I J R B A T, Issue (XI) Vol (II) May 2023 : 64-66
A Double-Blind Peer Reviewed & Refereed Journal
OPEN ACCESS
e-ISSN 2347 – 517X
Original Article
INTERNATIONAL JOURNAL OF RESEARCHES IN BIOSCIENCES, AGRICULTURE AND TECHNOLOGY
 www.ijrbat.in

DEEP LEARNING POWERED FIREWALL ANOMALY MANAGEMENT ENVIRONMENT USING CONVOLUTION AND RECURRENT NEURAL NETWORK

Asfiya Shireen Shaikh Mukhtar[1] and Ghousiya Farheen Shaikh Mukhtar[2]
[1]Computer Science Department, Shivaji Science College, Nagpur
[2]Computer Science department, S S maniar college, Nagpur
Corresponding Email: asfiyashireen768@gmail.com, sonyshaikh7@gmail.com

Communicated : 12.01.2023 | Revision : 16.02.2023 & 23.02.2023 Accepted : 22.03.2023 | Published : 30.05.2023

ABSTRACT:
A firewall is a technology that connects a network to one or more external networks by acting as the network's interface. It is responsible for implementing the network's security policy by deciding which packets should be permitted to travel across the network based on criteria set by the network administrator. Any error in the formulation of the rules may result in the security of the system being compromised, as unwanted traffic may be allowed to pass through while appropriate traffic is prevented from passing through. An anomaly in policy may result from manual rule formation because it produces a collection of regulations that conflicts with itself, redundant with itself, or overshadowed with itself, which is a result of the manual defining of rules. Manual identification and resolution of these anomalies is necessary, but it is a time-consuming and error-prone task that must be done by hand. Previous research on abnormalities in firewall policy has mostly focused on the analysis and identification of these anomalies, with little attention paid to the causes of these anomalies. Previous works describe the potential relationships between rules, as well as the anomalies that may occur as a result of the relationships, and they provide methods for identifying the anomalies through the analysis of the rules in question.
In this research, we present a method for identifying the anomalies through the analysis of the rules in question separately by Convolution Neural Network and Recurrent Neural Network.

Keywords :- Firewall, Neural Network, CNN models, Internet Network.

INTRODUCTION :

A firewall's job is to examine packets and decide whether they should be accepted or rejected based on a set of rules. These rules are frequently in opposition, resulting in oddities. Maintaining firewall rules is a bit of a challenge. Any firewall's performance is measured by the characteristics of its policy configuration and rule set. The algorithm implemented in a tool which identifies the anomalies automatically in rule set by placing the new rule in its appropriate position.

Any network's security protocol is enforced via a firewall, which may filter out undesirable traffic. A set of rules that have been created based on predetermined security policy requirements and are used to make filtering decisions. Firewall policies promotes the effective service of firewalls. Rule-based segmentation for firewall policy anomaly identification and Optimizing rule order which not only identify and remove Firewall Policy Anomalies but also reduces Packet-Rule searching time to improve system performance. The Heuristic Approximation Algorithm is used to Optimize Rule list. The following are the objectives of the paper

1. To study Firewall Technology and its application in Traffic management and Internet Intrusion Detection
2. To develop the Convolution Neural Network Powered Firewall Anomaly Management Environment with unique architecture implementation on Local and Internet Network.
3. To develop the Recurrent Neural Network Powered Firewall Anomaly Management Environment with unique architecture implementation on Local and Internet Network.

http://doi.org/10.29369/ijrbat.2023.02.1.0011

4. To Develop the comparative analytics for CNN and RNN system for developing the optimized AI enabled Firewall Anomaly Management Environment.

A single perceptron (or neuron) can be imagined as a Logistic Regression. Artificial Neural Network, or ANN, is a group of multiple perceptron's/ neurons at each layer. ANN consist of three-layer Input, Hidden and Output. The input layer accepts the inputs, the hidden layer processes the inputs, and the output layer produces the result. Essentially, each layer tries to learn certain weights.

ANN can be used to solve problems related to:

- Tabular data
- Image data
- Text data

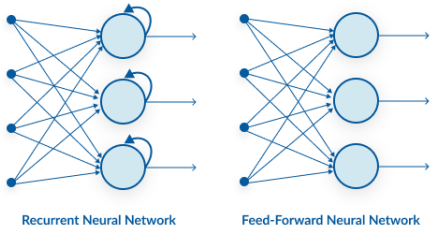
In our problem statement the data will be in the Tabular and Text format. We will be using python and R datasets to do the analytics.

Advantages of Artificial Neural Network (ANN)

Artificial Neural Network can learn any nonlinear function. Hence, these networks are popularly known as Universal Function Approximators. ANNs have the capacity to learn weights that map any input to the output. One of the main reasons behind universal approximation is the activation function. Activation functions introduce nonlinear properties to the network. This helps the network learn any complex relationship between input and output.

Recurrent Neural Network (RNN)

What is an RNN and why should you use it? Let us first try to understand the difference between an RNN and an ANN from the architecture perspective: A looping constraint on the hidden layer of ANN turns to RNN.



As you can see here, RNN has a recurrent connection on the hidden state. This looping constraint ensures that sequential information is captured in the input data. Here all the parameter in terms of firewall policy generation will be set up for RNN system for optimized prediction models.

Convolution Neural Network (CNN) – What is a CNN and Why Should you use it?

Convolutional neural networks (CNN) are all the rage in the deep learning community right now. These CNN models are being used across different applications and domains, and they are especially prevalent in image and video processing projects.

The building blocks of CNNs are filters with kernels. Kernels are used to extract the relevant features from the input using the convolution operation. Here all the parameter in terms of firewall policy generation will be set up for CNN system for optimized prediction models

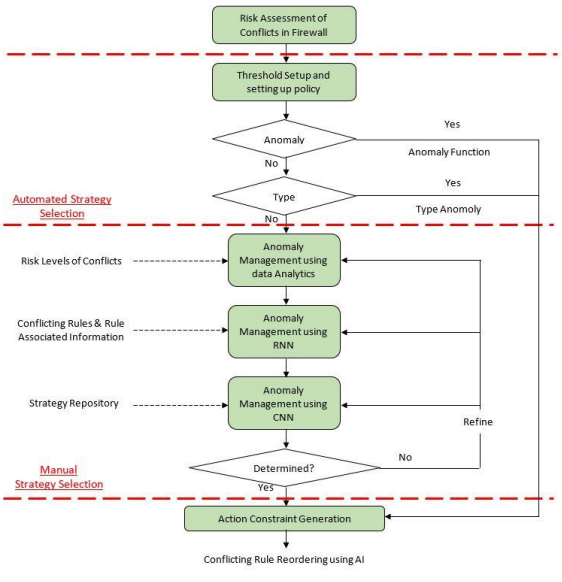


Figure: Proposed strategy-based Firewall data analytics and management using AI

http://doi.org/10.29369/ijrbat.2023.02.1.0011

CONCLUSION :

There has been lot of things proposed and worked by various researchers in the field of firewall decision diagram (FDD) to support consistent, complete, and compact firewall policy generation. Since anomaly discovery and resolution are indispensable processes in policy design and specification, all of those work we will be designing will be orthogonal to our work. The unique Firewall Technology and its application in Traffic management and Internet Intrusion Detection will be developed. The unique Convolution Neural Network Powered Firewall Anomaly Management Environment with unique architecture implementation on Local and Internet Network will be proposed. The unique Recurrent Neural Network Powered Firewall Anomaly Management Environment with unique architecture implementation on Local and Internet Network will be proposed. The unique comparative analytics for CNN and RNN system for developing the optimized AI enabled Firewall Anomaly Management Environment will be proposed.

REFERENCES:

Ehab S. Al-Shaer, Hazem H. Hamed. DePaul University, Modeling and Management of Firewall Policies. 2004 IEEE, eTransactions on Network and Service Management, Second Quarter, 2004

Hongxin Hu,Student Member,IEEE,Gail-Joon Ahn,Senior Member,IEEE,and Ketan Kulkarni," Detecting and Resolving Firewall Policy Anomalies" IEEE Transaction On Dependable And Secure Computing,Vol.9 ,No.3,MAY/JUNE 2012

Muhammad Abedin, Syeda Nessa, Latifur Khan, and Bhavani Thuraisingham. Detection and resolution of anomalies in firewall policy rules. In IFIP Annual Conference on Data and Applications Security and Privacy, pages 15–29. Springer, 2006.

FISHER RA. THE USE OF MULTIPLE MEASUREMENTS IN TAXONOMIC PROBLEMS. Ann Eugen1936;7:179–88. https://doi.org/10.1111/j.141809.1936 .tb02137.x.

Lincoln laboratory,1998 Darpa intrusion detection evaluation dataset, 1998. [Dataset]. Available:

https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset. [Accessed: Jan 19,2021].

A. Benelbahri, and A. Bouhoula, Tuple Based Approach for Anomalies Detection within Firewall Filtering Rules. ISCC 2007. 12th Vol , Iss , 1-4 pp. 63- 70.

Thi Bao Thu Le, Nicolas Anciaux, Sebastien Gilloton, Saliha Lallali, Philippe Pucheral, et al. Distributed Secure Search in the Personal Cloud. Proceedings of the 19th International Conference on Extending Database Technology, France, 2016.

Mukkamala S, Sung A, Abraham A. Intrusion detection using ensemble of soft computing and hard computing paradigms. J Network Comput Appl 2005;28(2):167–82.

http://doi.org/10.29369/ijrbat.2023.02.1.0011