Deep Learning Model with Optimization Strategies for DDoS Attack Detection in Cloud Computing

Radhika.P
Research Scholar
Department of Computer Science
Vel's Institute of Science, Technology and Advanced Studies
Chennai, Tamil Nadu, India
radhikaperumal0788@gmail.com

S. Kamalakkannan
Professor,
Department of Computer Science
Vel's Institute of Science, Technology and Advanced Studies
Chennai, Tamil Nadu, India
Kannan.scs@vistas.ac.in

***Abstract*— Cloud Computing (CC) remains as a chief research area for analysts because of its numerous applications and advantages. The dispersed nature of CC and its dependence on internet service poses several attacks and challenges. Mainly, the attacks like DDoS attempts to disrupt the online operations. Insider attacks cannot be detected using conventional detection techniques like firewalls. This study suggests a DDoS detection method for reducing the DDoS activity. The proposed work contributes under big data perspective by handling certain procedure for detection process. Data Generation phase is the initial step, and according to the work, DDoS dataset is considered under big data perspective. As the work is considered under the big data perspective, Map reduce (MR) framework is used, Mapper handles the data and process the feature extraction, which includes the extraction of raw features, Packet feature extractor, Improved Correlation and statistical Feature. Reducer provides the combined feature set. From the extracted feature set, appropriate features are selected via Weightage based Improved hybrid model combining the models like Long short term memory(LSTM) and Deep Maxout(DMO) networks is used. The weights of LSTM and DMO are optimally chosen using White Shark-Remora Optimization (WSROA) algorithm. Recursive Feature Elimination (RFE) process is used to precisely select the features for DDoS attack detection. The findings shows that the proposed hybrid bio-inspired algorithm outperforms with an accuracy of 94% compared to LSTM, Convolutional Neural Networks(CNN) and Deep Belief Networks(DBN)**

Keywords— Cloud Computing, Deep Learning, Denial of Service Attacks , Attack Detection, white shark-Remora optimization Algorithm, Bio-inspired Algorithms.

I. Introduction

Cloud computing is becoming more widely used across a variety of domains. However, the fundamental security flaws of CC create serious threats to its overall security. CC is a concept that allows technologically advanced and customizable computing assets such as networks, storage, servers, computer systems, etc. for cloud customers at cheap service prices. CC provides its products and services accordance to the pay-as-you-use policy (Kumar et al., 2022). CC is vulnerable to a number of current attacks, such as denial-of-service (DOS), distributed DoS, and DNS (domain name system) attacks.

DDoS attacks provide an increasingly prevalent risk to network security. This sort of attack attempts to inundate the targeted networks with fraudulent traffic until the network's available bandwidth is exhausted. Excessive traffic can significantly reduce system efficiency and, in severe situations, cause a full system crash. The cloud firewall dynamically screens incoming traffic. It can prevent damaging traffic patterns commonly utilized in DDoS attacks, such as traffic from known IP addresses that are malicious or bandwidth coming from many sources at the same time. Furthermore, countering DDoS attacks is difficult because of their enormous effect on physical computer hardware and network traffic(Kumar et al, 2024).

Bio-inspired optimization approaches are inspired by the complex, adaptive processes observed in nature and use algorithms like Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) to discover optimum solutions to complicated problems. In contrast, ML uses data and algorithms to find anomalies, patterns, and developments, making it ideal for identifying unexpected and previously unknown incursions. The core of hybrid techniques is their ability to combine the capabilities of bio-inspired optimization with ML. By doing so, they enable IDSs to adapt, learn, and grow in real time, allowing them to stay ahead of cyber attacks that are becoming increasingly sophisticated(Sherin et al., 2024).

Feature selection is an important stage for creating effective predictive models, especially those used to detect and predict DDoS assaults. It comprises finding and using the dataset's most important features (attributes), which has a substantial impact on the model's efficacy, efficiency, and interpretation(Han et al., 2024).

Deep learning models have demonstrated tremendous potential for detecting and mitigating DDoS attacks. DDoS assaults flood a network, server, or service with too much traffic, overwhelming resources and disrupting regular operations. DL models' capacity to understand complicated patterns in vast amounts of information about network traffic has made them useful in identifying and forecasting such attacks (Clinton et al., 2024). The main objectives of the study includes

- To examine the deep learning models for the detection of DDos attacks
- To propose a hybrid WSROA with LSTM and DMO

II. Related Works

Bakro et al.,(2024) presents a combined feature selection strategy that combines two bio-inspired algorithms: the grasshopper optimization algorithm (GOA) and the genetic algorithm (GA). The amalgamation of the above methods leads to a faster search for the best possible outcomes. The typical features are used to train a random forest (RF) classifier. Furthermore, the proposal tackles the issue of unbalanced data by using a hybrid technique: over-sampling the minority classes with an adaptive synthetic (ADASYN) method while using random under-sampling (RUS) for the majority of class as needed.

DDoS attacks are detected using a innovative method, an adaptive deep dilated ensemble (ADDE), which consists of one-dimensional convolutional neural network (1DCNN), deep temporal CNN(DTCNN), recurrent neural network (RNN), and bidirectional long short-term memory (Bi-LSTM). To get best results, the parameter tuning is conducted by employing the Hybrid Border Collie and Dragonfly Algorithm (HBCDA) technique(Aliar et al., 2024)

Uddin et al., (2024) investigates the impact of various forms of DoS and DDoS assaults on edge computing layers by exploring the weaknesses associated with different edge peripherals. Additionally, current detection and prevention strategies are being studied to solve these flaws. In addition, a conceptual framework is presented to prevent DDoS attacks on edge systems.

Effiong et al., (2024) designed a Danger Theory-based intrusion detection model for the Smart Grid, relying on the growing dendritic cells algorithm, a flagship of the artificial immune system, to enhance classical (RF and XGBoost) and DL (RNN, DBN, GRU, DNN, and LSTM) algorithms.

Rahamathulla et al.,(2024) provides a revolutionary NIDS for training and learning from vast volumes of data in a centralized setting. The enhanced Firefly Optimization Algorithm (IFOA), inspired by biology, is used to determine the optimal subset of characteristics for enhanced data representation and categorization. Furthermore, a hyper-tuned Extremely Randomized Trees (ERT) attack recognition model is created to reliably detect malicious behavior while minimizing false positives.

Najafi et al., (2024) creates extremely accurate models for identifying an extensive variety of cyberattacks using the lowest possible number of characteristics feasible, which is accomplished through thorough feature selection. We selected five, nine, and ten characteristics using the Artificial Bee Colony (ABC) and Flower Pollination Algorithm (FPA), with detection accuracy of above 90% using ACO, and 98.7% with FPA and 98.6% with the ABC.

A honey badger optimization method based on feature selection and Bi-LSTM was presented for DDoS attack prediction in a cloud environment. Getting input characteristics from the DDoS attack dataset is the first step in the process. After that, preprocessing steps like Z-Score and Bayesian normalization are applied to the input characteristics. The feature selection stage, which makes use of Honey Badger Optimization (HBO), receives preprocessed data. To select the best feature in this case, the features are chosen by reducing their MSE. The Bi-directional LSTM (Bi-LSTM) classifier, which forecasts DDoS attacks, is then fed the ideal attributes (Pandithurai et al., 2024).

III. Methodology

This section discusses the feature selection strategies like RFE and WSROA for selecting the appropriate features, followed by LSTM and DMO for the prediction of DDos attacks.

A. Preprocessing

In addition to noise, missing values, and incompatible data formats, the databases contain a large variety of nominal and digital data. Nevertheless, certain data points could have distorted or inconsistent values, which would lead to disappointing results and seriously impair the comprehension and functionality of ML models. Data cleaning involves replacing missing or NaN values with the mean of the corresponding characteristic in order to identify, rectify, or remove erroneous, incomplete, inconsequential, or inaccurate data. Since poor quality data can lead to skewed results, decreased accuracy, and higher error rates in a model, a significant portion of the work is focused on making sure the input data is clean and error-free. MapReduce can analyze and minimize huge-scale DDoS datasets by effectively collecting, filtering, and summarizing data. For example, it can aid in minimizing duplicated information, extracting certain characteristics, and consolidating traffic patterns for study.

B. Feature Selection with Recursive Feature Elimination (RFE)

RFE is an iterative feature selection strategy that recursively eliminates features from a dataset while evaluating the effectiveness of a machine learning model at every step. It begins by ranking all features according to their significance or relevance to the target variable, then eliminates the least significant feature(s) and continues the procedure until the desired model performance is achieved. RFE is widely used due to its ease of setup and usage, as well as its superior ability to pinpoint the features (columns) in a training dataset that are most crucial for predicting the target variable. The number of features to select and the technique to help select features are two important setup factors to take into account while using RFE. Though their appropriate adjustment is not crucial to the method's performance, both of these hyperparameters can be examined (rmi et al., 2022). The steps for REFE are as follows

Step-1 Train a model with all characteristics.
Step-2 Rank features using the model's significance characteristics, such coefficient or feature importance’s.
Step-3 Remove features: Remove the least significant feature or set of features.
Step-4 Keep performing steps 2 and 3 until you reach the required number of features.

C. White Shark -Remora Optimization (WSROA) algorithm

WSROA will enhance the parameters or hyperparameters of the algorithm created using RFE. It is a new algorithm for optimization based on the characteristics of white sharks and remora fish. It is an improved version of the Remora Optimization Algorithm (ROA) that is used to address difficult optimization issues, such as DDoS attack prediction. DDoS attacks pose an important risk to network security because they overwhelm a network or server with huge traffic, rendering it unreachable to users. Predicting DDoS assaults can assist limit their impact and optimization techniques like WSU-ROA are used to improve prediction accuracy by improving choosing features, identifying anomalies, or ML model parameters.

ROA was maximized by the use of the remora's parasitic features. In the environment of predicting DDoS attacks, feature selection is crucial for decreasing the problem's dimensionality while maintaining the most significant classification characteristics. WSROA improves feature selection by exploring all potential permutations (White Shark behavior) and it uses the potential groupings of features to increase the accuracy of DDoS detection algorithms. WSROA might search for appropriate subsets of characteristics (for example, network traffic data such as packet size, source IP address, traffic flow, and so on) to improve DDoS attack categorization and prediction. After the necessary characteristics have been chosen, WSU-ROA may be used to optimize hyperparameters of ML algorithms (e.g., SVM, RR, or Neural Networks) that categorize network traffic as normal or DDoS. This phase increases the preciseness and efficacy of the DDoS attack prediction system.

- Exploration: WSROA locates global optima by random search of the parameter space
- Exploitation: WSROA then adjusts the search to identify the most effective parameter set by assessing the model's fitness (accuracy) using the optimized features.

After optimization, a prediction model is trained on the chosen characteristics and optimized parameters. The program is able to predict probable DDoS assaults based on network traffic statistical data. The model's output can be either binary (attack vs. normal) or multi-class (kind of attack). The fitness function in WSU-ROA may be determined by accuracy, precision, recall, F1-score, or other assessment criteria(Pingale et al., 2024)

D. Long Short term memory and Deep Maxout

LSTM networks and DMO are strong techniques that can work together to create effective models for predicting DDoS attacks. LSTM is useful for time-series and sequential data, whereas DMO optimizes model performance via a dynamic activation method that improves the representation of features and prediction accuracy. A Hybrid LSTM and DMO model combines the advantages of LSTM networks for sequential prediction and DMO for detecting dynamic patterns in time-series data. This hybrid method may greatly improve the accuracy of time-series forecasting, finding anomalies, and dynamic system analysis, particularly when dealing with complicated, non-linear, and data with high dimensions. The steps involved in the hybrid LSTM and DMO for DDos attack prediction are as follows and it is shown in figure 1.

Design the LSTM model. :In the input layer prepare successive inputs, each representing a time frame of traffic data. For example, consider a succession of packet rates spaced 10 seconds apart. LSTM Layers stack one or more LSTM layers to detect temporal dependencies in traffic data. Then set the number of units (e.g., 64, 128) to balance efficiency and computational expenses and transfer the last layer's output to a dense layer for subsequent analysis (Rao et al.,2024).

Embed Deep Maxout Layers.:A Maxout network is a form of feedforward network that continuously chooses activation functions. It computes the greatest value from a series of linear transformations of the input, improving the model's capacity to detect non-linear trends. DMO is addedd by inserting a Maxout layer after the LSTM output or in completely linked layers. Each Maxout unit applies a max operation to multiple linear functions from the input. It improves feature representation through the acquisition of piecewise linear functions. It reduces overfitting owing to its intrinsic regularisation properties(Mohan et al., 2024) Finally , forecasting and Validation involves utilizing the learned LSTM model to forecast future outcomes and evaluate performance, compare projections to actual data.

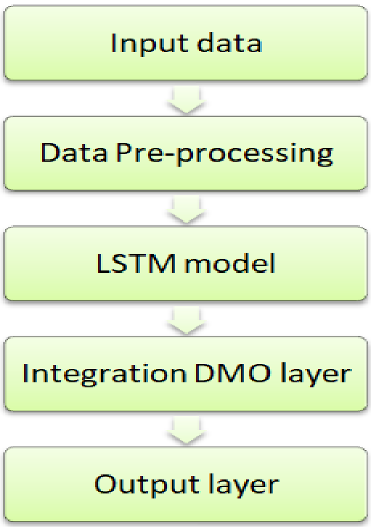

Figure 1. Workflow of LSTM –DMO

IV. Results and Findings

This section discusses the dataset description, evaluation measures and the performance analysis of the proposed hybrid LSTM-DMO using RFE and WSROA as a feature selection strategies with the other DL models like CNN, LSTM and DBN. The results were observed for the studied with and without feature selection and optimization strategies.

A. Dataset Description

This The CICDDoS2019 dataset was designed to train algorithms for detecting various forms of DDoS assaults. This dataset addresses the shortcomings identified in previous datasets. It includes both benign data and the most current typical DDoS assaults, which may be carried out at the application layer using TCP/UDP-based protocols, therefore accurately representing true real-world information.

B. Performance Measures

The proposed hybrid model with LSTM-DMO has been tested for its efficiency using the the performance indicators(Kannan et .al., 2024) given below.

Accuracy (ACC): This measure represents the fraction of correctly detected records compared to the total number of records, reflecting the model's performance.

$$\mathrm{ACC} = \frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}} \tag{1}$$

Recall (R): This notion relates to the percentage of actual attacks that were accurately predicted as such, out of the total number of attack incidents. It is often referred to as sensitivity (S), detection rate (DR), or true positive rate (TPR).

$$\mathrm{R} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FN}} \tag{2}$$

Precision (P): This metric measure the proportion of accurately anticipated assaults among the entire collection of instances classified as attacks.

$$\mathrm{P} = \frac{\mathrm{TP}}{\mathrm{TP} + \mathrm{FP}} \tag{3}$$

F1-score (F): This is a statistic used to assess a system's efficacy by taking into consideration both recall and accuracy, also known as the F1 measure.

$$\mathrm{F} = \frac{2}{1/\mathrm{Precision}+1/\mathrm{Recall}} \tag{4}$$

The proposed model is then compared with CNN, LSTM and DBN for the DDoS attacks predictions. The table 1 lists the performance measures values without Feature selection strategies.

TABLE 1. PERFORMANCE MEASURES WITHOUT FEATURE SELECTION

Methods /Measure	Accuracy	Precision	Recall	F1-Score
LSTM – DMO	94.21	93.56	93.23	93.78
CNN	91.16	90.45	91.11	91.18
LSTM	88.65	89.12	87.29	88.56
DBN	89.34	88.82	88.41	89.31

Table 1 lists the performance indicators values without applying the RFE and WSROA. It is found that the hybrid LST-DMO outperforms the other models.

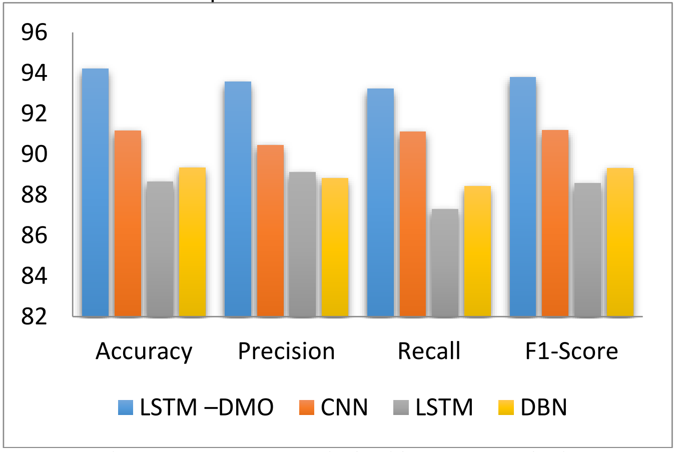

Figure 2. Measures vs Methods without Feature selection

Figure 2 presents the assessment of the proposed LSTM-DMO with LSTM, CNN and DBN for DDoS attack prediction. It is evident that the LSTM-DMO surpasses the other contrasted methods.

TABLE 2. PERFORMANCE MEASURES WITH FEATURE SELECTION STRATEGIES

Methods /Measure	Accuracy	Precision	Recall	F1-Score
LSTM – DMO	96.76	95.35	96.78	95.29
CNN	94.34	93.23	94.50	93.60
LSTM	91.5	89.3	91.6	90.45
DBN	91.78	89.34	92.00	90.67

Table 2 lists the various metrics values for the hybrid LSTM-DMO with feature selection strategies and the other contrasted methods like CNN, LSTM, and deep belief networks(DBN). It is found from the results that hybrid LSTM-DMO outperforms the other methods. Moreover, the application of feature selection strategies increases the efficiency of the models.

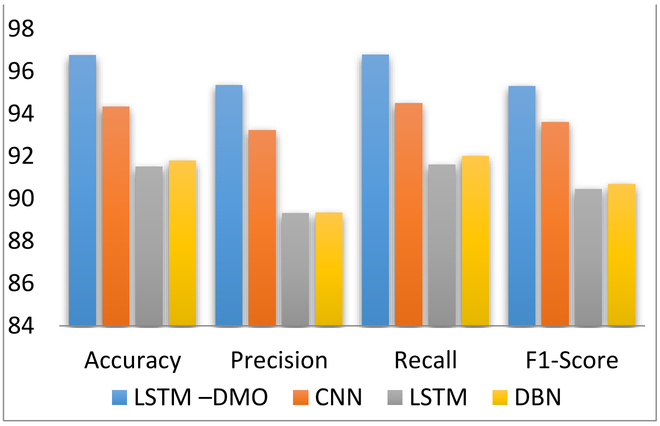

Figure 3. Methods vs Measures

Figure 3 shows the graphical representation of methods and measures in DDos attack prediction with feature extraction strategies. It is clear that LSTM-DMO performs the best in all parameters, with outstanding accuracy and recall. This makes LSTM-DMO ideal for detecting DDoS attacks since it identifies attacks correctly while generating a limited number of false positives and negatives. The F1-Score of 94.1% demonstrates its superior overall classification ability.

LSTM is an effective time-series forecasting method because it learns long-term dependencies from sequential data. DMO breaks down complex structures into understandable modes that capture the most important temporal aspects. Combining the two methods perform feature extraction (identifying important dynamic modes) suing DMO, while LSTM can use these modes to make accurate time-series predictions. DBN has the lowest accuracy, precision, and recall of the models. However, DBN has a lower F1-Score than CNN and LSTM-based models, making it less effective for predicting DDoS attacks in this scenario. RFE effectively minimizes the feature space by focusing on key predictors. WSROA optimizes parameters using a balanced exploration-exploitation technique modeled after symbiotic shark-remora behavior. The combined impact produces a highly efficient and understandable model for prediction tasks such as DDoS detection.

V. Conclusion

The hybrid LSTM and DMO model is an effective technique to manage complicated time-series data because it combines the capabilities of DMO and LSTM. The LSTM-DMO with RFE and WSROA outperforms the LSTM, CNN, and DBN in predicting the DDoS attacks with the accuracy of 96.35 %. This approach can be particularly useful in sectors where the data is extremely flexible and has long-term relationships, providing both accurate forecasts and interpretation. In the final analysis, the Hybrid Bio-Inspired DL Model offers a potential answer to the essential challenge of detecting DDoS attacks in cloud settings. By merging bio-inspired optimization with DL, the model provides excellent performance, flexibility, and scalability, helping to enhance safe and robust cloud computing systems. The future includes extending the suggested system to identify and mitigate DDoS attacks in real time, reducing the impact on cloud services while attacks are in progress and also merging the detection model with automated defensive measures to dynamically block or redirect malicious traffic

References

[1] R. R. Kumar, M. Shameem and C. Kumar, "A computational framework for ranking prediction of cloud services under fuzzy environment", Enterprise Inf. Syst., vol. 16, no. 1, pp. 167-187, Jan. 2022

[2] Bakro, M., Kumar, R. R., Husain, M., Ashraf, Z., Ali, A., Yaqoob, S. I., ... & Parveen, N. (2024). Building a cloud-IDS by hybrid bio-inspired feature selection algorithms along with random forest model. IEEE Access.

[3] I. Sharafaldin, A. H. Lashkari, S. Hakak and A. A. Ghorbani, "Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy", Proc. Int. Carnahan Conf. Secur. Technol. (ICCST), pp. 1-8, Oct. 2019.

[4] Kumar, S., Dwivedi, M., Kumar, M., & Gill, S. S. (2024). A comprehensive review of vulnerabilities and AI-enabled defense against DDoS attacks for securing cloud services. Computer Science Review, 53, 100661.

[5] Aliar, A. A. S., Gowri, V., & Abins, A. A. (2024). Detection of distributed denial of service attack using enhanced adaptive deep dilated ensemble with hybrid meta-heuristic approach. Transactions on Emerging Telecommunications Technologies, 35(1), e4921

[6] Uddin, R., Kumar, S. A., & Chamola, V. (2024). Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions. Ad Hoc Networks, 152, 103322.

[7] Efiong, J.E., Ajayi, T.O., Akinwale, A., Olajubu, E.A., Aderounmu, G.A. (2024). Towards a Bio-inspired Real-Time Intrusion Detection in the Smart Grid. In: Choudrie, J., Tuba, E., Perumal, T., Joshi, A. (eds) ICT for Intelligent Systems. ICTIS 2024. Smart Innovation, Systems and Technologies, vol 403. Springer, Singapore. https://doi.org/10.1007/978-981-97-5799-2_26

[8] Rahamathulla, M. Y., & Ramaiah, M. (2024). An intrusion attack classification using bio-inspired optimization technique and ensemble learning model for edge computing environments. Multimedia Tools and Applications, 1-28

[9] Hussein, A. A. (2024). A Survey on Bio-inspired Algorithms of Cybersecurity. Al-Salam Journal for Engineering and Technology, 3(1), 148-156.

[10] Sherin, R. J., Parkavi, K., & Vanitha, J. (2024). Hybrid Approaches Combining Bio-Inspired Optimization With Machine Learning in Intrusion Detection. In Bio-Inspired Intelligence for Smart Decision-Making (pp. 159-178). IGI Global.

[11] Najafi Mohsenabad, H., & Tut, M. A. (2024). Optimizing Cybersecurity Attack Detection in Computer Networks: A Comparative Analysis of Bio-Inspired Optimization Algorithms Using the CSE-CIC-IDS 2018 Dataset. Applied Sciences, 14(3), 1044. https://doi.org/10.3390/app14031044

[12] Pandithurai, O., Venkataiah, C., Tiwari, S., & Ramanjaneyulu, N. (2024). DDoS attack prediction using a honey badger optimization algorithm based feature selection and Bi-L

[13] Clinton, U. B., Hoque, N., & Robindro Singh, K. (2024). Classification of DDoS attack traffic on SDN network environment using deep learning. Cybersecurity, 7(1), 23.

[14] Han, D., Li, H., Fu, X., & Zhou, S. (2024). Traffic Feature Selection and Distributed Denial of Service Attack Detection in Software-Defined Networks Based on Machine Learning. Sensors, 24(13), 4344.

[15] Urmi, W. F., Uddin, M. N., Uddin, M. A., Talukder, M. A., Hasan, M. R., Paul, S., ... & Imran, F. (2024). A stacked ensemble approach to detect cyber attacks based on feature selection techniques. International Journal of Cognitive Computing in Engineering, 5, 316-331.

[16] Pingale, S. V., & Sutar, S. R. (2022). Remora whale optimization-based hybrid deep learning for network intrusion detection using CNN features. Expert Systems with Applications, 210, 118476.

[17] Rao, G. S., Patra, P. S. K., Narayana, V. A., Reddy, A. R., Reddy, G. V., & Eshwar, D. (2024). DDoSNet: Detection and prediction of DDoS attacks from realistic multidimensional dataset in IoT network environment. Egyptian Informatics Journal, 27, 100526.

[18] Mohan, M., Tamizhazhagan, V., & Balaji, S. (2024). Staked deep ensemble model for intruder behaviour detection and classification in cloud. Multimedia Tools and Applications, 83(19), 57861-57892.

[19] Kannan, B., Sakthivanitha, M., Jayashree, S., & Maruthi, R. (2024, June). Prediction of Cyber Attacks Utilizing Deep Learning Model using Network/Web Traffic Data. In 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC) (pp. 363-367). IEEE.