Artificial Neural Network Model for Predicting Fraudulent Attacks

1Archana P, 2Divyabhariithi P, 3Camry Joshya Y, 4Sudha

1Assistant Professor, Department of ECE, Karpagam College of Engineering, Coimbatore,
2Assistant Professor, Department of ECE, Veltech Rangarajan Dr.Sagunthala R&D Institute of Science and Technology, Chennai.
3Assistant Professor, Department of ECE, Karpagam College of Engineering, Coimbatore.
4Assistant Professor, Department of ECE, SONA College of Technology, Salem.

Abstract. Now a days Artificial Intelligence is an emerging technology. Neural network concepts used in many applications at present situation. The usage of internet increases day by day as well as the lack of security increases day by day. Mainly phishing scams emerges highly in case of network security. In this paper Neural network concepts, how to train and test the data using Artificial neural network has been discussed which gives an brief idea about usage of Neural net concepts in field of Network security. The properties such as feed forward back propagation network form, gradient descent momentum training purpose, sigmoid transfer function, supervised learning model used to train the model for predicting fraudulent attacks.

Index Terms – Artificial intelligence, neural network, phishing, network security, feedforward back propagation, sigmoid transfer function.

1. Introduction
Artificial neural network is artificial representation of neural net of our human brain. Since it is man made it is called as artificial neural net. ANN is cast-off to predict output based on provided input. Initially network model should be trained with inputs and subsequent outputs, So the prediction is possible. The purpose of the ANN is to develop the computing model in order to carry out various engineering models that stimulated by both performance as well as structure of our biological net. Neural networks are comprised of neurons. So, the structure and performance of our human brain is being considered for developing a computer-based model. But the artificially human made models does not reach near the performance of the biological system, because human brain is a superior super computer. It is difficult to model exactly as biological net. In a biological network (human brain) there are 1011 neurons and these neurons are interconnected with each other so that the data are transferred or processed.

2. Model for Predicting Fraudulent Attacks
The operations of biological neuron are naturally asynchronous. Asynchronous means executing multiple tasks at a time. Because of this the performance of artificial models cannot be nearer to the biological neural network.

A. Output Biological neural network- Features
   - Robust and Fault tolerance: The deterioration of nerve cells never disturb the performance pointedly. In case of ANN if there is any system related degradation, obviously the performance level will get decreased.
   - Elasticity: The net inevitably corrects to original environment with pre-programmed advices. In case of ANN it will not adjust automatically to new environment.
   - In case ANN it is highly impossible to work on different data conditions.

B. The human brain
There are numerous neural cells in human brain its work is to progress the information. The cell present in the brain imitates the processor. All the cells can relate as well as can progress parallelly. A neuron consists, of a core, dendrites is used for arriving evidence and an axon through dendrites for outgoing evidence is conceded to related neurons.

![Fig1. Block Diagram of Neurons](image)

Impulses is nothing but the datas of information through electric signals these transmit the data from one neuron to another neurons. An electric pulse travels laterally with axon this triggers the nerve ending of an neuron to release chemical messengers called neurotransmitters. Where two neurons meet there is a small gap called a synapse. These chemicals diffuse across the synapse and bind with receptor molecules of the membrane of the next neuron. The binding of neurotransmitter to the receptors stimulate the second neurons to transmit an electrical impulse along its axon. Each neurons exchange the data with the help of dendrites. Input signals which are received by the neurons dendrited are supplemented and transported laterally to neuron axons. When the threshold is exceeded the neuron exchanges info to other neuron by which that neuron gets triggered. When the threshold is not reached then the information will not transferred. The relationship within neurons is adaptive in nature. It means connective construction is altering. The knowledge skill of human mind depends on adaption.

![Fig.2. Biotic and Artificial Neuron](image)

C. Nervous Net

Neural net is non-natural depiction of the human intelligence that attempts to pretend its knowledge method. Wildlife can respond adaptively to fluctuations with both exterior and interior atmosphere and
with the help of their nervous system they accomplish these attributes. The word non-natural implies neural net are executed in processor agendas that can handle huge figure of required computations through this knowledge method.

![Fig.3. Outline of ANN](image)

Artificial neurons: Both non-natural and biotic neurons are same and their performance is also same. Data is directed to neuron by received weight.

![Fig.4. ANN](image)

In this input is operated through propagation. The weights that are connected with the inputs are considered. Both the added value and the threshold value will be related by neuron stimulation role. If the result is greater than the threshold range it will be considered or it will be ignored. If the results are greater the neurons will deliver the information. In output by using the activation function the neurons delivered information will be calculated. They have dynamic range among 0 and +1 and -1 and +1. Many activation functions differ in terms of complexity and output.

Assumptions made: The positions on the neurons of received synapse is inappropriate. Every node will be having an one received value, and this node can transport to other nodes. All inputs will occur at equal stretch are remained activated at the equal level and it is long enough for competition to happen. An substitute is to postulate the presence of buffers to stock weighted inputs inside nodes.

Activation function: By using this activation process only neural net is processed. The input to output conversion is done using this activation processes and also it links the neural net without the help of activation process. Both the neural net process and linear process will be same. If the output is directly related to the input it is known as linear process.

\[ Y = 2x + 1 \]
\[ Y = f(x) \]

Sigmoid: It can create a sigmoid arch, which is a arch with an S drift.
Habitually, sigmoid function denotes to distinct event of the logistic role.

Choosing proper activation functions is the best key to create a network performance at its finest and to obtain respectable training. There is no rule of thumb in the field of neural networks. It all depends on your data and in what form you want the data to be transformed, after passing through the activation function. For a particular activation function, the graph of the function should be studied thoroughly.

In neural net, the neurons layers are formed by grouping neuron. Each and every neuron is linked to other neurons. First neural net receives the data and it is sent to input and then sent to output by none, single or more layers

SUPERVISED LEARNING-
The learning procedure of a neural net can be supervised and unsupervised. Supervised; The desires output is already known is known as supervised. Networks response of input is calculated. The variance among real and desired outputs is done for weight alteration.

TYPES OF ANN
Numerous kinds of neural net present. They can be distinguished by types (feedforward and feedback), their construction, the learning process they practice.

PERCEPTION MODEL:
The perceptron regularly practices a step purpose, which returns 1 if the biased sum of inputs overdo a threshold, and 0 or else. When layers of perceptron are joint together, they create a multilayer planning, and this produces the essential difficulty of neural net processing. The generally used planning for neural networks are Multi-Layer perceptron.

FORWARD PROPAGATION
The process as of input layers to hidden layers and again to output layer is named as forward propagation. The sums(input*weights)+bias is at each layer and then the activation process is broadcasted to the next layer. The following layer will be hidden layer or the output. The structure of neural net uses huge number of hidden layers to give increase to deep Neural Network(DNN). these copies are named feed
forward since data streams through the function being assessed from x, over the midway calculations used to describe, and lastly to output y. There are neither feedback connections in which outputs of the model are fed back. A commonly used supervised learning algorithm is the backpropagation algorithm.

D. Procedure Feed Forward-Back Propagation Algorithm

Set the network with casual weights training cases, the steps are Forward pass: Calculate network’s error, that is, the variance among the chosen output and real output. Backward pass: For layers, initialising with output layer again to input layer. Shows network layers output through precise input Adapts the weights in the current layer to lessen the error problems.

Randomly choose original ethics for the parameter of the model. Compute the grades G of the error function with respect to each parameter of the model. modify the models parameters so that they move in the direction of decreasing the error, that is, in the track of G. Reappearance steps 2 and 3 until the values of G approaches zero.

Learning rate and momentum coefficient
The knowledge rate is a public parameter which disturbs the speediness at which the ANN touches the bottom period. The momentum parameter can avoid the system from meeting to a local minutest or saddle point. A high momentum parameter can be used to surge the speediness of convergence of the system, but can create a risk of overshooting the minimum, because of this the system becomes unstable. A momentum coefficient that is too low cannot reliably avoid local minima, and also can minimise the training pf the system.

WEIGHT AND BIAS:
Bias is like the intercept added in a linear equation. It is an additional parameter and it can modify the output within the weighted sum of inputs to the neurons.

Output = sum(weight*input) + bias

3. Experimental Results
The simulation of the work is done using MATLAB 2015a with the help of the neural network tool first train the network later simulate. In nn data manager there are input data, output statistics, target statistics, input delay, error statistics and coat interruption conditions. Before simulation the training and testing data should be segregated priorly. In MATLAB enter the training target and testing datas by creating separate files using new variables. For this work supervised learning algorithm is used. Now in NN tool import the training data. In input there are four neurons. The model fitting is done in graphical interface user. The ANN should have 3 different files input data for training the network, output for unsupervised learning and testing data. The developed model can be stored and that can be used for further predictions. If the value is not between the range then prediction cannot be obtained.
Once model is developed need to validate for the purpose of prediction. In new variable enter train, target and test data. In NN tool manager the input is fed using import. The process consists of develop ANN model and train ANN model. Input training data consists of 4 neuron, the output is the target data. To create the model need to provide properties.

For training the data, supervised learning algorithm is used, properties such as for Network type feedforward back propagation is used because it produces good results, working out for job gradient Momentum is used. System itself will take random value (weight) according to the output because of back propagation it adjust the weight. If slope is zero GDM it produces perfect prediction.
For performance function mean square error is considered. If the no of layers is two then it means hidden layer + output layer, if number of layers is 3 it means two hidden layers +output layer. If the hidden layer increases the complexity as well as the computation time will also get increases to develop the model.

4. Conclusion and Future Scope

The neural network approaches by training and testing the data using nn tools increased the network security by reducing the fraudulent attacks. Epoch means iteration. Due to repetitive iteration the network model is validated. The developed model itself take the random weight (value) according to the output because of back propagation it adjust the weight The usage of sigmoid transfer function provided better function. It ranges from -1 to 1 or 0 to 1. The sigmoid function produced predicted result of 99%. Thus the NN tool model can reduces the fraudulent attacks by which the Phishing attacks can be minimized.

Other Neural networks like Convolutional neural network can be used and output can be compared for optimized results.

5. References

[1] S. Naseer, Y. Saleem, S. Khalid, M. K. Bashir, J. Han, M. M. Iqbal, and K. Han, “Enhanced network anomaly detection based on deep neural networks,” IEEE Access, vol. 6, pp. 48231–48246, 2018.
[2] B.-C. Zhang, G.-Y. Hu, Z.-J. Zhou, Y.-M. Zhang, P.-L. Qiao, and L.-L. Chang, “Network intrusion detection based on directed acyclic graph and belief rule base,” Electron. Telecommun. Res. Inst. J., vol. 39, no. 4, pp. 592–604, Aug. 2017
[3] W. Wang, Y. Sheng, and J. Wang, “HAST-IDS: Learning hierarchical spatial-temporal features using deep neural networks to improve intrusion detection,” IEEE Access, vol. 6, pp. 1792–1806, 2018.
[4] M. K. Hussein, N. Bin Zainal, and A. N. Jaber, “Data security analysis for DDoS defense of cloud based networks,” in Proc. IEEE Student Conf. Res. Develop. (SCoReD), Kuala Lumpur, Malaysia, Dec. 2015, pp. 305–310.
[5] S. S. Sekharian and K. Kandasamy, “Profiling SIEM tools and correlation engines for security analytics,” in Proc. Int. Conf. Wireless Commun., Signal Process. Netw. (WiSPNET), Mar. 2017, pp. 717–721.
[6] N. Hubballi and V. Suryanarayanan, “False alarm minimization techniques in signature-based intrusion detection systems: A survey,” Comput. Commun., vol. 49, p. 1A17, Aug. 2014.
[7] A. Naser, M. A. Majid, M. F. Zolkipli, and S. Anwar, “Trusting cloud computing for personal files,” in Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC), Busan, South Korea, Oct. 2014, pp. 488–489.
[8] Y. Shen, E. Mariconti, P. A. Vervier, and G. Stringhini, “Tiresias: Predicting security events through deep learning,” in Proc. ACM CCS, Toronto, ON, Canada, Oct. 2018, pp. 592–605.
[9] K. Soska and N. Christin, “Automatically detecting vulnerable Websites before they turn malicious,” in Proc. USENIX Secur. Symp., San Diego, CA, USA, 2014, pp. 625–640.
[10] Natarajan, B., Obaidat, M.S., Sadoun, B., Manoharan, R., Ramachandran, S. and Velusamy, N., 2020. New Clustering-Based Semantic Service Selection and User Preferential Model. IEEE Systems Journal. DOI: 10.1109/JSYST.2020.3025407.
[11] Nataraj, S.K., Al-Turjman, F., Adom, A.H., Sitharthan, R., Rajesh, M. and Kumar, R., 2020. Intelligent Robotic Chair with Thought Control and Communication Aid Using Higher Order Spectra Band Features. IEEE Sensors Journal, DOI: 10.1109/JSEN.2020.3020971.
[12] Babu, R.G., Obaidat, M.S., Amudha, V., Manoharan, R. and Sitharthan, R., 2020. Comparative analysis of distributive linear and non-linear optimised spectrum sensing clustering techniques in cognitive radio network systems. IET Networks, DOI: 10.1049/iet-net.2020.0122.
[13] Sitharthan, R., Yuvaraj, S., Padmanabhan, S., Holm-Nielsen, J.B., Sujith, M., Rajesh, M., Prabaharan, N. and Vengatesan, K., 2021. Piezoelectric energy harvester converting wind aerodynamic energy into electrical energy for microelectronic application. IET Renewable Power Generation, DOI: 10.1049/rpg2.12119.

[14] Sitharthan, R., Sujatha Krishnamoorthy, Padmanaban Sanjeevikumar, Jens Bo Holm-Nielsen, R. Raja Singh, and M. Rajesh. "Torque ripple minimization of PMSM using an adaptive Elman neural network-controlled feedback linearization-based direct torque control strategy." International Transactions on Electrical Energy Systems 31, no. 1 (2021): e12685. DOI: 10.1002/2050-7038.12685.