IJCSE International Journal of Computer Sciences and Engineering Open Access
Review Paper Vol.7, Special Issue.3, Feb. 2019 E-ISSN: 2347-2693

Novel Approach for Intrusion Detection Using Back Propagation Algorithm

D.K. Singh[1*], M. Shrivastava[2]

[1]Dept. of Computer Science and Engineering, SOS, Engg. & Technology, GGV, Bilaspur (C.G.), India

[*]*Corresponding Author: devendra.singh170@gmail.com, Tel.: +91-98274-71404*

Available online at: www.ijcseonline.org

Abstract— Intruders are available anywhere. They want to take the benefits of the hidden or confidential information of the user. They are trying access by the different – different techniques. Intruder finding is a big problem at the current time. So that security is important to secure our system or confidential information of any organization. Intrusion Detection System (IDS) is a popular technique for finding intruders that will be available on a network. We will use the KDD CUP 99 dataset for the training purpose of the Back Propagation based IDS model. BPN is an algorithm of the artificial neural network. KDD CUP 99 dataset are authentic dataset for the intruders. This data set will be collected by the UCI Repository.

Keywords— Intrusion Detection System (IDS), Backpropagation (BPN) algorithm, Cloud Computing (CC), Support Vector Machine (SVM), Network Intrusion Detection System.

I. INTRODUCTION

Intrusion detection is a big problem in a network security. Intruders are always available on our computer network. They are continuously trying to access our important information that will be available on the computer network. The artificial neural network is a technique of a soft computing [11]. Backpropagation (BPN) algorithm is a use for training our model for finding the intruder on computer network [12]. IDS are techniques to find intrusion on the computer network. We are trying to develop the one secure model for network security. BPN use for develops the IDS model. BPN will be used for training purpose of our developed model. We will generate the final output of our model and include in this paper [13,14].

II. THE PROBLEM OF WORK

Intrusion detection is a problem of a computer network. Computer security is affected by the intruders. Security is very important for our important information that will be available in our computer system. A computer network is not secure because every time intruders are available on our network. They are always trying access our system by different – different logics. They are continuously applying in our computer system for access.

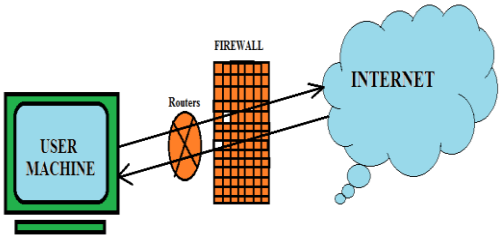

Figure 1. User machine accessing the Internet

So that security is very important in the computer network. We are trying to develop the IDS model for finding the intrusion by using the BPN.

III. CLASSIFICATION OF DATASET KDD'99:

This dataset is classified into five types. These are the following [12]:

- **Normal:** No Attack.
- **Denial of Service (DoS):** Attacker can make computing and memory resources too busy or too full or denies user access.
- **User to Root (U2R):** In this attack sniffing user password and exploit Vulnerability of the user.
- **Root to Local (R2L):** In this attack occupies the system and generate the packets and send it and use the vulnerability of the user and take the benefits of the user.

- **Prob attack:** In this attack, attacker attempt to gather information about the network of connected computers and also control the security information.

Hear, there is in two group's first one is the normal group (i.e. no attack) and the second one is an attack group. In these groups that are DoS, U2R, R2U and Prob attack.

IV. LITERATURE REVIEW

Neda Afzali Seresht, et al., 2014 [1] has been proposed a successful mechanism for distributed intrusion detection system that is agent-based approach by using Artificial Immune System (AIS). This is beneficial for anomaly IDS.

Yuxin Meng et al., 2014 [2] has been proposed as a hash-based contextual signatures scheme. These schemes combine the original intrusion detection signatures. The author proposed 3-tuple {Cl, Sig, H} the generic contextual for easily find intruders.

Chirag Modi et al., 2013 [3] giving a survey paper an Intrusion Detection System. By this survey, they find the effect of different intrusions affecting cloud resources and services. They discussed all types of attack and, IDS/IPS techniques used in cloud computing. Soft computing techniques used for find intrusion can improve the security level in the cloud server.

Igino Corona et al., 2013[4] authors did the survey on the adversarial attack against IDS. They provide the following original contributions: (a) a general taxonomy of attack tactics against IDSs; (b) an extensive description of how such attacks can be implemented by exploiting IDS weaknesses at different attraction levels; (c) for each attack implementation.

Hesham Altwaijry et al., 2012[5] in this paper authors describe the naïve Bayesian classifier in this paper and the importance of the paper is to find possible intrusion attack. Bayesian classifier performances for finding intrusion are in high detection rate and reduce the false positive alert rate.

Shahaboddin Shamshirband et al., 2013 [6] author worked in the wireless sensor networks and mob ad-hoc network. Find intrusions in the sensor network and also find the attacks on mob ad-hoc networks.
Guisong Liu et al., 2007[7] author used principal component analysis (PCA) as a classification and neural networks to find intrusions. The neural network is used for online computing. PCANN is suitable for online computing for find misuse detection and anomaly detection.

P. Arun Raj Kumar et al., 2011 [8] authors have been given detection technique of Distributed Denial of Service (DDoS) attack by using the machine learning technique like neural classifier. In this paper author using Resilient Back Propagation (RBP) as a base classifier.

Bin Luo et al., 2014 [9] according to Four-Angle-Star based Visualized feature generation (FASVFG) approach is based on four angle star image. FASVFG is a classifier achieves high accuracy in the validation experiment.

Mohsen Rouached et al., 2012 [10] author using event calculus-based specification for improving the efficiency of the Network Intrusion Detection (NIDS) process. It is very important for finding known attack with high accuracy.

V. METHODOLOGY

To develop the IDS model, we have used as input in the recently used IDS model is 25062. For testing, we have used 70% of data from the dataset and 15% for data validation and finally remaining 15% of the dataset will be used as a testing dataset. 17543 data used as an input in our model and 3759 datasets will be used as a validation and finally remain approx will be used as a testing dataset (3759 datasets). The result of our model is shown in Fig (2), Fig (3), Fig (4) and Fig (5).

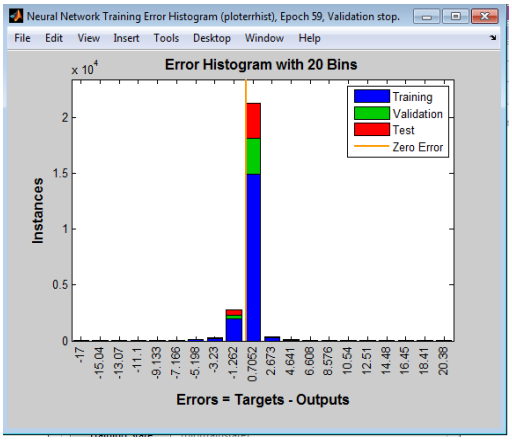

Figure 2. Training Error Histogram

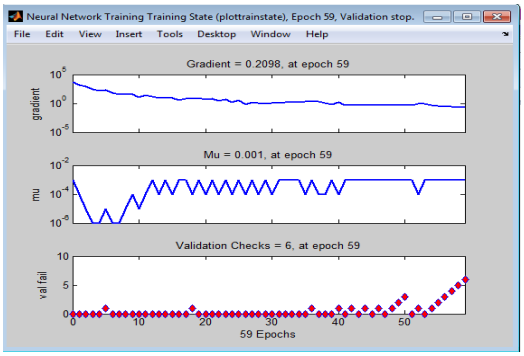

Figure 3. Training state of ANN

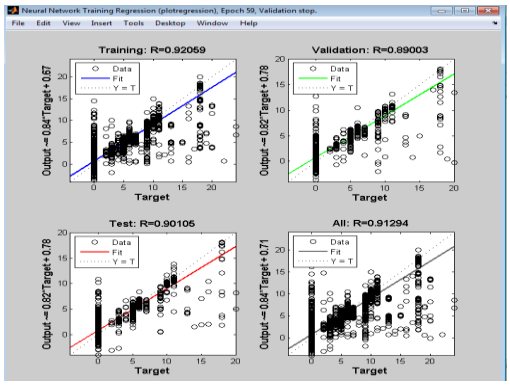

Figure 4. Training regression of ANN

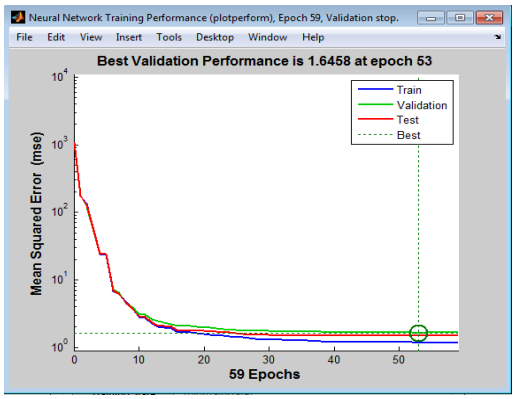

Figure 5. Training Performance of ANN

VI. CONCLUSION

By using MATLAB 2012b we have used for developing the IDS model and we have provided the input values on our model of KDD99 dataset [14]. Training is important so that we have trained the ANN with using BPN algorithm. Finally, we get the result of finding intrusion into the computer network. By using this model we can find the attack on the computer network or not. We can find by using our IDS model.

REFERENCES

[1] Neda Afzali Seresht, Reza Azmi: "*MAID-IDS, A distributed IDS using multi-agent AIS approach*", Elsevier, published the Journal of Engineering Applications of Artificial Intelligence, 35, pp 286-298, 2014.

[2] Yuxin Meng, Lam-For Kwok "*Adaptive Non-critical alarm reduction using Hash-based Contextual signatures in intrusion detection*", Elsevier, published in the Journal of Computer Communications, 38, pp 50-59, 2014.

[3] Chirag Modi, Dhiren Patel, Bhavesh Borisanya, Hiren Patel, Avi Patel, Muttukrishnan Rajaranjan "*A survey of intrusion detection techniques in Cloud*", Elsevier, published the Journal of Network and Computer Applications, Vol.-35, Issue-1, pp 42-57, 2013.

[4] Igino Corona, Giorgio Giacinto, Fabio Roli, 2013 "*Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues*", Elsevier, published in the Journal of Information Sciences, Elsevier, 239, pp 201-225, 2013.

[5] Hesham Altwaijry, Saeed Algarny "*Bayesian-based intrusion detection system*", King Saud University, published in Journal of King Saud University – Computer and Information Sciences, Producing and Hosting by Elsevier, 24, pp 1-6, 2012.

[6] Shahaboddin Shamshirband, Nor Badrul Anuar, Miss Laiha Mat Kiah, Ahmed Patel "*An appraisal and Design of a multi-agent system based on computational intelligence techniques*", published in Science Direct, Elsevier, pp 2105-2127, 2013.

[7] Guisong Liu, Zhang Yi, Shangming Yang "*A hierarchical intrusion detection model based on the PCA neural networks*", published in Science Direct, Elsevier, pp 1561-1568, 2007.

[8] P. Arun Raj Kumar, S. Selvakumar "*Distributed denial of service attack detection using an ensemble of neural classifier*", Elsevier, published in the Journal of Computer Communications, pp 1328-1341, 2011.

[9] Bin Luo, Jingbo Xia "*A novel intrusion detection system based on feature generation with visualization strategy*", Elsevier, published the Journal of Expert Systems with Applications, pp 4139-4147, 2014.

[10] Mohsen Rouached, Hassen Sallay "*An Efficient Formal Framework for Intrusion Detection Systems*", Elsevier, published the journal of Procedia Computer Science, 10, pp 968-975, 2012.

[11] https://technet.microsoft.com/en-us/library/cc959354.aspx

[12] Mahbod Tavallaee "*Detail Analysis of the KDD CUP 99 Data Set*", Proceeding of the 2009 IEEE Symposium on Computational Intelligence in Security and Defense application (CISDA 2009), 2009.

[13] Wikipedia, www.wikipedia.org.

[14] Data collection form Knowledge Discovery Dataset, UCI Repository http://kdd.ics.uci.edu/databases/kddcup99.

Authors Profile

Devendra Kumar Singh

Mr. D K Singh pursed Bachelor of Engineering from B. U. University of Bhopal (MP), 2000 and Master of Engineering from AAI-DU Allahabad (UP) in year 2006. He is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science & Engineering, SOS, E&T, G. G. V. Bilaspur (C.G.) since 2005. He is a member of AIENG. He has published more than 10 research papers in reputed international journals. His main research work focuses on Intrusion Detection System. He has 12 years of teaching experience and 3 years of Research Experience.

Manish Shrivastava

Manish Shrivastava, Assistant Professor Department of Computer Science & Engineering, Institute of Technology, Guru Ghasidas University, Bilaspur, obtained his M. Tech. Degree from DAVV, Indore, and Ph. D. from Guru Ghasidas University, Bilaspur. He has about fifteen years of teaching and research experience, he has a number of papers in various national and international journals to his credit. His field of interest is network security, served as chairman board of studies, computer science & engineering, Guru Ghasidas , Bilaspur, life member, Indian Society for Technical Education, Senior member IACSIT .

