TEST Engineering & Management

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

Whale Swarm Optimization Algorithm (WSO) to implement an Efficient and Enhanced Deep Neural Network based IDS for Cloud Environments

Neeraj Varshney, Abhay Chaturvedi
Department of Computer Engineering & Applications
Department of Electronics & Communication Engineering
GLA, University, Mathura, India-281406
neeraj.varshney@gla.ac.in shashi.shekhar@gla.ac.in

Article Info
Volume 82
Page Number: 116 - 124
Publication Issue:
January-February 2020

Abstract
Currently, cloud computing has turned up into a predominant feature among the users in organizations and companies. The two chief problems encountered by cloud service providers and the corresponding clients are security and efficiency. Cloud based services involve security risks, as cloud computing acts as a simulated collection of resources offered in an open environment which is termed as Internet. One of the major challenges for both cloud service providers and cloud users is detection of intrusions and attacks caused by unauthorized users. Consequently it has become more vital to construct an effective detection system for intrusion, towards detecting suspicious happenings and intruders both internal and external to the CC framework through network traffic monitoring, despite the fact of maintaining performance and also quality of service. We propose a smart approach in this research work, applying whale swarm optimization algorithm (WSO) to automatically develop a Deep Neural Network (DNN) based Anomaly Network Intrusion Detection System (ANIDS). For the proposed system, the concept of reverse learning is initiated in the actual whale swarm optimization algorithm so as to achieve optimization. This approach boosts the capability of node search process and also the rate of speed of the global search procedure is increased. For the purpose of simulation and validation of the proposed system, CloudSim 4.0 simulator platform and Kyoto 2006+ dataset version 2015 are utilized. The attained results of experiments reveal that, in contrast to various customary and recent methodologies, the proposed IDS accomplishes better detection rate and lesser false positive rate.

Article History
Article Received: *14 March 2019*
Revised: *27 May 2019*
Accepted: *16 October 2019*
Publication: *01 January 2020*

Keywords: *cloud computing, network intrusion detection system, deep neural network, optimization, anomaly detection, Kyoto 2006+ dataset, whale swarm optimization algorithm..*

1 Introduction

In the recent times, Information and Communication Technology (ICT) is transforming significantly and the emergence of novel paradigms are being witnessed. In this course of revolutionary move, Cloud Computing (CC) is a momentous achievement. CC is stated by the National Institute of Standards and Technology (NIST) in the role of computational standard which provides appropriate, on-demand, network access of a public collection of resources such as networks, storage, applications, servers and so on through Internet for gratifying the computing necessity of users [1,2,3,4]. Users who are provided the resources could be serviced speedily that could be done with least work of administration or interactions with the provider of services could also be released [5]. The fascinating characteristics of Cloud computing (CC) endure to

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

energize its incorporation in several sectors comprising governments, education, business, entertainment, and still more [6]. The on-demand and pay-as-you-go elastic functions of Cloud attributes are switching the computing structure of the enterprise, changing from the data centers that are off premises to the infrastructures that are on premises which gained access over Internet and controlled by cloud hosting providers [1]. Progress of CC has emerged as a multidimensional advancement having the ability to maintain a wide range of usages. It has come to light as a breakaway in the Internet usage. Consequently, CC is a subject of significant impact at present and has been evidenced as a booster for companies that are small in the speedily evolving world. For affording several constructive services through the Internet, it serves as an anatomy [7].Other appealing benefits of cloud computing are reduction in hardware cost as there is no need for the users to have their own efficient processors or even any other hardware possessions, high storage volume, sustained and rapid advancement and bring up to date of the services, worldwide access to documents which means that the users can retrieve their needed applications and documents merely by getting connected to the Internet by being in the place where they remain, sharing of resources, acceleration and time saving, parallel processing [8].On the other hand, few of the vital drawbacks of cloud computing are efficiency, faith and privacy, security, proprietorship and control, expense of connection bandwidth, fault tolerance and fault recovery and availability [8].

Data privacy and data safety are the principal obstacles to the progress of CC, as the services provided by cloud computing are accessible through Internet. Furthermore, the open and decentralized characteristic of CC has given rise to this type of computing which is liable to intrusions and cyber attacks [8, 9]. One of the crucial issues of security over Cloud is to perceive and avoid intrusions of network as the backbone of Cloud is the network, and henceforth the susceptibilities in network influence straight away the Cloud's security [2]. With every year moving off, not only there arises the increase in the quantity of threats, but also the threat background has turned more different, with attackers operating trickier to encounter new possibilities of attack and conceal their imprints while acting so. In recent years, in spite of the obvious growth of the information security technologies, on the road to overcome the prevailing methods of detecting intrusions in Cloud environments, intrusions and attacks still persist [10]. Attackers created new state-of-the-art methodologies that are competent enough to demolish the whole Cloud platform or even most in extremely a short span of time. A devastating DDoS attack recently has bring to ground, around 70 essential Internet services such as Twitter,Paypal,Amazon, Github and so on. The benefits of Cloud Computing and IoT (Internet of Things) are abused by the attackers to produce a huge volume of attack traffic which could be exceeding 665 Gb/s [11]. In the year 2017, ransom ware attacks shook up several banks, large telecom companies, National Health Service hospitals in the United Kingdom, and natural gas companies, whereas in 74 countries huge count of systems were subjected to hacking[12].Therefore, attack and intrusion tools have turned out to be much advanced challenging network Cloud IDSs by huge degrees of network traffic data, vigorous and complicated activities and different sorts of attacks [13]. It is hence evident that a network Cloud IDS has to evaluate huge bulk of network traffic data, effectively detect the new deeds of attack and attain high accuracy with low false. Nevertheless, preprocessing, analyzing and detecting intrusions in Cloud atmospheres utilizing conventional methodologies have become much expensive in the form of time, budget and computation. Hence, competent intrusion detection in Cloud environments necessitates acquiring new intellectual techniques such as Machine Learning techniques [13].

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

In the proposed work, a Machine Learning based intrusion detection system for Cloud environments is presented. To construct automatically a network intrusion detection system (NIDS) based on Deep Neural Network (DNN) by using a Whale Swarm optimization Algorithm (WSO) is propose here

2 Preliminaries

In this segment we offer the needed context in order to recognize the issue. The initial section briefs on the concepts of Deep Neural Network (DNN). The following segment explains the function of a standard GA and the final segment concisely explains Adaptive Genetic Algorithms, specifically the Adaptive Mutation Algorithm that is applied in the proposed work. A. Deep Neural Network (DNN) is a multilayer feed forward neural network [14]. As depicted in figure 1, DNN encompasses an input layer, followed by several of the hidden layers and ending up with an output layer. The network depicted, the information travels in a single direction, advancing from the input nodes, passing over the hidden nodes and finally to the output nodes. There is no cycles or loops present in the network. Direct connections exist between every neuron present in one layer to the neurons in the following layers. For studying the weights of the network, the Back Propagation Learning Algorithm is utilized [15]. Because of the following two factors, Feed forward neural networks are prevalent [15]:

- They possess the capability to provide much closer related approximations for complex multivariate nonlinear functions directly from the input values.
- They possess a robust modeling capacity for a greater category of artificial and natural happenings.

DNNs having several hidden layers and several units per layer are much more flexible models. This initiates them to be able to structure highly complicated and vastly nonlinear relationships amongst inputs and output [16].For this reason, DNNs have been adequately researched in a machine learning research field, and extensively applied for applications in speech recognition, computer vision and image processing, etc. [17]. DNN like that is shown in figure 1 is implemented for this research since it realizes amazing classification performance.

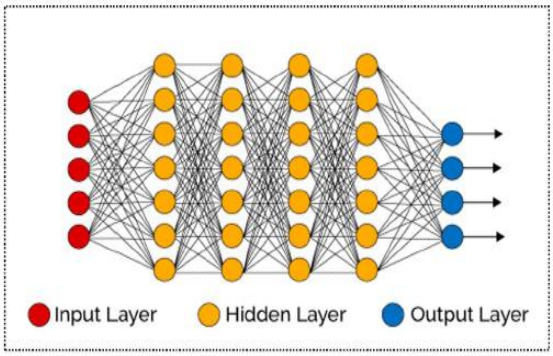

Figure 1: Deep learning neural network (DNN) Model

Whale Swarm Algorithm

Whales are mammals that live in the ocean and have intense group communication capability and high IQ. Size of the whales is comparatively huge, and generally dominated by the community. They can produce a variety of melodious sounds in seawater, and the spread of a very wide range. Social whales exercise ultrasound in order to communicate with their peers to complete prey, migration and other activities. When food is located by a whale, it will produce some sound to notify other whales about the amount of food and other information. Accordingly, every whale receives a huge amount of information from nearby whales and then determines to travel towards the nearest and most food-bearing spot. To develop a new target optimization algorithm, this predatory behavior of whales in the vocal communication stimulated the scholars [18]. In this paper, we use the characteristics of optimization of whale swarm optimization algorithm and apply it in wireless sensor network coverage optimization.

When it preys, the whale progresses forcefully to the optimal one if it is nearby to the optimal distance. Whereas, if the distance is long, the whale moves slowly toward it. From this kind of motion

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

rule grounded on ultrasonic decay, a new formula is attained, which prepares the algorithm not get jammed in local optimum prematurely, and also assists to obtain multiple global optimal solutions. The random movement of whale X under the assistance of optimal whale Y is defined by the following formula [19]:

$$x_i^{t+1} = x_i^t + rand\left(0, \rho_0 . e^{-\eta - d_{xy}}\right) * (y_i^t - x_i^t) \quad (1)$$

Where x_i^t and x_i^{t+1} are the i element of X iteration position in the step t and step $t+1$, respectively; y_i^t is the iteration position of step t for the i element of X; d_{xy} is the distance between X and Y; $rand\left(0, \rho_0 . e^{-\eta d_{xy}}\right) * (y_i^t - x_i^t)$represents random number from 0 to $\rho_0 . e^{-\eta - d_{xy}}$; ρ_0 represents distribution intensity.

By means of ultrasonic sound, whales in the water exchange information. But the intensity of ultrasonic sign falloff rapidly. Hence the distance from the wave source d and propagation intensity ρ can be expressed as:

$$\rho = \rho_0 . e^{-\eta d} \quad (2)$$

$$\eta = 20 . \frac{\ln(0.25)}{d_{max}} \quad (3)$$

Where ρ_0 represents wave source intensity, d_{max} represents the maximum distance between any two whales in the search area, η represents the attenuation factor (depending on the physicochemical properties of the medium and the nature of the ultrasound). When η is constant, ρ decreases exponentially with increasing d, which indicates that there is a limitation for the transmission range of the ultrasonic wave. The message carried by it may be distorted, in case the signal source is out of the propagation range. According to a large number of experiments, the $\rho_0 = 2$ is the most appropriate value.

Whale Group Optimization Algorithm Improvement

It is evident from the fundamental whale swarm algorithm that the population size and the initialization of the individual whale position have an immense impact on the speed of solving the whale swarm algorithm and the precision of the solution. If a whale is positioned distant from other whales in the population, it will move very slowly during optimization and iteration, which will decelerate the solution speed and escalate the solution time; at the same time, it is easier to fall into the local optimum during the searching.

With the aim of solving this issue, this paper enhances the actual algorithm and introduces the backward learning algorithm [20] to initialize the whale population position, which can effectively prevent generating poorly positioned individuals. The initialization process is as described below:

1 Randomly initialize whale populations, $N = \{X_{ij}\}, i = 1,2,3 \ldots S_n,\ j = 1,2,3 \ldots P, S_n$ denotes the number of whales, and P is the dimension which signifies the optimal solution.

2 Calculate the reverse population $' = \{X_{ij}'\}, X_{ij}' = X_{min,j} + X_{max,j} - X_{ij}'$, where $X_{max,j}$ and $X_{min,j}$ represent the maximum an minimum values in the jth element of the population.

3 To compute the fitness of the whale position, choose a n S species population with a smaller fitness for the initial whale population in $\{N = \{X_{ij}\} | N' = \{X_{ij}'\}$.As illustrated in Fig.1, the algorithm steps can be defined as follow:

Step1: Set the size of the population ie,.the number of sensor nodes, the use of reverse learning algorithm to initialize the whale population

Step2: Initialize WSA parameters, attenuation factor, the number of iterations, ,etc

Step3: Calculate the fitness value of each whale individual, and register the best individual with the smallest fitness value

Step4: Determine whether there is a better (nearest) individual around each whale individual, and if so, move to a better individual randomly according to Eq. (8); otherwise, continue to recycle

Step5: If the termination condition is satisfied, that is, all the optimal solutions of WSN coverage are

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

located, then all the best individuals are output, otherwise, the procedure returns to step 4
Step6: evaluate iteration number reached else step 3 is repeated on loop. If maximum iterations are reached then the process of algorithm gets exit.

3 Proposed System in a Cloud Network

Maintenance of network traffic, confidentiality, performance, availability and integrity are primary objectives in the proposed research that support for intruder detection internally and externally of Cloud Computing. It impairs the hinder attacks and enhances security in real time of the Cloud Datacenter. figure 1 explicates two strategic positions on NIDS:

- Cloud's Front-End: intrusions and attacks in network are detected by positioning NIDS on front end of Cloud network. In addition, any online hosts of zombie and any hackers trying to break firewalls to access internal cloud are prevented here. Thus NIDS performance overcomes the pitfalls of defense in firewall and offers security layer in productive.
- Cloud's Back-End: intrusion detection in network internally is aimed as objective in back end process via sensors of NIDS positioning sensors on processing servers. Virtual switch influences many virtual machines to inter communicate in a virtual environment with no detachment of physical server. Network traffic monitored by LAN's Network security devices and unlocking security attacks are possible to traverse the security appliances on un requiring traffic in specific of firewall. Unique VM is compromised in initial point of an attacker/hacker and exploits similar hypervisor in supporting all springboard to influence the extra VMs. a vast hack domain chance is offered to attackers without appropriate monitor and detection. In turn, many threats and risks are increasing in wide-open environment virtually and objective hypervisor primarily with Hyper jacking as well as VM escape give out in theft of VM, migration of VM, and Inter-VM traffic. the virtual traffic are monitored by NIDS and traffic flow in and out of server processing in physical network.

Installing individual NIDS on all virtual machine is avoided as of extra work, downing of the VM function, complex management because of dynamic VM, migrated VM and stipulated or de-stipulated VM.

4 Proposed Methodology

A Deep Neural Network (DNN) based anomaly Network IDS (NIDS) is proposed based on WSO automatically. one input layer, two hidden layers and one output layer are included in DNN as Back Propagation Neural network (BPNN). Number of attributes/features determine the nodes in the input layer accordingly with connection vector of instance as of datasets IDS via DNN, while WSO generates the number of nodes in hidden layer. Value =1 in the output layer for input pattern classification by DNN as normal traffic else 0 to identify intrusion. Thus proposed research includes 4 stages with first two stages for associated and examined intensely several functions in BPNN or DNN based IDS. type of classifier with its performance by determination of applicable parameters. employed to construct that or that affect its performance. Values of table 1are efficient parameters [20]: nodes of input layer are accordingly with selected features/attributes, data Normalization, Neural Network Architecture, hidden layer nodes, function of Activation or transfer, rate of Learning and term in Momentum. Citation of each parameter, values of two and four equivalent and applicable are concentrated in studied works for detection of intrusion.

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

Table I. Parameters values and performance of a BPNN or a DNN based IDS

Parameters	Different values
Number of attributes	12 attributes of KDD Cup 99 [20]
	17 attributes of KDD Cup 99 [21]
	14 attributes of Kyoto 2006+ [22]
	27 attributes of ITOS dataset [23]
Normalization	Min-max normalization [24]
	Statistical normalization [25]
Activation function	Hyperbolic tangent [26]
	Sigmoid [27]

DNN hidden layers with nodes are generated by WSO in random manner will randomly and also rate of Learning values and term in Momentum. parameters are identified and validated by algorithm of WSO. Dataset of Kyoto 2006+ University Benchmark are used for evaluation in IDS [28]. machine learning issues are resolved ie., traning and testing results of KDD or NSL-KDD with such a dataset [29]. But fails in scenario of network and eternal complexity holding cyber-attacks. 24 features within Kyoto dataset with multivariate attributes, 15 features of relevant, 14 features of conventional, plus 10 features for analysis are chosen for feature selection [30]. Features from benchmark dataset of KDD cup 99 choose input features for DNN and Label feature represented by 01 to check the record as normal or attacked one and explicate the sort of attacks. 14 constant inputs are considered in DNN accordingly with Kyoto dataset features of 2006+.

Stage 3: the primary two elements must be well determined in WSO's productive application.

Set population size as well as apply reverse learning algorithm to initialize the whale position.

WSO initialization of parameters

Evaluation of whales Calculate its fitness U(i))

while meet the number of iterations do

fori=1 to N do

Find better Y near U(i);

if Y exist then

U(i) move to Y according to formula 8;

Evaluate U(i);

end if

end for

end while

return global optimal solution

Optimization problem are analyzed by selecting of AUC metric for function fitness [20]. Misclassifications of packets network are eliminated by parameters of AUC in IDSs. It outperforms maximum Rate in Detection and minimum in rate of False Positive on account of arithmetic mean of DR and TNR (1-FPR) in AUC (3). If DR value get rise and low in FPR in (3) leads well performance and increase in AUC. Thence, AUC is well organized metric in validating IDS and act as crucial for better function fitness.

AUC FPR = + = + - (DR TNR) / 2 (DR (1)) / 2 (3)

5 Experimental Results

The basic feature required to implement this proposal are Windows 10 – 64 bits PC along 32 GB RAM and CPU Intel(R) Core-i7 2700K CPU. CloudSim simulator 4.0 is used for simulation and taken dataset are Kyoto relating date December 31, 2015. Network connections of double classes, records in normal as 23062 and records in attack as 286006 are included here. 60% of training data and 40% of testing dataset are considered for evaluation and tabulated in table 3. 24 features within Kyoto dataset, 15 features of relevant, 14 features of conventional are chosen for feature selection [30]. Features from benchmark dataset of KDD cup 99 choose input features for DNN and Label feature represented by 01. Quantitative attributes are obtained from data preprocessing, Min-Max normalization [24] and qualitative data from the hybrid normalization (probability function) [32]. Execution time and rate of classification are obtained well based on quantitative attributes and qualitative attributes as function in probability [33].

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

Table III. Datasets for testing and training by size and distribution

Datasets	Intrusive records	Normal Records	Total records
Full Kyoto dataset of 2015-12-31	286006	23062	309068
Training dataset (60% of Kyoto dataset of 2015-12-31)	171604	13838	185442
Testing dataset (40% of Kyoto dataset of 2015-12-31	114402	9224	123626

The end process of WSO sequence of generations 200, better results are obtained and the fit value permits to built ANIDSDNNWSO.

Table IV. Performance and parameters of best IDS based DNN

Parameters	Value	Performance metric	Approaches Value (%)	
			SAGA	Proposed WSO
Number of nodes in input layer	14	Accuracy	99.87	99.91
Number of nodes in hidden layer 01	11	Precision	99.99	99.99
Number of nodes in hidden layer 02	5	Detection Rate (DR)	99.87	99.90
Number of nodes in output layer	1	False Negative Rate (FNR)	0.13	0.11
Activation Function	Sigmoid function	False positive rate (FPR)	0.10`	0.12
Data Normalization	Min max Normalization	True Negative Rate (TNR)	99.90	99.91
Learning rate	8.764739560 218389E-7	F-score	0.99	0.99.5
Momentum rate	1.296589703 486271E-4	AUC	99.88	99.90

ANIDS-DNNIWSO metrics are tabulated in Table 4 along performances. 99.90% is achieved in DR, 0.10% in FPR (),0.99 in F-score and also attains optimal percentage for on recall/detection rate and precision. These values are tabulated in table 4. At conclusion, metric value of AUC is 99.88% to overcome of misclassifications and aim at prior and final conclusion. Thence proposed is appropriate to all applications of IDS potentially.

6 Conclusion

A clever method is designed for high detection precision and low false warnings aiming at the objective of efficient ANIDS preventing attacks from cloud environments internally and externally. It is based on IDS recognized Deep Neural network (DNN). Whale swarm optimization (WSO) approach is used for determining optimal values inclusive of the parameters in IDS dependent DNN (IDSDNN). Accordingly, towards end process of WSO process, IDSDNN are built from the optimal or near-optimal values of parameters named "ANIDS-DNNWSO". It attains maximum rate of detection and minimum low false positive rate. results on Experiment are obtained on environment of dataset CloudSim 4.0 and CICIDS2017. It influences the research proposed to state of art. Additionally, IDS on Front-End and Back-End of the Cloud are selected to function well for detection and attack prevention in real applications of impairing security of the Cloud Datacenter.

References

1. Idhammad, M., Afdel, K., and Belouch, M. 2018. Distributed Intrusion Detection System for Cloud Environments based on Data Mining techniques.

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

Procedia Computer Science. 127, C (Mar. 2018), 35-41. DOI= https://doi.org/10.1016/j.procs.2018.01.095.

2. Chiba, Z., Abghour, N., Moussaid, K., and Rida, M. 2016. A cooperative and hybrid network intrusion detection framework in cloud computing based on snort and optimized back propagation neural network. Procedia Computer Science. 83 (May. 2016), 1200-1206. DOI= https://doi.org/10.1016/j.procs.2016.04.249.
3. Mehmood, Y., Shibli, M. A., Habiba, U., and Masood, R. 2013. Intrusion detection system in cloud computing: challenges and opportunities. In Proceedings of 2013 2nd National Conference on Information Assurance (NCIA) (Rawalpindi, Pakistan, December 11-12, 2013). IEEE. 59-66. DOI=https://doi.org/10.1109/NCIA.2013.6725325.
4. Chiba, Z., Abghour, N., Moussaid, K., and Rida, M. 2018. A Review of Intrusion Detection Systems in Cloud Computing. In Security and Privacy in Smart Sensor Networks. IGI Global, 253-283. DOI= https://doi.org/10.4018/978-1-5225-5736-4.ch012
5. Mell, P., and Grance, T. 2011. The NIST definition of cloud computing. http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.
6. Fernandes, D. A., Soares, L. F., Gomes, J. V., Freire, M. M., and Inácio, P. R. 2014. Security issues in cloud environments: a survey. International Journal of Information Security. 13, 2 (Apr. 2014), 113-170. DOI= https://doi.org/10.1007/s10207-013-0208-7.
7. Ghosh, P., Jha, S., Dutta, R., and Phadikar, S. 2016. Intrusion Detection System Based on BCS-GA in Cloud Environment. In Proceedings of International Conference on Emerging Research in Computing, Information, Communication and and Applications (Bangalore, India, July 23-30, 2016). ERCICA 2016. Springer, Singapore, Singapore, 393- 403. DOI= https://doi.org/10.1007/978-981-10-4741- 1_35.
8. Hatef, M. A., Shaker, V., Jabbarpour, M. R., Jung, J., and Zarrabi, H. 2018. HIDCC: A hybrid intrusion detection approach in cloud computing. Concurrency and Computation: Practice and Experience, 30, 3 (May 2017), 1-10. DOI= https://doi.org/10.1002/cpe.4171.
9. Riaz, A., Ahmad, H. F., Kiani, A. K., Qadir, J., Rasool, R., and Younis, U. 2017. Intrusion Detection Systems in Cloud Computing: A Contemporary Review of Techniques and Solutions. Journal of Information Science and Engineering, 33, 3 (May 2017), 611-634. DOI= https://doi.org/10.6688/JISE.2017.33.3.2.
10. Iqbal, S., Kiah, M. L. M., Dhaghighi, B., Hussain, M., Khan, S., Khan, M. K., and Choo, K. K. R. 2016. On cloud security attacks: A taxonomy and intrusion detection and prevention as a service. Journal of Network and Computer Applications. 74 (Oct. 2016), 98-120. DOI= https://doi.org/10.1016/j.jnca.2016.08.016.
11. Wikipedia, 2016 dyncyberattack. https://en.wikipedia.org/wiki/2016_Dyn_cyberattack.
12. Valenzuela, I. 2016. Prediction 2017: I survived a ransomware attack in my cloud!. Technical Report. McAfee.
13. W. Wang, L. Ren, L. Chen, and Y. Ding, "Intrusion detection and security calculation in industrial cloud storage based on an improved dynamic immune algorithm," Information Sciences, in press.
14. K. Han, D. Yu, and I. Tashev, "Speech emotion recognition using deep neural network and extreme learning machine," In Fifteenth annual conference of the international speech communication association, 2014, pp. 223-227.
15. S. S. Roy, A. Mallik, R. Gulati, M. S. Obaidat, and P. V. Krishna, "A deep learning based artificial neural network approach for intrusion detection," in International Conference on Mathematics and Computing, 2017, pp. 44-53.
16. G. Hinton et al. "Deep neural networks for acoustic modeling in speech recognition," IEEE Signal processing magazine, vol. 26, no. 6, pp. 82-97, November 2012.
17. M. J. Kang and J. W. Kang, "A novel intrusion detection method using deep neural network for in-vehicle network security," in 2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), 2016, pp. 1–5.
18. Mirjalili, S., Lewis, A.: The Whale Optimization Algorithm. Advances in Engineering Software, 51-67. (2016)

January - February 2020
ISSN: 0193 - 4120 Page No. 116 - 124

19. Zeng, B., Gao, L., Li, X.: Whale Swarm Algorithm for Function Optimization. Intelligent Computing Theories and Application. (2017)
20. Z. Chiba, N. Abghour, K. Moussaid, A. El Omri, and M. Rida, "A novel architecture combined with optimal parameters for back propagation neural networks applied to anomaly network intrusion detection," Computers & Security, vol. 75, pp. 36-58, February 2018.
21. C. N. Modi, and D. Patel, "A novel hybrid-network intrusion detection system (H-NIDS) in cloud computing," in 2013 IEEE Symposium on Computational Intelligence in Cyber Security (CICS), 2013, pp. 23-30.
22. D. A. Musbau, J. K. Alhassan, "Ensemble learning approach for the Enhancement of performance of intrusion detection system," in International Conference on Information and Communication Technology and its Applications (ICTA 2018), 2018, pp. 1-8.
23. D. Singh, D. Patel, B. Borisaniya,, and C. Modi, "Collaborative ids framework for cloud," International Journal of Network Security, vol. 18, no. 4, pp. 699-709, July 2016.
24. W. Wang, X. Zhang, S. Gombault, and S. J. Knapskog, "Attribute normalization in network intrusion detection," In 2009 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009, pp. 448-453.
25. S. Kumar, and A. Yadav, "Increasing performance of intrusion detection system using neural network," in 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014, pp. 546-550.
26. R. Sen, M. Chattopadhyay, and N. Sen, "An efficient approach to develop an intrusion detection system based on multi layerbackpropagation neural network algorithm: IDS using BPNN algorithm," in Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research, 2015, pp. 105–108.
27. Gaidhane, C. Vaidya, and Raghuwanshi, M. "Intrusion detection and attack classification using back-propagation neural network," International Journal of Engineering Research & Technology (IJERT), vol. 3, no. 3, March 2014.