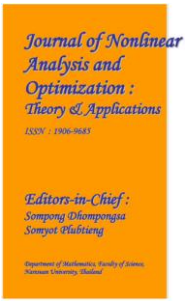
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.7 : 2024
ISSN : **1906-9685**



EXTREMELY BOOSTED NEURAL NETWORK FOR MORE ACCURATE MULTI-STAGE CYBER ATTACK PREDICTION IN CLOUD COMPUTING ENVIRONMENT

Ms.P.Monisha, Assistant Professor**,** Pg Department of Computer Applications**,** Marudhar Kesari Jain College for Women Vaniyambadi

Abstract

There is an increase in cyber attacks directed at the network behind firewalls. An all-inclusive approach is proposed in this assessment to deal with the problem of identifying new, complicated threats and the appropriate counter measures. In particular, zero-day attacks and multi-step assaults, which are made up of a number of different phases,some malicious and others benign, illustrate this problem well. In this paper, we propose a highly Boosted Neural
Network to detect the multi-stageattack scenario. It demonstrated the results of executing various machine learning algorithms and proposed an enormously boosted neural network. The evaluation results of the Multi-Step Cyber-Attack Dataset (MSCAD) show that the proposed Extremely Boosted Neural Network can predict the multi-stage cyber attack.. Such accurate prediction plays a vital role in managing cyber attacks in real-time communication.
Keywords: Cyber security, machine learning , neural network, attacks

Introduction

Data processing has risen in various fields, including geography, engineering, business, finance, and healthcare. Using cloud computing for data processing has become widely accepted. High-performance computing services are delivered through the Internet, and substantial scientific applications are run using this technique. You may use cloud computing to get three services: Infra structure as a service, Platform as a service, and software as a service (SaaS). In the form of services, the Infra structure as a Service (IaaS) cloud offers cloud customers access to vast computer hardware infrastructure platforms and software resources. On the other hand, users can only run an application on the Internet in a SaaS
cloud; however, in a Platform as a service (PaaS) cloud, customers may utilize the existing Platform to build their application . Private, public, communal, and hybrid cloud computing
models exist. For businesses with similar needs, the Community cloud model is essential. When a faulty management system is used, the performance of the submitted the process of
applications/workflows is reduced. In cloud computing settings, workflow is a popular way to represent high-volume data-processing systems . Graph nodes represent the computing jobs, while graph edges reflect the relationships among the graph's activities. The DAG
is used to depict a workflow. The application's scientific requirements determine the DAG's size. Neural Network-based approach to detecting multi-stage assaults to overcome the mentioned issues. The following is a list of our most important contributions.

- There are two levels of time series and stage features built into a long-term memory network.
- The stage features layer is introduced to store and calculate historical data to detect the distinct stages with varied durations in multi-stage assaults. This is followed by an analysis of the time-series characteristics layer to determine if the current data falls within an attack timeframe.
- Multi-stage cyber attack dataset is used in the comparison tests. Using a variety of datasets, our method has an accuracy rate of at least 91% and a false negative rate of no more than 6.75%. The false positive and false negative rates are lowered by at least 65.83% and 65.26%, respectively, compared to the current systems. Neural Network-based approach to detecting multi-stage assaults to overcome the mentioned issues.

The following outlines Bayesian network:
A prevalent type of probabilistic graphical model is the Bayesian network. They have a framework, and then there are the parameters. A directed acyclic graph (DAG) shows interdependencies and conditional independences between random variables at each node
depicts the predictors and targets in Bayesian Network for predicting the attack. The color code represents the level of different importance. The splits the attributes into two categories indicated by different colors. One category is Predicators, and another is Target. The importance of predicators lies between 0 and 1 (0.0, 0.2, 0.4, 0.6, 0.8 & 1.0). The parameters are a set of node-specific conditional probability distributions. Suppose you need a compact,
adaptable, and easily interpretable representation of a joint probability distribution . In that
case, a Bayesian network is a way to go.

Related work
This section mainly covers the review of existing cloud security research work. It expressed that work toward robotized location and recognizable proof of multi-step digital assault situations would benefit fundamentally from a technique and language for displaying such situations. The idea of assault designs was acquainted with work with the reuse of nonexclusive modules in the assault demonstrating process. They was utilized in a model execution of a situation acknowledgment motor that consumed first-level security cautions
progressively and produced reports that distinguish multi-step assault situations found in the alarm stream. Cauldron consequently planned all ways of weakness through
networks by connecting, totaling, normalizing, and intertwining information from various sources. It gave a refined perception of assault ways and consequently produced alleviation proposals. Adaptable demonstrating upheld multi-step examination of firewall rules have weakness, with assault vectors inside the organization and from an external perspective.
They depicted already relationship given Caldron assault charts, examining mission influence from assaults. They utilized information mining to handle alarms to create input for
to determine the expected appropriation likelihood. Their framework had the option to stream continuous learned standards. This framework had the option to find designs in the multi-stage assault naturally and order aggressors in view of their way of behaving. By doing this,
our framework can successfully anticipate conduct and assailants and survey the risk level of various gatherings of aggressors. Furthermore, the lengthy language upheld the joining of
outer danger knowledge and permitted us to reference current danger pointers. With this methodology, they could make nonexclusive marks that keep them awake to date.
Neural network
A Neural network is an assortment of calculations in light of a harsh model of the human cerebrum. Marking or gathering crude information is one way they decipher tactile information as machine discernment. All certifiable information, including pictures, sounds,
text, and time series, should be converted into the mathematical examples they comprehend, which are put away in vectors . We can utilize brain organizations to arrange and classes information. Bunching and grouping might be considered a layer on top of the information you store and make due. Utilizing a marked dataset to prepare, they help bunch unlabeled
information in light of similitudes among the model information sources.
Artificial neural networks architecture:
Neural networks work in a way like that of neurons in the human sensory system. Warren S McCulloch and Walter Pitts concocted the expression “Brain Networks” in the mid-1970s. We should take a gander at the design of ANNs to find out how they work. A neuron is enclosed by its membrane. The membrane on the end bulb is called the membrane, and the membrane upon which the end bulb strikes is called the postsynaptic membrane. There are three crucial layers in a brain organization .
Input Layers: An ANN’s initial layer, the input layer, accepts input data in text, numbers, audio files, picture pixels, etc. It is responsible for parsing this data.

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

Output Layers: The result of the center layer's careful calculations is acquired in the result layer. Various variables and hyper-boundaries impact the model's exhibition in a brain organization. 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. It consists of 18 neurons and 3 Biases on the network. The Hopfield model is both an optimization model as well an association model. Hopfield is a constraint satisfaction algorithms-based model. It is symmetric and asynchronous in nature as compared. As a node in a network, each one has its unique weight . The transfer function is employed in conjunction with the bias to calculate the weighted total of the inputs and bias. There are nodes in each tier. In a node, computing occurs similarly to how neurons activate when they receive enough input in the human brain . When an algorithm is trying to learn how to classify data, a node uses coefficients or weights to either amplify or dampen each input. This helps the algorithm decide which inputs are most important for learning how to classify data correctly. Node activation functions evaluate the total of these input-weighted product. Based on Connection types, we can have Static (feed-forward) or Dynamic (feedback) ANN, and based on topology, we can have a Single layer, Multilayer.

Extremely boosted neural network for multi-stage Cyber attack prediction:

Currently, most neural network ensemble approaches aggregate all the available neural networks into one large group. However, the efficacy of this method has yet to be adequately demonstrated. When analyzing how the ensemble and its neural networks interact, combining many neural networks is proven more advantageous than all the available ones. This concept has the potential to be applied to the formation of compelling ensembles. Neural network ensemble learning is the practice of using many neural networks to solve a problem. As a result of regression and classification, this study found that ensembles with only a few rather than all available neural networks may be more effective. The majority now makes systems predictions using a mix of neural networks .

Performance of extremely boosted neural network

We have presented a novel approach to predicting the multi-stage cyber attack using an Extremely Boosted Neural Network. Our general formulation can include the prediction of attacks at the level of Brute Force, ICMP Flood, Normal, and Ports .It shows the accuracy level of the model's different numbers, and predictors used to predict the cyber attacks. As compared to prior research, this proposed method can generate significantly accurate Labels. Lastly, the authors have shown the proposed model's performance with existing techniques studied in the related work and different machine learning algorithms .This table demonstrates the accuracy level achieved by seven different techniques. It may be reconstructed as including the detailed performance of the proposed model. The information is graphically represented which proves that the proposed model achieved the maximum level of accuracy (99.798%) .

Conclusion

The proposed neural network for predicting multi-stage cyber assaults is developed in this study. It puts the intricate assaults into perspective by illustrating how they may be detected and investigated, two of the essential functions in the security area. Here, we outline a complete framework for studying complex assaults, their related analytical methodologies, and their primary uses in security: detection and investigation. This paradigm makes it easier to categorize new, complex dangers and the countermeasures that go along with them, such as Artificial Intelligence. Our model for Multi-stage Cyber attack prediction outperforms .

References

1. Simaiya S, VinayGautam UK, Lilhore (2021) AtulGarg, PinakiGhosh, Naresh Kumar Trivedi, and AbhineetAnand. "EEPSA: Energy Efficiency Priority Scheduling

Algorithm for Cloud Computing." In 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), pp. 1064–1069. IEEE,
2. Lilhore UK, Simaiya S, Maheshwari S, Manhar A, Kumar S (2020) Cloud performance evaluation: hybrid load balancing model based on modified particle swarm optimization and improved algorithms.
3. Torkura KA, Sukmana MIH, Cheng F, Meinel C (2020) CloudStrike: Chaos Engineering for Security and Resiliency in Cloud Infrastructure.
4. Alturki R, Alyamani HJ, Ikram MA, Rahman MA, Alshehri MD, Khan F, Haleem M (2021) Sensor-Cloud Architecture .
5. Alouffi B, Hasnain M, Alharbi A, Alosaimi W, Alyami H, Ayaz M (2021) A
Systematic Literature Review on Cloud Computing Security: Threats and Mitigation Strategies.
6. Musman S, Turner AJ (2018) A game-oriented approach to minimizing cyber security risk.
7. Musman S, Turner A (2018) A game theoretic approach to cyber security
risk management.
8. Mirsky Y, Doitshman T, Elovici Y, Shabtai A (2018) Kitsune:.
9. Parrend P, Navarro J, Guigou F, Deruyver A, Collet P (2018) Foundations
and applications of artificial intelligence
10.Kathiravelu P, Zaiman Z, Gichoya J, Veiga L, Banerjee I (2022) Towards an internet-scale overlay network for latency-aware decentralized workflows at the edge.