Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2013, Article ID 364575, 12 pages
http://dx.doi.org/10.1155/2013/364575

Research Article

A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment

Sanchika Gupta,[1] Padam Kumar,[1] and Ajith Abraham[2,3]

[1] *Department of Electronics and Computer Engineering, Indian Institute of Technology Roorkee, Roorkee, Uttarakhand 247667, India*
[2] *Machine Intelligence Research Labs (MIR Labs), Scientific Network for Innovation and Research Excellence (SNIRE), Auburn, WA 98071, USA*
[3] *IT4Innovations-Center of Excellence, VSB-Technical University of Ostrava, Ostrava-Poruba 70833, Czech Republic*

Correspondence should be addressed to Sanchika Gupta; dr.sanchikagupta@gmail.com

Received 2 December 2012; Revised 6 February 2013; Accepted 10 February 2013

Academic Editor: Sunilkumar S. Manvi

Cloud computing provides network based access to computing and data storage services on a pay per usage model. Cloud provides better utilization of resources and hence a reduced service access cost to individuals. Cloud services include software as a service, platform as a service, and infrastructure as a service. Cloud computing virtually and dynamically distributes the computing and data resources to a variety of users, based on their needs, with the use of virtualization technologies. As Cloud computing is a shared facility and is accessed remotely, it is vulnerable to various attacks including host and network based attacks (Brown 2012, and Grance 2009) and hence requires immediate attention. This paper identifies vulnerabilities responsible for well-known network based attacks on cloud and does a critical analysis on the security measures available in cloud environment. This paper focuses on a nonconventional technique for securing cloud network from malicious insiders and outsiders with the use of network profiling. With network profiling, a profile is created for each virtual machine (VM) in cloud that describes network behavior of each cloud user (an assigned VM). The behavior gathered is then used for determination (detection) of network attacks on cloud. The novelty of the approach lies in the early detection of network attacks with robustness and minimum complexity. The proposed technique can be deployed with minimal changes to existing cloud environment. An initial prototype implementation is verified and tested on private cloud with a fully functional implementation under progress.

1. Introduction

Cloud computing according to National Institute of Standards and Technology (NIST) is a service that is provided in the form of computing power and data storage, remotely over internet (network based access) with minimal efforts for resource allocation, management, and release [1]. The US National Institute of Standards and Technology (NIST) has captured five essential cloud characteristics which are [1, 2]

(1) on-demand self-service,

(2) ubiquitous network access,

(3) resource pooling,

(4) rapid elasticity,

(5) measured service.

Cloud computing provides three major services to its users at various layers of computing. These include [1] the following:

(1) software as a service, where a user buys software and application services from cloud service provider in the form of readily and frequently used software such as word processing and data processing software with user having control over its usage but not over the software working and operations,

(2) platform as a service, where a user is provided with a platform that can vary from backend supports (for user's own software to run over cloud vendor's space) to provisions for having support for uploading and using third party software on vendor's platform. Here, a user has full control on which software to run and

how the software will behave but has dependency on the platform support such as compilers, operating system, and execution frameworks provided by cloud vendor,

(3) infrastructure as a service, where a user will have a decent amount of control over the computing infrastructure and storage and he can decide which platform compilers, operating systems, and so forth and software he needs to deploy with full control over them.

With major service providers on the field such as Google, Rackspace, Amazon, and Microsoft cloud computing is one of the most popular forms of computing utilized by users nowadays [3]. The users vary from small companies that wish to use computing and storage infrastructures on a pay per usage model (generally infrastructure and platforms for deploying their own software products) to normal everyday internet users who want to use services such as software, data storage, and platform as a service remotely over internet [3]. The major facility that Cloud computing provides and that makes it different is that it is highly scalable form of computing and can be allocated, reallocated, and released with minimal managerial efforts [1].

The base of Cloud computing lies over virtualization technologies that provide a way to dynamically allocate virtual replicas of physical resources, including memory, processor, and other computing and storage resources. Many of the virtualization software provide facility for creating virtual replicas of physical resources including VMware [4], XEN, and Virtual Box. The virtual replicas provide a way through which users can access the single physical resource simultaneously which eventually increases the resource utilization. As Cloud computing is a remotely accessed form of service and is used by various users, it is vulnerable to attacks ranging from host based attacks to network based attacks and attacks on data storage [5–9].

Cloud environment is vulnerable to a large number of attacks because of the vulnerabilities present in it due to its distributed nature [5, 6]. We have identified vulnerabilities that lead to threats for cloud network environment. The motivation for network attack detection lies in the fact that there is a rapid increase in the number of network based attacks in cloud. We have gathered the statistics of well-known network attacks on cloud that are launched recently. These include the following.

(1) The Dropbox (which is a well-known cloud based file sharing facility) getting hacked in July 2012 [10], in this attack, the user personal information which was hacked by attacker from third party websites is used to access Dropbox accounts of users. According to Dropbox, the user name and passwords stolen from other websites about a user are tested on Dropbox accounts. In a large number of the attempts, hackers got success.

(2) Attack on Sony PlayStation network which is the second largest attack in US history: this attack took place on May 13, 2011 and has breached online data of Sony PlayStation network [11].

(3) Attack over Amazon EC2 cloud: this attack took place in October 2009 and caused Bit Bucket's servers down for 19 hours [12, 13].

(4) Stratfor (a well-known geopolitical analysis service provider) found its servers breached in the last quarter of 2011 [14].

(5) In 2011, an attack on Epsilon (an email marketing company) led to leakage of user credentials such as their names and email addresses through penetrating their customer databases [15].

All such cloud network attacks are a combination of well-known basic network attacks in a specialized manner. We have categorized all such attacks that play as ingredients for specialized cloud network attacks. The well-known and possible network attacks from malicious insiders, users, and outsiders on cloud and the vulnerabilities associated with them are shown in Table 1.

2. Related Work

2.1. The Present Scenario. Various different measures to improve the security of network of either distributed or standalone systems are already known to be researched, proposed, and deployed. Some of the measures include firewalls, network intrusion detection, and prevention systems.

The concept of intrusion detection was known since past and was first proposed by a well-known researcher named Anderson in 1980s [30]. Since the concept was very effective in increasing the security measures of end systems, it gets popularized and now is used and applied in various domains of security.

Since past various intrusion detection and information security approaches for securing Cloud have been proposed and are in practice [27, 31–42], but the concept of network intrusion detection and prevention systems and its deployment strategies over cloud infrastructure, which will be efficient and lightweight, is still going on, because cloud vendors are also interested in a solution that can be deployed and maintained at low cost [5]. Summary of some of the research work carried out in the area of network intrusion detection and prevention in cloud is as follows.

Table 2 provides an abstract description of the work done by the researchers in the area of network intrusion detection in cloud. The table describes the problem areas identified by the researches which are followed by the brief description of the scheme. The table also provides information about the drawbacks of the schemes over cloud with their performance analysis.

2.2. Research Gaps Identified

(1) Existing schemes that do network intrusion detection without VM Profiling are complex as they look for all kinds of attacks on every VM irrespective of the fact that some VMs never launch them.

Table 1: Cloud network attacks and vulnerabilities.

Cloud network attack	Source	Description	Effects	Vulnerabilities and root cause
DoS and DDoS [4] SYN flooding attack (TCP SYN flood) Smurf attack (ICMP flood) Ping of death (ICMP flood) Low rate Denial-of-service attacks (TCP's slow-time-scale dynamics of RTO)	Outside attackers, malicious insiders, and Cloud users	This is an attack over cloud networking environment that either disrupt or degrade the service or make the network unusable for the Cloud users through unwanted packet flooding	Degrade network service to cloud users or completely make it unusable during the time it is active	Vulnerabilities in network protocols, undetected spoofing not handling packets flooding of a particular type
TCP session hijacking [16]	Outside attackers (generally), but can also be fired from malicious users and insiders	In this type of attack, an attacker steals, or hijacks, a session between a trusted client on cloud and the cloud network server	Can disrupt the normal usage of cloud services and will affect the quality of service User session secret information can be accessible through the session hijacking activities	Failing to detect IP spoofing Network sniffing to obtain TCP session information
Reused IP addresses [17]		In cloud dynamically provisioning of network resources, the IP address associated with a user is assigned to a new user when the old user moves out of a network	Some other user will access the data as the address still resides in the DNS caches Some attacks that are targeted on the IP address of the previous user cause the new user to face the problem	Delay in management of DNS caches Failing to identify frequent communications
DNS attacks [17]	Outside attackers, malicious insiders, and malicious Cloud users	If through some means a malicious user or insider is able to change the internal mapping the naive users will be directed to malicious locations for getting access to resources	If the mapping of cloud's login website is manipulated in global DNS which is considered as a change in external mapping will result in loss of user's personal information because of entering it into deceptive websites	Failing to detect malicious communication with privileged facilities such as DNS
Network penetration [18] IP random options, SMB session mixing, TCP urgent pointer, and MSRPC object reference	Outside attackers (generally), but can also be fired from malicious insiders and users	Network penetration is an attack on cloud, in which the attacker tries to penetrate the network infrastructure by evading the network security measures through advanced network evasion techniques	Some of the techniques include port scanning which looks for specific open ports and gathers information about the system, so that further specific network attacks can be launched	Vulnerabilities in network protocols
Fragmentation attack [19] Tiny fragment attack, overlapping fragment attack	Outside attackers (generally), but can also be launched by malicious insiders	IP fragmentation is the process of breaking down a single IP datagram into smaller packets to be transmitted to different locations. IP fragmentation attacks use various IP datagram fragmentations to disguise their TCP packets from a target's IP filtering devices	Uses all the memory resources in a virtual system and renders the machine unusable	Undetected subverted packets

Table 1: Continued.

Cloud network attack	Source	Description	Effects	Vulnerabilities and root cause
Traffic analysis [20] Deep packet inspection	Malicious insiders and users	Traffic analysis is a technique in which a malicious user or insider analyses the internal or external network and extracts the information about the traffic by interpreting the unencrypted portions of the traffic	This can help them to launch more specific attacks such as TCP hijacking	Failing to identify unidentified and bulk unwanted communications of insiders and cloud users
Passive eavesdropping [21]	Malicious insiders and Cloud users	The attacker simply monitors the traffic traversing the network and may store it for further analysis afterwards	This can help an insider to obtain the information about the network utilization with the information flowing over network from a specific set of cloud users that can help them plan their activities targeted over them	Failing to identify bulk unauthorized communication
Active eavesdropping [21]	Malicious insiders, Cloud users	In this type of attack, the attacker can either modify a packet being transmitted or can inject a new packet into the cloud network	Goal of the attacker is to prevent the authentic packet from reaching its authentic destination. One of the methods for accomplishing this is to modify a packet's destination IP address while in transit	Unidentified communication sessions

(2) A Normal analysis which includes detection of all well-known attacks from data coming from a large group of VMs on cloud infrastructure is inefficient in the sense that it will waste computing resources for detection of attacks that never happen from a large group of authentic virtual machines.

(3) Proposed schemes that deploy IDS at individual virtual machines are vulnerable to host manipulation attacks. Host can subvert the individual IDS or sensors deployed at any virtual machine which will make it difficult to detect network intrusions.

(4) Intrusion detection systems which are either signature based or anomaly based are not robust and efficient. This is because signature based detection cannot detect new attacks on the cloud while anomaly based detection systems are not very accurate. Hence, a combination of both is a requirement.

(5) There is no concept of ranked detection earlier, that can possibly decrease the amount of time it takes for detecting and responding back to network intrusions in cloud.

The above finding demonstrates the fact that there is an immediate need for a new concept of network intrusion detection for cloud environment that will take the benefits of both signature and anomaly based detection systems with added use of VM profiling that will make it efficient low cost and more responsive in case of frequent and well-known network attacks.

3. The Profile Based Network IDS

Based on the research gaps identified in previous techniques, we have provided a novel architecture for securing cloud towards network based attacks. Our proposed profile based network intrusion detection system is a novel architecture for detecting intrusion from virtual machines (internal entities such as malicious cloud users and insiders) and external entities (outside attackers) on a cloud infrastructure. Our research focuses on providing robust security to cloud network with minimized cost. The cost is in terms of computational power, storage, and communication cost. We have designed and developed a prototype implementation of profile based (anomaly cum signature based) intrusion prevention system for cloud networking infrastructure that will reside in privileged domain and will detect, prevent, and respond to commonly known cloud network attacks.

In our proposed architecture, the total network traffic at privileged domain is filtered based on VM's IP addresses. Network intrusion detection is performed on the packets coming from a particular virtual machine based on its profile. A VM profile describes the attacks that are possible on it for, for example, a VM profile may have entries (thresholds) that

Table 2: Description of previous techniques.

Title	Problem areas identified	Brief description	Drawbacks	Performance analysis
A cooperative IDS Framework for Cloud computing networks [22]	To reduce the impact of denial of service (DoS) and distributed denial of service (DDoS) attacks, to introduce cooperation in intrusion detection system (IDS)	Idea of cooperative IDS in cloud IDS deployed in each Cloud computing region IDS cooperates and exchanges alerts to reduce DDoS impacts	This architecture provides intrusion detection only at Cloud provider's end and not at client's end.	Increase little effort compared with intrusion prevention system (SNORT) but prevent the system from single point of failure
Intrusion detection in the cloud [23]	Operator of the IDS should be the user, not the administrator	An extensible IDS management architecture is proposed, with several distributed intrusion detection sensors deployed and a single central control and management unit	The output of different sensors is not standardized due to different technologies and formats	Extensibility, efficient management, and compatibility to virtualization based context
Multilevel IDS and log management in Cloud computing [24]	More secure cloud, more resources for computation Huge amount of log entries	Method is proposed that enables Cloud computing system to achieve both effectiveness of using the system resource and strength of the security service without tradeoff between them	The solution is cost effective; however, such reduction in network and file monitoring modules require consideration for complete solution However, reduction in resources when complete solution is deployed will be a question	Effective resource usage and economical cost reduction
Integrating a Network IDS into an open source Cloud computing environment [25]	Risks introduce due to resource sharing requirement Misconfigured remote data storage which exposes user's private data	The issue of detecting denial-of-service attacks targeting session initiation protocol (SIP) flooding attack instances targeting services hosted within a cloud is addressed	The detection process is expensive, overloaded Cluster controller (CC) is a bottleneck and during the attack other virtual machines (VMs) running concurrently with the attacked one underwent performance degradation	When a single IDS is placed close to the CC, it is able to monitor all traffic flowing to and from the cloud but the single IDS is heavily loaded thus allowing for coordinated attack
Twin Clouds: an architecture for secure Cloud computing [26]	For secure computation techniques available Fully homomorphic encryption—low efficiency Tamper-proof hardware—expensive and relatively slow	The architecture proposed consists of two clouds (twins) A trusted cloud and a commodity cloud; further the Security critical operations are performed by the trusted cloud and performance critical operations are performed on encrypted data by the commodity cloud	The concept of division of operations and its handling by different clouds require major concerns The deployment and maintenance of such architecture of cloud will require noticeable changes in the underlying infrastructure that may raise questions on its performance and acceptance in real-world scenario	Maximum utilization of expensive resources of the trusted cloud High loads of queries are processed on demand by commodity cloud
A VMM based intrusion prevention system in Cloud computing environment [27]	File integrity monitoring, network defense	Proposed VMFence in a virtualization based Cloud computing environment, which is used to monitor network flow and file integrity in real time	More computationally complex as it checks for attack patterns from data coming via all VMs connected to the privileged domain	Useful for a virtualization based Cloud computing environment, especially for multicore CPU

Table 2: Continued.

Title	Problem areas identified	Brief description	Drawbacks	Performance analysis
Intrusion analysis with deep packet inspection: increasing efficiency of packet based investigations [28]	Efficient deep packet inspection scheme	Described the effectiveness of a utility that was developed to improve retrospective packet analysis which was tested against actual data center traffic from a large ISP providing cloud services	The concept of deep packet inspection for network security attack detection works efficiently for small and simpler enterprise networks	Deep packet inspection scheme will demand a decent amount of resources which will make the concept have concerns in its real-time implementations
Intrusion detection system in Cloud computing environment [29]	Instance based IDS. reducing load	Proposed IDS in which each instance of the IDS has to monitor only a single user Advantage of having fewer loads on single IDS, and hence, the number of packets dropped will also be less	The host can subvert the individual IDS deployed at any VM which will then not be able to detect network intrusions	Individual IDS must have to follow the same set of standards for information communication

dictate that a TCP SYN flooding attack is frequent from it to other VMs on the cloud infrastructure, or it is facing SYN floods from the external world or from other Cloud VMs. This information is gathered by the analysis of signatures of TCP SYN flooding attack in VM network traffic for a period of time. This information is gathered during the initial phase when the VM is assigned to a user and is working in its normal behaviour.

It contains parameters that describe VM's normal incoming and outgoing network traffic behaviour. Hence, whenever packets coming from that VM are collected, they are first analysed for TCP SYN flooding attack, if they are the most frequent attack pattern on that VM. This profile also ranks attacks on the basis of their frequency for, for example, if a particular VM is responsible for TCP SYN flooding attack more frequently than any other attack that is launched from it (in previous history), then it will be analysed first for TCP SYN flooding attack patterns in the traffic than for any other attack pattern. The historical information resides in the profile that ranks the attack patterns and is dynamic in nature. The recently detected attack signature is ranked the highest one in the profile, and the network traffic is detected for attack patterns based on the pattern rank. Hence, the attacks, which are more frequent will be analysed first as they are highly ranked than other signatures in the attack signature db. Also VM profiling helps in developing efficient IDS as VM's traffic is not analysed for all the attacks but only for those attacks which are frequent from them.

This profile of well-known attacks from a virtual machine is created on the basis of anomaly detection component. When a virtual machine is assigned and allocated, the virtual machine traffic is analysed through an anomaly detection component. If an anomaly is detected, the profile of that virtual machine is updated with the attack pattern detected. When an entry is made for that attack in the profile of a virtual machine, the analysis component is informed not to analyse the traffic for known attack patterns on the data coming from that virtual machine for adding them in VM profile as they already exists in the database. But anomaly detection components update the rank of the attack based on the frequency or probability of the attack from VM network behaviour. This anomaly detection component also stores the network characteristic of a particular VM such as bandwidth utilization, packet loss rate, and connection type (secure or not) with signatures of well-known attacks possible or can be launched from that VM as obtained from attack signature db.

Our proposed scheme is deployed at cloud administrator or the privileged cloud service monitor virtual machine which administers and detects attack patterns from other virtual machines allocated to cloud users. Our analysis shows that VM profile based detection increases efficiency and robustness compared to other intrusion detection or prevention architectures. VM profile based network intrusion detection system component collects network packets coming from virtual interfaces of various VMs. As the virtual network interfaces of virtual machines are connected through virtual bridge which privileged domain can access, installing a network packet sniffer on privileged domain is an easiest way to sniff packets for detecting intrusions. Our scheme for detecting intrusions is different from existing network intrusion detection systems as it takes care of virtual machine profile while analysing network packets for intrusion. Virtual machine profile defines what network attacks a virtual machine is vulnerable to with thresholds of the frequent attack patterns detected with their rank.

This helps the intrusion detection component to apply checks only for those intrusions that are possible on a particular virtual machine. VM profile creation, management, and updation will be performed by policy manager component of S-ProIPS. The efficiency is achieved by checking attack patterns on network traffic from a VM only for frequently happening or most probable attacks instead of searching all attack patterns possible. Hence, this will reduce rigorous detection for all attack patterns on the data coming from all

VMs even when a large population of VMs are not involved and also are not a victim of such attacks in normal network behaviour. The robustness is achieved as if some specific attack happens over a VM for the first time, it will get detected through the general network security checks applied over data coming from all VMs and newly detected attacks will be added to the VM profile with needed parameters for further detection in future. A common database that contains signature of basic attacks such as packet flooding and which detects abnormal spikes in network traffic always runs in background and contains minimal signatures for pattern matching over all network data which makes this technique a complete one. Our network intrusion detection system is anomaly cum signature based. Whenever a new VM is assigned to a user, its empty profile is created in the VM profile db this is the database for storing VM profile information.

VM profile is a tuple consisting of various features that can be added automatically on the basis of intrusions a particular VM can launch or can suffer in cloud infrastructure. Now, the network packets coming from VMs are analysed for well-known network anomalies, and if an anomaly is detected for a particular VM, its profile is updated with the signature ID of the anomaly detected, which is present in the attack signature db. If such a signature is absent in the attack signature db, a new rule is added in the database. The VM profile is also updated with the parameters needed to detect such intrusions in future. For, for example, a scenario can be as follows: a user (malicious insider or cloud user) does a TCP SYN flooding DDoS attack from a particular VM. The anomaly detection component detects the attack and updates the empty profile of that user with signature ID of TCP SYN flooding attack already present in Attack Signature db. One of the parameters that can be added for such a frequency based attack is threshold. Hence, the VM profile will have a defined value of threshold for detecting a TCP SYN flooding attack on it.

After profile creation, the data (network packets) obtained from that virtual machine is looked for attacks whose signatures are present in VM profile database and match them with attack signature db, and if a match occurs, it sends this information to detection and notification component. After checking for known attacks in a ranked manner, the data from that virtual machine is analysed for anomalies other than signature entries present in attack signature db. Detection and notification component (alert & response) detect the type of attack based on the information received from network intrusion detection system and generate appropriate responses and notifications to handle the attacks on cloud infrastructure. For, for example, responses can be shutting down a particular VM, if it is compromised and is generating DDoS attacks on cloud infrastructure. Notification includes generating and sending alerts to policy manager, so that policies for a particular VM can be updated to prevent such attacks in future. Policy manager (a part of alert & response generation component) can generate new policies and signatures and send them to VM profile db. Our goal is to develop an efficient intrusion detection system in cloud and profile based detection is a way to achieve the same. The design of the proposed architecture is shown in Figure 1. The description of profile based intrusion detection system working can be explained in terms of stages which are as follows.

3.1. Initial Profile Creation Stage. This is the stage which applies when new VMs are allocated to users in cloud. During this stage, the whole traffic from the newly allocated VM is passed through a rigorous checking of attack patterns for a particular time period that can be configured by the administrator. The attack patterns are present in attack signature db. Based on the attack patterns found in the traffic and based on the behavioral analysis of traffic patterns, a profile for a particular VM is created that explains the behavior of the network with probable attacks that it can launch towards other VMs. It also infers the attacks that are possible over that VM. The profile contains the unique identity of attack patterns (referred from attack signature db) that need to be checked on the traffic from that VM during network intrusion detection stage (normal traffic flow path). The description of the steps according to Figure 1 is as follows.

(1) In step 1, the network traffic coming from virtual network is gathered at virtual network interface present at the privileged VM.

(2) In step 2, the traffic is classified based on the virtual private IP addresses allocated to VM and passed to attack signature db. The attack signature db contains signature of well-known attacks. The VM is analyzed for patterns of attack that it can probably launch or can be vulnerable to in future, based on the behavior of network traffic it has. Like if, from the patterns of attack signature db, it is matched and analyzed that VM-1 generally fires a huge amount of ICMP echo request queries in a small time on cloud VM, there is a probability in future, that the VM can try ping flooding over other cloud VMs. Another example is when traffic of a VM has a huge amount of queries to other systems on certain ports which are used for obtaining system overview than there exists a possibility that cloud user or insider may try such queries over cloud operational systems such as privileged VM and routers to obtain necessary information for launching more severe attacks.

The profile db is updated with the signatures, so that the system will be analyzed for those attack patterns in ranked manner after which general attack patterns are searched for by network intrusion detection system. The traffic is routed to this path of a certain VM for a specified time interval that can be configured for a particular VM to obtain necessary profile information initially. The statistical behavioral analysis of the traffic is also analyzed in this stage and stored in the db that contains percentage of network bandwidth utilization, packet loss ratio, percentage of unencrypted traffic flow, and so forth. The major difference between the common signature detection in background with signatures getting matched through VM profile db is that the matching of attack patterns at VM through VM profile db is fast and more

Table 3: Demonstrating VM profile db for DDoS attack detection.

Attack pattern signature ID	Max. threshold/N packets	N packets	Rank for detection	Attack frequency on VM (in times)
0x0001 (TCP SYN)	50	500	2	600
0x0012 (UDP flood)	100	400	1	750
0x0023 (ICMP flood)	70	500	3	500

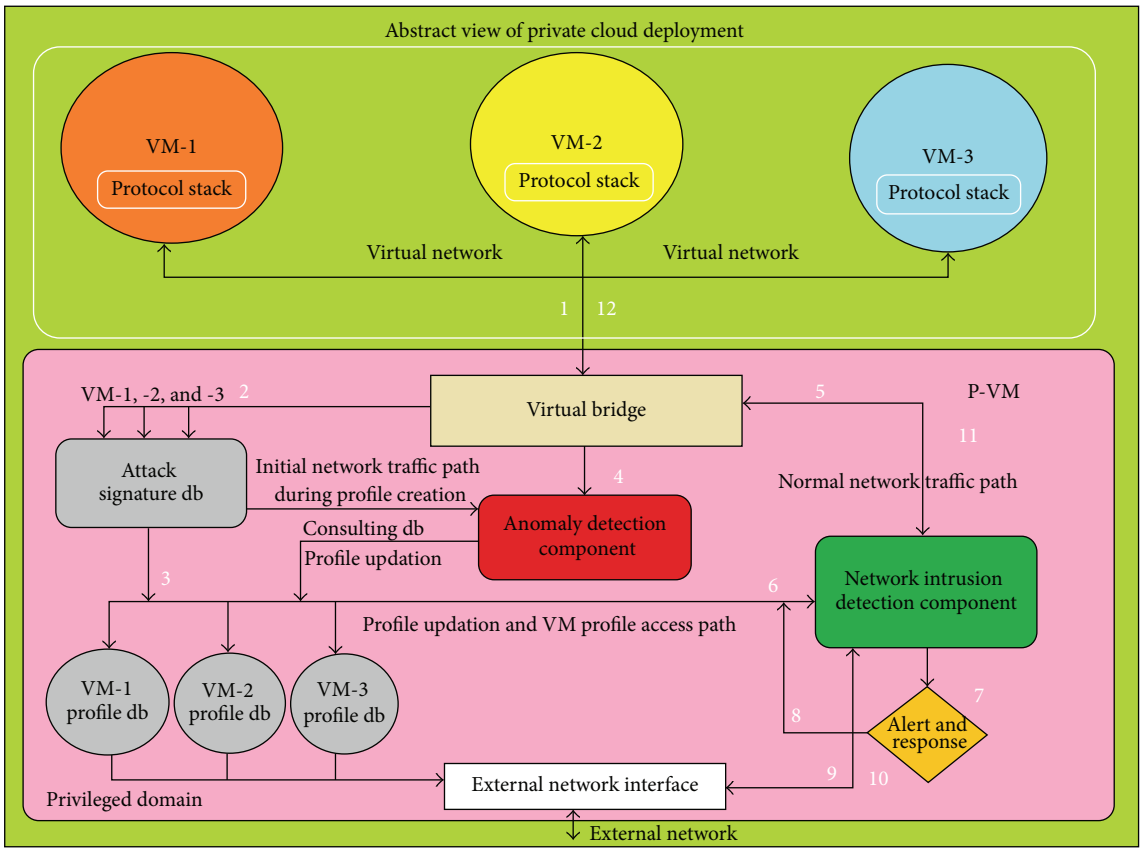

Figure 1: The design of profile based network IDS.

frequent compared to the detection of common signature in background at all traffics. This causes early detection of more frequent attacks and also completes detection of other attacks that are possible but with a saving of resources as the common signature matching is slow as it does rule matching operations after every N packet. It means it searches for attack pattern per N packet to identify intrusion saving resources in terms of pattern matching operations.

(3) In step 3, the values obtained by analysis on the network traffic are added to each individual profile of the VMs.

(4) The example VM profile db is shown in Table 3 which is specific to DDoS attack detection while Table 4 describes common attack signature db.

3.2. Anomaly Detection Stage. In the anomaly detection stage, the data from the normal traffic path is obtained from the virtual bridge of a VM and is checked consistently for other probable attack pattern behavior. So in this way, robustness is achieved, as after the VM profile creation in the first stage, the VM profile is updated based on the attack patterns as detected in the data coming from a particular VM. The concept lies in ranking the attack patterns in the profile db to improve the time taken for detection as the first attack pattern stored in profile db of a VM is the most probable attack that can be launched to or from other VMs. Also the statistical analysis updates the behavioral measures of network traffic that help in detecting anomalous network behavior over the traffic to and from a particular VM. This helps in detecting intrusions targeted from malicious outsiders towards that VM such as DDoS attacks. The steps are described as follows.

(1) In step 4, the data coming from virtual bridge is analyzed for network traffic coming from VMs for new attack patterns from attack signature db. Also the known attack patterns in the db are updated based on the frequency of patterns found in the db, so if their frequency is less, they are ranked less in attack signature db for their detection.

Table 4: Common attack signature db.

Attack pattern signature ID	Behavior in abnormal traffic pattern	Signature description for inspection (Perl)
0x0001 (TCP SYN)	>40/500 packets	If($TCP-> {"flags"}==SYN)
0x0023 (ICMP flood)	>65/500 packets	If($IPFRAME-> {proto}==IP_PROTO_ICMP)

3.3. Network Intrusion Detection Stage. In this stage, the normal traffic flow path from virtual bridge is obtained and analyzed for attack patterns from VM profile db. The traffic of each VM is analyzed for its statistical network behavior and attack pattern from its VM profile db. The anomaly or attack pattern (behavioral anomaly detection and attack pattern signature based detection) found is then reported to the alert and response generation component. The alert and response generation component generates alert and sends it to the administrator for further analysis, while in background it changes the ranking of attack patterns in the VM profile db with their parameters updated for efficient and timely detection of the similar attack for the next time. Various steps in Figure 1 during this stage are described as follows.

(1) Step 5 shows the outgoing connection to network intrusion detection component which will divide the flow into individual VM traffic for performing intrusion detection.

(2) Step 6 shows the access to VM profile db by the network intrusion detection component. Based on the specific attack patterns and their ranking in VM profile db, the network intrusion detection component checks the network traffic coming from a particular VM for attack patterns. It also checks the anomalous behavioral changes if any after consulting its statistical behavior over a period of time which is stored in VM profile db.

(3) Step 7 describes that the output of network intrusion detection component is passed to alert and response generation component if any anomaly or intrusion is detected.

(4) In step 8, the response is sent to VM profile db; the response includes increasing the ranking of a particular attack pattern as its occurrence is found and hence is more probable to come in future. Hence, its rank needs to be updated, so that it will be searched relatively earlier to ensure early detection of such frequent attacks.

(5) Step 9 shows the outgoing traffic from network intrusion detection component, if it is not containing general attack patterns, specific attack patterns as described by VM profile db and an anomalous traffic behavior.

(6) Step 10 shows the incoming traffic received by network intrusion detection component. This traffic based on the VM is addressed and analyzed and then passed to the virtual machine for which it is meant. Any anomalous behavior is passed to alert and response generation component.

(7) Step 11 shows the travel of the benign traffic to the virtual bridge which is then transferred to the virtual machine.

4. Results and Discussion

Currently, we have done a prototype implementation of the proposed work in private cloud and have assessed its effectiveness in terms of the network attacks it can prevent. The details of its prototype implementation with advantages are shown in the following subsections.

4.1. Prototype Implementation. The prototype implementation of the proposed work is in progress. We have analyzed the design and started working over it. We are using Perl 5.2.14 as our programming platform for sniffing packets from the virtual network interface of the Cloud network on the privileged domain virtual machine. The private cloud setup is using Open Nebula [43], and individual virtual machines are running variety of OS including Windows 7, 32 bit and Ubuntu 10. The traffic of all the VMs connected virtually through virtual network interface is sniffed using Perl well-known libraries for packet capture including Net: pcap [44] and others. The data of individual VM is analyzed for attack signatures present in attack signature db for prototype implementation; we have taken into consideration DDoS attack scenarios with SYN flooding to provide a proof of concept. The attack signature db contains signature as SYN packets with parameter as maximum number of SYN packets per N packets. This parameter is recorded during VM allocation with normal run. The maximum number of packets per N packets is from a collection of M runs of period of N packets each. The VMs are analyzed for both incoming and outgoing traffic packets for SYN packets. The initial profile for each VM for detecting this attack is created based on the pattern found. However, if during initial profile creation time it crosses some predefined well-defined threshold then immediate actions are taken during initial profile creation time only. In anomaly detection stage, the normal traffic is analyzed for a specified delta in the amount of TCP SYN packets in particular time frame. If the delta increases, the profile is updated with the value.

In the detection stage, the TCP SYN packets are looked over every specified number of packets (N packets) to look over the SYN pattern and its resemblance with the pattern existing in the database for both incoming and outgoing traffic. For the detection of such DDOS attacks, we have taken behavioral and statistical analysis as measure. Hence, we look at the percentage change in the number of SYN packets. If the scenario shows that their percentage is increasing with time

Table 5: Current attacks and proposed scheme.

Cloud network attack	VM profile based detection
DoS and DDoS [18] SYN flooding attack (TCP SYN flood) Smurf attack (ICMP flood) Ping of death (ICMP flood) Low-rate denial-of-service attacks (TCP's slow-time-scale dynamics of RTO)	(1) VM profile stores traffic behavior of incoming and outgoing traffics over a period of time. It looks for attack patterns for flooding attacks such as TCP SYN and ICMP and their counts in benign usage of virtual machine. For every DDOS attack pattern, profile stores the threshold of attack packets per N packets. This threshold obtained during normal VM behavior is then used during detection of DDOS attacks. (2) DDOS attack detection uses the threshold stored in VM profile database. (3) Anomaly detection components updates attack signature db periodically, and hence, network intrusion detection component can thwart such attacks concretely for each VM. (4) The attacks are identified and tackled in timely manner as they are ranked based on the probability and frequency of such patterns found during initial profile creation and anomaly detection stages.
TCP hijacking [16]	(1) VM inside the cloud environment can easily be checked for promiscuous mode set and can be matched with VMs profiles which generally have this feature disabled (2) The packet loss statistics of victim VM due to session hijacking will result in anomalous behaviour which will be detected by the network intrusion detection component.
Reused IP addresses [17]	The VM profile will have the IP address allocated to it. During each disconnection, it is ensured by the centralized management component that the IP address of disconnected VM must not be directly given to a new VM or existing VM before a certain period of time till all pending or ongoing connections shuts up.
DNS attacks [17]	(1) Privileged VMs having DNS control have a list of IP addresses that are allowed to communicate with DNS services. This information is stored in VM profile. (2) Hence, unauthorized communication with unrecognized IP addresses by either Insiders or Outsiders will get detected and handled.
Network penetration [18] IP random options, SMB session mixing, TCP urgent pointer, and MSRPC object reference	(1) These signatures will get detected by the network intrusion detection system as it runs common attack pattern signature matching for data coming from all VMs. (2) Such well-known signatures are not VM specific and will get detected by network intrusion detection system over traffic coming from all VMs, that is, without consulting individual VM profile but through common attack signature matching.
Fragmentation attack [19] Tiny fragment attack, overlapping fragment attack	As these attacks are also not VM specific they will get detected by the network intrusion detection system through its general attack packet signature pattern matchings.
Traffic analysis [20] Deep packet inspection	(1) Traffic analysis of cloud network either as a whole or VM specific launched by cloud user or insider VM can be detected; as for doing such operation they will set to promiscuous mode which can be checked synchronously over cloud VMs. (2) And if their profile have promiscuous mode as disabled the anomalous behaviour will get detected.
Passive eavesdropping [21]	Profile and promiscuous mode feature can detect such attempts.
Active eavesdropping [21]	Unidentified and unauthorized communication can be detected through VM profile as it has trusted and frequently used IP addresses. Also profile and promiscuous mode feature will detect such attempts.

we alert the subsystems to inform the admin about the scenario and to take appropriate actions. Even if the DDoS attack is through multiple sources from outside the cloud network, we can stop it as we have the profile of a particular virtual machine known to us, and hence, when a drastic change comes up, such attacks are easily detected and can be resolved by just notifying the VM user of anomalous happenings and shifting him to some different IP address or by blocking the communication from malicious IP addresses. And this will not only detect attacks from malicious outsiders but will also detect malicious insiders that are doing DDoS attacks and can pinpoint the source if inside to cloud environment, as it maintain, the profile of both incoming and outgoing traffics. This is the prototype implementation of the concept; however, the signatures for implementing fully functional prototype are already analyzed, and the implementation for such an intrusion prevention system is under progress. The result will be analyzed in terms of speed of detection of DDoS attacks compared to traditional schemes and the resources required for detection in terms of computational and storage complexity.

4.2. Advantages of Proposed Scheme. The proposed scheme if deployed will provide security to well-known threats over

network in cloud both from malicious cloud users, insiders, and outsiders. Table 5 shows the description of cloud network attacks and how they will be handled by the proposed scheme.

5. Conclusions

This paper is focused on an approach of profile based network intrusion detection for providing security to cloud environment. It is a signature cum behavior based network intrusion detection system. The concept is of creating a VM profile db that will describe the attack patterns that needs to be looked over on the VM specific traffic. The VM profile db also contains the attacks in a ranked manner which will ensure timely detection as the patterns will be searched in the traffic in a ranked manner. The profile of a new VM is created in VM profile creation stage where a VM is taken into consideration for a specific amount of time for profiling its behavior for detecting packet flooding attacks such as denial-of-service attacks and also for finding such patterns including others that can be possible in future from that VM or over it, in the cloud network. The profile is updated for new attack patterns and synchronizes attack patterns parameters by anomaly detection component, whereas the network intrusion detection system divides the incoming and outgoing traffics and analyses the network for anomalous behavior for attacks based on the individual profiles of particular VMs. The intrusions are informed to alert and response generation component that then takes necessary actions such as responding to current malicious activities taking place and updating the VM profile with new attack or updating the ranking of attacks for timely detection. The prototype implementation for detecting TCP flooding TCP SYN flooding attack has been done, and the results show, such concept of profile based detection can be applied for detection of all known signature and anomalous behavior based network attacks. The implementation of a complete profile based network intrusion detection system is under progress.

Acknowledgments

This work was supported by the framework of the IT4 Innovations Centre of Excellence project, reg. no. CZ.1.05/1.1.00/02.0070 by operational programme "Research and Development for Innovations" funded by the Structural Funds of the European Union and state budget of the Czech Republic, EU.

References

[1] E. Brown, "NIST issues cloud computing guidelines for managing security and privacy," National Institute of Standards and Technology Special Publication 800-144, January 2012.

[2] P. M. a. T. Grance, *Effectively and Securely Using the Cloud Computing Paradigm (V0. 25)*, US National Institute of Standards and Technology, 2009.

[3] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-oriented cloud computing: vision, hype, and reality for delivering IT services as computing utilities," in *Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications (HPCC '08)*, pp. 5–13, September 2008.

[4] "Mware security and compliance," 2010.

[5] "Top threats to cloud computing," in *Cloud Security Alliance*, 2012.

[6] E. N. a. I. S. Agency, "Cloud Computing Security Risk Assessment," November 2009.

[7] B. Grobauer, T. Walloschek, and E. Stöcker, "Understanding cloud computing vulnerabilities," *IEEE Security and Privacy*, vol. 9, no. 2, pp. 50–57, 2011.

[8] "Does cloud computing compromise clients?" 2009.

[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 1, pp. 1–11, 2011.

[10] "Dropbox account hijacked," 2012.

[11] Bloomerg, "Attack on Sony Play station Network exploiting Amazon Cloud Services," 2011.

[12] C. Metz, *Attack on Amazon Cloud Services, Bitbucket's Servers Down*, London, UK, 2009.

[13] "Hackers find a home in Amazon's EC2 cloud," 2009.

[14] B. Dima, "Top 5: corporate losses due to hacking," 2012.

[15] D. W, "Hackers attack Epsilon database, phishing spree anticipated," 2012.

[16] D. L. K. Lam and B. Smith, "Theft on the web: prevent session hijacking," in *Technet Magazine: Microsoft*, 2005.

[17] R. C. R. Bhadauria, N. Chaki, and S. Sanyal, "A survey on security issues in cloud computing," http://arxiv.org/abs/1109.5388.

[18] I. S. Institute, *DDoS Attack Categorization*, University of Southern California.

[19] Wikipedia, "IP fragmentation attacks," 2013.

[20] G. Danezis, "Introducing traffic analysis, attacks, defences and public policy issues. .," in *Proceedings of the Santa's Crypto Get-together*, 2005.

[21] P. D. M. Sherr, "Eavesdropping," *SpringerReference*.

[22] C. C. Lo, C. C. Huang, and J. Ku, "A cooperative intrusion detection system framework for cloud computing networks," in *Proceedings of the 39th International Conference on Parallel Processing Workshops (ICPPW '10)*, pp. 280–284, September 2010.

[23] S. Roschke, C. Feng, and C. Meinel, "Intrusion detection in the cloud," in *Proceedings of the 8th IEEE International Symposium on Dependable, Autonomic and Secure Computing (DASC '09)*, pp. 729–734, December 2009.

[24] L. Jun-Ho, P. Min-Woo, E. Jung-Ho, and C. Tai-Myoung, "Multi-level intrusion detection system and log management in cloud computing," in *Proceedings of the13th International Conference on Advanced Communication Technology (ICACT '11)*, pp. 552–555, February 2011.

[25] C. Mazzariello, R. Bifulco, and R. Canonico, "Integrating a network IDS into an open source cloud computing environment," in *Proceedings of the 6th International Conference on Information Assurance and Security (IAS '10)*, pp. 265–270, August 2010.

[26] S. N. S. Bugiel, A. -R. Sadeghi, and T. Schneider, "Twin clouds: an architecture for secure cloud computing," in *Proceedings of the Workshop on Cryptography and Security in Clouds Zurich*, pp. 1–11, 2011.

[27] H. Jin, G. Xiang, D. Zou et al., "A VMM-based intrusion prevention system in cloud computing environment," *The Journal of Supercomputing*, pp. 1–19, 2011.

[28] D. Smallwood and A. Vance, "Intrusion analysis with deep packet inspection: increasing efficiency of packet based investigations," in *Proceedings of the International Conference on Cloud and Service Computing (CSC '11)*, pp. 342–347, 2011.

[29] S. N. Dhage, B. B. Meshram, R. Rawat, S. Padawe, M. Paingaokar, and A. Misra, "Intrusion detection system in cloud computing environment," in *Proceedings of the International Conference and Workshop on Emerging Trends in Technology (ICWET '11)*, pp. 235–239, Mumbai, India, February 2011.

[30] J. P. Anderson, *Computer Security Threat Monitoring and Surveillance*, Fort Washington, Pa, USA, 1980.

[31] T. Udaya, V. Vijay, and A. Naveen, "Intrusion detection techniques for infrastructure as a service cloud," in *Proceedings of the 9th IEEE International Conference on Dependable, Autonomic and Secure Computing*, IEEE Computer Society, pp. 744–751, Sydney, Australia, 2011.

[32] W. Cong, W. Qian, R. Kui, and L. Wenjing, "Ensuring data storage security in cloud computing," in *Proceedings of the 17th International Workshop on Quality of Service (IWQoS '09)*, pp. 1–9, July 2009.

[33] J. Arshad, P. Townend, and J. Xu, "An automatic intrusion diagnosis approach for clouds," *International Journal of Automation and Computing*, vol. 8, pp. 286–296, 2011.

[34] P. Angin, B. Bhargava, R. Ranchal et al., "An entity-centric approach for privacy and identity management in cloud computing," in *Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS '10)*, pp. 177–183, November 2010.

[35] S. Bharadwaja, S. Weiqing, M. Niamat, and S. Fangyang, "Collabra: a xen hypervisor based collaborative intrusion detection system," in *Proceedings of the 8th International Conference on Information Technology: New Generations (ITNG '11)*, pp. 695–700, Las Vegas, Nev, USA, 2011.

[36] B. Borisaniya, A. Patel, D. Patel et al., "Incorporating honeypot for intrusion detection in cloud infrastructure," in *Trust Management VI*, vol. 374, pp. 84–96, Springer, Boston, Mass, USA, 2012.

[37] L. Flavio and P. Roberto Di, "Secure virtualization for cloud computing," *Journal of Network and Computer Applications*, vol. 34, no. 4, pp. 1113–1122, 2011.

[38] S. Gupta, S. Horrow, and A. Sardana, "IDS based defense for cloud based mobile infrastructure as a service," in *Proceedings of the 8th IEEE World Congress on Services (SERVICES)*, pp. 199–202, Honalulu, Hawaii, USA, 2012.

[39] A. S. Ibrahim, J. Hamlyn-Harris, J. Grundy, and M. Almorsy, "CloudSec: a security monitoring appliance for Virtual Machines in the IaaS cloud model," in *Proceedings of the 5th International Conference on Network and System Security (NSS '11)*, pp. 113–120, 2011.

[40] R. Ranchal, B. Bhargava, L. B. Othmane et al., "Protection of identity information in cloud computing without trusted third party," in *Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS '10)*, pp. 368–372, November 2010.

[41] P. T. J. Arshad and J. Xu, "A novel intrusion severity analysis approach for Clouds," *Future Generation Computer Systems*, vol. 28, pp. 965–1154, 2011.

[42] S. Pal, S. Khatua, N. Chaki, and S. Sanyal, "A new trusted and collaborative agent based approach for ensuring cloud security," http://arxiv.org/abs/1108.4100.

[43] O. Nebula, "Open nebula, enterprise cloud and data center virtualization," Open Nebula.org, Open Source Data Center Virtualization, 2013, http://opennebula.org/.

[44] T. Potter, "Net-Pcap-0.17," CPAN.