A Collaborative Network Intrusion Detection System (C-NIDS) in Cloud Computing

Zayed Al Haddad[1], Mostafa Hanoune[1] and Abdelaziz Mamouni[1]

[1]Laboratory of Information Technology and Modeling, Faculty of Sciences Ben M'sik,
Hassan II University of Casablanca, Morocco

Abstract: In recent years, Cloud computing has emerged as a new paradigm for delivering highly scalable and on-demand shared pool IT resources such as networks, servers, storage, applications and services through internet. It enables IT managers to provision services to users faster and in a cost-effective way. As a result, this technology is used by an increasing number of end users. On the other hand, existing security deficiencies and vulnerabilities of underlying technologies can leave an open door for intruders. Indeed, one of the major security issues in Cloud is to protect against distributed attacks and other malicious activities on the network that can affect confidentiality, availability and integrity of Cloud resources. In order to solve these problems, we propose a Collaborative Network Intrusion Detection System (C-NIDS) to detect network attacks in Cloud by monitoring network traffic, while offering high accuracy by addressing newer challenges, namely, intrusion detection in virtual network, monitoring high traffic, scalability and resistance capability. In our NIDS framework, we use Snort as a signature based detection to detect known attacks, while for detecting network anomaly; we use Support Vector Machine (SVM). Moreover, in this framework, the NIDS sensors deployed in Cloud operate in collaborative way to oppose the coordinated attacks against cloud infrastructure and knowledge base remains up-to-date.

Keywords: Security, Cloud Computing, NIDS, Cloud based IDS, Virtual infrastructure.

1. Introduction

Nowadays, Cloud Computing is the most emerging technology that is rapidly being adopted by the IT industry due to its cost effective nature, easy accessibility, efficient resources utilization and the pay per use service[1]. It offers ubiquitous, convenient, demand-based access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be quickly provisioned and released with minimal management effort or service provider interaction[2]. Cloud is a blend of existing technologies such as grid computing, utility computing and virtualization. However, Virtualisation is a key technical component of cloud computing[3][4]. It abstracts the underlying hardware resources, thereby providing virtually the similar infrastructure to cloud users as on a physical platform. Virtualization provides additional cost saving benefits as well as enhances flexibility. However, Cloud is easy target for intruders due to much vulnerability involved in it[4]. Indeed, the major security challenge in Cloud computing is to detect and prevent distributed attacks and malicious activities on the network that can affect Cloud resources and offered services. According to [5][6][7][8], Cloud suffers from insider and outsider threads. Insider attack (e.g. user at client side, provider side and provider itself) may perform malicious activity from within the Cloud network. Outsider attack often performs various attacks from outside the Cloud network viz; IP spoofing, Address Resolution Protocol spoofing, Routing Information Protocol attack, inserting malicious network traffic, etc. Consequently, traditional network security measures such as firewall. Firewalls are better to stop many outsider attacks. However, insider attacks as well as some complicated outsider attacks can't be tackled effectively by it. For this, the intrusion detection systems (IDS) come into play. It serves to automating the process of intrusion detection. IDS monitor network, system or host activities for policy violations or malicious activities, creates and sends reports to a management station or system administrator. However, the alerts generated by IDS are not always relevant to actual intrusion due to false negatives and false positives which affect the performance and accuracy of IDS. Moreover, isolated IDSs are not able to detect Denial of Service (DoS) and Distributed DoS (DDoS) attacks.

In this paper, we propose a new collaborative framework that integrates a Collaborative Network Intrusion Detection System(C-NIDS) to Cloud. We deploy our NIDS sensors at the front end as well as at the back end on Virtual Machine Monitor (VMM) to monitor and detect network intrusions in traditional as well as in virtual network, while reducing false alarm rate and improve accuracy of NIDS. We use both techniques namely, signature based detection and anomaly detection. Snort as a signature based detection is used to detect known attacks, while for detecting unknown attacks, we use support vector machine (SVM). There are two advantages by using SVM [9] [10]:

- As a classification algorithm, SVM calculated the optimum solution of distance that is the fairest classification. SVM can resolve issues related to false positives or negatives.
- Volume of model that SVM used for classification is small. Consequently, it helps to reduce detection time.

In addition, combining Snort and SVM in our NIDS improves the efficiency of the Snort from the intelligent classifying detection, applies SVM to Snort: train the network data while running, and select the learning sample initiatively, transform the sample data feature into rules, classify the data and detect unknown attack effectively. By using central log database, NIDS placed in other regions work in collaborative manner, they update their base (knowledge and behaviour base) by getting alerts stored in the central log database. This helps to reduce computational cost for detecting intrusions at other regions and enhance the accuracy of attacks detection. Our main aim is to reduce impact of network attacks, while ensuring higher detection rate and lower false positive rate with an affordable computational cost.

The rest of this paper is organized as follows. Section 2 discusses the existing security approaches and frameworks which the proposal is based. Section 3 presents the proposed security framework and explains its general functionality. The proposed framework is discussed in section 4. Section 5 concludes our research work with references at the end.

2. Literature review

There have been several security approaches and frameworks proposed for Cloud. In [6], a novel security framework has been proposed. This framework integrates Hybrid-Network Intrusion Detection System (H-NIDS) to cloud using the classifiers Bayesian, associative and decision tree as an anomaly detection and snort as a Signature based detection to implement this framework. Performance and detection efficiency of H-NIDS have been evaluated for ensuring its feasibility in cloud. According to the authors, this framework has higher detection rate and low false positives at an affordable computational cost. However, the associative classifier generates a high number of false positives, while individually used it.

Vieira et al. [9] have proposed a Grid and Cloud Intrusion Detection System (GCCIDS). In this architecture, Intrusion detection is done in a cooperative manner. Each node of Cloud identifies suspicious events and informs the other nodes. It uses both techniques viz; signature based detection and anomaly detection. For detect unknown attacks, feed-forward artificial neural network is used. When any attack or intrusion is detected, alert system informs other nodes. So, this approach is efficient for detecting known as well as unknown attacks. The result shows that the false positive and false negative alarm rate is very low. However, it requires more training time and samples for detection accuracy.

Tupakula et al. [12] have proposed a model based on a hypervisor. A hypervisor solution embeds as a software layer to control the physical resources and it allows running multiple operating systems. Hypervisor is capable to enhance the efficiency of intrusion detection in cloud. The proposed model improves the reliability and availability of the system. In fact, the infrastructure can be secured most of the time. However, it has not presented any solution to heal the system if the infrastructure collapsed due to the high severe attacks over the system.

Kholidy and Baiardi [13] have proposed a framework with a P2P solution for cloud and no central manager coordinator. The framework’s architecture distributes the processing load at several cloud locations and separates the user tasks from the cloud so that the intrusion detector become invisible to attackers. It includes an audit system to discover these attackers. Moreover, it also summarizes a high intensive number of alerts. The proposed system is scalable. However, it is not sufficient for detecting large scale distributed attacks and there is no central correlation handler to amalgamate all the alert information consistently to detect intrusions.

Gul and Hussain[14] have proposed a multi-threaded NIDS based on three modules viz; capture, reporting and analysis and processing module. This model allows to solve the problem of Cross Site Scripting (XXS) and DDoS attacks. However, the implementation details are not provided.

Dhage et al. [15] have proposed an architecture in which the IDS controller deploys a mini IDS instance between the user and cloud service provider. Whenever the user wants to access any service, it is duty of the IDS controller to provide IDS instance to that user. IDS instance monitors each of the user’s activities and sends a log of complete session to IDS controller which will be stored in cloud logs. The next time when the user starts session, IDS controller will query the Knowledge Base. It can use neural networks to learn new pattern. According to the authors, the main advantage is the reduction in workload because it is split between multiple instances to carry the work in a better way rather than letting single IDS for the whole cloud. However, it is a theoretical model.

Araújo et al. [7] have proposed an Elastic and Internal Cloud-based Detection System (EICIDS), which is based on protection of virtual machines against internal users who can use some VMs to perform malicious activities. Monitoring of virtual machines is done by IDS sensors dispersed in the cloud environment, and the instantiation of these sensors is made in each VM, where the packets passing in VMs are captured and subsequently analyzed for the identification of threats. Thus, the entire virtual environment is monitored, while the remaining components of EICIDS reside outside the virtual environment are thus protected from possible attacks by compromised VMs. However, the architecture of EICIDS is centralized IDS_admin and there is no signature generation system.

Idress et al. [16] have proposed an integrated and hybrid Intrusion Detection and Prevention System (IDPS) solution comprising hybrid Network Intrusion Detection and Prevention System (NIDPS), hybrid Host Intrusion Detection and Prevention Systems (HIDPS) and a centralized Intrusion Detection Prevention Operations Centre (IDPOC). Design of NIDPS and HIDPS are similar except the Multi-threading approach introduced in NIDPS to efficiently process the large throughput and high speed network traffic. The detection engines of NIDPS and HIDPS are customized according to the specific threat domains of network and hosts. Each IDPS is integrated with SNORT based misuse detection engine and Bayesian classifier, Decision tree and Naïve Bayes techniques based anomaly detection engine. Operations of individual IDPS are closely monitored, organized and upgraded with the help of a supervisor unit, which also communicates with the IDPOC for overall joint operations. This system is designed to detect known and unknown attacks in cloud, VoIP and standard networks as well as Next Generation Networks (NGN) with customized databases for each scenario. However, it is a theoretical model.

Modi et al. [17] have proposed and implemented a HIDS which uses Bayesian classifier to predict that the given event is attack or not, and Snort to detect known attacks. This framework, signature based detection technique is applied prior to anomaly detection, resulting in better detection time. However, it requires more training samples for detection accuracy.

In[18], a novel Collaborative IDS Framework has been proposed for Cloud. This framework integrates Snort to detect the known attacks using signature matching. To detect unknown attacks, anomaly detection system (ADS) is built using Decision Tree Classifier and Support Vector Machine (SVM). Alert Correlation and automatic signature generation reduce the impact of DoS and DDoS attacks and increase the performance and accuracy of IDS. However, it requires a high training time.

Al-Mousa et Nasir [19] have proposed a cloud based cooperative intrusion detection and prevention system (cl-CIDPS). Cl-CIDPS uses both techniques viz; signature based detection and anomaly detection in a network based IDPS, distributed in different cloud regions. The proposed scheme follows peer-to-peer communication principles. It used NeSSi2 to evaluate the system performance and detection rate. The results show significant improves in the performance for both detection modes (signature based detection and anomaly detection). However, it requires several extensions. Indeed, Cloud regions can be extended to incorporate more than two regions. Moreover, data collected from cl-CIDPS can be correlated with data collected from other security tools. Now, we provide in table I an analytical study of above approaches and frameworks (H-NIDS) proposed for Cloud Computing.

Table I. Analytical study of Cloud based H-NIDS

Features **References**	**IDS type**	**Detection time**	**Positioning**	**Advantages**	**Limitations/Challenges**
a novel security (H-NIDS) in cloud, 2013[6]	Network based	Real time	On each host machine	It has higher detection rate and low false positives at an affordable computational cost	Associative classifier generates a high number of false positives, while individually used it
Intrusion Detection for Grid /Cloud 2010[11]	Host based	Real time	On each node	False rate for unknown attack is lower since ANN used	Requires more training samples as well as more time for detecting intrusions effectively
Intrusion Detection for IaaS Cloud, 2011[12]	VMM based	Real time	On hypervisor (VMM)	Efficient for attack detection in cloud because the VMM has complete control of the system	This model has not presented any solution to heal the system if the infrastructure collapsed
CIDS: A framework for Intrusion Detection in Cloud, 2012[13]	Host based and Network based	Real time	On each node	a scalable and elastic architecture with a P2P solution for Grid and cloud computing	It is not sufficient for detecting large scale distributed attacks and there is no central correlation handler
IDS for cloud computing 2012[14]	distributed	Real time	At the processing server	Can process and analyze a large flow of network packets	Implementation details are not given to prove the concept
IDS in Cloud Environment, 2011[15]	Host based and network based	Real time	On each node	The number of packets dropped will be less due to the lesser load which single IDS instance will have.	Experimental results are not provided
EICIDS-Elastic and Internal Cloud-based IDS, 2015[7]	Host based	Real time	On each node and outside the Cloud	EICIDS reside outside the virtual environment, and thus protected from attacks	The architecture of EICIDS is centralized, this it is not tolerant to failure
Framework for Distributed and Self-healing Hybrid IDPS, 2013[16]	Host based and network based	Real time	On hypervisor	Multi- threaded processing for optimum speed and throughput and versatile coverage scenarios	High computation cost
NIDS in Cloud, 2012 [17]	Network based	Real time	At the processing server	Detection rate is very high	Requires more number of training samples
Collaborative IDS Framework for Cloud, 2015[18]	Network based	Real time	On each cluster	Protects against DDoS attacks	Requires more training samples
A Cloud Based Cooperative framework, 2015[19]	Network based	Real time	in each edge node	Improved detection rate	Cloud regions can be extended to incorporate more than two regions

Our proposed framework provides solution to limitations existing in these approaches and frameworks.

3. Proposed framework for Network Intrusion Detection System in cloud computing

3.1 Integration of C-NIDS in Cloud

The principal objective of our proposed (C-NIDS) is to design and integrate a Network Intrusion Detection System (NIDS) that can detect network intrusions in Cloud environment, while reducing false alarm rate with affordable computational and communication cost. Therefore, our NIDS is able to handle heavy traffic in cloud without dropping packets. According to[20], there are different positioning of NIDS in Cloud viz; on front-end, on back-end (or processing server) and on each virtual machine. Integrating NIDS module on front end of Cloud helps to detect network intrusions at external network of Cloud. However, it is not able to detect attack at internal network of Cloud; positioning NIDS module on processing server helps to detect intrusions at internal network of Cloud. It will also detect the intrusions coming from external network. But, large number of packets passing through server will result in packet dropping and NIDS may be overloaded; integration of NIDS on each VM helps user for detecting intrusion on his VM. Such configuration requires multiple instances of NIDS, which makes complex management of NIDS since VMs are dynamically migrated, provisioned or deprovisioned.

As shown in the Figure.1, we propose to deploy our NIDS sensors at the front end as well as at the back end on Virtual Machine Monitor (VMM) to detect external and internal attacks and to efficiently deal with the attacks on the customer virtual machines in the Cloud infrastructure. Indeed, the VMM has complete control on the resources, good visibility into the internal state of the virtual machines and isolated from the virtual machines.

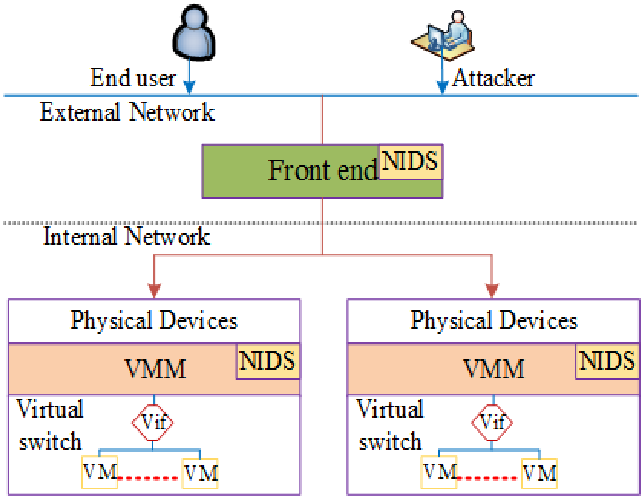

Figure 1. Positions of NIDS in Cloud

3.2 Architecture of our C-NIDS framework

The architecture of proposed framework (C-NIDS) is shown in the Figure 2. It mainly consists of five components, namely: Packet Sniffing, Signature based Detection, Anomaly Detection, Alert System and Central Log Database.

3.2.1 *Packet Sniffing*

From the network, the packet sniffing captures the in-bound and out-bound network packets for auditing using lipcap library. For this purpose, packet sniffing tools can be used (e.g Wireshark). So, these packets are inspected in real-time by signature based detection technique.

3.2.2 *Signature based Detection*

We use knowledge base that is generated based on preconfigured and predefined network attack rules. In knowledge base, we store Cloud related known attack rules. Snort process and matches the captured packets against pre-defined set of rules stored in the knowledge base to find any correlation. If it detects an attack, it determines the nature of the attack and sends warning message to Alert System. The normal packets, specified by Snort, are forwarded to Anomaly Detection for further processing. Snort is working on rules which can be written in any language and rules can be easily read and modified.

3.2.3 *Anomaly detection*

The anomaly detection system (ADS) is built using Support Vector Machine (SVM). In learning phase, ADS is trained using previously observed network behaviours that are stored in behaviour base. It predicts the class label (Intrusion or Normal) of the given network packets. If it finds any intrusion, it sends warning message to Alert system, whereas the packet is considered as legitimate packet and allowed to Cloud infrastructure.

3.2.4 *Alert System*

It generates alerts about intrusion that is determined either by signature based detection system or anomaly detection system. It stores alerted intrusion in the central log database where intrusion alerts from NIDS sensors at other regions are stored.

3.2.5 *Central Log Database*

It is used for NIDS sensors deployed on other regions. Other NIDS sensors update their bases with alerts logged in central log database. So, Next time, such intrusion can be easily detected by using the signature based detection system at other regions. This reduces computational cost and enhances the accuracy of NIDS.

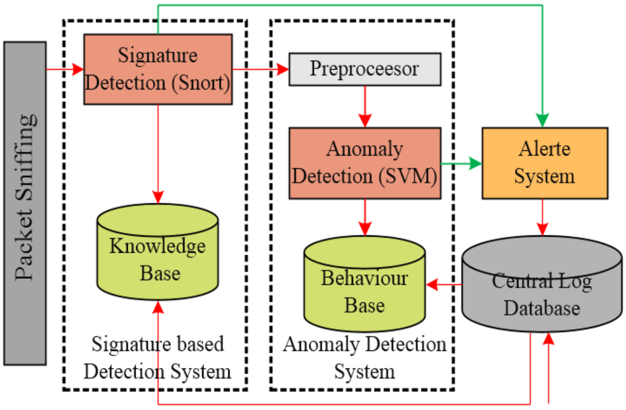

Figure 2. Architecture of C-NIDS framework proposed

3.3 Workflow of our C-NIDS proposed

As shown in the Figure.3, network traffic is captured from network (external or internal) and parsed into multiple threads for concurrent execution and sent to the signature based detection. By adopting the concurrent executing threads the performance could be optimized in terms of latency and packet loss. Then signature based detection technique is applied on captured packets to detect intrusions. It logs intrusion packets in central alert database. Non-intrusion packets are pre-processed for anomaly detection using pre-processor component. Anomaly detection (SVM) is applied to predict class label (normal or intrusion) of non-intrusion packets by observing behaviour base. Intrusions (predicted by anomaly detection) are logged into central alert database. Otherwise, the normal packets are considered as normal and allowed into the system. NIDS sensors deployed on other regions updates their knowledge base with the alerts found in central alert database.

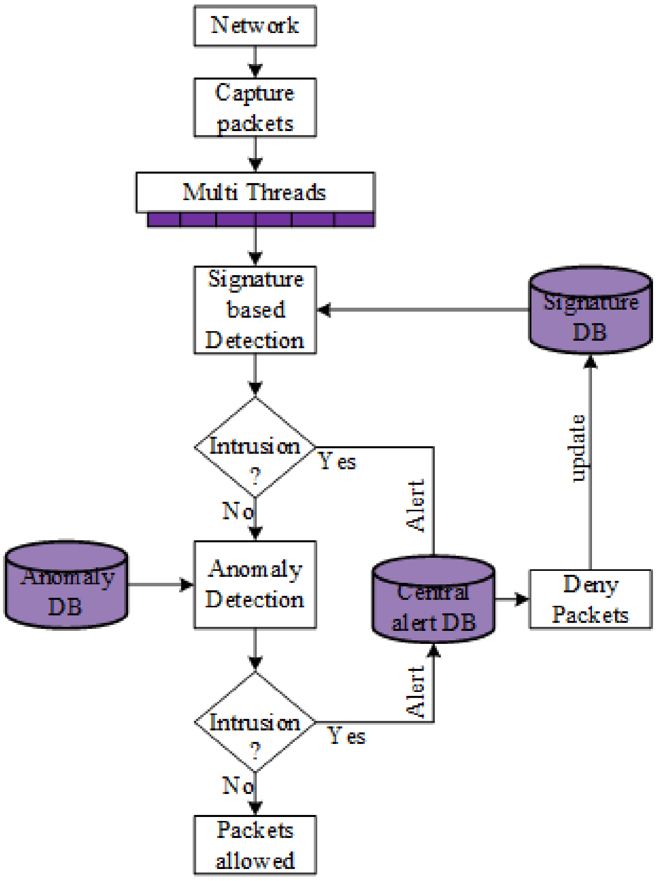

Figure 3. Workflow of C-NIDS proposed

4. Discussion

Nowadays, Cloud computing has emerged as an important paradigm in the use of computing resources as a service over the Internet. It enables IT managers to provision services to users faster and in a cost-effective way. Apart from these advantages, security of Cloud resources is the biggest concern. Indeed, Cloud suffers from traditional attacks such as Address Resolution Protocol (ARP) Spoofing, man-in-the-middle attack, Denial of Service (DoS) and Distributed DoS (DDoS) attacks, etc[4]. These attacks can affect Cloud resources and offered services. Consequently, many Cloud providers (like Windows Azure, Eucalyptus, etc.) use firewalls. Firewalls are better to prevent many outsider attacks. However, insider attacks as well as some complicated outsider attacks cannot be detected by it. For instance, if there is an attack on port 25 (Mail server), firewall cannot differentiate normal traffic from attack traffic. To overcome these issues, we propose a Collaborative Framework for Network Intrusion Detection System (C-NIDS) in Cloud Computing that uses Snort and Support Vector Machine (SVM). Our framework is deployed at the front end as well as at the back end on Virtual Machine Monitor (VMM) to detect external and internal attacks, coming either from internal physical network or the virtual network on Virtual Machine Monitor. Our NIDS uses both signature based and anomaly based techniques to improve detection accuracy. The signature based detection technique is applied prior to anomaly detection, resulted in reducing computational cost and detection time. In addition, by using Central log database, NIDS sensors deployed in cloud work in collaborative manner, they update their bases by getting packets stored in the central log database. So, next time, such intrusion can be easily detected by using the signature based detection system at other servers. This also helps to reduce computational cost and enhances the accuracy of NIDS in overall the cloud. In general, our proposed NIDS is able to detect a high number of intrusions with low false positives and low false negatives at the network layer. It has capability for detecting known as well as unknown attacks efficiently, while most of other existing solutions[21] [20] [22] [23] [24]can detect only known attacks.

5. Conclusions and Future Works

Cloud Computing is the most emerging technology that is rapidly being adopted by the IT industry due to its cost effective nature, easy accessibility, efficient resources utilization and the pay per use service. One of the major security issue in Cloud computing is to detect distributed attacks and malicious activities on the network that can affect Cloud resources and offered services. To overcome this issue, in this paper, we proposed a new framework (C-NIDS) that integrates SVM classifier techniques and Snort based network intrusion detection system in Cloud infrastructure. Our C-NIDS uses two distinct techniques (signature based and anomaly base) which are complementing each other. Therefore, it is able to detect known as well as unknown attacks in Cloud infrastructure. The collaboration between NIDS prevents the coordinated attacks against cloud infrastructure and knowledge base remains up-to-date. We are planning in the future work to implement our NIDS module in open source Cloud environment, enhance SVM performance and improve training speed and detection accuracy of SVM model to put more complete smart IDS into practice.

References

[1] A. M. Lonea, D. E. Popescu, and H. Tianfield, “Detecting DDoS attacks in cloud computing environment”, International Journal of Computers Communications & Control, vol. 8, no. 1, pp. 70–78, 2013.

[2] M. Peter and G. Timothy, “The NIST Definition of Cloud Computing”, National Institute of Standards and Technology, availbale in:<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf >, Sep. 2011.

[3] H. Wu, Y. Ding, C. Winer, and L. Yao, “Network security for virtual machine in cloud computing”, 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT), Seoul, pp. 18–21 , 2010.

[4] N. Jeyanthi, and N. C. S. Iyengar, “Packet Resonance Strategy: A Spoof Attack Detection and Prevention Mechanism in Cloud Computing Environment”., Vol. 4, No. 3, p. 163-173, 2012.

[5] C. N. Modi and K. Acha, “Virtualization layer security challenges and intrusion detection/prevention systems in cloud computing: a comprehensive review”, The Journal of Supercomputing, Jul. 2016.

[6] lockheed Martin, “Awareness, Trust and Security to Shape Government Cloud Adoption”. available in :<http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/Cloud-Computing-White-Paper.pdf>, Apr.2010.

[7] C. Modi and D. Patel, “A Novel hybrid-Network Intrusion Detection System (H-NIDS) in Cloud Computing”, the IEEE Symposium Computational Intelligence in Cyber Security (CICS), Singapore, India, pp. 23–30, 2013.

[8] J. D. Araújo, D. de Andrade Rodrigues, L. S. de Melo, and Z. Abdelouahab, “EICIDS-elastic and internal cloud-based detection system”, International Journal of Communication Networks and Information Security (IJCNIS), vol. 7, no. 1, p. 34, 2015.

[9] N. Jeyanthi, N. C. S. Iyengar, P. M. Kumar, and A. Kannammal, “An enhanced entropy approach to detect and prevent DDoS in cloud environment”, International Journal of Communication Networks and Information Security(IJCNIS)., vol. 5, no. 2, p. 110, 2013.

[10] J. H. Song, G. Zhao, and J. Y. Song, “Research on Property and Model Optimization of Multiclass SVM for NIDS”, Applied Mechanics and Materials, vol. 347, pp. 3696–3701, 2013.

[11] D. S. Kim and J. S. Park, “Network-based intrusion detection with support vector machines”, International Conference on Information Networking, , Cheju Island, Korea, pp. 747–756, 2003.

[12] [12] K. Vieira, A. Schulter, C. Westphall, and C. Westphall, “Intrusion detection for grid and cloud computing”, IT Professional Magazine, vol. 12, no. 4, pp. 38–43, 2010.

[13] U. Tupakula, V. Varadharajan, and N. Akku, “Intrusion Detection Techniques for Infrastructure as a Service Cloud”, Ninth International Conference on Dependable, Autonomic and Secure Computing, Sydney-NSW, pp. 744–751, 2011.

[14] H. A. Kholidy and F. Baiardi, “CIDS: A Framework for Intrusion Detection in Cloud Systems”, Ninth International Conference on Information Technology - New Generations, Las Vegas-NV, pp. 379–385, 2012.

[15] I. Gul and M. Hussain, “Distributed cloud intrusion detection model”, International Journal of Advanced Science and Technology, vol. 34, pp. 71–82, Sep. 2011.

[16] S. N. Dhage, B. B. Meshram, and R. Rawat, “Intrusion Detection System in Cloud Computing Environment”, the International Conference & Workshop on Emerging Trends in Technology ICWET ’11, Mumbai-India, pp. 235–239, 2011.

[17] F. Idress, R. Muttukrishnan, and M. A.Y, “Framework for Distributed and Self-healing Hybrid Intrusion Detection and Prevention System”, the International Conference on ICT Convergence (ICTC), Jeju, pp. 277–282, 2013.

[18] C. Modi, D. Patel, R. Muttukrishnan, and A. Patel, “Bayesian Classifier and Snort based Network Intrusion Detection System in Cloud Computing”, Third International Conference on Computing Communication & Networking Technologies (ICCCNT), Coimbatore-India, pp. 1–7, 2012.

[19] S. Dinesh, P. Dhiren, B. Bhavesh, and M. Chirag, “Collaborative IDS Framework for Cloud”, International Journal of Network Security, vol. 18, no. 4, pp. 99–709, Sep. 2015.

[20] Z. Al-Mousa and Q. Nasir, “cl-CIDPS: A Cloud Computing Based Cooperative Intrusion Detection and Prevention System Framework”, Future Network Systems and Security, vol. 523, R. Doss, S. Piramuthu, and W. Zhou, Eds. Cham: Springer International Publishing, pp. 181–194, 2015.

[21] C. N. Modi, D. R. Patel, A. Patel, and M. Rajarajan, “Integrating Signature Apriori based Network Intrusion Detection System (NIDS) in Cloud Computing”, Procedia Technology., vol. 6, pp. 905–912, 2012.

[22] C.C Lo, C.C huang, and J.ku, “Cooperative Intrusion Detection System Framework for Cloud Computing”, IEEE International Conference on Ubi-Media Computing, San Diego-CA, pp. 280–284, 2008.

[23] S.Ram, “Secure Cloud computing based on mutual intrusion detection system”, International journal of computer application, vol. 2, no. 1, pp. 57–67, 2012.

[24] C. Mazzariello, R. Bifulco, and R. Canonico, “Integrating a network ids into an open source cloud computing environment”, Sixth International Conference on Information Assurance and Security (IAS), Atlanta-GA, pp. 265–270, 2010.

[25] S. Roschke, F. Cheng, and C. Meinel, “An Extensible and Virtualization-Compatible IDS Management Architecture”, Fifth International Conference on Information Assurance and Security, Xi'an, pp. 130–134, 2009.