International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 11 Issue 6 ǁ June 2023 ǁ PP. 305-306

Cyber-attacks and its Prediction in Cloud environment using Artificial Neural Network

[1]Binu C T, [2]Dr.S.Mohan Kumar
Email: [1]binu.ct@cmr.edu.in, [2]drsmohankumar@gmail.com
[1]PhD Scholar, Computer Science & Engineering, CMR University, Bengaluru
[2]Supervisor, Director, QA Research &Innovation, CMR University, Bengaluru

Abstract:
Cyber-attacks are very common nowadays and predict them and prevent them is a challenging topic. Self-organized type of Artificial Neural Network (ANN) is the solution to predict the various attacks in the cloud. There are mainly two techniques in ANN namely based on interconnection and based on functionality. There are various attacks include broken authentication, Data breaches, Hacked interfaces and APIs, Exploited system vulnerabilities, Account hijacking, Permanent data loss, Cloud service abuses, DoS attacks, Service hijacking, VM Hopping, Platform-as-a-service (PaaS) security issues, Third-party relationships, Underlying infrastructure security Cloning.
Keywords: *Cyber attacks,cloud computing,Artificial Neural Network*

Date of Submission: 05-06-2023 Date of acceptance: 18-06-2023

I. INTRODUCTION

Data processing has improved its impact on various fields, including geography, engineering, business, finance, and healthcare. In Artificial Neural Network have mainly three layer includes Input layer, Hidden layers and Output layers.

Input Layers: An ANN's initial layer, the input layer, accepts input in text, numbers, audio files, picture pixels, etc. It is responsible for parsing this data through single format.

Hidden Layers: The hidden layers of the ANN model may be found in the centre. As in the case of a perceptron, there can be only one hidden layer, or there can be several. These hidden layers execute various mathematical equations to compute on the incoming data and detect the patterns that are part of them.

Output Layer: The result of the center layer's careful calculations is acquired in the result layer. Various variables and boundaries impact on the result which is gained by refactoring.These boundaries altogether affect the result of ANNs. Weights, biases, learning rates, batch sizes, etc., are some of these factors. The ANN's nodes are all equally important.

II. ARTIFICIAL NEURAL NETWORK

Self-organized type of Artificial Neural Network. However, we have classified types of ANN on the following basis:

Based on Interconnection:

- Feed Forward:

Pass the data to the neural network to get the solution in the feed forward technique.

- Feedback/Recurrent Networks:

Try to get the same result as in feed forward to verify for a feedback

Based on the Functionality:

- Perceptron Network:

It's based on the analysis of available to future data

- Back Propagation Network:

It's based on the analysis of future to available sample data

- Hopfield Network:

It's based on past to present to future data analysis

- Cascading neural network.

Here it's combine two neural network based on a same data

- Counter propagation network:

Here it's combine two neural network based on a past and present data

III. SECURITY ISSUES AND PREDICTION

Broken authentication:
Many developers kept credentials in the source code and hackers attack the system by executing the application.Feed forward to predict the broken authentication.
Data breaches:
The attackers target the data centers and have data breaches .Back Propagation Network in ANN to predict this attack.
API Hacking
APIs and other interfaces may cause the vulnerabilities in the system. Hopfield Network to predict API Hacking from server side.
Phishing:
The attackers manipulate transactions, and modify data through phishing. Cascading neural network in ANN to predict this attack.
Diligence knowledge:
The risks are a factor where the customers unaware of more details about the cloud and it may cause financial risk. Counter propagation network is a part of ANN to avoid diligence knowledge.
Cloud service abuses:
Some attackers use cloud to attack the system or a network through Denial of Service The monitoring data with policy verification avoids cloud service abuses. Back Propagation Network to predict the cloud service abuses.
Denial of Service attacks:
There are two types of DoS including asymmetric and application level.Cascading neural network is the solution to predict DoS.
Malicious attacks:
The attackers may enter into the same network and execute the malicious applications and it may occur from outside as well as inside. Perceptron Network to predict the malicious attack.
Platform security issues:
There is an allocation of platform to get Platform as a Service(PaaS). Back Propagation Network to predict platform security issues.
Third party relationship:
Programming language is the third party in the cloud application and the attackers uses the same code to attack the system. Cascading neural network to predict third party relationship.
Infrastructure Security:
The infrastructure which located in different locations and connected through a virtual private network (VPN) and it may cause network issue when VPN is down. Back Propagation Network helps to predict the infrastructure security issues.

Cloning:
Replicating data in data centers and it cause data leakage. Recurrent Networks is the way to predict the cloning.

Identity management:
Identity management allow us to authenticating the users through their credentials. Two factor authentication in the content manager helps avoid the issue related to identity management. Recurrent network is the way to predict issues identity management.

REFERENCES

[1]. Extremely boosted neural network for more accurate multi‑stage Cyber-attack prediction in cloud computing environment, Surjeet Dalal1, Poongodi Manoharan2*, Lilhore Umesh Kumar3,4, Bijeta Seth5, Deema Mohammed alsekait6,Sarita Simaiya3,4, Mounir Hamdi2 and Kaamran Raahemifar7,8,9, Journal of Cloud Computing:Advances, Systems and Applications,2023.
[2]. Design of Intrusion Detection System based on Cyborg intelligence for security of Cloud Network Traffic of Smart Cities, Edeh Michael Onyema1, Surjeet Dalal2*, Carlos Andrés Tavera Romero3 , Bijeta Seth4, Praise Young5 and Mohd Anas Wajid, Journal of Cloud Computing:Advances, Systems and Applications,2022.
[3]. Cloud Computing Security issues challenges and opportunities Vaikunth Pai T.1 & P. S. Aithal1, International Journal of Management, Technology and Social Sciences (IJMTS), 2016.
[4]. Cloud Computing and Security Issues, Rohan Jathanna*, Dhanamma Jagli**,International Journal of Engineering Research and Application,2017.
[5]. Cloud‑based deep learning‑assisted system for diagnosis of sports injuries, Xiaoe Wu1, Jincheng Zhou2,3, Maoxing Zheng1,2, Shanwei Chen4, Dan Wang2,3,5, Joseph Anajemba6,Guangnan Zhang2*, Maha Abdelhaq7, Raed Alsaqour8 and Mueen Uddin9, Journal of Cloud Computing: Advances, Systems and Applications,2022.