Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 83 (2016) 1200 – 1206

Procedia Computer Science

The 2nd International Workshop on Mobile Cloud Computing Systems, Management, and Security (MCSMS-2016)

A Cooperative and Hybrid Network Intrusion Detection Framework in Cloud Computing Based on Snort and Optimized Back Propagation Neural Network

Z.Chiba*, N.Abghour, K.Moussaid, A.El omri, M.Rida

Team of Modeling and Optimization of mobile services, Faculty of Sciences, Hassan II University of Casablanca, 20100, Casablanca, Morocco

Abstract

Cloud computing provides a framework for supporting end users easily attaching powerful services and applications through Internet. To give secure and reliable services in cloud computing environment is an important issue. Providing security requires more than user authentication with passwords or digital certificates and confidentiality in data transmission, because it is vulnerable and prone to network intrusions that affect confidentiality, availability and integrity of Cloud resources and offered services. To detect DoS attack and other network level malicious activities in Cloud, use of only traditional firewall is not an efficient solution. In this paper, we propose a cooperative and hybrid network intrusion detection system (CH-NIDS) to detect network attacks in the Cloud environment by monitoring network traffic, while maintaining performance and service quality. In our NIDS framework, we use Snort as a signature based detection to detect known attacks, while for detecting network anomaly, we use Back-Propagation Neural network (BPN). By applying snort prior to the BPN classifier, BPN has to detect only unknown attacks. So, detection time is reduced. To solve the problem of slow convergence of BPN and being easy to fall into local optimum, we propose to optimize the parameters of it by using an optimization algorithm in order to ensure high detection rate, high accuracy, low false positives and low false negatives with affordable computational cost. In addition, in this framework, the IDSs operate in cooperative way to oppose the DoS and DDoS attacks by sharing alerts stored in central log. In this way, unknown attacks that were detected by any IDS can easily be detected by others IDSs. This also helps to reduce computational cost for detecting intrusions at others IDS, and improve detection rate in overall the Cloud environment.

Peer-review under responsibility of the Conference Program Chairs

Keywords: Cloud computing; Network intrusion detection; Back-propagation neural network; Snort; Optimization algorithm

* Zouhair Chiba. Tel.: +212-671-657-123.
E-mail address: chiba.zouhair@gmail.com

Peer-review under responsibility of the Conference Program Chairs
doi:10.1016/j.procs.2016.04.249

1. Introduction

Cloud computing (CC) is rapidly growing computational model in today's IT world. It delivers convenient, on-demand network access to a shared pool of configurable computing resources (e.g. Networks, servers, storage, applications, etc.), "as service" on the internet for satisfying computing demand of users[1].

A recent survey performed by Cloud Security Alliance (CSA) & IEEE, indicates that enterprises across sectors are eager to adopt cloud computing but that security are needed both to accelerate cloud adoption on a wide scale and to respond to regulatory drivers[3]. One of major security issues in Cloud is to detect and prevent network intrusions since the network is the backbone of Cloud, and hence vulnerabilities in network directly affect the security of Cloud. L. Marti from Cyber Security division[6] stated that main concern after data security is an intrusion detection and prevention in the Cloud.

There are principally two types of threads; insider (attackers within a Cloud network) and outsider (attackers outside the Cloud network) considered in Cloud Network.

- Insider attackers: Authorized Cloud users may attempt to gain (and misuse) unauthorized privileges. Insiders may commit frauds and disclose information to other (or modify information intentionally). This poses a serious trust issue. For example, an internal DoS attack demonstrated against the Amazon Elastic Compute Cloud (EC2)[7].
- Outsider attackers: can be called as the network attackers who are able to perform different attacks as IP spoofing, Address Resolution Protocol (ARP spoofing), DNS poisoning, man-in-the-middle, Denial of Service (Dos)/Distributed Denial of service (DDoS) attacks, phishing attack, user to root attack, Port scanning, attack on virtual machine (VM) or hypervisor such BLUEPILL and DKSM through which hackers can be able to compromise installed-hypervisor to gain control over the host, Backdoor channel attacks etc.

These attacks affect the integrity, confidentiality, and availability of Cloud resources and offered services. To address above issues, major Cloud providers (like Amazon ECC, Window Azure, Rack Space, Eucalyptus, Open Nebula etc.) use the firewall. Firewall protects the front access points of system and is treated as the first line of defense. As firewall sniffs the network packets only at the boundary of a network, insider attacks cannot be detected by it. Few DoS or DDoS attacks are too complex to detect using traditional firewall. For example, if there is an attack on port 80 (web service), firewall cannot differentiate normal and legitimate traffic from DoS attack traffic [8]. Thus, use of only traditional firewall to block all the intrusions is not an efficient solution. Another solution is to deploy network based intrusion detection system[10] (NIDS) in Cloud computing. NIDS captures the network packets and applies intrusion detection techniques on captured packets in order to detect networks attacks.

1.1 Our contribution

We propose a new security framework that integrates a cooperative and hybrid-NIDS to Cloud (offering Iaas). We deploy our CH-NIDS at the Front end on Cloud Controller, as well as at on Back end on each processing server (hosting VM) in order to detect both internal and external network intrusions in Cloud Environment. In this framework, we use both the techniques; signature based detection and anomaly based detection. Snort as a signature based detection is used to detect known attacks, while for detecting network anomaly, we use an optimized Back Propagation Neural network (BPN). Several researchers used BPN approach for detection intrusion attacks, because it has shown good capability in detecting attacks[2]. But, according to many researches, BPN has the following weaknesses[5, 12]:

- Slow detection speed.
- Low detection accuracy.
- Easy to fall into local minimum value.
- Slow convergence speed.

In order to solve the problems above, we propose to optimize the BPN by using an optimization algorithm. Combining signature based detection and anomaly detection in our NIDS module improves detection accuracy; since they are complimenting each other. In addition, the signature based detection technique is applied prior to anomaly detection, which reduces the computational cost. BPN classifier has to detect only unknown attacks, because known attacks are already detected by Snort and denied. By using central log of malicious packets detected,

NIDS placed on all the servers work in cooperative manner, they update their bases (knowledge base and behavior base) by getting alerts stored in the central log. So, any unknown attack (that was previously detected at any server) can be easily detected by Snort at other servers. This also helps to reduce computational cost for detecting intrusions at other servers, and improve detection rate in overall the Cloud. Our main aim is to reduce impact of network attacks (known attacks, and unknown attacks), while ensuring higher detection rate, lower false positive rate and lower false negative rate with an affordable computational cost.

The rest of this paper is organized as follows: Section 2 discusses existing NIDS approaches to Cloud. A detailed description of the proposed framework is discussed in section 3. Section 4 summaries the conclusions and future work with the references at the end.

2. Related Works

C.C.Lo[10] et al. proposed to deploy individual NIDS module in each Cloud region. In case of intrusion detection, it drops the attacker's packet, and then sends alert messages to other regions using agents. At each region, an alert produced by other regions are gathered to determine whether it is true or false. This is done by calculating the severity of an alert. These approaches are convenient for preventing Cloud from DDoS attack. However the computational and communication effort is augmented.

N.Modi[9] et al. have integrated a signature Apriori based NIDS to Cloud. Signature Apriori takes network packets and known attack signatures as input and generates new derived rules that are updated in the Snort. Therefore, Snort is able to detect known attacks and derivative of known attacks in the Cloud. This approach improves the efficiency of Snort. However, it cannot detect unknown attacks.

Manthira Moorthy[13] S et al. have proposed security architecture for cloud, in which a virtual host based intrusion detection system was placed between router and Cloud host. The developed IDS consists of three components namely: Event Auditor, IDS service (combination of analyze system and Alert system) and CIDD (Cloud Intrusion Detection Data Sets). The analyzer system examines the content of packet against the cloud intrusion datasets signatures stored in CIDD by means of pattern matching. The experiments conducted by the authors show that the proposed IDS was able to detect 80% of random sets of cloud attacks and no false positive alarm is raised while filtering background traffic received form DARPA dataset. However, results show that latency in IDS is increasing according to background traffic, and a breaking point was identified at 2 mbps, in which, the IDS generated an error and stopped. Therefore, an unstable interval was determined between 1.5 to 2 mbps.

Jaimin K. Khatri and Girish Khilari[16] have proposed an architecture which provides implementation of Sericata IDS as network IDS in the backend of Cloud environment. The aim of Sericata IDS is to secure the virtualized servers on hypervisors in the cloud platform from attackers and various threats. The main function of Sericata IDS in the network is capturing of all coming packets from external users and destined to virtualized servers, analyzing these packets and finally sending alert if a packet is matching one of rules stored into Sericata configuration file. However, the proposed model can't detect insider attacks, network intrusions in virtual network as well as known attacks.

Sanchika Gupta[17] and Padam Kumar have proposed an approach to detect malicious program executions at client VM's in Cloud environment, with the use of a new technique of Immediate System Call signature detection. In this approach, for every unique System Call (user program or system program), the list of all Immediate System Calls following it is identified, and created from its normal execution logs, and such signatures are stored and then used as baseline for anomalous program detections. This method is based on the fact that whenever the program is subverted or is executed in a malicious way on a client, it causes a deviation in the Immediate System Call sequence pattern corresponding to each unique System Calls. This deviation can easily be detected and logged for generating alerts to Cloud Admin. Cloud admin then react on it either by uninstalling the malicious software from client or by replacing the software with its valid replica. However, the detection of malicious programs is not in real time, because of the periodic nature of the proposed anomaly detection module. In addition, the detection module can detect only subversions of programs whose the signatures of their immediate system calls are already generated, and also the reaction to an attack is not automatic, it is decided by the cloud admin.

B. Al –Shadaifat[22] et al. have proposed an anomaly intrusion detection model to deal with attacks and security violations in cloud environment. The proposed approach consists of Hopefield Artificial Network and Simulating Annealing as aggregator. The framework for anomaly IDS is divided into three stages: Dataset Grouping, Hopfield Artificial Neural Network (HANN) and Simulating Annealing aggregator. According to experiments performed by

authors, the proposed model provides a detection rate <=93%, which can be considered as a weak detection rate compared with methods in [19, 20, 21]. For gain better detection rate, more enhancements must be conducted by exploring the impact of network features in detection rate.

Our proposed framework provides solution to limitations existing in these approaches and others[4, 9,14,15,18] researches. In this paper, we propose a cooperative and hybrid approach that combines two network intrusion detection techniques; signature based detection and anomaly detection. In misuse detection, we employ Snort, whereas in anomaly detection, we use Back-Propagation neural network detector optimized by an optimization algorithm to get the optimal connections weights of BNP. Therefore, the detection accuracy and efficiency of BNP detector will be improved.

3. CH-NIDS in the Cloud: Cooperative and Hybrid Security Framework

3.1 Integrating NIDS in cloud datacenter

The aim of the proposed CH-NIDS is to detect any violation of the security policy on the computer system. It allows detecting and stopping attacks in real time impairing the security of the Cloud Datacenter.

As shown in figure 1, we propose to deploy our NIDS on two strategic positions:

- NIDS on Front-End of Cloud: Integrating NIDS module on front end of Cloud helps to detect network intrusions from external network of Cloud. However, it is not able to detect attack at internal network of Cloud.
- NIDS on Back-End: Positioning NIDS module on processing server helps to detect intrusions at internal network of Cloud. In a virtual environment, we have several virtual machines on the same physical server, and they can inter-communicate through the virtual switch without leaving the physical server. Therefore, network security devices on the LAN can't monitor this network traffic; if the traffic does not need to pass through security appliances primarily a firewall, therefore, a loophole for all kinds of security attacks will be opened. Thus, the starting point of an attacker is compromising only one VM, and using it as a springboard to take control of the other VMs within the same hypervisor. This is generally done without being monitored or detected, giving the attacker a vast hack domain. Moreover, the virtual environment is exposed to several threats, centered mostly on the hypervisor: Hyper jacking, VM escape, VM migration, VM theft and Inter-VM traffic.

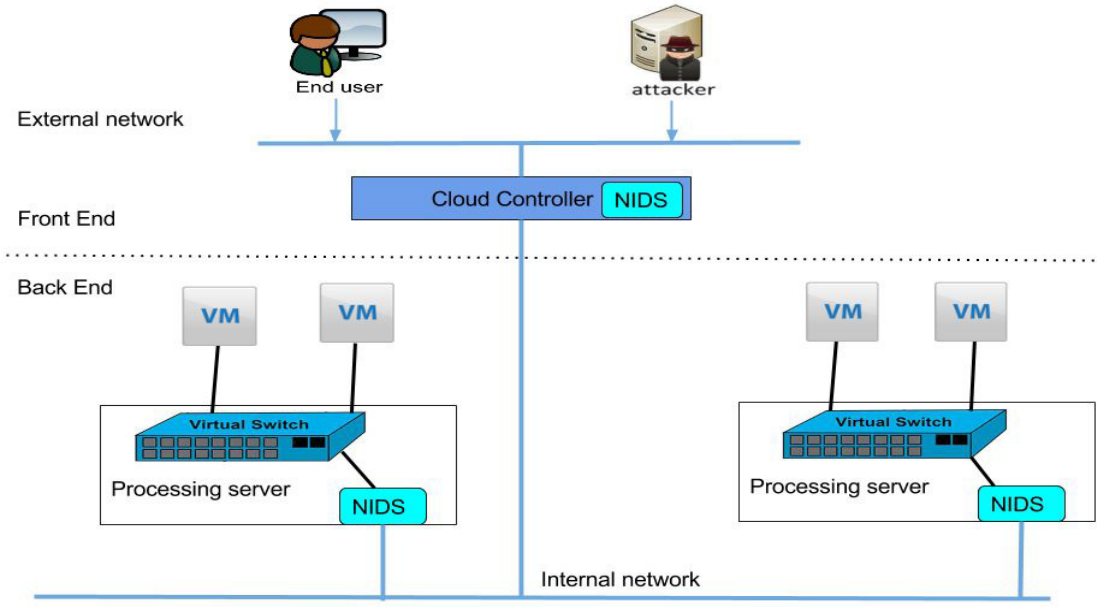

Fig. 1. Positions of NIDS in the Cloud

Our NIDS is designed to monitor that virtual traffic, and also the flow of traffic from or to the processing server on the physical network. We haven't chosen to install the NIDS on each virtual machine because it will be an additional burden; it will weigh down the work of the VM. In addition, such configuration requires multiple instances of NIDS, which makes complex management of NIDS whereas VMs are dynamically migrated, provisioned or de-provisioned.

3.2 Architecture of proposed NIDS framework

The architecture of proposed CH-NIDS as shown in figure 2 consists of mainly four modules; Signature based detection, Anomaly detection, Alert System and Central log of malicious packets.

- Signature based detection: It consists of two components; Snort and the misuse detection database. This database is generated based on predefined network attack rules. Snort matches the captured packets with rules stored in misuse base to find any correlation. In this case, it determines the nature of the attack and send alert message to "Alert System". The non-intrusion packets are forwarded to "Anomaly detection" module for more investigation. One of the advantages for using this technique is that we can easily update misuse base without modifying exiting rules.
- Anomaly detection: It is composed of three components; Back Propagation neural network algorithm (BPN), a module based on an optimization algorithm to overcome the weakness of BPN mentioned in subsection 1.1, and an anomaly detection database. In learning phase, the BPN classifier is trained using malicious and normal packets stored in anomaly detection database. In detecting phase, the BPN predicts the class of the given network packets. If it is normal, it is allowed to access to Cloud infrastructure, else it is denied and "Alert System" is notified.

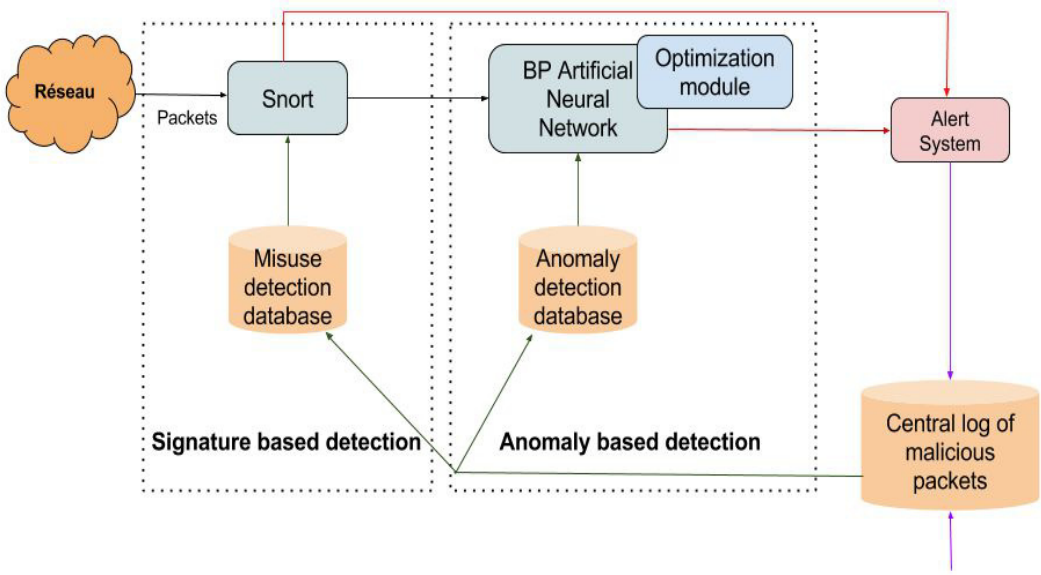

Fig. 2. Architecture of proposed CH-NIDS framework

- Alert System: generates alerts about intrusions that are determined either by snort or BP neural network classifier. It stores alerted intrusion in central log database.
- Central log of malicious packets: It used by CH-NIDS deployed on others hosts to update their bases with alerts found in alert database. So, the next time, such intrusion can be easily detected by Snort at others hosts. This reduces computational cost, and also time detection in overall the Cloud.

3.3 Workflow of proposed NIDS framework

In Our NIDS module, we use both techniques (signature based and anomaly based) that are complimented each other. As shown in figure 3, network packets are captured from physical and virtual network. Then, signature based technique is applied on captured packets to detect intrusions using Snort. It consists of matching the captured packets with rules stored in attack signature database. If any correspondence is found, an alert is generated and stored in central log database. Then, alerted packet is denied. Non-intrusion packets are forwarded to the optimized BPN classifier, which is applied to predict class label (normal or intrusion) of these packets.
If it finds any intrusion, it will be alerted and stored in central log base. Otherwise, BPN considers those packets as legitimate packets and allowed to access the system. NIDS on others servers update their bases with alerts logging in central log base.

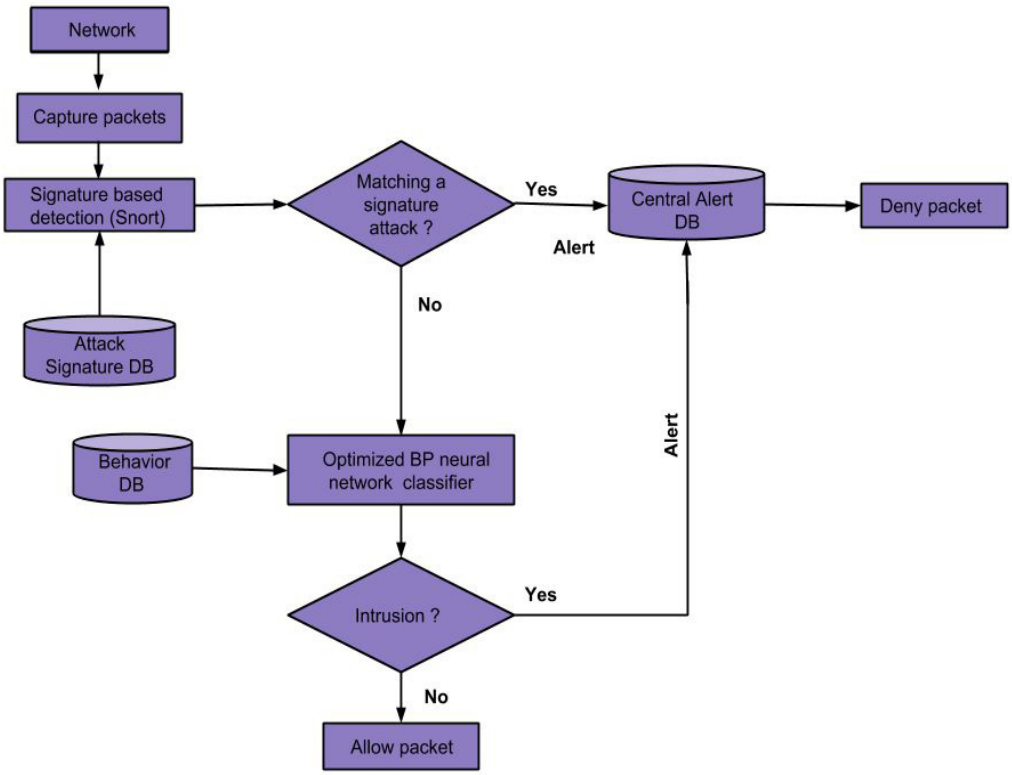

Fig. 3. Workflow of proposed NIDS

4. Conclusion and Future Work

Security in cloud computing is a major concern which is slowing the adoption of cloud by the corporate. One of major security issues in Cloud is to detect and prevent network intrusions since the network is the backbone of Cloud, and hence vulnerabilities in network directly affect the security of Cloud. To detect Dos attack and other network level malicious activities in Cloud, use of only traditional firewall is not an efficient solution. In this paper, we proposed a Cooperative and Hybrid NIDS (CH-NIDS) framework for Cloud environment (i.e. IaaS), that integrates Snort and Back-Propagation Neural Network classifier optimized by a module based on an optimization

algorithm to overcome the weakness of BPN. Our proposed NIDS is deployed at Front end and Back end of the Cloud to detect external attacks and internal attacks, coming either from internal physical network of the cloud or the virtual network on host machines.

Our NIDS uses the signature based and anomaly based techniques to improve detection accuracy. Therefore, it is able to detect known as unknown attacks in Cloud. We have applied a signature based technique prior to anomaly technique, resulted in reducing computational cost. In addition, by using central log of malicious packets detected, NIDS placed on all the servers work in cooperative manner, they update their bases (knowledge base and behavior base) by getting alerts stored in the central log. So, any unknown attack (that was previously detected at any server) can be easily detected by Snort at other servers. This also helps to reduce computational cost for detecting intrusions at other servers, and improve detection rate in overall the Cloud.

Our proposed NIDS is designed to have high detection rate, high accuracy with low false positives, low false negatives and affordable computational cost. Our future work is implementing our module NIDS in open source Cloud environment like Eucalytus, proposing and testing our optimization algorithm for BNP classifier.

References

1. NIST SP 800-145, The NIST Definition of Cloud Computing, http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf (2011).
2. R.Gaidhane, C. Vaidya, M. Raghuwanshi, Intrusion Detection and Attack Classification using Back-propagation Neural Network, International Journal of Engineering Research & Technology 3(3) (2014) 1112- 1115.
3. M.Jouini, L.Ben Arfa Rabai, Surveying and Analyzing Security Problems in Cloud Computing Environments, in: Computational Intelligence and Security (CIS), 2014 IEE Tenth International Conference on, 2014, pp.689-693.
4. A. V. Dastjerdi, K. A. Bakar, S. G. H. Tabatabaei, Distributed Intrusion Detection in Clouds using Mobile Agents, in: Advanced Engineering Computing and Applications in Sciences (ADVCOMP), 2009 IEEE Third International Conference on, 2009, pp. 175-180.
5. K.Gang, H.Y. Han, The Research of Network Intrusion Detection Technology Based on Genetic Algorithm and BP Neural Network, Applied Mechanics and Materials 599-601 (2014) 726-730.
6. L.Martin, Awareness, Trust and Security to Shape Government Cloud Adoption, White paper, http://www.ca.com/~/media/Files/IndustryResearch/lm-cyber-security_gov- Cloud-adopt_233481.pdf (2010).
7. Black Hat presentation demo vids: Amazon, http://www.sensepost.com/blog/3797.html (2009).
8. Denial-of-service attack, https://en.wikipedia.org/wiki/Denial-of-service_attack (2015).
9. N. Modi, D. R. Patel, M. Rajarajan, Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing, in: 2nd International Conference on Communication, Computing and Security (ICCCS-2012), 2012, pp.905- 912.
10. C.C.Lo, C.C. Huang; J.Ku, A Cooperative Intrusion Detection System Framework for Cloud Computing Networks, in: 39th IEEE International Conference on Parallel Processing Workshops (ICPPW 2012), 2012, pp. 280-284.
11. C. Mazzariello, R. Bifulco and R. Canonico, Integrating a Network IDS into an Open Source Cloud Computing Environment, in: Information Assurance and Security (IAS), 2010 IEEE Sixth International Conference on, 2010, pp. 265-270.
12. Z.Qing-Qing, Z.Qian, F.Yue-jiang, Ant Colony Algorithm Based on Improved Neural Network Algorithm and its Application, Applied Mechanics and Materials 543-547 (2014) 2116-2119.
13. S.M.Manthira, M.Rajeswari, Virtual Host based Intrusion Detection System for Cloud, International Journal of Engineering and Technology (IJET) 5(6) (2014) 5023- 5029.
14. S.Roschke, C.Feng, C.Meinel, An extensible and virtualization compatible IDS management architecture, in: Information Assurance and Security, 2009 Fifth International Conference on, 2009, pp.130–134.
15. S.Ram, Secure cloud computing based on mutual intrusion detection system, Int. J. Comput.Appl. 2(1) (2012) 57–67.
16. J.K. Khatri, G.Khilari, Advancement in Virtualization Based Intrusion Detection System in Cloud Environment, International Journal of Science, Engineering and Technology Research (IJSETR) 4(5) (2015) 1510-1514.
17. S.Gupta, P.Kumar, Immediate System Call Sequence Based Approach for Detecting Malicious Program Executions in Cloud Environment, Wireless Personal Communications 81(1) (2015) 405-425.
18. V.Mishra, V.K.Vijay, S.Tazi, Intrusion Detection System with Snort in Cloud Computing: Advanced IDS, in: ICT for Sustainable Development, Advances in Intelligent Systems and Computing, 2016 International Conference on, 2016, pp.457-465.
19. W.Gang, H.Jinxing, M.jian, H. Lihua, A new approach to intrusion detection using Artificial Neural Networks and fuzzy clustering, Expert Systems with Applications International Journal, 37(9) (2010) 6225–6232.
20. L. Shih-Wei, Y. Kuo-Ching, L.Chou-Yuan., L. Zne-Jung, An intelligent algorithm with feature selection and decision rules applied to anomaly intrusion detection, Expert Systems with Applications International Journal 12(10) (2010) 3285–3290.
21. P.Biswajit, O. Olugbenga, M.Priyanka, Training of Intelligent Intrusion Detection System using Neuro Fuzzy, in: Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), 2014 15th IEEE/ACIS International Conference on, 2014, pp.1-6.
22. B.Al-Shdaifat, W.S.Alsharafat, M.el-bashir, Applying Hopfield Artificial Network and Simulating Annealing for Cloud Intrusion Detection, Journal of Information Security Research 6(2) (2015) June 2015 49-53.