International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

An Enhanced DNN Model for Cyber Attack Detection using Seagull Adapted Elephant Herding Optimization Algorithm

Katikam Mahesh*, Dr.Kunjam Nageswara Rao

Submitted:11/03/2024 **Revised**: 26/04/2024 **Accepted**: 03/05/2024

Abstract: Life today is significantly more comfortable thanks to numerous digital devices and the internet to support them. Every good thing has a bad side, and the same is true in today's digital world. The internet has made a beneficial difference to our lives today, but it also presents a significant difficulty in protecting private information. This gives rise to cyberattacks. Attack Detection is a major challenge in network security. Traditional Gradient Boosting Algorithms Such as GBM, XGBoost, LightGBM, CatBoost Algorithm Performs Poor Detection of Different attacks, such as malicious software attacks, phishing attacks, and denial-of-service attacks. This paper introduces a novel DNN- Seagull Adapted Elephant Herding Optimization Algorithm (DNN- SAEHOA) to Improve Detection Attacks automatically with Publicly Available Input dataset UNSW NB-15 with Variance Threshold (VT) is a simple approach to feature selection. It removes all features whose variance cannot meet a defined threshold. Improve accuracy.

Keywords*: Cyber Attack Detection, Deep Neural Network, Seagull Adapted Elephant Herding Optimization Algorithm, Feature Selection,* Categorization *Accuracy, Network Security*

1. Introduction

Deep neural networks (DNNs) evolved as an appropriate choice this year for correcting for a long time. In this research, we use DNNs to three distinct cyber security projects Android malware classification, an incident detection 2]. Each use case's data set includes real samples that illustrate both benign and harmful behaviours. Running a series of experimentation on network parameters and network configurations can reveal a highly efficient DNN network design. Numerous algorithms for optimization inspired on biology, nervous structures, and swarm intelligence, based on the state of birds, fish, bees, ants, bats, frogs, elephants, and cats, and the wolves, are being suggested in the literature [3].

2. Related Works

The rapid growth of the size and difficulty of optimization problems implies that the traditional algorithms for optimization are becoming less trustworthy for managing issues [2]. V. Santucci; M. Bialetti, & A. Milani. An algebraic makeup for swarm and algorithms of evolution in optimization combinatorial. Metaheuristic algorithms [3–4]. Sarhan Mohanad, Siamak Layeghy, Nour Moustafa, and Marius Portmann. NetFlow Datasets for Machine Learning-Powered Network Intrusion Detection. Yet they fail to detect accurately. H.Xu; Q. Cao; H. Fu; C. Fu; H. Chen; & J. Su. The Use of a Support Vector Machine Model Based on an Improved Elephant Herding Optimization Algorithm in Network Intrusion. No Deals About Accuracy is known to be a successful fix to this problem. However, those investigations do poorly in terms of crime detection.

3. Proposed Methodology

The design of the attack detection approach is based on the principle of the security system which continuously monitors the data traffic in the network systems to Detect different types of security attacks. The attack detection approach is designed using a hybrid DNN- Seagull Adapted Elephant Herding Optimization Algorithm for detecting the cyber-attacks in the network systems that are injected into the system by the attackers. The malicious attacks in the network allows the attackers to exploit the system data and obtain unauthorized access to the confidential network information The preliminary aim of the proposed attack detection framework is to develop an efficient model based on feature selection and optimization using a metaheuristic DNN-SAEHOA algorithm. The selection of important features helps in reducing the computational complexity of the DNN- SAEHOA model and improving the performance efficiency. In this study, the features are selected for each specific type of attack using the Variance Threshold and the selected features are used to train the DNN- SAEHOA model for detecting cyber-attacks. The stages involved the implementation of the proposed CNN-GRU model for attack detection are described in the below subsections.

[1]*Andhra University College of Engineering Visakhapatnam, INDIA*
ORCID ID: 0009-0000-0707-1117
[2] *Andhra University College of Engineering Visakhapatnam, INDIA*
ORCID ID: 0009-0005-2779-0238

3.1 Data Collection

UNSW-NB 15, was an internet intrusion dataset. It features raw network packets. The initial training collection has 175,341 records, while the testing set has 82,332 records. that are different sorts, which include attack and normal

ID	Feature	ID	Feature	ID	Feature
1	attack_cat	16	dloss	31	response_body_len
2	dur	17	sinpkt	32	ct_srv_src
3	proto	18	dinpkt	33	ct_state_ttl
4	service	19	sjit	34	ct_dst_ltm
5	state	20	djit	35	ct_src_dport_ltm
6	spkts	21	swin	36	ct_dst_sport_ltm
7	dpkts	22	stcpb	37	ct_dst_src_ltm
8	sbytes	23	dtrcpb	38	is_ftp_login
9	dbytes	24	dwin	39	ct_ftp_cmd
10	rate	25	tcprtt	40	ct_flw_http_mthd
11	sttl	26	synack	41	ct_src_ltm
12	dttl	27	ackdat	42	ct_srv_dst
13	sload	28	smean	43	is_sm_ips_ports
14	dload	29	dmean		
15	sloss	30	trans_depth		

Fig 1 Features of UNSW-NB15 Dataset

3.2 Data Preprocessing

After creating a unified dataset, the data is preprocessed to eliminate uncertainties and redundancies from the dataset. Different uncertainties such as handling missing values, removing duplicates are filtered out to ensure data consistency. Preprocessing the data in order to ensure the quality and integrity of the dataset before further analysis or modeling. In this stage, an Exploratory data analysis (EDA) is performed to analyze and visualize the data along with basic exploration tasks such as displaying the first and last rows to understand data structure, checking shape (number of rows and columns, examining column names to identify features, checking for null values to ensure data integrity and analyzing the distribution of the target column ('Label') to understand class distribution

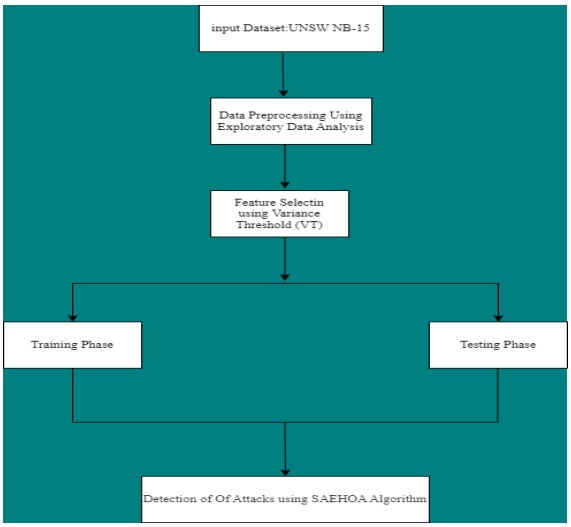

Fig. 2 Framework of the proposed hybrid SAEHOA Model

3.3 Feature Selection

Finding a feature is the method of choice of a subset of the original features. so as to reduce the feature space to an optimal value according to one particular criterion. Feature selection is a significant step in the feature a development process. In text categorization problems, words in particular just do not appear a lot. Variance Threshold (VT) is a crucial approach to feature selection. It removes any features whose variance does not meet a particular threshold, boosting accuracy.

$$VT=Var[X]=p(1-p)$$

```
>>> from sklearn.feature_selection import VarianceThreshold
>>> X = [[0, 2, 0, 3], [0, 1, 4, 3], [0, 1, 1, 3]]
>>> selector = VarianceThreshold()
>>> selector.fit_transform(X)
array([[2, 0],
       [1, 4],
       [1, 1]])
```

For Remove Unwanted Features and select required Features

3.4 DNN model for Attack Detection

Deep neural networks can often have a heavily complex hidden layer design with different tiers, which might include a max-pooling layer, a layer with convolution, a layer that is dense, and other layers. These additional layers provide the model a way to spot problems better and offer the best solutions for difficult endeavours. As opposed to an ANN, a deeper neural network has more layers, or depth, and each layer gives the model greater complexity while enabling it to examine inputs rapidly and offer the ideal viable reply.

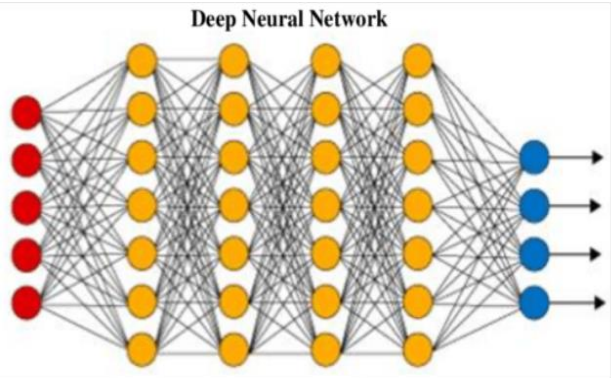

Fig 3 deep neural networks

3.5 Seagull Adapted Elephant Herding Optimization Algorithm (SAEHOA)

Elephants belong to the largest living things on land. The African and Asian elephants are two traditionally recognized species. A long trunk was the most representative marker, offering numerous purposes such as breathing, lifting water, and grasping objects. Elephants are amiable in nature, with complicated female-calf connections between individuals. An elephant group is

made up by several clans, each led by a matriarch, normally the oldest cow. A clan consists of a single female her calves, or a group of related females.

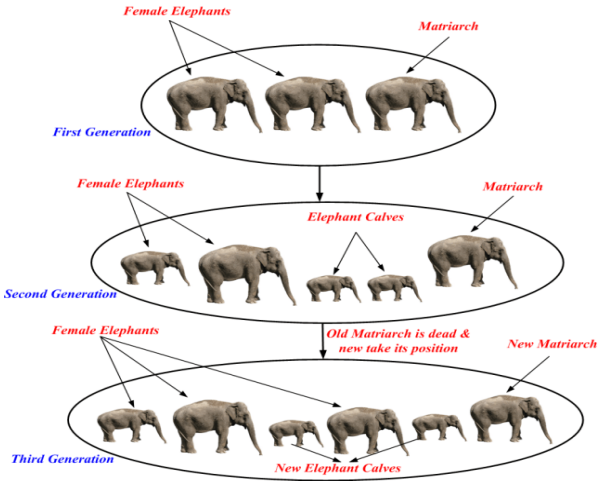

Fig 4 Architecture for Attack Detection

The pseudocode of the HBOA algorithm

Input: Dataset UNSW-NB15

Steps for SAEHOA Algorithms

Step1: Pick the group to start with from a few distinct groups.
Step2: Check to the operator that adjusts the clan.
Step3: Pick out the operator that divisions.
Step4: Commit the best feasible solution to store.
Step 5: Determine the Hold Value Limit.
Step 6: Recognize Diverse Features.
Step 7: If not, go returning to Step 3.
Step 8: Stop

4. Experiment Results

This section discusses the evaluation of the proposed DNN- SAEHOA Algorithms using Accuracy defines the percentage of number of correctly identified cyber-attacks which is defined in the below equation:

(TP+TN)/(TP+TN+Fp+FN) = accuracy.

4.1 Experimental results

The proposed DNN- SAEHOA Algorithms is tested and simulated for Detection Accuracy

Table 1. Comparative Analysis

Model/Algorithm	**Accuracy**
XGBoost	80 %
LightGBM	83 %
CatBoost	85.33 %
The Proposed DNN-SAEHOA Algorithms	92.43 %

As inferred from the experimental results, the proposed DNN- SAEHOA Algorithms outperforms other models by achieving a phenomenal accuracy. Results validate the effectiveness of the optimized DNN- SAEHOA Algorithms

5. Conclusion

This research work discusses the implementation of a hybrid classifier combining DNN- SAEHOA Algorithms for Detected the cyber threats in the network system. One of the important security challenges associated with network security is the introduction of potential attacks which has an adverse Effects on the performance of network systems. The DNN- SAEHOA Algorithms was designed and simulated for monitoring the network continuously in order to identify and detect cyber-attacks. The data was pre-processed to ensure the consistency and the problem of data imbalance was addressed using the EDA The essential and relevant features are extracted and selected from the dataset using a VT (variance Threshold) in order to simplify the Detection process. For detecting the security attacks, the CNN-GRU model is trained to Detect the data instances into normal or attack. The DNN-SAEHOA Algorithms is evaluated using different metrics and results show that the DNN- SAEHOA Algorithms algorithm outperforms other Deep Learning Techniques in terms of achieving a highest accuracy of 92.43%. With UNBC NB-15 Publicly Available Dataset For future work, the study intends to investigate To Detect Some more Attacks Along with Accuracy We Can Also Take More Evolution Metrics Such as Precision, Recall, f1 -score, and Support

Acknowledgement:

I would like to express my profound gratitude to Dr. Kunjam Nageswara Rao Professor Department of Computer Science and System Engineering in Andhra University Andhra Pradesh, Visakhapatnam India, for giving Guidance and Support to Review and Given suggestion.

Author Contribution:

All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Katikam Mahesh, Dr Kunjam Nageswara Rao, and all authors commented on previous versions of the manuscript.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Pant M, Kumar S (2022) Particle swarm optimization and intuitionistic fuzzy set-based novel method for fuzzy time series forecasting. Granul Compute 7(2):285–303

[2] Santucci, V.; Baioletti, M.; Milani, A. An algebraic framework for swarm and evolutionary algorithms in combinatorial optimization. Swarm Evol. Compute. 2020, 55, 100673.

[3] Sarhan, Mohanad, Siamak Layeghy, Nour Moustafa, and Marius Portmann. NetFlow Datasets for Machine Learning-Based Network Intrusion Detection Systems. In *Big Data Technologies and Applications: 10th EAI International Conference, BDTA 2020, and 13th EAI International Conference on Wireless Internet, WiCON 2020, Virtual Event, December 11, 2020, Proceedings* (p. 117). Springer Nature.

[4] Xu, H.; Cao, Q.; Fu, H.; Fu, C.; Chen, H.; Su, J. Application of Support Vector Machine Model Based on an Improved Elephant Herding Optimization Algorithm in Network Intrusion Detection; Springer: Singapore, 2019; pp. 283–295.

[5] Prasad, C., Subbaramaiah, K. and Sujatha, P. (2019). Cost–benefit analysis for optimal DG placement in distribution systems by using elephant herding optimization algorithm. Renewables: Wind, Water, and Solar, 6(1).

[6] Rizk-Allah, R.M.; El-Sehiemy, R.A.; Wang, G.-G. A novel parallel hurricane optimization algorithm for secure emission/economic load dispatch solution. Appl. Soft Comput. 2018, 63, 206–222.

[7] Jino Ramson, S.R.; Lova Raju, K.; Vishnu, S.; Anagnostopoulos, T. Nature inspired optimization techniques for image processing-a short review. In Nature Inspired Optimization Techniques for Image Processing Applications; Springer: Cham, Switzerland, 20 September 2018; Volume 150, pp. 113–145.

[8] Pan, Z., Guo, Q. and Sun, H. (2015). Impacts of optimization interval on home energy scheduling for thermostatically controlled appliances. CSEE Journal of Power and Energy Systems, 1(2), pp.90-100.