 doi:10.20944/preprints202104.0183.v1

Taskeen Zaidi
Department of Computer Science & Engineering
Shri Ramswaroop Memorial University
Barabanki
email_id:taskeenzaidi867@gmail.com; taskeen.cse@srmu.ac.in

A Network Intrusion Based Detection System for Cloud Computing Environment

Abstract: Cloud computing is an emerging area which provide on demand computing resources and services through internet. It is faster and efficient technique but prone to severe security attacks. In this paper author have proposed a Network Intrusion Detection System (NIDS) to detect attacks at front end and backend when bulky flow of data packets flowing in a cloud environment. In our framework we used Signature based detection system for identifying the intruder and the Anomaly based detection system for detecting network attacks. The NIDS sensors were placed in a collaborative manner to prevent the attacks and to update the knowledge bases. Author have used supervised learning model to detect abnormal behavior of packets from network traffic. The dataset were trained and tested in terms of precision, recall, accuracy and model build time to select the best machine-learning model for detection of intruder and to improve the computational time and performance.

Keywords—Intrusion detection systems; machine learning; NSL-KDD; feature selection; classification model; SBDS, ABDS, Snort, SVM

1.INTRODUCTION AND RELATED WORK

Nowadays cloud network security is very important issue because intruder attacks the system using different ways like DoS, DDoS, spoofing, U2R ,R2L and so on. Various methods were used to protect the security like firewalls, cryptography but these methods are not very defensive to detect intrusion in distributed environment. Detection of intruder is a challenging issue. The Intrusion Detection System(IDS) with intelligent security features were used to detect attacker and to protect the cloud computing system. The IDS may be incorporated as host based or network based. In this paper intrusion detection will be represented using Signature Based Detection System(SBDS) and Anomaly Based Detection System(ABDS) etc. In this work any abnormal behavior showing by data packet is treated as an attack.

The proposed C-NIDS detects network intrusion in cloud environment, handle rigid traffic in cloud without packet loss/drop. In the paper authors[16] explained placement and integration of NIDS in various ways using front end ,back end and on virtual machine. It was detected that if we positioned and integrate NIDS on front end then network intrusion on external network will be easily identified and if NIDS is integrated on virtual machine then the user will detect intrusion on his own virtual machine very efficiently. It was also observed that NIDS that implemented on Virtual machine is very complex to handle. The NIDS integrated on front end, back end as well as on virtual machine for detection of external and internal intruders in the cloud environment.

A solution using Dempster-Shafer Theory (DST) was proposed by authors[1] to detect and visualize Distributed Denial of Service(DDoS) attacks in cloud computing environment. The characteristics, services, models of cloud computing environment is very well explained in [2]. To prevent information leakage through firewalls a well known approach develop and explained by authors[3].A collaborative CIDS was proposed by authors[4] using Snort to detect the

 doi:10.20944/preprints202104.0183.v1

intruders using Signature matching. An anomaly detection system was integrated using decision tree approach and Support Vector Machine(SVM) to reduce DoS and DDoS attacks in cloud computing environment. The problem in network security has been solved using a new approach that is Network Security Situation Awareness (NSSA)[5,6]. The commercial and open source implementation for detection of malicious behavior in network environment was well observed by Vieira etal.[7].A hybrid scheme was explained by authors[8] that combines advantages of deep belief network and support vector machine. The attacks were also classified into five classes: normal, R2L,DoS,U2R and probing. The performance was evaluated using NSL-KDD dataset. A classifier using Radial Basic Function (RBF) neural network and fuzzy clustering was explained by authors [9] to detect and prevent network attacks occurrence. The authors also examined the results on NSL-KDD dataset and analyzed that proposed model has higher accuracy than existing classification system. NIDS is used to monitor network traffic in cloud computing environment to protect the cloud from security threats. The intruders were detected by tracking IP and TCP header of each packet. A signature based and Anomaly based approach is used for observing abnormal behavior of packets was by authors[10].An optimize soft computing tool is proposed by authors[11] for intrusion detection through genetic algorithm and Back Propagation Neural Network(BPNN) to detect attacks under cloud environment. The Cloudsim 4.0 and DARPA datasets were used for simulation. A Hybrid Network Intrusion Detection System (H-NIDS) was proposed by authors [12] to detect internal and external attacks in cloud environment. It is also consist of seven modules and it was analyzed that proposed system has reduced computational and communication cost. A secure architecture for cloud proposed by authors [13]which is based on virtual host intrusion detection. It is composed of three components and the experimental results suggested that proposed IDS is helpful for detection of random set of cloud attacks. Mehmood etal.[14] has proposed Distributed Intrusion Detection System using mobile agents in cloud computing[DIDMACC] for detection of attacks in cloud environment. The mobile agents were used to carry intrusion related data and to detect intruder in distributed cloud environment. But proposed system was unable to detect zero day attacks and unknown attacks. A novel collaborative IDS was proposed by authors[15] for cloud environment. The proposed framework was integrated at each cluster and bully election algorithm is used to elect best cluster for integration of Collaborative Unit(CU). A decision tree classifier and SVM is used to improve detection accuracy and efficiency of cloud system and for detection of intruder [16]. A nonconventional method was proposed by authors [17] to secure cloud environment from malicious attackers with use of network profiling. The prototype was verified and tested on private cloud infrastructure. An automatic intrusion detection approach for cloud was proposed [18] and evaluated at architecture level and experimental level. A survey work was conducted by authors [19] to analyze the Cloud Network Intrusion Detection System(C-NIDS) methods using machine learning algorithms[MLA].The challenges, future scope for MLA usage in cloud based network intrusion detection system was also discussed[20].A Host Based Intrusion Detection System(HIDS) was proposed to identify LAN attacks and proposed scheme was validated with different attack scenarios[21].The HIDS was proposed by authors[22] using log file analysis technology and neural network technology. The log file analysis method used for misuse detection and neural network used for anomaly detection. Both the techniques combined and implemented to improve efficiency of intrusion detection system. Different techniques were discussed for intrusion detection and prevention[23] in cloud computing environment. The advantages and disadvantages of IDS were discussed. Several security challenges were studied to make cloud environment secure and reliable. Random forest classifier is used to classify the KDDCUP'99 dataset according to the features[24]. A high level design of SAAS architecture was performed and a prototype of an autonomous agent was developed and evaluated. It was depicted that autonomous agent approach is sufficient to detect cloud related security problem and used to create cloud based audit system[25]. The cloud based attacks and vulnerabilities were analysed through cloud models[26]. The importance of intrusion detection system and prevention from attacks were discussed. A new immediate Syscall technique was proposed by authors[27] to detect malicious attacks in cloud environment. This technique requires low cost and is platform independent. This technique is validated on University of Mexico dataset for detecting intruders. The performance was estimated on open nebula and virtual box[28].Cloud security issues were studied and several key topics like threats, vulnerabilities, attacks were studied. Several open research topics to secure cloud computing environment were also studied[29].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 April 2021 doi:10.20944/preprints202104.0183.v1

2.CLOUD BASED INTRUSION DETECTION SYSTEM:

2.1.Intrusion in Cloud:

Intrusion Detection System (IDS) is used to monitor network traffic and to scan illegal activities in cloud system. IDS also issues alert to the cloud administrator about vulnerable attack. The IDS may be classified as Host-Based IDS(HIDS),Hypervisor-Based IDS(HyIDS) and Network-Based IDS(NIDS).In the current work we have implemented NIDS at network point to detect anomalies during data transmission in network. The intruder may be external or internal causes network security attacks. According to National Institute of Standards and Technology (NIST) an intruder effects the privacy, integrity and availability of resources and services in cloud computing environment. Sometime the attackers illegally access the system file and valuable information also. The most prominent attacks under cloud environment are: Insider attacks, DoS, DDoS, Port scanning, back door channel attacks, U2R and R2L.

2.1.Insider Attacks: Insider attack or insider threat is a malicious attack on network by a user that has authorized access to the system. This attack affects computer security by stealing information from a file. The insider attacker also affects the system performance and capacity.

2.2 DoS attack: In DoS attackers prevent legitimate user to access the resource and services. The attacker sends the bulk messages to the server with invalid IP addresses. The server will not find the destination address when trying to send reply back and then in between this attacker will sent more invalid requests to the server before sever closes the connection. In this manner the server will keep on busy and after certain amount of time the system will crash.

2.3 DDoS: In DDoS multiple computer system attacks a target, such as server or website to cause denial of service and unavailability of resources. The attackers intention is to make website and services inoperable.

2.4 Port scanning: The attackers surveillance the computer port. It is a open door hacking method in which hacker illegally tried to interrupt computer or operating system.

2.5 Backdoor channel attack: In backdoor attack the applications that provide remote access to the computer were used for attacks.

2.6 User to Root (U2L):In this attack attackers tried to access the system with root privilege.

2.7 Remote to Local (R2L): The attacker tries to access system remotely.

3.C-NIDS STRUCTURE

In the current work the C-NIDS structure consists of:

a) Wireshark
b) Signature based detection
c) Anomaly based detection
d) Alert system
e) Central log database

a) Wireshark: The in bound and outbound packet will be capture by using pcap library. Packet sniffing tool is used for this purpose.

b) Signature Based Detection: In this system a knowledge base generated based on predefined network attack rules. Cloud related attacks rules were also incorporated in knowledge base. Snort matches the inflow packets with rules stored in knowledge base to find the

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 April 2021 doi:10.20944/preprints202104.0183.v1

correlation. If any intruder is identified then a warning message is sent to alert it and other packets were forwarded to anomaly detection system for further processing.

c) Snort is a software which is used to perform real time traffic analysis and packet tracking on the network. Snort may be used as packet sniffer, packet logger or NIDS.NIDS enable Snort to detect intrusion threat by analyzing traffic threat. The Snort analyzed the packet without any loss.

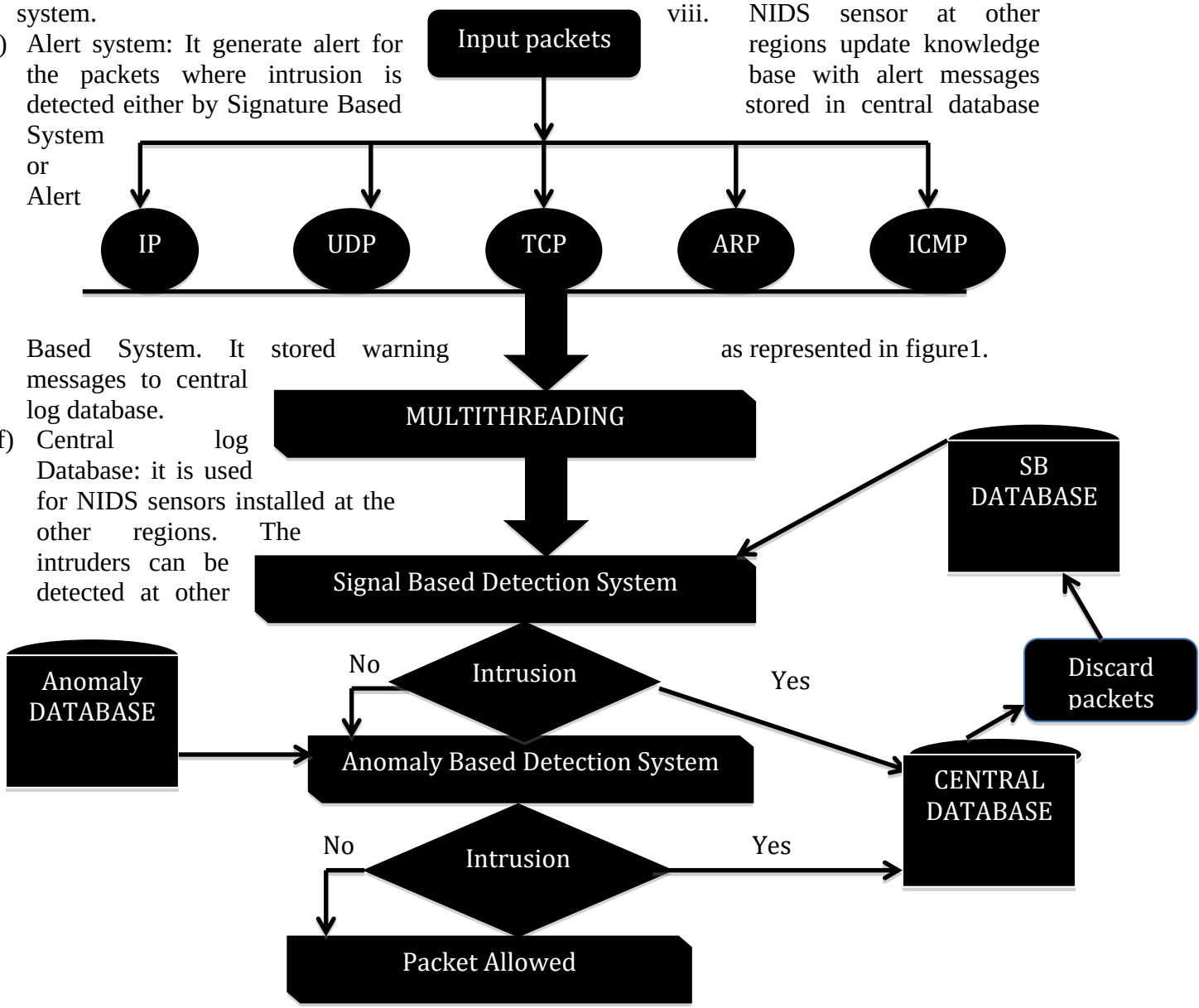
d) Anomaly Detection System: It is built using Support Vector Machine(SVM).It is useful for predicting class label(normal or intruder) of the packets. If any intruder is detected then a warning is send to alert system.

e) Alert system: It generate alert for the packets where intrusion is detected either by Signature Based System or Anomaly Based System. It stored warning messages to central log database.

f) Central log Database: it is used for NIDS sensors installed at the other regions. The intruders can be detected at other regions using signature based detection.

3.1 Workflow:

i. Network traffic is for internal and external network.
ii. It is sent to Signature Based Detection System as multiple threads.
iii. The Signature Based Detection System detects intrusion into packets.
iv. Intruder packets will be stored in Central database.
v. Non intruder packets sent to Alert Based System to label class(normal or intruder) by observing behavior base.
vi. Intruder class label stored to central database.
vii. Normal packets will be allowed to flow.
viii. NIDS sensor at other regions update knowledge base with alert messages stored in central database as represented in figure1.



Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 April 2021 doi:10.20944/preprints202104.0183.v1

Attack type	DATA SET	SEARCH METHOD	FEATURES	TOTAL NO.OF FEATURES
Multiple attacks	1	Best first search	1,4,6,7,11,13,21,23,27,29	10
	2	Rank search	2,3,5,8,9,10,12,14,15,16,17, 18,19,20,22,24,25,26,28,30	20

Figure 1: Cloud Based-Network Intrusion Detection System(C-NIDS)

Table1: Features Selection

4.Advantages of Proposed Model:

i. High amount of data can be handled.
ii. Computation time will be reduced.
iii. The external and internal attacks will be prevented.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 April 2021 doi:10.20944/preprints202104.0183.v1

iv. Multithreading will allow packets processing concurrently which is an efficient approach.

5.DATA SET PREPARATION

Two subset od datasets were prepared from input traffic like TCP,ICMP etc. For the dataset1 best search method is used and dataset2 uses rank search method .The dataset were classified using machine learning approach models i.e. Naïve Bayes and Random forest model as represented in Table1.

5.1.1Naïve Bayes: It is a machine learning probabilistic model based on Bayes theorem using which we find the probability of happening of an event if an event already occurred. The features were independent and donot affect the other.

5.1.2 Random forest: It is a learning model which consist of number of decision tree. Every tree provides independent decision and the decision were merged to get a unique decision by mac polling method. This method provides greater diversity.

5.2PERFORMANCE COMPARISON:

(i) Precision: Total positive/total positive+ false positive
(ii) Recall: total positive/total positive+ false negative
(iii)Accuracy: it reflects the classified instances.

6.SIMULATION RESULTS:

For simulation an open source data mining tool WEKA is used that provides Graphical User Interface to train and test data with different parameters. We have evaluated NSL-KDD dataset through two algorithm i.e. best search and rank search on 2 datasets and results were tested through Naïve Bayes and Random Forest model.

6.1 PERFORMANCE ANALYSIS:

Simulation is visualized on python visualization tool and the result were shown in Table2.Random forest perform better for dataset 1 and 2 and it is also depicted that overall performance depends on feature selection.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 6 April 2021 doi:10.20944/preprints202104.0183.v1

Table2: Performance Analysis of Classification Models

Classification model	Data set	Precision	Recall	Model build time
Naïve Bayes	1	0.553	0.613	38.74s
	2	0.659	0.693	63.21s
Random Forest	1	0.717	0.823	432.23s
	2	0.812	0.712	323.46s

7.DISCUSSION

Cloud computing is an advancement to the distributed computing using which user can access any resources or services through internet. It is very popular and emerging technology which provide services on demand. But apart from that cloud computing is not secure as attacks like ARP spoofing, Man in the middle attack, Denial of service attack and DDoS attacks were very common. Due to this many service providers uses firewalls to prevent services from attacks, but sometime attacks were not detected by the firewalls also. Author have proposed a new approach that is Network Intrusion Detection System (NIDS) for cloud computing environment using Snort and SVM. The NIDS sensors were installed at frontend and backend for detecting external and internal attacks. The signature based detection system(SBDS) and Anomaly based detection system(ABDS) used to identify intruder packet and then a warning message will be generated and put in central database. NIDS sensors were deployed in collaborative manner and the knowledge bases updating depends upon packet stored in central database. This will be helpful in detection of intrusion easily by Signature Based Detection System. So overall computational cost will be reduced. NIDS proposed by author has high capability of detecting the intruders with reduced cost.

CONCLUSION

The cloud computing is an emerging technology in IT industry but suffers major

security issue is to protect it from internal and external attacks. To prevent attacks in cloud environment author have proposed C-NIDS based on intruder detection at front end and backend and at virtual machine level. The signature based detection system detects the intruder and then Anomaly based detection system sent the warning through a message. Intruder packet were placed in a central database log file and this data will be shared to all servers of the other regions so that from next time intruder will be discarded and this will reduce the computational time for processing. Simulation results based on python visualization tool shows that Random forest model provide better accuracy and efficiency.This work will be further extended by analyzing the overhead done by multiple NIDS running instances in cloud environment.

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, available in:<http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpub lication800-145.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]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.

[5]E. U. Opara, O. A. Soluade, “ Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities,” International Journal of Electronics and Information Engineering, Vol. 3, No. 1, pp. 10-18, 2018.

[6] A. Tayal, N. Mishra, S. Sharma, “Active monitoring & postmortem forensic analysis of network threats: A survey,” International Journal of Electronics and Information Engineering, Vol. 6, No. 1, pp. 49-59, 2017.

[7] K. Vieira, A. Schulter, C. Westphall, C. Westphall, “Intrusion detection for grid and cloud computing,” It Professional, Vol. 12, No. 4, pp. 38-43, 2010.

[8] Salama M.A., Eid H.F., Ramadan R.A., Darwish A., Hassanien A.E. (2011) Hybrid Intelligent Intrusion Detection Scheme. In: Gaspar-Cunha A., Takahashi R., Schaefer G., Costa L. (eds) Soft Computing in Industrial Applications. Advances in Intelligent and Soft Computing, vol 96. Springer, Berlin, Heidelberg.

[9] M. Amini, J. Rezaeenour, E. Hadavandi, “ A neural network ensemble classifier for effective intrusion detection using fuzzy clustering and radial basis function

networks," International Journal on Artificial Intelligence Tools, Vol. 25, No. 02, pp. 1550033-1550062, 2016.

[10]A.A. Mohd, P. Angelov, "Anomalous Behaviour Detection Based on Heterogeneous Data and Data Fusion," Soft Computing, Vol. 22, No. 10, pp. 3187-3201, 2017.

[11] Z. Chiba, N. Abghour, K. Moussaid, A. El Omri and M. Rida, "New Anomaly Network Intrusion Detection System in Cloud Environment Based on Optimized Back Propagation Neural Network Using Improved Genetic Algorithm", International Journal of Communication Networks and Information Security 79 (IJCNIS) Vol. 11, No. 1, April 2019

[12] N. Modi and D. Patel, "A novel hybrid-network intrusion detection system (H-NIDS) in cloud computing", 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), Singapore, Singapore, pp. 23-30,2013.

[13] M. Moorthy, M. Rajeswari, "Virtual host based intrusion detection system for cloud,"Journal of Engineering & Technology, pp. 0975-4024, 2013.

[14] Y. Mehmood, M. A. Shibli, A. Kanwal, R. Masood, "Distributed intrusion detection system using mobile agents in cloud computing environment," 2015 Conference on Information Assurance and Cyber Security (CIACS), Rawalpindi, Pakistan, pp. 1-8, 2015.

[15] D. Singh, D. Patel, B. Borisaniya, C. Modi, "Collaborative ids framework for cloud," Journal of Network Security, Vol. 18, No. 4, pp. 699-709, 2016.

[16] 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.

[17] Gupta, S., Kumar, P., & Abraham, A. (2013). A Profile Based Network Intrusion Detection and Prevention System for Securing Cloud Environment. *International Journal of Distributed Sensor Networks*. https://doi.org/10.1155/2013/364575

[18] Arshad, J., Townend, P. & Xu, J. International Journal of Automation and Computing (2011) 8: 286. https://doi.org/10.1007/s11633-011-0584-2

[19] Nathan Keegan, Soo-Yeon Ji, Aastha Chaudhary, Claude Concolato, Byunggu Yu[1]and Dong Hyun Jeong," A survey of cloud-based network intrusion detection analysis ",Human Centric Computing and Information Sciences(2016),6:19, DOI 10.1186/s13673-016-0076-z

[20] Mohanad Albayati and Biju Issac**,"** Analysis of Intelligent Classifiers and Enhancing the Detection Accuracy for Intrusion Detection System**",** International Journal of Computational Intelligence Systems, Volume 8, Issue 5**,** September 2015, Pages 841 – 853.

[21] Barbhuiya F et al (2011) An active host-based intrusion detection system for

 doi:10.20944/preprints202104.0183.v1

ARP-related attacks and its verification. Int J Net Sec App 3(3):163–180

[22]Ying L, Yan Z, Jia O (2010) The design and implementation of host- based intrusion detection system. In: Third International Sym- posium on Intelligent Information Technology and Security Information, Jinggangshan, pp 595–598

[23]Modi C et al (2013) A survey of intrusion detection techniques in cloud. J Netw Comp App 36:42–57

[24]Htun P, Khaing K (2013) Important roles of data mining techniques for anomaly intrusion detection system. Int J Adv Res Comp Eng Tech 2(5):1850–1854

[25]Doelitzscher F et al (2012) An agent based business aware incident detection system for cloud environments. J Cloud Comp Adv Sys App 1–9. doi:10.1186/2192-113X-1-9

[26]Iqbal, M. L. M. Kiah, B. Dhaghighi, M. Hussain, S. Khan, M. K. Khan, K.-K. R. Choo, On cloud security attacks: A taxonomy and intrusion detection and prevention as a service, Journal of Network and Computer Applications 74 (2016) 98–120

[27]S. Gupta, P. Kumar, An immediate system call sequence based approach for detecting malicious program executions in cloud environment,Wireless Personal Communications 81 (1) (2015) 405–425.

[28]V. Varadharajan, U. Tupakula, Security as a service model for cloud environment, IEEE Transactions on network and Service management11 (1) (2014) 60–75.

[29]A. Fernandes, L. F. Soares, J. V. Gomes, M. M. Freire, P. R. In´acio, Security issues in cloud environments: a survey, International Journalof Information Security 13 (2) (2014) 113–170