Intrusion Detection Techniques in Cloud Computing: A Review

Nurudeen Mahmud Ibrahim
Department of Computer Science
Universiti Teknologi Malaysia

Anazida Zainal
Department of Computer Science
Universiti Teknologi Malaysia

ABSTRACT
In this paper a review of cloud-based intrusion detection system was provided. The review gives a detailed taxonomy of the existing approaches adopted by researchers in cloud intrusion detection system. The components of the taxonomy are the detection domain, detection technique, strategy for creating normal profile the architectural structure adopted by the intrusion detection system and the detection time. Based on the review open problems and research direction in cloud intrusion detection was provided.

General Terms
Review

Keywords
Cloud computing, Security, Review, Taxonomy, Intrusion Detection Techniques

1. INTRODUCTION
The National Institute of Standard and Technology (NIST) defines cloud computing as a computing paradigm that offers on-demand network access to a shared computing resources eg.(Networks, servers, storage, application and services), that can be provided readily with little management effort or interaction from service provider [1]. Cloud computing has revolutionized the conventional usage of hardware and software resources. Organizations do not need to purchase and maintain expensive hardware and software as they can subscribe for it on a pay-per-use basis. Due to its instant scalability, virtualisation, resource optimization, economic benefit through reduction of capital and operational expenditure, cloud computing has become an attractive technology with a rapid pace of acceptance in the IT community [2]. The Cloud model is made up four deployment models and three delivery model. The Cloud deployment models are public, private and hybrid cloud while the service models are Infrastructure-as-a-Service (IaaS), the Platform-as-a Service (PaaS) and the Software-as-a-Service (SaaS) [3]. Cloud computing is a promising and emerging IT technology with enormous potentials and benefits to customers; however there are underlying security issues and vulnerabilities [4-6]. For instance an adversary with malicious intent can take advantage of the rich features of cloud computing such as multi-tenancy and resource pooling to compromise the data security and privacy [7]. In this paper, a review of intrusion detection techniques in cloud computing was provided, a taxonomy of cloud computing according to detection domain, detection technique, architecture, strategy for creating normal profile and detection time was discussed. Based on the review, research issues in cloud computing was identified. The remainder of this paper is organized as follows: section 2 discusses on related reviews in cloud IDS, section 3 discusses a taxonomy of IDS in cloud computing, section 4 concludes the paper and suggests future research directions.

2. RELATED WORKS
In [7] Osainaiye *et al*. conducted a survey on approaches to detect both application-bug level and infrastructure level DDoS attack in cloud computing. However, the review was limited to only detecting DDoS attack and does not cover other kind of attacks. In [8] Patel *et. al* conducted a survey on intrusion detection and prevention techniques in cloud computing and also provides a taxonomy of IDS in cloud that comprises of the structural and functional layer of IDS in the cloud. Also, requirements for cloud IDS was provided. Modi *et al.* [9] and Raghav et al. [10] surveyed IDPS systems for cloud computing however, different from Raghav *et a*l. [10] , Modi *et al.* [9] further provides advantages and disadvantages of various IDPS techniques and subsequently highlights security issues that need to be addressed to improve cloud security. In [11] Sari conducted a review on existing cloud IDS technique and also performed a comparative study on the measures taken by Dropbox, Google Drive and iCloud to secure its cloud infrastructure. The above review papers provided recent research on existing cloud-based IDS however, these approaches lack a comprehensive taxonomy on research in cloud IDS.

3. INTRUSION DETECTION SYSTEMS
Intrusion detection is the process of monitoring activities happening in a system or a network and investigating it for signs of security incidents that breaches or presents impending threat of breach to a systems security policy or standard security practice. There are different classifications of IDS depending on the target of protection IDS can be categorized as host-based (HIDS) and network-based (NIDS) or application based. Also, IDS can be classified into signature-based and anomaly detection depending on whether the kind of attack to be detected is known beforehand or unknown [12].

3.1 Taxonomy of Cloud-based IDS
Intrusion detection is the process of monitoring activities happening in a system or a network and investigating it for signs of security incidents that breaches or presents impending threat of breach to a systems security policy or standard security practice. As shown in Fig. 1, there are different classifications of IDS depending on the target of protection IDS can be categorized as host-based (HIDS) and network-based (NIDS). Also, IDS can be classified into signature-based and anomaly detection depending on whether the kind of attack to be detected is known beforehand or unknown. In terms of normal profile creation IDS can statically create normal profile or adopt a dynamic strategy to update the normal profile. The IDS architecture can be centralized where IDS analyses data obtained from a single monitored system

and distributed where the IDS obtains information from multiple system under surveillance with a view to analyzing coordinated attack. IDS detection time can be performed offline or in real time.

3.1.1 Detection Domain

The detection domain is the IDS source of information. To obtain relevant attack data, virtually all IDS monitors a computer host /network or application [13]. Host-based IDS monitors a single host for security related events. Network-based IDS monitors network traffic with a view to identify attack or malicious events violating security policy while application based monitors a particular application.

3.1.2 Detection Techniques

Depending on the approach used to monitor and recognize malicious events, cloud-based intrusion detection systems can be categorized into three main techniques: signature based anomaly detection and hybrid technique.

3.1.2.1 Signature-Based

The Signature-based technique to intrusion detection system identifies malicious events by defining a collection of rules that can be used to determine attack patterns. Consequently, the signature based approach has high detection accuracy when identifying intrusion. However, this approach can only detect known attacks and minor differences in the predefined attack pattern may not be detected by the signature based technique. The technique also requires the regular update of the signature database to capture new forms of attack [14]. Example of tools used in signature-based IDS is snort. Snort uses the packet header (e.g. Source address, destination address, port) and its options (e.g. payload, metadata), to identify if a network traffic that tallies to an already known signature. Existing research work in the cloud using signature based detection technique is described as follows: Ficco *et al*. [15] presented a framework for offering IDS in a distributed cloud setting. The approach involves the gathering of information at various layers of the cloud architecture, such as the IaaS, PaaS, and SaaS using security components deployed at the various cloud layer. Signature of various kinds of attack are monitored in order to link these attacks to the predefined signatures. Signature based tool such as Snort was used for this purpose. Tupakala *et al* [16] proposed a signature based architecture and prototype IDS tool for cloud offering IaaS. The architecture is comprised of the following component. (a) Packet Screener; (b) The OS library and repository and (c) The detection component. These components work collectively to ensure that all inbound and outbound traffics are devoid of malicious content, if malicious content are found the packet is dropped. Chouhan *et al.* [17] proposed an approach for detecting malware in a virtualized context. The approach monitors network traffic in order to detect malicious activities. Traffic emanating from every virtual machine is monitored and an alert is triggered if malicious activity is detected.

3.1.2.2 Anomaly Detection

Anomaly detection system is the identification of events that deviates from normal system behavior. Different approaches have been proposed for anomaly detection such as: statistical based technique, machine learning and knowledge based technique. Anomaly detection technique basically operates by obtaining data pertaining to normal system behavior over a given time period and then identify anomalous behavior by applying either of the aforementioned technique. Anomaly detection techniques can be used for cloud to detect unknown attacks at different levels such as IaaS, PaaS SaaS [9].The three major categorization of anomaly-based IDS are: statistical-based, knowledge-based and machine learning. In statistical based technique, random observations are used to represent system behavior. Knowledge-based IDS uses knowledge pre-defined in the system to capture attacks. The machine learning techniques use models created as a basis for classifying normal or anomalous data [18].

3.1.2.2.1 Statistical-Based Technique

Anomaly detection using statistical profile involves observing the data of the current network profile and comparing it against the statistical profile previously trained [19]. In the cloud, statistical-based technique have been employed for anomaly detection. Zakarya [20] proposed an entropy based statistical technique and packet dropping algorithm for detecting DDoS. The distribution ratio of the entropy is utilized to determine flow of attack. Ismail *et al* [21] proposed a model for detecting DDoS attack in the cloud environment using covariance matrix. Similar research work in statistical based cloud IDS are the work of Gupta and Kumar [22] and Shamsomoali and Zareapoor [23].

3.1.2.2.2 Knowledge-Based Techniques

The prevalently used technique for the knowledge-based IDS is the use of expert system. Similar to other anomaly detection

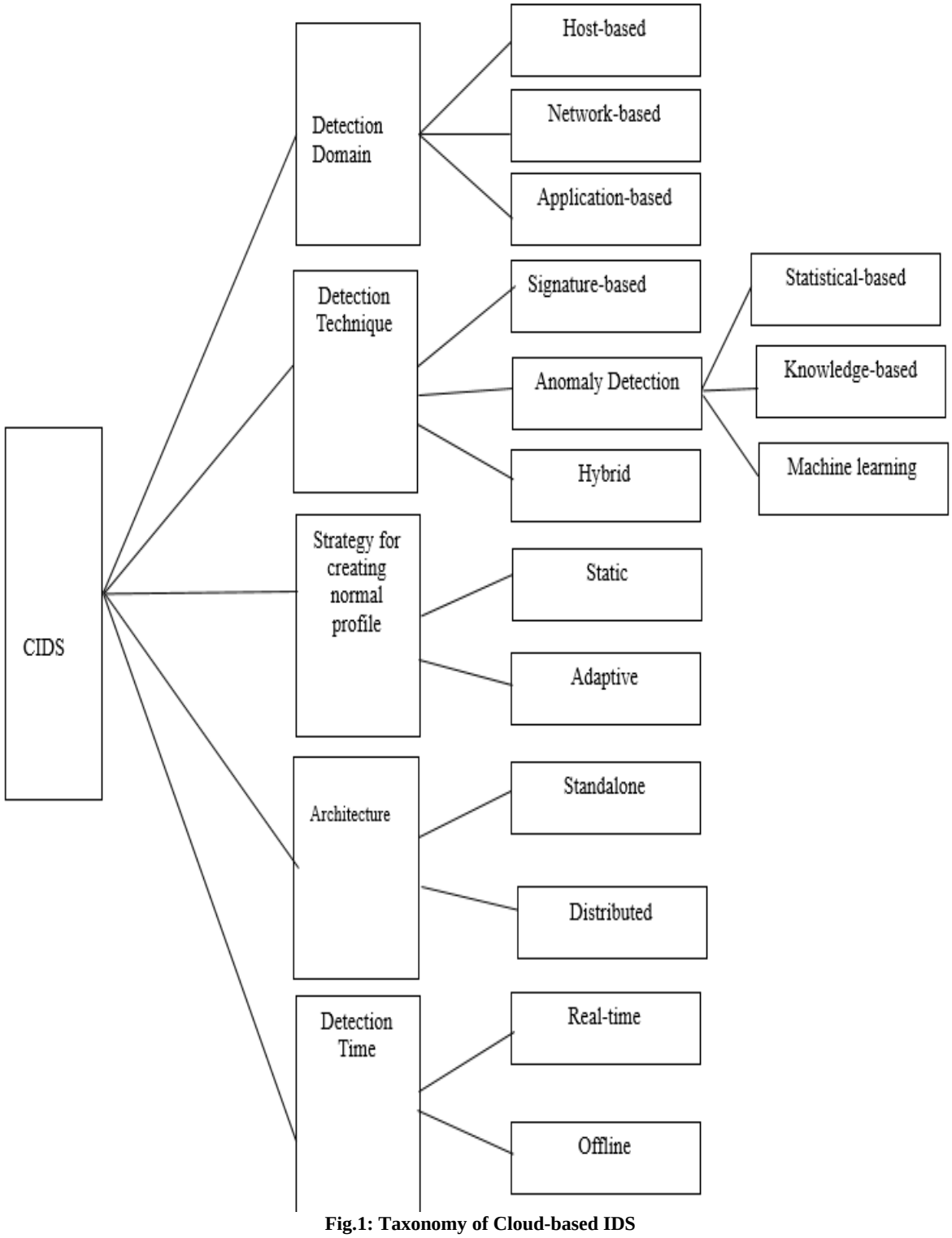

Fig.1: Taxonomy of Cloud-based IDS

techniques, expert systems can fall into different categories [19]. Expert system anomaly detection technique operates by employing a set of rules to classify the audit data. In some cases knowledge based anomaly detection system are specification based, where the model of the anomaly detection technique is designed using a collection of rules that specifies the normal system behavior. Other approaches for specifying system behavior in knowledge-based IDS is the use of finite state machine (FSM) [24].Modelling language that can be used for this purpose are N-grams, UML and LOTOS.

3.1.2.2.3 Machine Learning

Machine learning techniques create a model that is used to classify the pattern analyzed. This approach uses dataset for training the model however these processes often results in computing overhead. Often, machine learning overlaps with the statistical technique but the machine learning technique emphasizes on improving the performance of the model from the previous data learnt. These attribute makes machine learning more desirable but the major downside is the computing overhead. Below is some of the widely used machine learning techniques [19].

3.1.2.2.3.1 Bayesian Network

A Bayesian network creates a stochastic relation among variable observed. This approach is employed for anomaly detection alongside statistical approaches. The advantage of Bayesian network is its ability to encode interrelationships among variables and classifying events and also its ability to incorporate previously acquired knowledge and data during prediction [25].The major disadvantage is that it bears a lot of similarities with approaches based on threshold and has high computation demand [26].

3.1.2.2.3.2 Markov Models

Markov models can be classified into Markov chains and Hidden Markov models. A Markov chain is a collection of linked states via a transition probability on which the capability and the layout of the model is dependent on. The probabilities related to the transition are deduced during the training stage from the normal behavior of the system. Anomaly detection is then conducted through the comparison of the associated probability derived from the sequence observed with a predefined threshold. In a hidden Markov model, the states are not observable but when a state is visited an observation is recorded that is a probabilistic function of the state [27]. In the cloud HMM have been employed for host-based IDS in [28].

3.1.2.2.3.3 Neural Network

Neural network functions based on the emulation of the human brain. It is widely used in anomaly detection owing to their flexibility and adaptive ability to contextual variation. Neural network is employed in order to create a profile for a user to predict next command from previous sequence in order to identify anomalous traffic pattern. Pandeeswari and Kumar [29] proposed an anomaly detection technique for classifying four kinds of network attacks: U2R, Probe, DoS, R2L using Fuzzy C-Mean clustering-ANN to enhance efficacy of anomaly detection techniques suffering from detection inaccuracies of infrequent attacks. Also Xiong *et al* [30] proposed two approaches for detecting anomaly in communication in the cloud network traffic by using two techniques as follows: synergetic neural network and catastrophe theory.

3.1.2.2.3.4 Fuzzy Logic Technique

Fuzzy logic originates from fuzzy set theory where reasoning is estimated and not derived exactly from predicate logic. The application of anomaly detection in fuzzy logic is because the feature of the traffic to be observed is considered as imprecise variable. Observation that falls within a given interval are considered to be normal. Fuzzy logic has been successfully applied to detect attacks such as port scan, probe etc. The main disadvantage of the scheme is the high resource consumption [31].

3.1.2.2.3.5 Clustering and Outlier Detection

Clustering technique use the measurement of similarity or distance to group data observed into clusters. Fundamentally the technique chooses a point to represent each cluster and the new data point are classified under a cluster according to their proximity to the point representing the cluster. Certain point that does not fall under any cluster are considered outliers and termed as anomaly in the anomaly detection process. Clustering technique is also used in cloud-based IDS. Shirazi *et al.* [32] assessed the impact of VM migration to detection of anomaly by performing experiments using clustering. They reported in their work a high degradation of anomaly detection technique in the event of VM migration.

3.1.2.2.1.6 Support Vector Machine

SVM is a type of machine learning algorithm that is developed by Vapnik [33]. Due to the robust performance of SVM when dealing with noisy and sparse data, it has become a system of choice in many machine learning applications. SVM finds a hyper-plane in the feature space corresponding to the non-linear decision boundary [34]. For cloud-based IDS Singh *et al.* [35] proposed a hybrid and collaborative IDS using both signature-based technique and anomaly detection. The signature-based technique uses snort for detecting predefined attacks while the anomaly detection system uses decision tree classifier and SVM for detecting distributed attacks. The approach is however not adaptive and therefore results in poor performance when reference model changes.

3.1.2.3 Hybrid Techniques

Hybrid detection techniques use the combination of two or more of above techniques in order to improve the efficacy of the IDS. Modi *et al.*[9] proposed an approach for intrusion detection in the cloud that employs both anomaly detection and the signature based approach by combining the use of Snort and Decision Tree Classifier. Biedermann and Katzenbeisser [36] proposed a hybrid based approach for detecting computer worms in the cloud. They used a centralized virtual machine introspection (VMI) to collect information about the virtual machine running in the cloud back-end in order to detect malicious programming spreading in the network. Similar Hybrid cloud IDS is the work of Kholidy and Baraidi [37].

Table 1: Summary of research in Cloud-based IDS

Reference	Detection Domain			Detection Technique			Strategy for creating normal profile		Architecture		Detection Time		Dataset used for validation
	Host-based	Network-based	Application-based	Signature-based	Anomaly Detection	Hybrid	Static	Adaptive	Standalone	Distributed	Offline	Real-time	
[43]		✓			✓		✓		✓		✓		KDDCup 1999
[38]	✓				✓			✓	✓		✓		Simulation with XEN
[39]		✓			✓		✓		✓		✓		Simulation with Flame tool and SWITCH
[40]		✓		✓			✓			✓	✓		Not specified
[41]		✓			✓		✓			✓	✓		Not specified
[42]	✓				✓			✓	✓		✓		Simulation with XEN
[43]	✓					✓	✓			✓	✓		Not specified
[44]		✓				✓		✓		✓	✓		Not specified
[32]		✓			✓		✓		✓		✓		Simulation (KVM)
[44]		✓			✓			✓	✓		✓		UCLA dataset
[45]		✓			✓		✓		✓		✓		KDDcup 1999
[46]		✓			✓		✓		✓		✓		KDDcup1999
[48]	✓			✓			✓			✓	✓		Simulation with XEN
[49]		✓		✓				✓	✓		✓		Not specified
[50]		✓		✓				✓		✓	✓		Not specified
[35]		✓				✓	✓			✓	✓		NSL-KDD
[51]	✓				✓			✓		✓	✓		Not specified
[52]		✓			✓			✓		✓	✓		KDDcup 1999
[53]		✓			✓		✓				✓		KDDcup 1999
[54]		✓			✓			✓	✓		✓		KDDcup 199
[28]	✓				✓		✓		✓		✓		Simualtion (KVM)
[21]		✓				✓	✓		✓		✓		Simulation (VMware)
[30]		✓				✓		✓		✓	✓		KDDcup 1999
[16]		✓		✓			✓		✓		✓		Simulation XEN
[37]	✓					✓	✓			✓	✓		Not specified

3.1.3 Strategies for Creating Normal Profile

The normal profile creation can be static or dynamically updated in order to prevent false alarm caused by changing normal pattern. Research work in cloud-based IDS has employed both static and dynamic approach for normal profile creation.

3.1.3.1 Static Technique

For anomaly detection a static IDS performs a one-time training of the IDS and does not update the reference model even when change occurs. Majority of the research in cloud-based IDS, have employed the static approach. [9, 15, 16, 17.20, 21, 22, 23] etc. However, the static approach have limitations as it does not adapt to changing environment.

3.1.3.2 Adaptive Technique

The dynamic or adaptive IDS adopt a dynamic strategy to update the reference model to cope with dynamic changes in the cloud environment. Research works in cloud that employing the adaptive approach for designing IDS are [31, 38, 42, 44, 48, 49,].

3.1.4 Architectural Structure

The architectural structure of an IDS can be categorized into two: standalone and collaborative. A standalone IDS only monitors a single host or network while the collaborative IDS is comprised of many IDS over different host or networks that share alert information among each other to detect coordinated attacks. However mist of these approaches are based on theoretical framework and not empirically validated.

3.1.4.1 Standalone

The standalone IDS only monitors a single host or network to detect attacks. Because a standalone IDS monitors a network or host independently its capability to detect coordinated attacks is limited. In the cloud a number of research work is conducted on standalone IDS [9, 15, 20, 21, 22, 23, 28, 29, 30].

3.1.4.2 Distributed/Collaborative

A collaborative IDS is comprised of many IDS over different sub networks or host that share alerts among each other to detect coordinated attacks. A collaborative IDS have the potentials of detecting attacks shared over several host or networks by correlating attack evidence across several sub network [8].Research work on collaborative cloud-based IDS are [35,36,37,40,41,49].

3.1.5 Detection Time

Depending on the time the IDS detect a security incident, IDS can be categorized as either real-time or offline. Real-time IDS offers prompt attack identification at the moment of the incident and can instantly flag any violation of the configured policy and can provide appropriate response to mitigate or halt the attack. The real time IDS learns the models incrementally on an instance by instance basis. This approach to learning is suitable when all the data is not available but comes on an instance by instance basis. Past Intrusion can also be identified through offline analysis of the IDS audit source. According to the literature surveyed (Table 1) all cloud-based IDS perform off-line detection.

4. CONCLUSION

In this paper a review of existing intrusion detection techniques in cloud computing was provided. The review gives a taxonomy of cloud-based IDS according to the detection domain, detection technique, and strategy for creating normal profile, the IDS architecture and the time of detection. Based on the review open issues in cloud-based IDS was identified and suggestion for future research was made. The research shows that a number of research work have been conducted in cloud-based IDS. The research work in cloud IDS spans various detection technique, domain, architectural structure and detection time. However, the open research issues in cloud-based IDS is the presence of high false alarm owing to highly dynamic environment with nodes dynamically added and removed therefore, IDS are required to possess the capability that will cope with the dynamic cloud environment. Also, the distributed cloud nature makes its susceptible to distributed attack; however, majority of existing approach to detecting distributed attack in IDS using collaborative IDS are not validated.

5. ACKNOWLEDGMENT

This work is supported by the Ministry of higher Education (MOHE) and Research Management Center (RMC) at the Universiti Teknologi Malaysia under Fundamental Research Grant (FRGS) (VOT R.J130000.7828.4F809.)

6. REFERENCES

[1] Mell, P., and Tim G. 2011. The NIST definition of cloud computing.

[2] Gupta, S., and Padam K.. 2015. An Immediate System Call Sequence Based Approach for Detecting Malicious Program Executions in Cloud Environment. Wireless Personal Communications 81(1):405-425.

[3] Tsai, W. K, Xin, S., and Janaka B. 2010. Service-oriented cloud computing architecture. Information Technology: New Generations (ITNG), 2010 Seventh International Conference on, 2010, pp. 684-689. IEEE.

[4] Chonka, A., Xiang,Y. Zhou, W. and Bonti A. 2011. Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks. Journal of Network and Computer Applications 34(4):1097-1107.

[5] Khorshed, M., T, Shawkat A, and Saleh A W. 2012. A survey on gaps, threat remediation challenges and some thoughts for proactive attack detection in cloud computing. Future Generation computer systems 28(6):833-851.

[6] Sen, J. 2013. Security and privacy issues in cloud computing. Architectures and Protocols for Secure Information Technology Infrastructures: 1-45.

[7] Osanaiye, O., Kim-Kwang R. C., and Mqhele, D. 2016.Distributed denial of service (DDoS) resilience in cloud: review and conceptual cloud DDoS mitigation framework. Journal of Network and Computer Applications 67:147-165.

[8] Patel, A., Taghavi, M. Bakhtiyari, K. JúNior, J.C. 2013. An intrusion detection and prevention system in cloud computing: A systematic review. Journal of network and computer applications 36(1):25-41.

[9] Modi, C., Patel, D., Borisaniya, B. Patel, H., Patel, A., Rajarajan, M., 2013. A survey of intrusion detection techniques in cloud. Journal of Network and Computer Applications 36(1):42-57.

[10] Raghav, I., Shashi C., and Nitasha H. 2013. Intrusion Detection and Prevention in Cloud Environment: A

Systematic Review. International Journal of Computer Applications 68(24).

[11] Sari, A. 2015. A Review of Anomaly Detection Systems in Cloud Networks and Survey of Cloud Security Measures in Cloud Storage Applications. Journal of Information Security 6(02):142.

[12] Scarfone, K., and Peter M. 2007. Guide to intrusion detection and prevention systems (idps). NIST special publication 800(2007):94.

[13] Yeung, D., and Yuxin, D. 2003. Host-based intrusion detection using dynamic and static behavioral models. Pattern recognition 36(1):229-243.

[14] Kruegel, C., and Thomas T. 2000. A survey on intrusion detection systems. TU Vienna, Austria, 2000. Citeseer.

[15] Ficco, M., Luca Tasquier, and Rocco Aversa 2013. Intrusion detection in cloud computing. P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), 2013 Eighth International Conference on, 2013, pp. 276-283. IEEE.

[16] Tupakula, Udaya, Vijay V., and Naveen A. 2011. Intrusion detection techniques for infrastructure as a service cloud. Dependable, Autonomic and Secure Computing (DASC), 2011 IEEE Ninth International Conference on, 2011, pp. 744-751. IEEE.

[17] Chouhan, P. K., Haggan M.,McWilliams G. 2011 Network Based Malware Detection within Virtualised Environments. Euro-Par 2014: Parallel Processing Workshops, 2014, pp. 335-346. Springer.

[18] Garcia-Teodoro, P., Diaz, J. Verdejo, G.M. Fernandez, E. V. 2009. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers & security 28(1):18-28.

[19] Denning, D. E, and Peter, G. N. 1985. Requirements and model for IDES—a real-time intrusion detection expert system. Document A005, SRI International 333.

[20] Zakarya, M. 2013. DDoS Verification and Attack Packet Dropping Algorithm in Cloud Computing. World Applied Sciences Journal 23(11):1418-1424.

[21] Ismail, M. N., Aborujilah A., Musa, S. 2013. Detecting flooding based DoS attack in cloud computing environment using covariance matrix approach. Proceedings of the 7th International Conference on Ubiquitous Information Management and Communication, 2013, pp. 36. ACM.

[22] Gupta, S., Padam K., and Ajith A. 2011. A profile based network intrusion detection and prevention system for securing cloud environment. International Journal of Distributed Sensor Networks 2013.

[23] Shamsolmoali, P., and Masoumeh Z.. 2014. Statistical-based filtering system against DDOS attacks in cloud computing. Advances in Computing, Communications and Informatics (ICACCI, 2014 International Conference on, 2014, pp. 1234-1239. IEEE.

[24] Estevez-Tapiador, J. M, Pedro G. T. and Jesus E. D. 2003. Stochastic protocol modeling for anomaly based network intrusion detection. Information Assurance, 2003. IWIAS 2003. Proceedings. First IEEE International Workshop on, 2003, pp. 3-12. IEEE.

[25] Heckerman, D. 1998. A tutorial on learning with Bayesian networks: Springer.

[26] Kruegel, C. M., Darren, R. , Fredick, V. 2003. Bayesian event classification for intrusion detection. Computer Security Applications Conference, 2003. Proceedings. 19th Annual, 2003, pp. 14-23. IEEE.

[27] Hu, J., Yu,X. , Qiu, H. Chen. 2009. A simple and efficient hidden Markov model scheme for host-based anomaly intrusion detection. Network, IEEE 23(1):42-47.

[28] Alarifi, S., and Stephen W. 2013. Anomaly detection for ephemeral cloud IaaS virtual machines. *In* Network and system security. Pp. 321-335: Springer.

[29] Pandeeswari, N, and Ganesh K. 2015. Anomaly Detection System in Cloud Environment Using Fuzzy Clustering Based ANN. Mobile Networks and Applications: 1-12.

[30] Xiong W,Y. Laurence, P. Wen-Chih, W, Xiofei, Q. Yanzhen 2014. Anomaly secure detection methods by analyzing dynamic characteristics of the network traffic in cloud communications. Information Sciences 258:403-415.

[31] Mandi G, Sirhind 2013. Survey paper on data mining techniques of intrusion detection.

[32] Shirazi, N., Simpson S., Marnerides, A., Watson, M., Mauthe A.,and Hutchison D. 2014. Assessing the impact of intra-cloud live migration on anomaly detection. Cloud Networking (CloudNet), 2014 IEEE 3rd International Conference on, 2014, pp. 52-57. IEEE.

[33] Vapnik, Vladimir Naumovich, and Vlamimir Vapnik1998. Statistical learning theory. Volume 1: Wiley New York.

[34] Furey, T. S., Cristianini N., Duffy, N., Bednarski, D.W.. 2000. Support vector machine classification and validation of cancer tissue samples using microarray expression data. Bioinformatics 16(10):906-914.

[35] Adamova, Kirila, S. Dominik, P. Benhard, S.Paul 2014. Network anomaly detection in the cloud: The challenges of virtual service migration. Communications (ICC), 2014 IEEE International Conference on, 2014, pp. 3770-3775. IEEE

[36] Lo, C.-C., Huang, C.-C. and Ku, J. (2010). A cooperative intrusion detection system framework for cloud computing networks. Proceedings of the 2010b *2010 39th International Conference on Parallel Processing Workshops*, 280-284.

[37] Man, N. D. and Huh, E.-N. (2012). A collaborative intrusion detection system framework for cloud computing. Proceedings of the 2012 *Proceedings of the International Conference on IT Convergence and Security 2011*, 91-109.

[38] Huang, T., Zhu, Y., Wu, Y., Bressan, S. and Dobbie, G. (2016). Anomaly detection and identification scheme for VM live migration in cloud infrastructure. *Future Generation Computer Systems*, 56, 736-745.

[39] Muthurajkumar, S., Kulothungan, K., Vijayalakshmi, M., Jaisankar, N. and Kannan, A. (2013). A Rough Set based Feature Selection Algorithm for Effective Intrusion Detection in Cloud Model.

[40] Maiti, S., Garai, C. and Dasgupta, R. (2015). A detection mechanism of DoS attack using adaptive NSA algorithm in cloud environment. Proceedings of the 2015 *Computing, Communication and Security (ICCCS), 2015 International Conference on*, 1-7.

[41] Zhou, L.-H., Liu, Y.-H. and Chen, G.-L. (2011). A feature selection algorithm to intrusion detection based on cloud model and multi-objective particle swarm optimization. Proceedings of the 2011 *Computational Intelligence and Design (ISCID), 2011 Fourth International Symposium on*, 182-185.

[42] Kannan, A., Maguire, G. Q., Sharma, A. and Schoo, P. (2012). Genetic algorithm based feature selection algorithm for effective intrusion detection in cloud networks. Proceedings of the 2012 *Data Mining Workshops (ICDMW), 2012 IEEE 12th International Conference on*, 416-423.

[43] Bharadwaja, S., Sun, W., Niamat, M. and Shen, F. (2011). Collabra: a xen hypervisor based collaborative intrusion detection system. Proceedings of the 2011 *Information technology: New generations (ITNG), 2011 eighth international conference on*, 695-700.

[44] Giannakou, A., Rillling, L., Pazat, J.-L., Majorczyk, F. and Morin, C. (2015). Towards Self Adaptable Security Monitoring in IaaS Clouds. Proceedings of the 2015 *Cluster, Cloud and Grid Computing (CCGrid), 2015 15th IEEE/ACM International Symposium on*, 737-740.

[45] Toumi, H., Talea, A., Marzak, B., Eddaoui, A. and Talea, M. (2015). Cooperative trust framework for cloud computing based on mobile agents. *International Journal of Communication Networks and Information Security*, 7(2), 106

[46] Li, Z., Sun, W. and Wang, L. (2012). A neural network based distributed intrusion detection system on cloud platform. Proceedings of the 2012 *2012 IEEE 2nd International Conference on Cloud Computing and Intelligence Systems*, 75-79.

[47] Nagarajan, P. and Perumal, G. (2015). A Neuro Fuzzy Based Intrusion Detection System for a Cloud Data Center Using Adaptive Learning. *Cybernetics and Information Technologies*, 15(3), 88-103.