IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Addendum – Artificial Neural Network Security In Java

Niravkumar K Patel

University of the Cumberlands

Spring 2023 –Full Term

Abstract

Artificial Neural Network is one of the entail techniques in Artificial Intelligence for Cyber Security or policies. There are several benefits to using AI-based cyber risk analytics to improve organizational resilience and better comprehend cyber risk analytics to enhance organization. Multilayer security, convolutional networks, recurrent neural networks, self-organizing maps, deep transfer learning, as well as their ensembles and hybrid approaches, can be used to handle cycler networks efficiently. The goal of the network is to generate secure infrastructure as per input and transmit to the device as per the required output. Neural networks may be used to handle several cybersecurity problems. MLP-based networks are designed to identify the security threat of the application, provide malware protection, identify botnet traffic, and build trustworthy IOT systems. MLP is a critical feature to scale the request differently and build vulnerable IOT systems. MLP will provide the number of hidden layers, neurons, and iteration processes, solving a complex security problem and model computationally costly. This is the technique to generate security applications for infrastructure in Artificial Intelligence. It will analyze the application complexity of security and write the algorithm for different types of security, such as network security, application security, SSL security, cryptography security, and file transfer security. We don't need to spend more time designing the application for this security. It will analyze the code and write the scenario based on the application. It will generate different types of test cases also, such as functional, Integration, Code level testing,

INTRODUCTION

CPS theory evolved from control theory and control system engineering. It will focus on sophisticated software entities' physical features and utilization to create network and system capabilities. CPSs connect biological and engineering systems, bridging the cyber and physical network. IoT is based on computer science and internet technology; it focuses primarily on the interconnection, interoperability, and integration of biological components on the internet. This integrates the IOT automation of CPSs in production situations in real-time as the IOT industry matures over the next decade. We will analyze the application that enables artificial intelligence through real-time processing, sensing, and actuation across these new systems and give cyber structure system analysis capabilities. We will focus on artificial intelligence, a notion combined with cyber-physical and social components of hazards associated with deploying new technologies. There are two research projects. We will provide an up-to-date summary of the current and cyber risk analytics breakthroughs. This will give current standards into a new risk analytics feedback loop to generate shared core terminology and techniques. Another one is providing a novel way to understand cyber network risk and the roles of AI in future CPS. We are storing all the data in Spark. The IOT has been an excellent technological augmentation that transformed living in living into a high-tech lifestyle in terms of data streams. CPS and IOT generate vast amounts of data streams and powerful analytical tools for analysis. We need AI-assisted tools to clean up data noise and inconsistencies. CPS architecture covers an extensive range of topics. CPS will combat malicious supply chain components altered from their design to disturb or perform unethical functions. Hyperconnectivity in the digital supply chain must be promoted in addition to designing the process standardization. It is proposed that software engineers provide high-security assurance and application security.

Background

The attack detection tool is essential for providing safety in application and network security systems. These tools are entirely dependent on the attacking system and detection. Moreover, detection also prevents the attack and identifies the types of attack. A few attempts have been made in the field of attack detection. It is an artificial neural network supporting an ideal specification of the attack detection system, and it will solve the problems of different types of systems. Artificial neural Technologies will identify the attack, diagnose depth internally, and make an appropriate algorithm to secure the application and network. If. the attack occurs again with the same types, it will block all the requests and notify the principal engineer to make some critical changes. A host bases IDS evaluation information found on a single or multiple host system, including operating system content.

IDS will evaluate the packets that have been transferred via the network. All packages are captured through a set of sensors. It will analyze the stream of packets traveling across the web. There are two main significant processes, misuse and anomaly detection, which work by identifying activities that vary from established patterns for users or groups of users. It will typically involve the creation of a knowledge-based profile creation and monitoring capabilities continuously. The second technique compares the user's activities with the known behaviors of attackers attempting to penetrate an application. Attack detection tools will be used to evaluate parameters such as false positive, false negative, and detection rate. A false positive and false negative detection rate. A false positive occurs when the system identifies an action. Whether it will be a legitimate request or not. If the request is fraudulent, negative happens, then it moves to be taken care of, but the system allows it to pass on non-intrusive behavior. A neural network would be capable of analyzing the data from the web. If the data is incomplete or the request is not fully satisfied,

The network will process the data and collect all the information in a non-linear fashion because the attack has happened from multiple attackers, the ability to process data from several sources in a non-linear manner. The artificial neural networks will detect variant types of attacks and unknown attacks, and cluster patterns share similar features.Probing Attack and Its types:

These are various parameters and algorithms of the systems.

IP sweep: It probes the network to discover available services. It will find out which machine to be attacked.

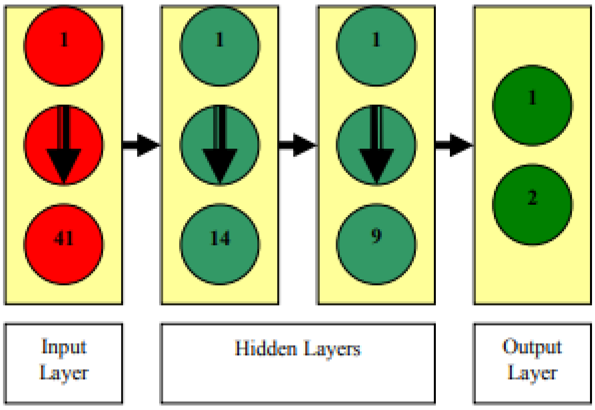
Port sweep: If the service is available on the network, it will attack the network intruder.

Nmap is a complete and flexible tool for scanning a network randomly or sequentially. Intruders use this tool for monitoring network parameters that would help them from attacking the system.

Satan: It is an administration tool to collect information about the network transmission. An attacker can use this information.

Architecture:

The artificial neural network architecture is used in the feedforward approach. A feed-forward neural net comprises several consecutive layers and components, each one connected to the next connection. The design of a feed-forward neural network with four layers connected with three synapses. Each layer is composed of a certain number of, and each transfer. function.



The input layer will contain 41 neurons for data sets— fields and characteristics for attack detection on the network. e output layer consists of two neurons that will process regular abnormal packets. There is no accurate formula for this selection of layers, but we can make it by comparing the sections to see which one is best.

Implementation:

Dataset and testing: The efficiency of a neural network is based on the training data and the collection of critical problems. T will be obtained in three ways. R al traffic by using sanitized traffic and simulated traffic. The first option is to get training data by collecting accurate data and attacking an organization. A l the packets would be honest, and it is intolerable to attack the organization. The first option to obtain the data is collecting accurate data and tracking the organization via packets. A l the private information is shared via secure processes and mechanisms. It is possible to release sensitive data since it is infeasible to verify because of the large volume of data. T here is another way to collect and obtain data via a testbed network and generate background traffic on the web.

Preprocessing Datasets:

This is the process of how the data set is to be used for the experiment. The data set is preprocessed for input to our developed system. T is a data set consisting of numeric and symbolic features, and the application converts into numeric form to provide feedback in neural networks. The application can replace the extended with a specific numeric, comma with a semicolon, regular with 0,1, and attack with 1,0. The data set is ready to be used for the training and testing neural networks.

Determining the NN architecture:

There are no algorithms for obtaining the number of hidden layers and their neurons. The application uses resilient backpropagation algorithms to train the net because it will converge very quickly. I used the sign of the backpropagted gradient to change the biases of the net. The feedforward input training pattern, calculation and backpropagation of the associated error, and adjustment of the weights.

Testing the system:

The weight of the neural network is frozen, and the neural network's performance is evaluated. T sting the neural network involves two steps. W ich are verified the steps and recall steps. In the verification process, neural networks are tested against the data used in training. The verification step aims to try how well the training neural network learned in the training patterns. If the neural network were trained successfully, the output produced by the neural network would be like the actual output. I will contain one input, two hidden, and one output layer. Each layer includes neurons processing elements that take information and give its work after applying it through synapses. The synapse acts as a transmission medium between the layers of the topology. The forward and backward propagation process will be completed through the synapse by on-and-back propagation. The system will show 98% accuracy in all the detection rats. I will monitor all the requests and collect the information regularly. Resilient backpropagation offers the best performance compared to the other neural network approaches. W implemented the proposed scheme using Java programming language, and the result of the implementation shows the proposed cryptography and decryption speed. In the notebook computer of Dell, the speed of the data encryption and decryption tested and the speed of the data encryption for the proposed scheme using software implementation is over that of RSA using hardware implementation. A higher encryption speed can be ensured in the actual time of ping communication.

Several tests were performed between two data set groups using vulnerable and non-vulnerable methods. A significant test was done to see the difference in specific parameters and was described with the two groups. The data set analysis revealed a statistical significance asymmetry of size and abstract syntax tree complexity between the vulnerability and non-vulnerability methods. Machine learning and neural network models create an unintended model bias, such as a biased model unable to identify the same security vulnerabilities.

The final step is to use the training word2vec to embed the keyword in trees as vectors, and every keyword tree is traversed. The string currently being read in part of the dictionary created by word2vec will be replaced by the index number corresponding to the dictionary entry. If the line is not part of the dictionary, then it will be replaced by the max index. The output of the process is a vector that represents the method. We have implemented different DDOS attacks at distinct levels to select the other input and artificial neural network patterns by creating an elite network infrastructure in a solitary environment. We carefully studied the results and compared them with authentic traffic to verify the characteristic way in which genuine traffic differs from attack traffic. This process segment demands comprehension of how distinctive protocols interchange data or communicate.

Conclusion

This is the process of identifying the type of attack and the process of detection in real-time systems. We have monitored all the logs as per attack and tried to secure the application and network using neural network AI. All the requests have been captured in real-time, and the process to identify the recommendation is positive or negative. If the request is negative, we will generate the algorithm, so If the request comes again, we will block those requests and take some respective actions against the attackers. The detection process will create data and monitor the submission, IPS, and hostname to communicate again in the same systems. We evaluated our designed solution with another related research on signature-based. I designed our solution to prevent malicious and fake data packets from reaching target devices. I also assessed this solution by training it with old existing and recently updated datasets, and our designed solution provided better results and detected DDOS attacks.

References

Rodes, B., Mahaffey,J., & Cannady, J. “Multiple Self Organizing Maps”. 23rd Security Information System (2000).

Fox, Kevin L., Henning, Rhonda R., and Reed, Jonathan H. (1990).“A Neural Network Approach Towards Intrusion Detection”. InProceedings of the 13th National Computer Security Conference.

Cannady J. Artificial neural networks for misuse detection. National Information Systems Security Conference; 1998. p. 368–81.

Hui Zhu; Bo Huang; Tanabe, Y.; Baba, T., Innovative Computing Information and Control, 2008. ICICIC apos; 08. 3rd International Conference on Volume, Issue, 18-20 June 2008, pp 509 – 509.

JJF Cerqueira, AGB Palhares, MK Madrid , Man and Cybernetics, 2002 IEEE International Conference, 2002.

Souza, B.A.; Brito, N.S.D.; et al, Comparison between backpropagation and RPROP algorithms applied to fault classification in transmission lines, S.S.B. Neural Networks, 2004. Proceedings. 2004 IEEE International Joint Conference on Volume 4, Issue, 25-29
July 2004 pp 2913 - 2918.