

A Novel Approach for Intrusion Detection and Prevention Technique for Cloud based on FVM Approach

Rameshwari Malik
M.Tech Scholar
Gurgaon College of Engineering,
Gurgaon, Haryana

Pramod Kumar
College Guide
Gurgaon College of Engineering,
Gurgaon, Haryana

ABSTRACT

Cloud computing visualize as the next generation computing technique for Information technology due to advantages provided by this technology. Cloud computing solutions are scalable, advanced and low cost. Its nature is distributed as cloud, it is indefensible to a large category of attacks are very frequent. Security is major challenge in cloud computing .This paper proposed the creation of FVM(forensic virtual machine) so that each virtual machine can be used as different security issue and which security issue have high probability can be classified using Bayesian classifier .An intrusion detection system proposed for monitoring the network against malicious attack . In this paper malicious attacks divided into three major categories first FVM used for detect unauthorized access, second used for malicious nodes and third one for IDS activity.

Keywords

Cloud computing, IDS, Bayesian classifier, SVM

1. INTRODUCTION

In the last decade, most people were concerned about obtaining computers in their offices, schools and homes. The main reason behind that was to get close to the world and communicate and exchange data via these devices. In contrast, today people are concerned about the Internet and its speed for effective and efficient communication. In addition, often they need extra services to the existing legacy service provided by the Internet. These services are known as some kinds of computing tasks that are delivered by the Internet Service Providers (ISP).

While getting required service is the users' demand, with the advanced development of the Internet tools around the world, attackers also aim to identify various loopholes in the operating system and networks. When we talk about Clouds, the main target of the attackers is to make illegitimate and unlawful attack to the available resources in the Cloud computing settings. In order to overcome these obstacles, some actions need be taken in the host based (HB) and network based (NB) level. Even though the use of intrusion detection system (IDS) is not guaranteed and cannot be considered as complete defense, we believe it can play a significant role in the Cloud security architecture [1]. Some organizations are using the intrusion detection system (IDS) for both Host Based and Network Based in the Cloud computing [2].The security protocols implemented to identify intrusions can be broadly summarized into the following: Intrusion detection systems (IDS) which are hardware and/or software mechanisms that detect and log inappropriate, incorrect, or anomalous activities and report these for further investigations [3].Intrusion Prevention Systems (IPS), which contain IDS functionality but more sophisticated systems that

are capable of taking immediate action in order to prevent or reduce the malicious behavior [4]. Thus, this work utilizes both systems: (IDS) and (IPS) and refers to it as Intrusion

Detection and Prevention System (IDPS). Furthermore, many works have been done in using one of the (IDS) techniques; either Anomaly Detection (AD) or Signature based Detection or hybrid of both. The ADS (Anomaly Detection System) can be used to detect unknown attacks in the networks which come from rogue nodes. In fact, such system is designed for the offline analysis due to their expensive processing and memory storage. On the other hand, the SD is used in this system to detect and identify manually the attack signature which is known as attacks in the real time traffic [5]. Therefore, both methods are essential in detecting the intrusions. So, we propose an hybrid scheme which makes use of both methods to detect the attacks as soon as possible and prevent the attackers from generating the malicious activities inside the Cloud.

Cloud is a prime target for malicious activities. There is a clear requirement to develop an automated and computationally inexpensive method of discovering malicious behaviorIt is also common for malware to abort processes such as anti-virus systems to prevent detectionIt is argued that as the Cloud is intended to handle large amounts of data, attackers can be sure of a high pay-off for their activities. This makes the Cloud a prime target for malicious activities.Cloud does not have any model which is tight enough to be adopted for real-time estimation of the target locationThere is a plethora of security concerns in cloud computing which still need to be tackled (e.g. confidentiality, auditability and Privileged User Access).

2. PRELIMINARIES

A. Cloud Computing

Cloud computing refers to the provision of computational resources on demand via a computer network. Users or clients can submit a task, such as word processing, to the service provider, such as Google, without actually possessing the required software or hardware. The consumer's computer may contain very little software or data (perhaps a minimal operating system and web browser only), serving as little more than a display terminal connected to the Internet. Since the Cloud is the underlying delivery mechanism, Cloud based applications and services may support any type of software application or service in use today [6]. The essential characteristics of Cloud Computing include [7]:

- On-demand self-service that enables users to consume computing capabilities (e.g., applications, server time, network storage) as and when required.
- Resource pooling that allows combining computing resources (e.g., hardware, software, processing, network

bandwidth) to serve multiple consumers - such resources being dynamically assigned.

- Rapid elasticity and scalability that allow functionalities and resources to be rapidly and automatically provisioned and scaled.
- Measured provision to optimize resource allocation and to provide a metering capability to determine usage for billing purposes Extension to existing hardware and application resources, thus, reducing the cost of additional resource provisioning.

B. FVM

FVMs are small Virtual Machines (VM) that can monitor other VMs to discover the symptoms in real-time via Virtual Machine Introspection (VMI). FVMs are small; each FVM is dedicated to identifying only one symptom. As a result, the crucial part of the code within the FVMs can be manually inspected. In addition, FVMs exchange messages via secure multi-cast channels to share information about the discovery of symptoms within the VMs. This allows the FVMs to conduct distributed monitoring; if an FVM detects a symptom in a virtual machine, it will inform other FVMs to come to its assistance in order to detect the presence of other symptoms. The more symptoms are detected, the more we can be sure of the possibility of malicious behavior. The FVMs report to a C&C centre that collects and collates the information. The FVMs, C&C and communication channel act as an autonomous system for dynamic defense. The C&C module can use the virtualization mechanism to “freeze” the VM by denying it any CPU cycles, effectively stopping the malicious activity. The memory will remain frozen until it can be quickly reviewed or alternatively can be copied for a complete forensic analysis.

C. Intrusion detection system (IDS)

Intrusion detection System monitors the violation of management and security policy and malicious activities in the computerized network. The intrusion can be caused by inside (legal users), or outside (illegal users) in the system. Nowadays recognition and prevention of intrusion is one of the most important mechanisms that provides security in networks and computer systems, and generally is used as a complemented security for firewalls. IDS systems created as a software and hardware system that each one has its specific properties. Hardware systems have been preferred to software system because of their speed and accuracy. But software systems are more common because of high compatibility with several operating systems

Intrusion detection techniques are usually classified into misuse detection and anomaly detection. Anomaly detection focuses on detecting unusual activity patterns in the observed data. Misuse detection methods are intended to recognize known attack patterns. Signature-based misuse detection techniques are currently most widely used in practice; however, interest is growing in the intrusion detection community to application of advanced machine learning techniques. Not uncommon is also a combination of anomaly and misuse detection in a single intrusion detection system

D. Intrusion prevention system(IPS)

The IPS classification system would depend on the platform of technology and detection of system. The operation platform has the general classification of IPS into the NIPS and the HIPS. There is a relativity of HIPS on the installation of the

network hosts and protection against the malwares. The IPS helps in keeping the system free from attacks and in the inspection of attack in real time. The detection mechanism takes into perspective the vulnerabilities of the frequently used programs and the detection of unusual activity that is there according to the connection sequences or the possibility of traffic. Additionally, IPSs are different types of additions that are related with the functioning of IDS, because of the monitoring of traffic for each of the systems for network traffic, along with the prevention of risks. The main kind of difference among them is the fact that the intrusion detection system is installed in-line with process and has the ability of blocking specific kinds of intrusions that have been detected.

E. Bayesian approach

The methodology provides a cost-effective solution to complement the existing surveillance systems, using the available wireless infrastructure and thus augmenting localization services without the costly (and unfeasible for logistic reasons) deployment of new equipment. The model, combined with target motion prediction, has been used to cast the localization problem into the framework of Bayesian estimation. Device-free localization can be used to track objects or malicious nodes moving in areas covered by a dense cooperative wireless network.

3. RELATED WORK

Adrian L. Shaw [8] research on Forensic Virtual Machines on Cloud attempts to provide its users with automatically scalable platforms to host many applications and operating systems. To allow for quick deployment, they are often homogenized to a few images, restricting the variations used within the Cloud. It is also common for malware to abort processes such as anti-virus systems to prevent detection. They view unusual changes to the registry and aborting processes as examples of symptoms of malware. Symptoms are different from malicious behavior; symptoms are detectable traces of activities that facilitate a malicious activity. There is a clear requirement to develop an automated and computationally inexpensive method of discovering malicious behavior as soon as it starts, such that remedial action can be adopted before substantial damage is caused. FVMs are small Virtual Machines (VM) that can monitor other VMs to discover the symptoms in real-time via Virtual Machine Introspection. FVMs are small; each FVM is dedicated to identifying only one symptom. As a result, the crucial part of the code within the FVMs can be manually inspected. In addition, FVMs exchange messages via secure multi-cast channels to share information about the discovery of symptoms within the VMs. This allows the FVMs to conduct distributed monitoring; if an FVM detects a symptom in a virtual machine, it will inform other FVMs to come to its assistance in order to detect the presence of other symptoms.

Robert John [9] research on the production of alerts by IDS, which is based on the true alarms where there is an instance of intrusion; however, there is a case of false alarms in case of detection by the systems, as the issue of ID can be judged by the degree of the identity and the lesser number of false alarms. Additionally, there can be the detection of intrusion patterns by the inspection of network packets through the use of signatures (pre-defined rules) and generation of alarms for system administrators. In looking at these methods of detection techniques

To build an IDS:

- Study the effectiveness of cloud computing.
- Specify a proper service and type of cloud computing.
- Determine the main security issues
- Measure the complicity of the most common attacks
- Identify the scenario and proper way of detecting DDoS attack and its method to apply the IDS in cloud.
- Specify the proper applications that should run on the system from the participants point of view

Monica Nicoli [10] proposed where both the average path-loss and the fluctuations of the received signal strength induced by the moving target are jointly modeled based on the theory of diffraction. A novel stochastic model is derived and used for the evaluation of fundamental performance limits. The model is proved to be tight enough to be adopted for real-time estimation of the target location. The proposed localization system is validated by extensive experimental studies in both indoor and outdoor environments. The model calibration is addressed in practical scenarios to compare the performance of different Bayesian online localization methods. The test-bed system supports efficient and flexible target tracking, without requiring any action from the end-users. In addition, the technology is proven to be readily applicable over the existing IEEE 802.15.4 compliant PHY layer standard, by adapting the low-level MAC firmware.

ShubhashisSengupta[11]studies aboutCommon security issues around cloud computing across four main categories:

Cloud infrastructure, platform and hosted code: This comprises concerns related to possible virtualization, storage and networking vulnerabilities. We cover vulnerabilities that may be inherent in the cloud software platform stack and hosted code, which gets migrated to cloud. We also discuss the physical data- center security aspects here.

Data: This category comprises the concerns around data integrity, data lock in, data remanence, provenance, and data confidentiality and user privacy specific concerns.

Access: This comprises the concern around cloud access (authentication, authorization and access control or AAA), encrypted data communication, and user identity management.

Compliance: Because of its size and disruptive influence, the cloud is attracting attention from regulatory agencies, especially around security audit, data location; operation trace-ability and compliance concerns.

Jun Ho Lee [12]done research on Multi level IDS method leads to effective resource usage by applying differentiated level of security strength to user based on the degree of anomaly. It is true that cloud computing is easy target of attack. For this reason, it is possible to judge all users and administrators as potential attacker and apply strong security policy to all traffic, but it is not efficient at all. So deal with the threat according to the level of anomaly.

Rui Xia[13]studies thatthere is various threats which should be taken care and malicious activities which are hard to detect like threats from the fellow user or by other customers. Availability and reliability issues and integrating provider and customer security systems.

4. PROPOSED WORK

The system architecture consists of FVM, IDS and IPS module and Bayesian Classifier. Firstly we proposed Forensic virtual machine to detect different types of malicious activities .Each forensic virtual machine have different purpose. First FVM detect malicious node on network with the help of intrusion detection system (IDS).Second FVM detect unauthorized access on network and third FVM used for IDS activities.

Design of FVM

1) FVM only reads: Virtualization allows both reading and writing into a VM. As a design principle, our FVMs never alter states of a VM. This ensures the integrity of the operation within the VM and also allows searching for malicious behavior while remaining hidden from hackers.

2) FVMs are small; one symptom per FVM: We design the FVMs to be small so that the clients can manually inspect their code and make sure of their integrity. In addition, although it is possible to create super size FVMs, in the interest of clarity, each FVM is designed to deal with identifying a single symptom. Creating small FVMs is a key step towards ensuring that our suggested symptom detection scheme is not introducing an easy attack vector into the overall system.

3) FVMs inspect one VM at a time: To avoid any possibility of leakage of information, an FVM will inspect only one VM at a time and will flush its memory before leaving to inspect another VM.

4) Secure communication: FVMs communicate with each other and the management system via sending messages through a secure multicast channel.

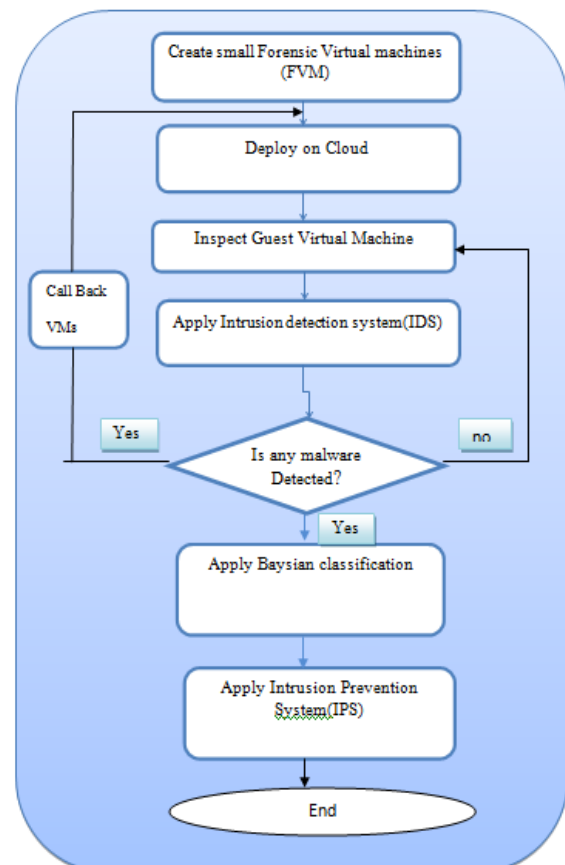


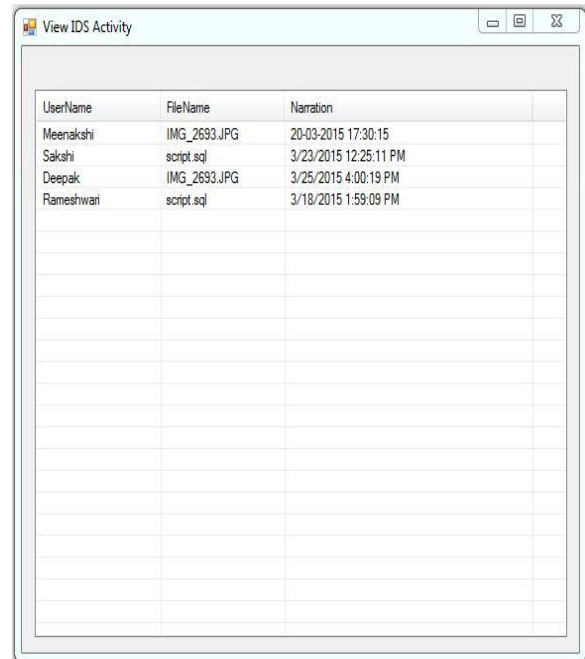
Fig1: Purposed system Structure

If any external VM tries to attack on network than FVM detects its activities and send this information to IPS(Intrusion prevention system).If any malicious activity have high probability than classified by Bayesian classifier and send this attack to IPS.IPS not only detect as well as prevent the cloud network. An overall architecture of proposed work given in figure1

5. IMPLEMENTATION DETAIL& RESULTS

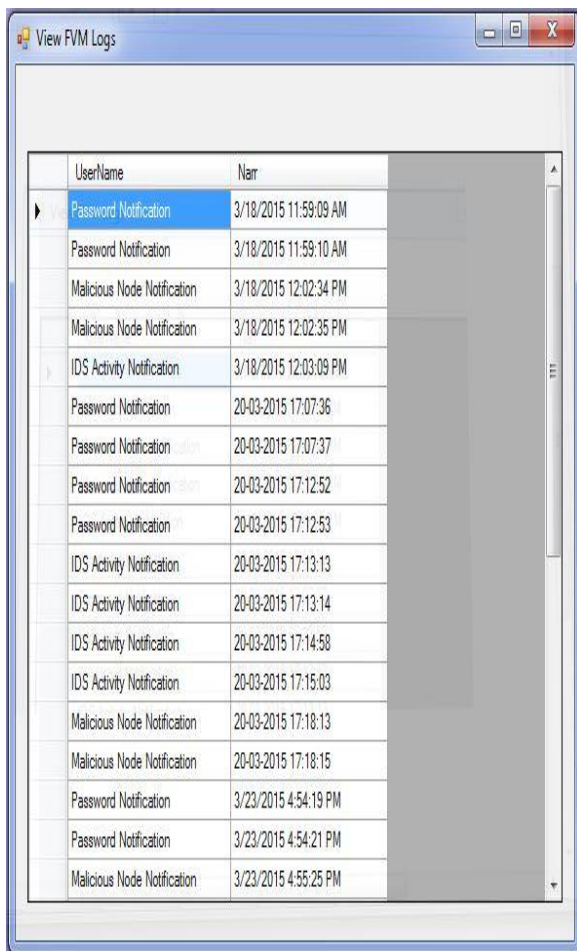
In our experiment, first we create FVMs for our cloud for security purpose. We developed three types of forensic virtual machine for different observation on guest virtual machines.Registered client over cloud is authenticated VMs. If any malicious or unauthorizedVM try to access or download or upload any file than IDS FVM create logs and send to server for detect malicious probability on the basis for frequency. With the help of Bayesian classification we classify more frequent malicious activities and send this report to IPS system for prevention.

1.) **IDS Log Creation:** Alog file has been created by IDS FVM for detection of malicious activity .If any guest VM does not perform any action over cloud and remains ideal then these types of VMs are prime target for malicious activities. That is why any guest VM which remain ideal or try to access over cloud it assumed malicious by IDS FVM. With the help of log file we measured the frequent VMs probability with the help of Bayesian classification and defined as malicious node.



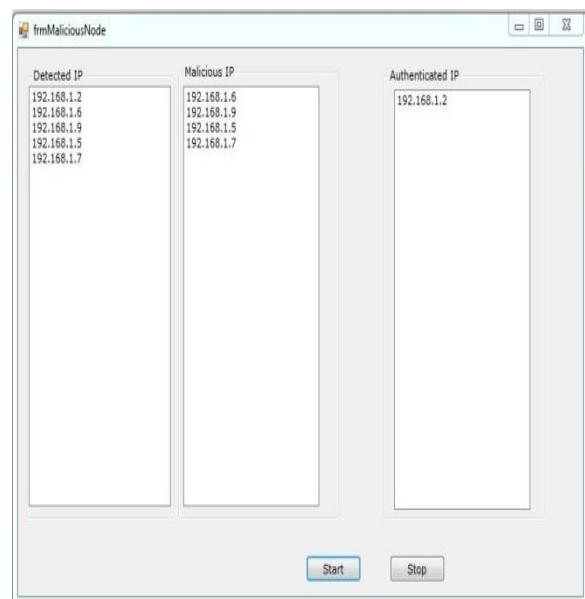
UserName	FileName	Narration
Meenakshi	IMG_2693.JPG	20-03-2015 17:30:15
Sakshi	script.sql	3/23/2015 12:25:11 PM
Deepak	IMG_2693.JPG	3/25/2015 4:00:19 PM
Rameshwari	script.sql	3/18/2015 1:59:09 PM

Fig3: Detection IDS activities



UserName	Narr
Password Notification	3/18/2015 11:59:09 AM
Password Notification	3/18/2015 11:59:10 AM
Malicious Node Notification	3/18/2015 12:02:34 PM
Malicious Node Notification	3/18/2015 12:02:35 PM
IDS Activity Notification	3/18/2015 12:03:09 PM
Password Notification	20-03-2015 17:07:36
Password Notification	20-03-2015 17:07:37
Password Notification	20-03-2015 17:12:52
Password Notification	20-03-2015 17:12:53
IDS Activity Notification	20-03-2015 17:13:13
IDS Activity Notification	20-03-2015 17:13:14
IDS Activity Notification	20-03-2015 17:14:58
IDS Activity Notification	20-03-2015 17:15:03
Malicious Node Notification	20-03-2015 17:18:13
Malicious Node Notification	20-03-2015 17:18:15
Password Notification	3/23/2015 4:54:19 PM
Password Notification	3/23/2015 4:54:21 PM
Malicious Node Notification	3/23/2015 4:55:25 PM

Fig 2: IDS FVM log file



Detected IP	Malicious IP	Authenticated IP
192.168.1.2	192.168.1.6	192.168.1.2
192.168.1.6	192.168.1.9	
192.168.1.9	192.168.1.5	
192.168.1.5	192.168.1.7	
192.168.1.7		

Fig4: Detection of malicious and unauthorized nodes by FVMs

6. CONCLUSION

Cloud computing is a fast growing technology over the internet, Hence security is the most important issue for concern about it .We proposed three FVM for different purpose for increasing it works on investigated and evaluated from three perspective vulnerability detection, Less overhead over cloud by using small FVMs, Increase privacy over cloud and enhanced efficiency by detecting malicious nodes using IDS. Finally, we showed that implementing our architecture is practical and feasible using current technology by implementing a prototype FVM IDS and demonstrating its ability to detect real attacks with acceptable performance.

7. REFERENCES

- [1] J. Mchugh, A. Christie, and J. Allen, “Defending Yourself: The Role of Intrusion Detection Systems”, *IEEE Software*, Volume 17, Issue 5, Sep.-Oct., pp. 42-51, 2000.
- [2] K .V .S .N .R .Rao , A. Pal, and M. R. Patra, “A Service Oriented Architectural Design for Building Intrusion Detection Systems”, *International Journal of Recent Trends in Engineering*, vol. 1, no. 2, pp. 11-14, 2009.
- [3] E – Banking - Appendix B : Glossary , [http : // www .ffiec .gov / ffiecinfobase / booklets / e_banking/ebanking_04_appx_b_glossary.html](http://www.ffiec.gov/ffiecinfobase/booklets/e_banking/ebanking_04_appx_b_glossary.html), Accessed on: 23/02/2012
- [4] Information Technology at Johns Hopkins – Glossary G-I, [http://www.it.jhmi.edu /glossary /ghi .html](http://www.it.jhmi.edu/glossary/ghi.html) , Accessed on: 23/02/2012
- [5] K .Hwang , M . Cai , Y . Chen , S . Member , and M .Qin, “Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes”, *IEEE transactions on dependable and secure computing*, vol. 4, no. 1, pp. 1-15, 2007.
- [6] P. Jain, D. Rane, and S. Patidar, “A Survey and analysis of Cloud Model-Based Security for Computing Secure Cloud Bursting and Aggregation in Renal Environment ”, *IEEE 2011 World Congress on Information and Communication Technologies*, pp. 456-461, 2011.
- [7] Z . Mahmood, “ Cloud Computing: Characteristics and Deployment Approaches”, 11th IEEE International Conference on Computer and Information Technology, pp. 121-126, 2011.
- [8] L. Shaw, BehzadBordbar, John Saxon, Keith Harrison, Chris I. Dalton. *Forensic Virtual Machines: Dynamic defence in the Cloud via Introspection Accessing*. *IEEE International Conference on Cloud Engineering*, 2014,UK
- [9] Robert John(UK), Saeed M. AlqahtaniMaqbool(UK) , Al Balushi(Oman).*An Intelligent Intrusion Prevention System for Cloud Computing (SIPSCC)*. *International Conference on Computational Science and Computational Intelligence*,2014
- [10] Monica Nicoli, Stefano Savazzi, Francesca Carminati, Michele Riva, *A Bayesian Approach to Device-Free Localisation: Modeling and Experimental Assessment*, *IEEE Journal Of Selected Topics In Signal Processing*, VOL. 8, February 2014
- [11] Shubhashis Sengupta , Vikrant Kaulgud, Vibhu Saujanya Sharma, *Cloud Computing Security - Trends and Research*, : *IEEE World Congress on Services*,2011
- [12] Jun Ho Lee , Min Woo Park , jung Ho Eom , Tai Myoung Chung,*Multi level Intrusion Detection System and Log Management in Cloud Computing*, *IEEE publishing* 2011.
- [13] Rui Xia, ChengqingZong, Shoushan Li, *Ensemble of feature sets and classification algorithms for sentiment classification*, *Information sciences* 2011