iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** V **Month of publication:** May 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Artificial Neural Network for Development of Intrusion Detection System

Ashish Agrawal[1] , Neelam Sahu[2]
[1,2] Dept of IT, Dr. C. V. Raman University, Kota, Bilaspur, Chhattisgarh, India

Abstract: ***In this digital age, information security is very challenging task to protect the information from suspicious person. All word has to become digital and information is been store in digital format. Today, there is great responsibility of information security. There are many techniques through which we can secure digital information. Intrusion Detection System (IDS) is one of the classification technique by which we can classify the intruder and unauthorized user and protect our information. In this paper we used Artificial Neural Network (ANN) for classification of normal and various types of attacks. ANN gives 99.34% and 99.44% of training and testing accuracy with 75-25% training-testing data partition in case of learning rate =0.3, and Hidden Layer (HL) =2.***
Keywords: Intrusion Detection System (IDS), Classification, Artificial Neural Network (ANN).

I. INTRODUCTION

Information security is a major challenge scenario in present era. Modern age will become to digitalized. Being patient, the whole world is going to be digitized and here is the information that is going to be the most important and sensitive thing in the world. Most of the author have done lot of research in field of information security. Intrusion Detection System is one of the good method to protect the information from the unauthorized user or intruder. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of computer system. Classification plays very important role to classify the unwanted data. Different authors have worked to develop the IDS. J. Jabez et al. (2015) [1]have presented the details of new approach called Outlier Detection approach to detect the intrusion in the computer network. There proposed approach was also been tested with the KDD data sets that are received from real world. Experimental results shows that proposed IDS system took less execution time and storage to predict and also the performance of proposed IDS is better than that of other existing machine learning approaches and can significantly detect almost all anomaly data in the computer network. Y. Maleh et al. (2015) [2] have evaluated the performance of their intrusion detection model using KDDcup'99 database and they studied the variations in detection rate and false positive, when the number of IDS increases in the network. They proposed a hybrid intrusion detection model for WSN. N. Sharma et al. (2016) [3] have observed several research works and they have compared with others techniques. This research provided a direction in the face of Intrusion detection improvement. J. Reddy et al. (2016) [4] have proposed a new virtual Honeynet architecture that implements virtual honeynet collaboration systems (VHCS) which can be able to overcome the honeypot module and security module problem. B. Sujitha et al. (2016) [5] have proposed MPSO (Multi-objective Particle Swarm Optimization) algorithm with discretization is proposed which can work with discrete and continuous type of attribute at the same time. They proposed the new system which can works dynamically to identify the new types of attacks. A. K. Shrivas et al. (2014) [6] have proposed ANN-Bayesian Net-GR technique for classification of attacks and normal data. The proposed model is tested on KDD99 and NSL-KDD data set to check the robustness of model. Finally our proposed model produces highest accuracy compare to others.

II. ARTIFICIAL NEURAL NETWORK (ANN)

Neural networks (Giudici, P., et al., 2009) [9] can be used for descriptive and predictive data mining. ANN is known as best classifier and is able to mine huge amount of data for classification. They were originally developed in the field of machine learning to try to imitate the neurophysiology of the human brain through the combination of simple computational elements (neurons) in a highly interconnected system. In this research work we have focus on learning rate and hidden layer. Learning rate updates the wheat at the time of learning and used to improve the performance of model. We have also used hidden layer one, two and three.

III. RESULTS AND DISCUSSION

This research work have used NSL-KDD data set to train and test the ANN. We have collected this data set from UCI

Volume 5 Issue V, May 2017
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

repository[].The data set consist 25192 instances, 41 features and 1 class. The class level consist 1 normal and four types of attacks. In this research work, we have used ANN for classification of various types of attacks and normal data. We have applied the NSL-KDD data set into ANN with 75-25% training-testing data partition in different learning and hidden layer. The accuracy of ANN is given in table I with different learning rate and hidden layer. The accuracy of ANN vary when we change learning rate and hidden layer. In case of hidden layer one, the training and testing accuracy of ANN is 99.33% and 99.36% with learning rate 0.3. In case of hidden layer two, the training and testing accuracy of ANN is 99.36% and 99.44% with learning rate 0.3. In case of hidden layer three, the training and testing accuracy of ANN is 99.44% and 99.36% with learning rate 0.1. Accuracy of ANN is best for classifying attacks and normal data when HL=2 and learning rate is 0.3. Figure 1 shows that accuracy of ANN with different hidden layer and learning rate.

Table I
Accuracy of ANN with 75-25% training-testing

Learning rate(α)	Hidden Layer=1		Hidden Layer=2		Hidden Layer=3	
	Training	Testing	Training	Testing	Training	Testing
0.9	94.27	94.23	97.96	97.70	80.65	80.74
0.8	94.63	94.58	97.72	97.59	94.50	94.21
0.7	98.10	97.87	97.89	97.60	97.30	97.17
0.6	98.06	97.84	98.35	98.13	83.74	83.68
0.5	98.13	97.94	98.62	98.45	90.88	90.68
0.4	99.32	99.30	99.36	99.34	98.24	98.03
0.3	**99.33**	**99.36**	**99.36**	**99.44**	99.16	99.22
0.2	99.19	99.31	98.77	98.43	98.58	98.50
0.1	98.64	98.51	98.75	98.51	**99.44**	**99.36**

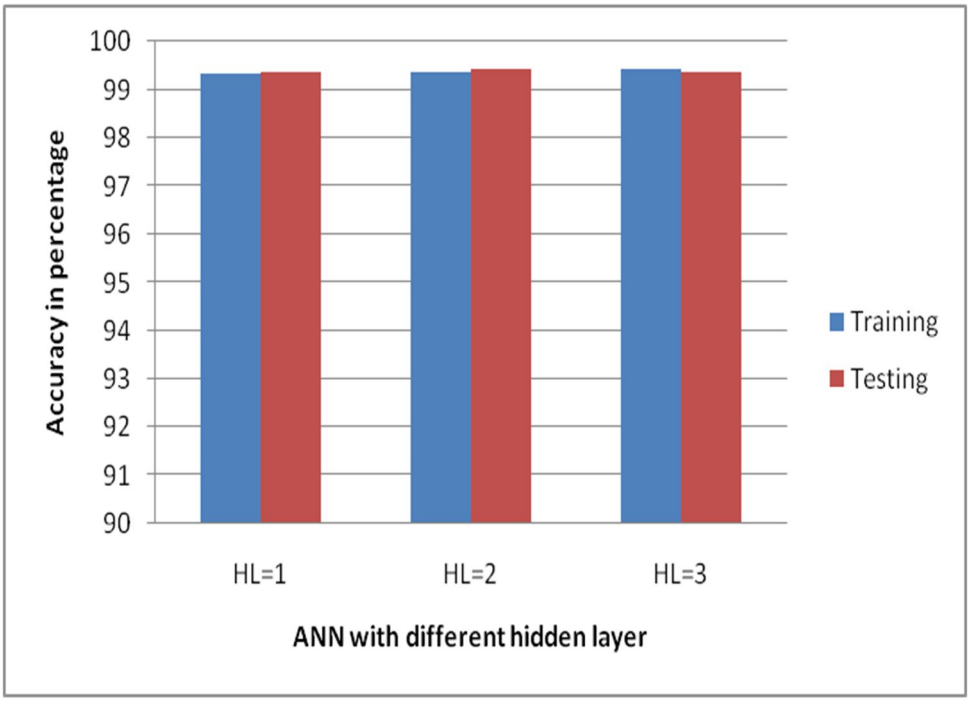


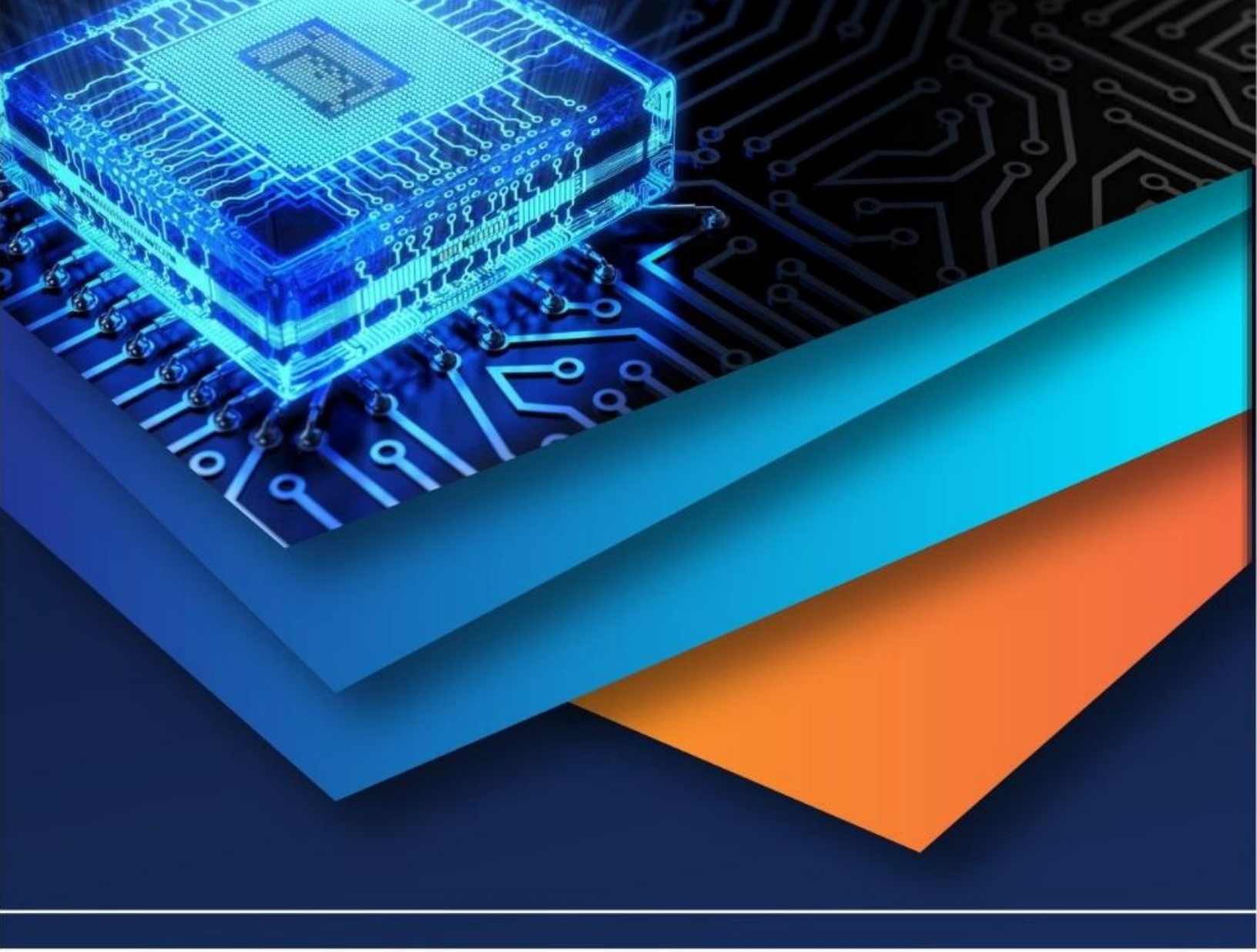
Fig. 1 Best accuracy of ANN with different hidden layer and learning rate

IV. CONCLUSION

Security of information play very informant role to protect the data from unauthorized users. Intrusion detection system is a classifier to classify and protect the system from various types of attacks. In this research work we have used ANN to classify the normal and four types of attacks like DoS, R2L, U2R and Probe attacks. We have trained and test the ANN model with different learning rate and different hidden layer, but achieved better results as 99.34% and 99.44% of training and testing accuracy with earning rate =0.3, and Hidden Layer (HL) =2.Our proposed model is robust and secure for classification of attacks.

REFERENCES

[1]. J. Jabez and B. Muthukumar, Intrusion Detection System (IDS): Anomaly Detection Using Outlier Detection Approach, International Conference on Intelligent Computing, Communication & Convergence organized by Inderscience Institute of Management and Technology Bhubaneswar, Odisha, India, Procedia Computer Science , Vol. 48, pp. 338 – 346,2015.
[2]. Y. Maleh, A. Ezzati , Y. Qasmaoui and M. Mbida, A Global Hybrid Intrusion Detection System for Wireless Sensor Networks, The 5th International Symposium on Frontiers in Ambient and Mobile Systems (FAMS 2015), Procedia Computer Science Vol. 52, pp. 1047 – 1052, 2015.
[3]. N. Sharma and B. Gaur, An approach for efficient intrusion detection for KDD dataset: a survey, International Journal of Advanced Technology and Engineering Exploration Vol. 3(18) , pp.72-76, 2016.
[4]. J. Reddy , S. K. Bharti., S. M. Mishra and K. S. Babu, Honeypot-Based Intrusion Detection System: A Performance Analysis, 3rd International Conference on Computing for Sustainable Global Development, 16th - 18th March, 2016 Bharati Vidyapeeth's Institute of Computer Applications and Management (BVICAM) New Delhi (INDIA), pp. 3947-3951, 2016.
[5]. B. Sujitha. and V. Kavitha , Intrusion Detection System Using F-SVM Based Layered Approach with Enhanced MPSO Feature Selection Algorithm, International Journal of Advanced Engineering Technology, Vol. 7(1), pp. 93-99.
[6]. A. K. Shrivas and A. K. Dewangan (2014) ,An Ensemble Model for Classification of Attacks with Feature Selection based on KDD99 and NSL-KDD Data Set, International Journal of Computer Applications, Vol. 99 (15), pp. 8-13, 2014
[7]. P. Giudici, Applied Data Mining for Business and Industry, 2nd edition, John Wiley & Sons, 2009
[8]. Available: http://www.ics.uci.edu/~mlearn/databases/



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY