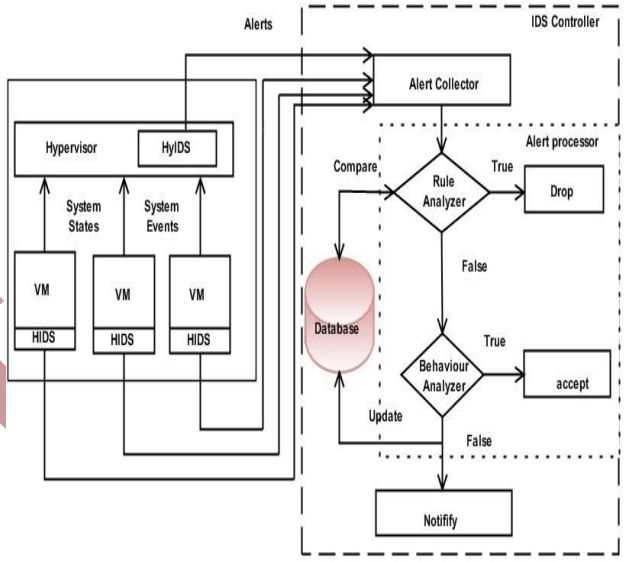

Fig.3 Working of the Proposed System

In this system, all the alerts sent by HIDS and HyIDS is received by the alert collector and then it is sent to the alert processor. In the HIDS, the Intrusion Detector will monitor the host VM for any intrusion by collecting data about network traffic, memory, file systems, logs, etc. to find potential threat. The the information by the intrusion detector are raw alert and sent to the data analyzer for further processing. If there is any anomalous behaviour or the events are deviated from the expected one then it will generate an alert and sent to the alert collector in IDS controller.

The HyIDS in the hypervisor will monitors and analyzed all the VMs by Virtual Machine Introspection (VMI) of all the matrices of the VM system states like message packet transmitted/received, system event logs, CPU utilization, etc. It monitors the kernel of guest

OS for the intrusion. It detects event that occur due to an attack rather than detecting the attacks. Any anomaly found then will generate an alert and sent it to the alert collector.

The alert collector will gather all the alerts from all the IDS units and extract important information from these alerts and then send this information to the alert processor for further processing task.

The alert processor will process the alerts from the IDSs and analyze and extract information by comparing the signature of the threat and analyzing the behavior and if the threat is found to be an attack then it will notify the user and admin and make a log of compromised VM, identification of suspicious attackers and details of recognized attacks. This information is then updated to the Database to prepare the policies and other counter measures against the compromised host or attackers.

IMPLEMENTATION

For implementating the proposed system, a simple cloud infrastructure is set up using Kernel Virtual Mcchine(KVM) hypervisor. For managing the VMs, Virtual Machine Monitor(VMM) is used and created 4 VMs. An open source HIDS,OSSEC is installed in each of the VM as an agent to collect the system datas and logs for analyzing any threat to the system and sent to the server to analyz and create alerts. To detect any threat to the hypervisor the HIDS is also installed. OSSEC perform the integrity checking and root kit detection function also. The VMM also gives the system statistics. By analyzing this together with the other parameters from the HIDS we can dectects and identified the infected system in the cloud and take up the necceasay actions.

FUTURE WORK AND CONCLUSION

In this paper we introduce HIDS as a hybrid system to work with virtual machine introspective. It exploits some characteristics in VMs in the cloud infrastructure, make it possible to extract data from the VMs for evaluation. HIDS are install in each VMs and these are monitor by a management server which collect all the data sent by the agent from different VM instances.

The implementation of the proposed system at present is applied to a small private cloud. An interesting future topic is the implementation of the fully functional HIDS agent to install automatically when the VM is created and also the we can work on securing hypervisor by creating a secure process for the host system . To practically apply the deployment, performance and scalability issues need to be considered as the next step.

REFERENCES

[1] Deepa Krishnan and Madhumita Chatterjee **"**An Adaptive Distributed Intrusion Detection System for Cloud Computing Framework*",* Springer publication, SNDS 2012, CCIS 335, pp. 466–473,

[2] Jason Nikolai, Yong Wang "Hypervisor-based Cloud Intrusion Detection System "**,** College of Business and Information Systems Dakota State University Madison,s,2014 pp.989-993.

[3] Kleber Vieira, Alexandre Schulter, Carlos Becker Westphall, and Carla Merkle Westphall**"** Intrusion Detection for Grid and Cloud Computing " , computer.org/ITPro July/Aug, IEEE-2010.pp.38-43.

[4] Lena AlMutair, Soha S. Zaghloul, "A New Virtualization-Based Security Architectureina Cloud Computing Environment " College of Computer and Information Science King Saud University Riyadh, KSA. ISBN: 978-0-9853483-3-5 ©2013 SDIWC,pp.667-686.

[5] Modi, C., Patel, D., Patel, H., Borisaniya, B., Patel, A. & Rajarajan, M. (2013). "A survey of intrusion detection techniques in Cloud". Journal of Network and Computer Applications,36(1), pp. 42-57. doi: 10.1016/j.jnca.2012.05.003 http://dx.doi.org/10.1016/j.jnca.2012.05.003

[6] Ms. Parag K. Shelke, Ms. Sneha Sontakke, Dr. A. D. Gawande, " Intrusion Detection System for Cloud Computing" International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012. pp.67-71.

[7] Nguyen Doan Man and Eui-Nam Huh"A Collaborative Intrusion Detection System Framework for Cloud Computing "**,** Proceedings of the International Conference on IT, Convergence and Security 2011, Springer Science+Business Media B.V. 2012.pp.91-109.

[8] Saeed M. Alqahtani, Maqbool Al Balushi, Robert John, "An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC)", International Conference on Computational Science and Computational Intelligence,2014,CPS, pp.152-158

[9] Sebastian Roschke, Feng Cheng, Christoph Meinel," Intrusion Detection in the Cloud" 8th IEEE International Conference on Dependable, Autonomic and Secure Computing.IEEE Computer Society,2009,pp.729-734

[10] Shaohua Teng, Chaoyu Zheng, Haibin Zhu, Dongning Liu and Wei Zhang"A Cooperative Intrusion Detection Model for Cloud Computing Networks "**,** International Journal of Security and Its Applications , Vol.8, No.3 (2014), pp. 107-118 .

[11] Tongwook Hwang, Youngsang Shin," Design of a Hypervisor-based Rootkit Detection Method for Virtualized Systems in Cloud Computing Environments" The 2013 AASRI Winter International Conference on Engineering and Technology. The Atlantis Press, pp.27-32.

[12] Tongwook Hwang, Youngsang Shin, Kyungho Son, Haeryong Park," Virtual Machine Introspection Based Rootkit Detection in Virtualized Environments", Life Science Journal 2014;11(7).pp.803-808

[13] Tal Garfinkel, Mendel Rosenblum, "A Virtual Machine Introspection Based Architecture for Intrusion Detection" Computer Science Department, Stanford University,2003.

[14] U. Oktay and O.K. Sahingoz, "Attack Types and Intrusion Detection Systems in Cloud Computing",6th International Information Security and Cryptography Conference, Turkey, Sept. 2013.pp.71-76