Optimizing Network Intrusion Detection with a Hybrid Adaptive Neuro Fuzzy Inference System and AVO-based Predictive Analysis

Dr. Sweety Bakyarani.E[1], Anil Pawar[2], Sridevi Gadde[3],
Mr. Eswar Patnala[4], Dr. P. Naresh[5], Prof. Ts. Dr. Yousef A. Baker El-Ebiary[6]

Department of Computer Science-Faculty of Science and Humanities, SRM Institute of Science and Technology, Kattankulathur, India 603203[1]
Professor, Department of Computer Engineering-Sanjivani College of Engineering, Savitribai Phule Pune University, Pune, India[2]
Assistant professor, Raghu Engineering College, Department of Computer Science and Engineering, AP, India[3]
Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, AP, India[4]
Assistant Professor, Electrical and Electronics Engineering Department, Gandhi Institute of Technology and Management Visakhapatnam, Andhra Pradesh, India[5]
Faculty of Informatics and Computing, UniSZA University, Malaysia[6]

***Abstract*—Protecting data and computer systems, as well as preserving the accessibility, integrity, and confidentiality of vital information in the face of constantly changing cyberthreats, requires the vital responsibility of detecting network intrusions. Existing intrusion detection models have limits in properly capturing and interpreting complex patterns in network behavior, which frequently leads to difficulties in robust feature selection and a lack of overall intrusion detection accuracy. The drawbacks of current methods are addressed by a unique approach to network intrusion detection presented in this paper. This framework discusses the difficulties presented by changing cyberthreats and the critical requirement for efficient intrusion detection in a society growing more networked by the day. Using a Hybrid Adaptive Neuro Fuzzy Inference System and African Vulture Optimization model with Min-Max normalization and data cleaning on the NSL-KDD dataset, the methodology outlined here overcomes issues with complex network behavior patterns and improves feature selection for precise identification of potential security threats. This approach meets the need for an effective intrusion detection system. Python software is used to implement the suggested model since it is flexible and reliable. The results show a notable improvement in accuracy, with the Hybrid Adaptive Neuro Fuzzy Inference System and African Vulture Optimization model surpassing previous approaches significantly and obtaining an exceptional accuracy rate of 99.3%. The accuracy of the proposed model was improved by African Vulture Optimization, rising from 99.2% to 99.3%. When compared to Artificial Neural Network (78.51%), Random Forest (92.21%), and Linear Support Vector Machine (97.4%), this amazing improvement is clear. When compared to other techniques, the suggested model exhibits an average accuracy gain of about 20.79%.**

Keywords*—Network intrusion; cyberthreats; normalization; African vulture optimization; data cleaning

I. INTRODUCTION

The Internet has smoothly merged into the framework of everyday life in the rapidly changing digital age, acting as a vital resource for both people and businesses. It now serves as the foundation for keeping records, company operations, and connectivity. The safety and confidentiality of online transactions, nevertheless, are an increasing worry brought on by this previously unheard-of dependence on the World Wide Web. Because of this, cybersecurity has become a crucial area of concern for both business and academics, motivating the commitment of significant funds to protect contemporary web-based networks from possible dangers and abnormalities [1]. Several cyber security issues have emerged, posing several potential hazards to the online lives [2]. Attackers frequently use the flaws in well-known software to target computer systems on networks. These attackers' damage may result in significant issues like service interruptions or even substantial financial losses [3]. In modern linked world, NIDSs are imperative for protecting the accessibility, security, and reliability of data [4]. The two primary types of methods used by NIDSs to do this are signature-based detection and anomaly-based detection [5]. In order to be very effective in recognizing assaults using widely recognized signatures and structures, signature-based NIDSs rely on predefined attack patterns [6]. Nevertheless, their susceptibility to novel attacks is a serious obstacle because they are unable to adjust to new dangers without foreknowledge. Fig. 1 shows the Network intrusion detection system.

There is still much space for enhancement of NIDS efficiency, despite major improvements. The enormous amount of information about network traffic produced, the rapidly changing technical environment, the sizeable collection of features that make up data sets for training and the requirement for actual intrusion detection provide difficulties [7]. The efficacy of NIDS and the speed of training models can both be hampered by unnecessary or redundant characteristics [8]. Because of this, improving the effectiveness of machine learning -based detection models require careful features subset selection and tuning. By defining and explaining what makes up usual network behavior, anomaly-based detection systems, on the other hand, can be used to discover assaults that are unknown or novel.

Both methods have advantages, but to handle the always changing network security concerns, constant advancements are needed [9]. Thus, in order to improve the accuracy of machine learning (ML)-based detection models, careful data subset selection and parameter optimization are required [10].

Different methods were used to fortify network defenses, each with their own advantages and disadvantages. By detecting known attacks using predetermined sequences of attacks, signature-based detection systems act as the initial line of protection [11]. It is impossible to overstate how successful they have historically been at identifying popular hazards. Nevertheless, because they rely on historical signatures for identification, these tools fail when faced with fresh, never-before-seen threats [12]. Anomaly-based Identification systems are skilled at identifying unidentified dangers based on models created around typical actions since they focus on the recognition of abnormalities from standard procedures [13]. As they may be able to identify new threats that signature-based systems overlook, these systems add a key layer of security [14]. Systems for detecting intrusions now depend heavily on machine learning techniques [15]. The focus of conventional methods is on implementing feature engineering and selection, which can be computationally demanding and could only collect deep characteristics, leading to subpar recognition rates. With the promise for higher precision and fewer positive results, artificial intelligence techniques have become widely used to detect fraudulent network traffic [16]. RNNs, CNNs and DRL are a few examples of deep learning techniques that have shown promise in overcoming the drawbacks of conventional machine learning.

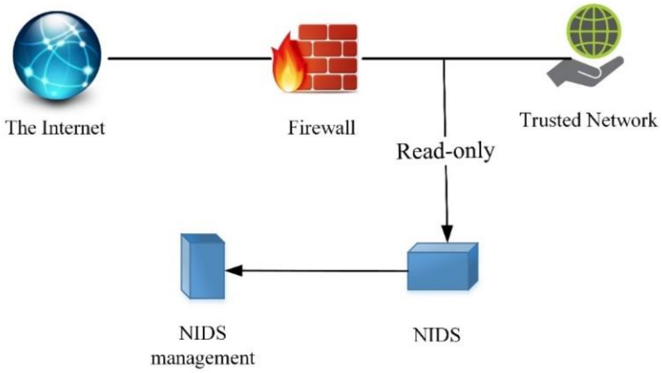

Fig. 1. NID system.

Ongoing improvements in NIDS are required due to the explosive growth of the Internet and the resulting rise in security threats [17]. To develop reliable and effective techniques and systems that precisely detect and react to unwanted or harmful actions within a computer network is the overarching problem statement for network intrusion detection. To safeguard the network's resources from many types of assaults, like as intrusions, infections with viruses, compromises of data, and denial-of-service attacks, this entails differentiating between normal network traffic and suspicious or malicious behavior. Key contributions of this work as follows:

- Data cleaning and Min-Max normalization are included in the study's thorough pre-processing procedure. These methods guarantee the dataset's dependability and quality, which improves the accuracy of subsequent intrusion detection analysis.
- African Vulture Optimization (AVO) provides a novel feature selection method based on the scavenging habits of vultures. By shrewdly determining the most pertinent features for network intrusion detection, it greatly improves model performance and interpretability.
- The Hybrid ANFIS (Adaptive Neuro-Fuzzy Inference System) Model is the central component of the research. The effective capturing of complex patterns in network behavior is made possible by the Hybrid ANFIS. In order to achieve accurate and exact intrusion detection, the model adapts and fine-tunes fuzzy rules through backpropagation.

An outline of the research is given in Section I. The Section II analyses the material that has already been written and highlights the need to handle particular modifications in Network Intrusion detection. Concerning the complexity of Network Intrusion detection, Section III defines the main research issue. Data collection, preprocessing, feature selection, and Hybrid ANFIS are described in Section IV of the paper. The research's importance in detecting Network Intrusion Detection is emphasized in Section V, which gives empirical findings, compares classifier performance, examines consequences and Section VI summaries the conclusion of the paper.

II. Related Works

An essential component of ensuring cybersecurity is intrusion detection and the capability to identify attacks. The aim of this study is on defending against assaults on cyberattack detectors built using machine learning. Here, an approach for adversarial machine learning detection was developed by Pawlicki, Choras, and Kozik [18]. In actuality, the confrontational nature of the surroundings in which they are used has not been taken into consideration while designing modern machine learning algorithms. Therefore, a variety of attacks are currently being directed towards machine learning systems. By constructing adversarial attacks using the four currently proposed approaches, this work assesses the potential of degrading the effectiveness of an intrusion recognition process at test time and then provides a mechanism to identify such assaults. Both artificial neural networks and four techniques for creating adversarial attacks have the necessary historical data. The five separate classifiers' outputs are contrasted, and a thorough explanation of the new detecting technique is provided. In this work intrusion detection systems have not yet been extensively studied in terms of identifying confrontational attacks on false neural networks. And also, it has high false positive rate.

Detecting network intrusions is crucial for maintaining digital security on the network. The primary analysis technique employed in the area of NID is the identification and evaluation of aberrant traffic by extracting statistical aspects of flow. However, because these features must be created and retrieved individually, the original flow data is frequently lost, which reduces the effectiveness of the detection process. In this study, instead of explicitly designing the process's features directly collected the flow's actual data details for evaluation. The deep hierarchical network, which incorporates the enhanced LSTM and LeNet-5 neural network is developed by Zhang et al. [19]. Instead of retraining a pair of networks independently, a feasible network cascade approach was designed to train the suggested hierarchical network simultaneously. A unique traffic collection system can need a lot of resources, including specialized hardware, software, and committed employees, to build and maintain. Managing large amounts of real-world traffic data might put a burden on the facilities available due to computational and storage needs. This strategy could cost a lot to implement in terms of infrastructure setup and ongoing maintenance.

The advancement of network infrastructure and technology has advanced quickly in the past few decades, and Internet services have extended throughout all industries. The prevalence of infringement has increased, and many contemporary systems have been breached, making the advancement of technology for information security to identify new attacks essential. An IDS that uses deep and machine learning algorithms to identify irregularities in network traffic is the greatest vital security-related technologies. Employing a deep neural network techniques and an outstanding network efficiency for network intrusion detection was proposed by Maithem and Al-sultany [20]. The primary purpose of this study is to use advanced IDS to find unidentified attack packages. In this model, detection of attacks is carried out in two different ways (binary categorization and several classes' classification). With regards to the high accurateness with multiclass categorization and with dual classification), the suggested system has demonstrated interesting results. It suggests that the research used deep learning approaches to detect network assaults with excellent classification accuracy. A number of significant flaws and restrictions demand attention. In order to make sure that these networks fail to biased in a specific dataset like the KDD Cup 99. For a viable implementation, it is also essential to handle data imbalance and address computational scalability difficulties.

The potential attack area for cyber hackers is expanding as additional gadgets with internet access come online. Many intrusion detection systems look for identified breaches using network communications characteristics. Despite depending on these fingerprints, investigators have recently employed a machine learning techniques to identify network threats. For an intrusion detection system that is ready for the market, these methods often have a high false-positive rate. Atefinia and Ahmadi [21] proposed a deep neural network model in this study to decrease the incidence of intrusion detection systems that overreact in response to anomalies. The trials make use of the CSE-CIC-IDS2018 dataset, and the models that emerge from them can be included into IDS to produce alerts or thwart upcoming assaults. Though seeking to reduce alarms that are unfounded, the creation of a modular deep neural network for intrusion detection has a number of possible downsides and difficulties. Complexity and interpretability problems can be introduced by modular neural networks. It might be demanding of resources and difficult to apply custom feature extractors and datasets to various contexts. Increasing the amount of training with large data systems carries the danger of over fitting, and there may be issues with data privacy and security.

The reviewed research papers bring up some of the shortcomings and difficulties that intrusion detection systems face, especially when dealing with large false-positive rates and aggressive attacks on neural networks. Handling large amounts of real-world traffic data can put a burden on resources and result in high maintenance and infrastructure expenditures. The reliability of these systems depends on the careful handling of notable problems such bias, data imbalance, and computing scalability. When working with big datasets, modular neural networks can add complexity and interpretability issues, requiring resources and putting data privacy at risk. The aforementioned studies highlight the necessity of continued investigation to surmount these constraints and augment the efficacy of intrusion detection systems with regard to the dynamic landscape of cyber threats.

III. Problem Statement

From the above literature reviews, the necessity to improve intrusion detection system's effectiveness as well as efficacy in order to safeguard computer networks and data against cyberattacks is the central issue in the arena of intrusion detection. Identifying earlier unidentified and changing attack strategies, maintaining sizable and imbalanced data sets, assuring real-time detection and response, and enhancing the comprehensibility of detection models are some of the current issues [21].

IV. Network Intrusion Detection using Hybrid ANFIS and AVO-based Predictive Analysis

The main measures made to improve the precision and effectiveness of the intrusion detection system was described in the methodology section of the network intrusion detection study. The NSL-KDD dataset, a labeled network intrusion detection dataset with a wide variety of network traffic scenarios, was the primary dataset used in this study. It commenced a thorough pre-processing step to guarantee the dataset was prepared for analysis. In order to standardize the data and prepare it for further analysis, this required data cleaning and Min-Max normalization. The process of feature selection, a crucial factor in determining the effectiveness of intrusion detection systems, forms the basis of the methodology. It used the ground-breaking African Vulture Optimization (AVO) method to address this. AVO provides a clever way to choose the most pertinent characteristics, optimizing the feature subset for better model performance and interpretability. It is inspired by the scavenging activity of vultures. After selecting features, the Hybrid Adaptive Neuro-Fuzzy Inference System (ANFIS) was put into use to detect intrusions. Fuzzy logic and neural networks are used with ANFIS to capture complex patterns in network behavior. It achieves accurate intrusion detection by fine-tuning fuzzy rules through backpropagation. By lowering false positives and increasing detection precision, this methodology seeks to strengthen network security in the end. Compared to alternative methods, this thorough framework exhibits an exceptional accuracy rate of 99.3%, proving its efficacy through rigorous experimentation. Fig. 2 shows the Overall Framework for Hybrid ANFIS and AVO-based Network Intrusion Detection.

A. *Data Collection*

The labeled network intrusion detection dataset known as NSL-KDD was utilized in numerous assignments to test various deep learning-based methods for developing various IDS techniques. Four types of characteristics—basic, time-based, content-based and host-based traffic features—can be distinguished among the 41 characteristics included in the NSL-KDD dataset. These traits' worth is mainly determined by their constant, separate, and symbolic nature. Five bout classes, including Normal Denial-of-Service (DoS), Root to Local (R2L), Probe, and Unauthorized to Root (U2R), are included in the NSL-KDD dataset. The attributes associated with each NSL-KDD data can be used to determine these attack classifications [22].

B. *Pre-processing with Data Cleaning and Min-Max Normalization*

Data preparation modifies the data ranges in an NSL-KDD dataset to improve information gathering and operation. The dataset's maximum and minimum ranges exhibit high contrast variance. The normalization of data during this phase lessens an algorithm's challenges.

Data cleaning procedures are used to eliminate data redundancy, noise, mistakes, and undesirable information from the dataset. Only the pertinent data may be processed subsequently in this process.

The normalization role, which contains a least and extreme algorithm and transforms the remaining data value between [-1, 1] and [0, 1], heavily relies on data scalability. The normalization formula is given in Eq. (1).

$$I'^{*} = \frac{D*'-D*'_{min}}{D*'_{max}-D*'_{min}} \tag{1}$$

The phrase I’ in Eq. (1) denotes the value of the input that has been transformed (or, more specifically, normalized). The terms $D'_{max}\ and\ D'_{min}$ stand for the supreme and lowest values of the input variable D', respectively, whereas the term D' stands for actual value [23].

C. *Feature Selection using African Vulture Optimization*

African Vulture Optimization, an innovative metaheuristic strategy based on the behavior of African Vultures, has become a popular choice for feature selection in network intrusion detection. The world's most common bird species, vultures, are usually carnivorous. They are dependent on scavengers to dissect carcasses because they are incapable of doing so themselves. African vultures have been reported to soar above 11,000 meters and to circle over great distances in search of possible food sources. However, once they locate a food supply, they have trouble getting to it quickly. The stronger vultures are frequently encircled by the less powerful ones, which delays the feeding process. The less dominant vultures gradually start looking for food when the dominant ones get tired. This distinctive scavenging behavior has prompted the creation of a novel metaheuristic method designed to tackle feature selection problems in the field of network intrusion detection [24].

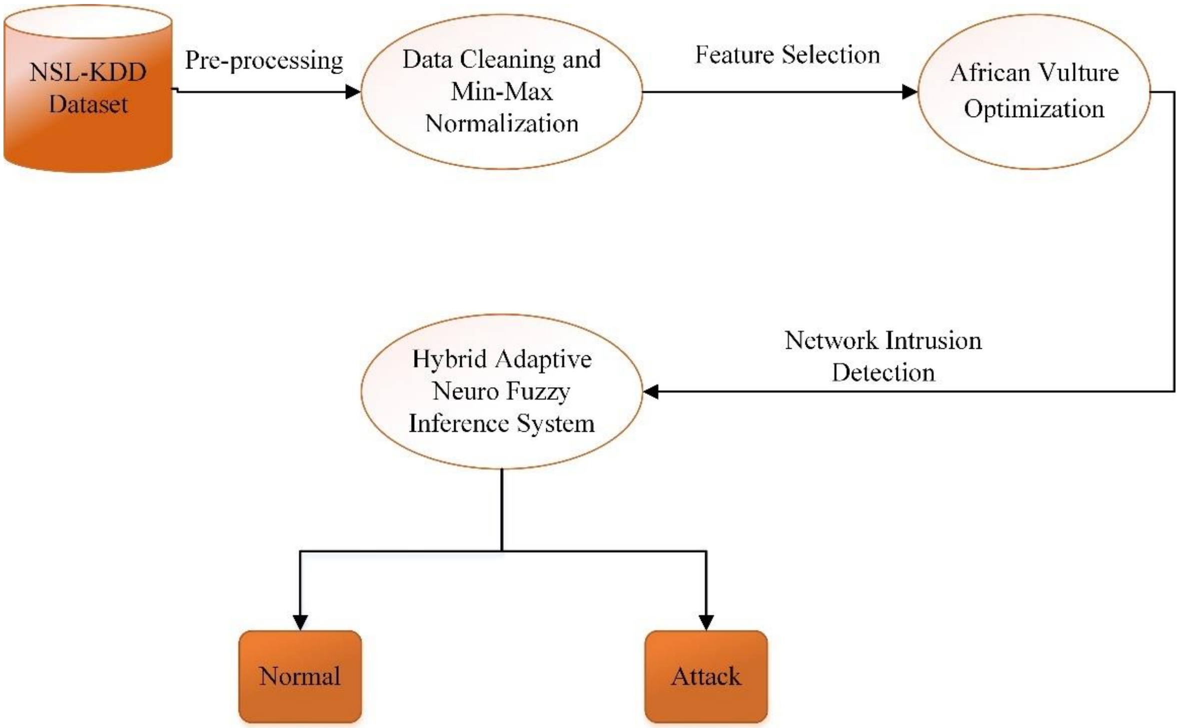
NSL-KDD Dataset
Pre-processing
Data Cleaning and Min-Max Normalization
Feature Selection
African Vulture Optimization
Network Intrusion Detection
Hybrid Adaptive Neuro Fuzzy Inference System
Normal
Attack

Fig. 2. Overall framework for hybrid ANFIS and AVO-based network intrusion detection.

Step 1: To ensure that every feature is given equal weight in the first stage of feature selection for network intrusion detection, try to increase the number of possible characteristics. Finding the highest-performing characteristics within a particular group is the main goal. Eq. (2) gives the description of this operation.

$$S(I) = \begin{cases} best\ vul_1, if\ Z_l = F_1 \\ best\ vul_2, if\ Z_l = F_2 \end{cases} \quad (2)$$

Here, F_1 and F_2 are parameters that were assessed before to optimization; they both have to be between 0 and 1, with the requirement that $F_1 + F_2 = 1$.

Step 2: Finding the features' "famine rate" is the focus of this step. Characteristics are rated according to how well they can advance the optimization, just like actual vultures fly in pursuit of food. Eq. (3) accurately depict this process mathematically:

$$V = (2 \times \tau + 1) \times n \times \left(1 - \frac{iter_l}{max_{iter}}\right) + I \quad (3)$$

In Eq. (3), τ denotes a random number between 0 and 1. The current iteration is indicated by $iter_l$, the total number of iterations is shown by max_{iter}r, and n is a constant that directs the optimization process through its stages of investigation and processing. There are restrictions on the variable d that fall between -2 and 2. If n is less than zero, it means that a feature is scarce, like vulture hunger, and if n is greater than one, it means that a trait is abundant, like a well-fed vulture.

Step 3: In order to facilitate feature selection, vultures are outfitted with random feature subsets that provide two possible configurations and a variable r_1 that has a range of zero to one. Eq. (4) and Eq. (5) provide the following mathematical breakdown of the technique used to choose the best feature set:

$$If\ r_1 \geq randr_1$$

$$S(l+1) = BV(l) - T(l) \times S \quad (4)$$

$$If\ r_1 < randr_1$$

$$S(l+1) = BV(l) - S + rand_2 \times ((ub - Ib) \times rand_3 + Ib \quad (5)$$

S here stands for the unique feature subsets that were selected at random when searching for the best features. The best-performing feature subsets are stored in BV, while the lower and upper bounds for feature values are represented by Ib and ub. Two random variables, rand2 and rand3, have values ranging from 0 to 1.

Step 4: The selected features are represented by the value of |S|, which splits this step into two halves. Both segments include rotational flights when 0.5 < |S| < 1. An active feature can be identified if |S| is greater than or equal to 0.5. During this stage, less significant features try to use the stronger ones to improve their performance. The position of the new feature set, designated as S(k+1), is found by applying Eq. (6), Eq. (7), and Eq. (8).

$$S(l+1) = \frac{best_1 + best_2}{2} \quad (6)$$

$$b_1 = best\ vul_1(l) - \frac{best\ vul_1(l) \times S(l)}{best\ vul_1(l) - S(l)^2} \times S \quad (7)$$

$$b_2 = best\ vul_2(l) - \frac{best\ vul_2(l) \times S(l)}{best\ vul_2(l) - S(l)^2} \times S \quad (8)$$

In the field of network intrusion detection, African Vulture Optimization (AVO) feature selection is a new method. Using a dynamic optimization process that imitates vulture foraging activity, AVO enhances intrusion detection systems' effectiveness by selecting pertinent features. The technique improves detection accuracy and reduces false positives by utilizing AVO, which guarantees that the most important characteristics are taken into account. This adds to the general stability and dependability of the network security configuration.

D. *Employing Hybrid Adaptive Neuro-Fuzzy Inference System for Intrusion Detection*

A hybrid ANFIS system for intrusion detection combines the features of fuzzy logic and neural networks to produce a flexible and adaptive solution for identifying network intrusions while reducing false positives. ANFIS contains of five layers, as shown in Fig. 3.

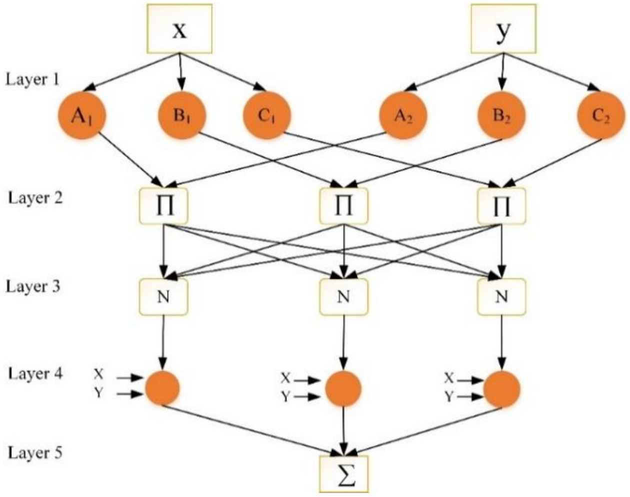

Fig. 3. ANFIS architecture.

The fuzzification layer is represented by Layer 1. It computes the membership function as follows in Eq. (9) and Eq. (10):

$$\lambda_{ai}(y) = \frac{1}{1 + \left[\left(\frac{y - c_{ai}}{\alpha_{ai}}\right)^2\right]\beta_{ai}} \quad (9)$$

$$\lambda_{b\mathrm{i}}(z) = \frac{1}{1 + \left[\left(\frac{z - c_{bi}}{\alpha_{bi}}\right)^2\right]\beta_{bi}} \quad (10)$$

Where, the bell function parameters are c_{ai}, c_{bi}, α_{ai}, α_{bi}, β_{ai}, and β_{ai}.

Layer 2 establishes the rules layer. Each node's firing power is represented by the output in Eq. (11):

$$\omega_i = [\lambda_{a\mathrm{i}}(y)] \times [\lambda_{b\mathrm{i}}(z)] \quad (11)$$

The normalization layer is designated as Layer 3. It adjusts the computed firing strength to be normal by Eq. (12).

$$\overline{\omega_i} = \frac{\omega_i}{\omega_1+\omega_2} \tag{12}$$

Hybrid ANFIS and AVO Algorithm

```
Load the input data
Perform preprocessing operation          //Data Cleaning and Min-Max Normalization

Select feature using AVO
Calculate the fitness of vultures
If s ≥ 1then
Upgrade vulture location using Eq. (5)
Otherwise
Upgrade vulture location using Eq. (6)
Network Intrusion Detection              //Hybrid ANFIS
Calculate RMSC of each particle
If goal achieved
Apply Optimal Particle Position
End
```

The consequent layer is represented by Layer 4. This layer's output is the result of multiplying the polynomial resulting from fuzzy rules by the normalized firing strength of Eq. (13):

$$\overline{\omega_i}F_i = \overline{\omega_\mathrm{i}}(p_\mathrm{i}y + q_\mathrm{i}\,z + r_i) \tag{13}$$

where, p_i, q_i and r_i are the consequent parameter sets.

The defuzzification layer was designated as Layer 5. The ANFIS output as a whole is what it produces by Eq. (14).

$$F = \sum_i \overline{\omega_i}F_i = \frac{\sum_i \omega_i F_i}{\sum_i \omega_i} \tag{14}$$

The learning algorithm must adjust each adjustable parameter in order for the initial training data to match the output of the ANFIS. The RMSE (Root Mean Square Error) between projected values and actual measurements is trained into the ANFIS model to get the lowest possible value. RMSE is characterized by Eq. (15):

$$RMSE = \sqrt{\frac{1}{N*}\sum_{\mathrm{i}=1}^{N*}(y-z)^2} \tag{15}$$

In Eq. (15), N* is the number of samples, y represents the actual measurement, z the forecasted value.

When optimizing Network Intrusion Detection with a Hybrid Adaptive Neuro-Fuzzy Inference System, the parameters of the African Vulture Optimization algorithm play a crucial role. In feature selection, AVO is essential to the intrusion detection system's overall efficacy. The optimization procedure is directly impacted by the particular parameters of the AVO algorithm, such as population size, convergence criterion, and number of iterations. The Hybrid ANFIS and AVO-based system's accuracy and efficiency are greatly impacted by fine-tuning these parameters, which improves predictive analysis. Through their interaction, AVO and the Hybrid ANFIS model provide a synergistic approach that successfully addresses the difficulties associated with network intrusion detection and highlights the significance of parameter tuning for obtaining better outcomes in cybersecurity applications. Overall process of the proposed model is given in Fig. 4.

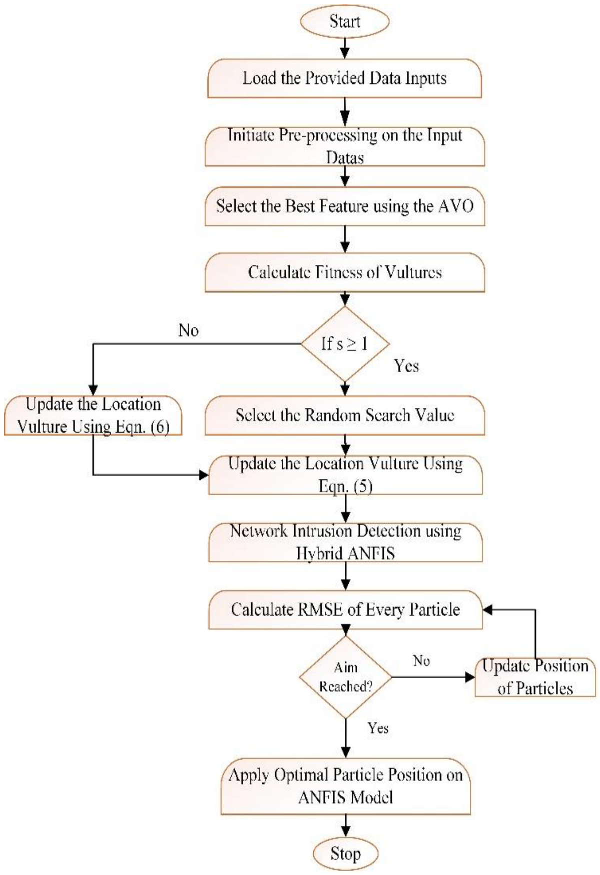
Start
Load the Provided Data Inputs
Initiate Pre-processing on the Input Datas
Select the Best Feature using the AVO
Calculate Fitness of Vultures
If s ≥ 1
No
Yes
Update the Location Vulture Using Eqn. (6)
Select the Random Search Value
Update the Location Vulture Using Eqn. (5)
Network Intrusion Detection using Hybrid ANFIS
Calculate RMSE of Every Particle
Aim Reached?
No
Update Position of Particles
Yes
Apply Optimal Particle Position on ANFIS Model
Stop

Fig. 4. Overall flowchart of proposed hybrid ANFIS and AVO.

V. Results and Discussions

The results of this extensive technique should be presented in the network intrusion detection study's results section. First, describe in detail how we trained and tested our intrusion detection system using the NSL-KDD dataset. Examine the pre-processing findings after the first round of data collection, emphasizing how much data cleaning and Min-Max normalization improved the dataset's analytical fit. Then the key feature selection procedure, where the African Vulture Optimization (AVO) approach was used. This data shows how well AVO performs in terms of identifying the most pertinent characteristics, refining the feature subset, and enhancing interpretability and performance of the model. The Hybrid Adaptive Neuro-Fuzzy Inference System (ANFIS) is an effective tool for intrusion detection. Its ability to capture complex patterns in network behavior is one of its most important applications. ANFIS optimizes fuzzy rules to provide extremely accurate intrusion detection through its backpropagation technique. The results show that this approach significantly improves detection precision while also lowering false positives, which strengthens network security in the end. Robust testing has generated empirical confirmation, demonstrating the framework's improved performance at a remarkable 99.3% accuracy rate—quite an accomplishment in comparison to other well-established methodologies. This method's effectiveness is confirmed by these results, which also highlight how much better network intrusion detection systems could become.

A. Training and Validation Accuracy of Hybrid ANFIS and AVO

Using 80% of the data for training and 20% for validation was the proposed strategy. The accuracy level and loss rate fluctuation graphs for the complete Hybrid ANFIS and AVO model procedure are shown in Fig. 5 and Fig. 6. When the training intervals of the Hybrid ANFIS and AVO model reach 100, the overall graph of the accurateness ratio and loss ratio stabilizes.

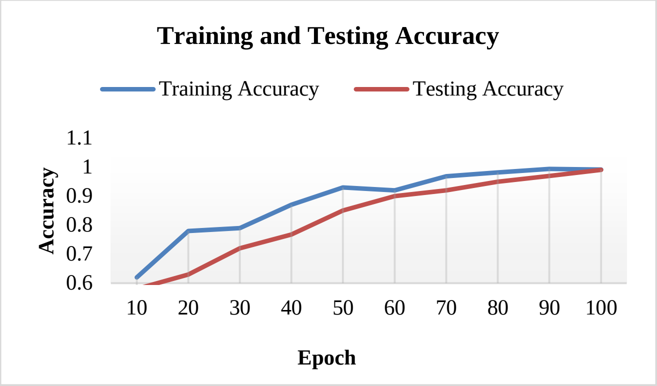

Fig. 5. Accuracy of training and testing values.

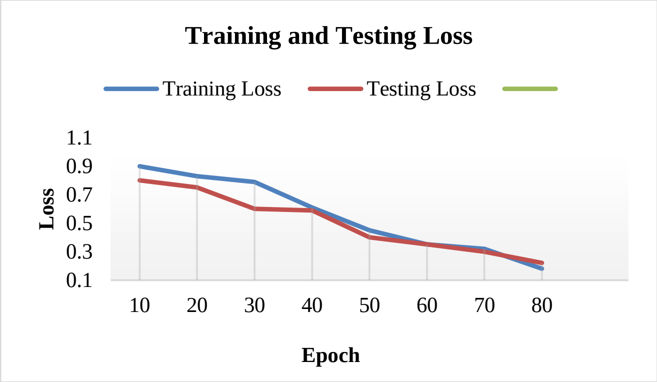

Fig. 6. Loss of training and testing values.

B. Evaluation of Performance

Recall, F1-score, precision, and accuracy were employed as comparison evaluation criteria. The model was evaluated using these parameters. They are shown below:

Accuracy: The prediction accuracy used to evaluate classification performances, as given in Eq. (16), is used to evaluate the classifier's overall performance.

$$A = \frac{TP\prime+TN\prime}{TP\prime+TN\prime+FP\prime+FN\prime} \tag{16}$$

Precision: The degree to which a collection of outcomes approve with one another is referred to as precision. The example is in Eq. (17).

$$P = \frac{TP\prime}{TP\prime+FP\prime} \tag{17}$$

Recall: To determine, below a convinced set of molds, a particular dependent variable, recall analysis, as illustrated in Eq. (18). This process is carried out within predetermined bounds that depend on one or more factors in the incoming data.

$$R = \frac{TP\prime}{TP\prime+FP\prime} \tag{18}$$

True positive pixels are denoted by TP', true negative pixels by TP', false positive pixels by FP', and false negative pixels by FN'.

F1-score: Recall and accuracy are related in the classification task. The F1-score definition is shown in Eq. (19).

$$F1 - score = 2 * \frac{Pr\,e * Re}{Pr\,e + Re} \tag{19}$$

The assessment results of the created Network intrusion detection system employing the combined strategy are shown in Table I.

TABLE I. PERFORMANCE METRICS OF HYBRID ANFIS AND AVO MODEL

Metrics	Values (%)
Accuracy	99.3
Precision	96.8
Recall	98.5
F1-Score	99.1

The performance indicators demonstrate the efficiency of the proposed model in detecting network intrusions, which is quite encouraging. With an astounding accuracy rate of 99.3%, the classification of network activity is classified with a high degree of overall accuracy. The system's precision in reducing false positives is demonstrated by the impressive score of 96.8% obtained by precision, a metric that gauges the model's ability to properly categorize incursions. Recall, which measures how well the model can identify real incursions, is also quite significant at 98.5%. A robust 99.1% is reached by the F1-Score, which balances recall and precision and highlights the system's well-balanced performance.

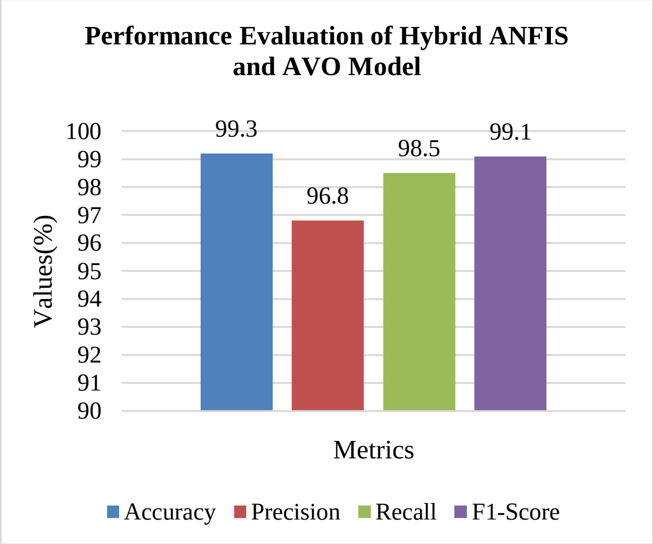

Fig. 7. Performance evaluation of hybrid ANFIS and AVO model.

These results demonstrate accurate and trustworthy anomaly detection with high values across key performance measures. The performance evaluation of the proposed Hybrid ANFIS and AVO model is shown in Fig. 7.

Table II shows the Accurateness, Recall, Precision and F1-score of the proposed approach with existing methods. The accuracy of the suggested method Hybrid ANFIS and AVO model (99.3%) is higher than the existing approaches ANN (78.51%), Random Forest (92.21%) and Linear SVM (97.4%).

Fig. 8 depicts the graphic depiction of the performance metrics of proposed with existing approaches. The precision of the suggested method Hybrid ANFIS and AVO model (96.8%) is higher than the existing ANN (96.6%), Random Forest (96.8%) and Linear SVM (97%). The recall of the suggested method Hybrid ANFIS and AVO model (98.5%) is higher than the existing approaches ANN (62.05%), Random Forest (61.5%) and Linear SVM (97%). The F1-score of the suggested method Hybrid ANFIS and AVO model (99.1%) is higher than the existing approaches ANN (75.5%), Random Forest (75.2%) and Linear SVM (97%).

The suggested model's graph shows how, as it reached a point of consistency using the provided hyperparameters, the accuracy of the training and validation sets rose quickly over a shorter period of time.

Before optimization the value of accuracy for proposed Hybrid ANFIS and AVO model is 99.2%. The accuracy achieved after optimization using Hybrid ANFIS and AVO model is 99.3%. The fitness of Hybrid ANFIS and AVO model is depicted in Fig. 9.

C. Discussion

This paper highlights the relevance of the results through a thorough analysis, including a comparison with existing methods, by combining African Vulture Optimization (AVO) with the Hybrid Adaptive Neuro-Fuzzy Inference System (ANFIS) for network intrusion detection. Using well-known performance indicators like recall, F1-score, accuracy, and precision, the validity and training accuracy of the new approach are carefully assessed. The Hybrid ANFIS and AVO model performs exceptionally well, outperforming existing models in the field with a 99.3% accuracy rate. The fitness improvement graph of the AVO model, which shows the efficiency of the optimization process and the ongoing improvement of feature selection over time, supporting the superiority of the model, provides evidence. Reducing false positives and improving detection precision is emphasized as a critical component of strengthening network security. The comparative analysis with traditional methods shows that the study's findings strengthen and advance the field of network intrusion detection. The methodology not simply performs better than other conventional ways like Random Forest (92.21%) [25], Artificial Neural Network (78.51%) [25], and Linear SVM (97.4%) [25], but it also shows potential for greatly enhancing the efficacy and dependability of intrusion detection systems. This verifies the methodology's applicability and offers solid solutions to the problems facing network security today.

TABLE II. PERFORMANCE METRICS OF PROPOSED METHOD

Methods	Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)
ANN [25]	78.51	96.6	62.05	75.5
Random Forest[25]	92.21	96.8	61.5	75.2
Linear SVM [25]	97.4	97	97	97
Hybrid ANFIS and AVO model	99.3	96.8	98.5	99.1

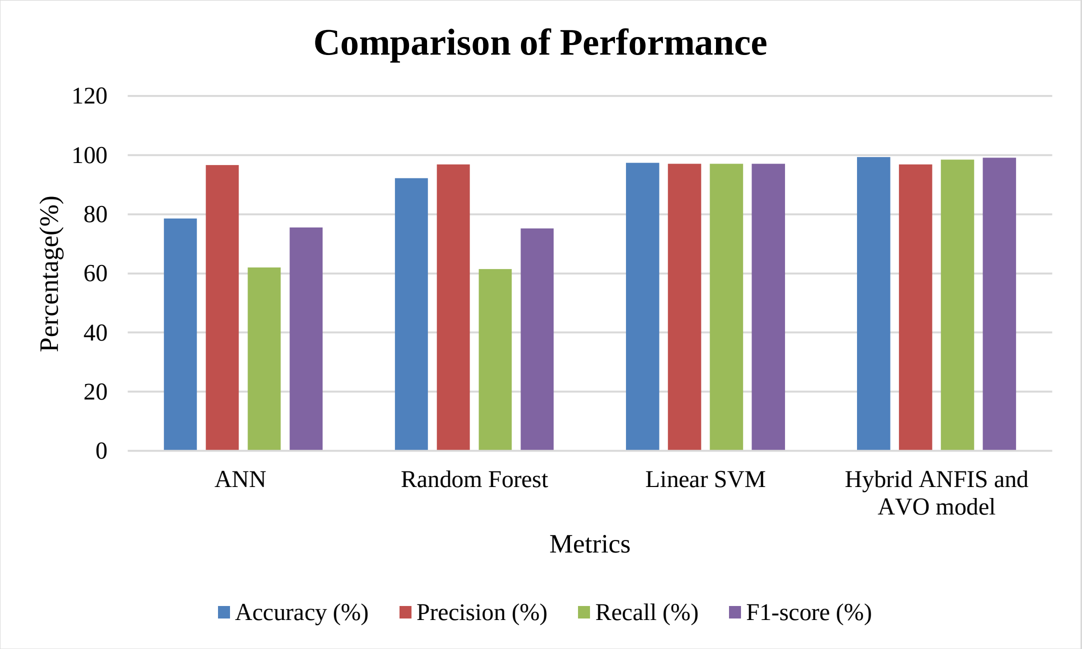

Fig. 8. Comparison of hybrid ANFIS and AVO model with existing models.

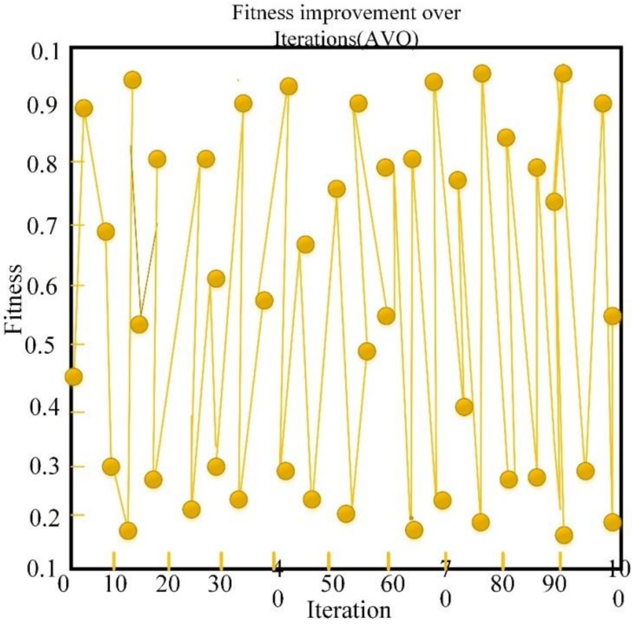

Fig. 9. Fitness improvement graph of AVO.

VI. Conclusion and Future Work

The integration of the Hybrid Adaptive Neuro-Fuzzy Inference System (ANFIS) with African Vulture Optimization (AVO) in this network intrusion detection system has produced remarkable outcomes. This novel approach is carefully assessed and contrasted in the discussion part, which also highlights its overall effectiveness, training correctness, and validity. This proposed model outperforms existing models in the industry with an accuracy rate of 99.3% after a thorough review utilizing key performance measures like recall, F1-score, precision, and accuracy. The fitness improvement of the AVO model is represented graphically, which highlights the efficacy of the optimization process by showing how feature selection is improved over time and how this leads to an improvement in the overall performance of the model. Especially, this approach solves a critical network security issue by decreasing false positives and improving detection accuracy at the same time. The comparison with current models demonstrates the significant advancements made in network intrusion detection. This strategy not only performs better than conventional techniques, but it also has the potential to greatly improve intrusion detection systems' dependability and effectiveness. These results validate the applicability of the approach to modern network security problems. This study's shortcomings include differences in the dataset's properties, which raise questions about how well-suited it is to different network contexts and the possibility of bias resulting from the traits unique to the dataset. Future research will concentrate on improving the hybrid ANFIS and AVO-based system's real-time deployment by implementing deep learning techniques. The strategy will be modified to handle new network security issues, especially those related to 5G and Internet of Things networks. The methodology will be expanded to handle scenarios involving multi-class intrusion detection, guaranteeing its relevance in a variety of dynamic cybersecurity environments.

References

[1] M. Injadat, A. Moubayed, A. B. Nassif, and A. Shami, “Multi-Stage Optimized Machine Learning Framework for Network Intrusion Detection,” IEEE Trans. Netw. Serv. Manage., vol. 18, no. 2, pp. 1803–1816, Jun. 2021, doi: 10.1109/TNSM.2020.3014929.

[2] B. Ghimire and D. B. Rawat, “Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things,” IEEE Internet Things J., vol. 9, no. 11, pp. 8229–8249, Jun. 2022, doi: 10.1109/JIOT.2022.3150363.

[3] H. Zhang, J.-L. Li, X.-M. Liu, and C. Dong, “Multi-dimensional feature fusion and stacking ensemble mechanism for network intrusion detection,” Future Generation Computer Systems, vol. 122, pp. 130–143, Sep. 2021, doi: 10.1016/j.future.2021.03.024.

[4] M. Sarhan, S. Layeghy, and M. Portmann, “Towards a Standard Feature Set for Network Intrusion Detection System Datasets,” Mobile Netw Appl, vol. 27, no. 1, pp. 357–370, Feb. 2022, doi: 10.1007/s11036-021-01843-0.

[5] P. Panagiotou, N. Mengidis, T. Tsikrika, S. Vrochidis, and I. Kompatsiaris, “Host-based Intrusion Detection Using Signature-based and AI-driven Anomaly Detection Methods,” ISIJ, vol. 50, pp. 37–48, 2021, doi: 10.11610/isij.5016.

[6] J. Kim, J. Kim, H. Kim, M. Shim, and E. Choi, “CNN-Based Network Intrusion Detection against Denial-of-Service Attacks,” Electronics, vol. 9, no. 6, p. 916, Jun. 2020, doi: 10.3390/electronics9060916.

[7] A. K. Ghosh, C. Michael, and M. Schatz, “A Real-Time Intrusion Detection System Based on Learning Program Behavior,” in Recent Advances in Intrusion Detection, vol. 1907, H. Debar, L. Mé, and S. F. Wu, Eds., in Lecture Notes in Computer Science, vol. 1907. , Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 93–109. doi: 10.1007/3-540-39945-3_7.

[8] E. Jaw and X. Wang, “Feature Selection and Ensemble-Based Intrusion Detection System: An Efficient and Comprehensive Approach,” Symmetry, vol. 13, no. 10, p. 1764, Sep. 2021, doi: 10.3390/sym13101764.

[9] Y. Fu, Y. Du, Z. Cao, Q. Li, and W. Xiang, “A Deep Learning Model for Network Intrusion Detection with Imbalanced Data,” Electronics, vol. 11, no. 6, p. 898, Mar. 2022, doi: 10.3390/electronics11060898.

[10] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, “BAT: Deep Learning Methods on Network Intrusion Detection Using NSL-KDD Dataset,” IEEE Access, vol. 8, pp. 29575–29585, 2020, doi: 10.1109/ACCESS.2020.2972627.

[11] M. Masdari and H. Khezri, “A survey and taxonomy of the fuzzy signature-based Intrusion Detection Systems,” Applied Soft Computing, vol. 92, p. 106301, Jul. 2020, doi: 10.1016/j.asoc.2020.106301.

[12] D. N. Mhawi, A. Aldallal, and S. Hassan, “Advanced Feature-Selection-Based Hybrid Ensemble Learning Algorithms for Network Intrusion Detection Systems,” Symmetry, vol. 14, no. 7, p. 1461, Jul. 2022, doi: 10.3390/sym14071461.

[13] S. Zavrak and M. Iskefiyeli, “Anomaly-Based Intrusion Detection From Network Flow Features Using Variational Autoencoder,” IEEE Access, vol. 8, pp. 108346–108358, 2020, doi: 10.1109/ACCESS.2020.3001350.

[14] A. O. Alzahrani and M. J. F. Alenazi, “Designing a Network Intrusion Detection System Based on Machine Learning for Software Defined Networks,” Future Internet, vol. 13, no. 5, p. 111, Apr. 2021, doi: 10.3390/fi13050111.

[15] J. B. Awotunde, C. Chakraborty, and A. E. Adeniyi, “Intrusion Detection in Industrial Internet of Things Network-Based on Deep Learning Model with Rule-Based Feature Selection,” Wireless Communications and Mobile Computing, vol. 2021, pp. 1–17, Sep. 2021, doi: 10.1155/2021/7154587.

[16] T. Tuan, H. Long, L. Son, I. Priyadarshini, R. Kumar, and N. Son, “Performance evaluation of Botnet DDoS attack detection using machine learning,” Evolutionary Intelligence, vol. 13, p. 3, Jun. 2020, doi: 10.1007/s12065-019-00310-w.

[17] Z. Fu, “Computer Network Intrusion Anomaly Detection with Recurrent Neural Network,” Mobile Information Systems, vol. 2022, pp. 1–11, Mar. 2022, doi: 10.1155/2022/6576023.

[18] M. Pawlicki, M. Choraś, and R. Kozik, “Defending network intrusion detection systems against adversarial evasion attacks,” Future Generation Computer Systems, vol. 110, pp. 148–154, Sep. 2020, doi: 10.1016/j.future.2020.04.013.

[19] Y. Zhang, X. Chen, L. Jin, X. Wang, and D. Guo, “Network Intrusion Detection: Based on Deep Hierarchical Network and Original Flow Data,” IEEE Access, vol. 7, pp. 37004–37016, 2019, doi: 10.1109/ACCESS.2019.2905041.

[20] M. Maithem and G. A. Al-sultany, “Network intrusion detection system using deep neural networks,” J. Phys.: Conf. Ser., vol. 1804, no. 1, p. 012138, Feb. 2021, doi: 10.1088/1742-6596/1804/1/012138.

[21] R. Atefinia and M. Ahmadi, “Network intrusion detection using multi-architectural modular deep neural network,” J Supercomput, vol. 77, no. 4, pp. 3571–3593, Apr. 2021, doi: 10.1007/s11227-020-03410-y.

[22] H. Alavizadeh, H. Alavizadeh, and J. Jang-Jaccard, “Deep Q-Learning Based Reinforcement Learning Approach for Network Intrusion Detection,” Computers, vol. 11, no. 3, p. 41, Mar. 2022, doi: 10.3390/computers11030041.

[23] S. Sivamohan and S. S. Sridhar, “An optimized model for network intrusion detection systems in industry 4.0 using XAI based Bi-LSTM framework,” Neural Comput & Applic, vol. 35, no. 15, pp. 11459–11475, May 2023, doi: 10.1007/s00521-023-08319-0.

[24] L. Hu, Y. Zhang, K. Chen, and S. Mobayen, “A COMPUTER-AIDED melanoma detection using deep learning and an improved African vulture optimization algorithm,” Int J Imaging Syst Tech, vol. 32, no. 6, pp. 2002–2016, Nov. 2022, doi: 10.1002/ima.22738.

[25] S. Sapre, P. Ahmadi, and K. Islam, “A Robust Comparison of the KDDCup99 and NSL-KDD IoT Network Intrusion Detection Datasets Through Various Machine Learning Algorithms.” arXiv, Dec. 31, 2019. Accessed: Sep. 19, 2023. [Online]. Available: http://arxiv.org/abs/1912.13204