Mesopotamian journal of Cybersecurity
Vol.5,No.1, **pp.** 1–10
DOI: https://doi.org/10.58496/MJCS/2025/001; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Enhancing Intrusion Detection Systems with Adaptive Neuro-Fuzzy Inference Systems

Jitender Sharma[1], Sonia [1], Karan Kumar [2,*], Pankaj Jain[3], Raed H. C. Alfilh[4], Hussein Alkattan[5,6]

[1] Yogananda School of AI Computers and Data Science, Shoolini University, Solan, Himachal Pradesh, India
[2] Department of Electronics & Communication Engineering, Maharishi Markandeshwar Engineering College, Maharishi Markandeshwar (Deemed to be University), Mullana, Ambala, Haryana, India
[3] SJJTU University, Churu Rajasthan, India.
[4]Refrigeration & Air-Conditioning Technical Engineering Department, College of Technical Engineering, The Islamic University, Najaf, Iraq.
[5] Department of System Programming, South Ural State University, Chelyabinsk 454080, Russia.
[6] Directorate of Environment in Najaf, Ministry of Environment, Najaf, Iraq.

ARTICLE INFO

Article history
Received 18 Oct 2024
Accepted 11 Dec 2024
Published 10 Jan 2025

Keywords
Network Security
Intrusion Prevention System
Intrusion Detection Systems
Machine Learning
Adaptive Neuro-Fuzzy Inference System
Feature Selection

ABSTRACT

Network security has become increasingly critical in recent years. Among the various aspects of network security and considering several approaches to network security, intrusion detection systems (IDSs) have gained considerable attention. The prominence of this factor, among other factors of network security, is due to its ability to address the complex and uncertain nature of security breaches. Whenever data flow over the network, precise categorization of normal and malicious data is necessary. Past IDS systems lack precise categorization. Thus, the present study focuses on the use of the adaptive neuro-fuzzy inference system (ANFIS) as a classifier to categorize network instances into malicious types and normal behavior. Using the KDD99 dataset, the performance of ANFIS is evaluated and compared with that of traditional machine learning models such as decision trees and multilayer perceptrons. Through experimentation with different membership functions, such as Gaussian, triangular, bell-shaped, and sigmoidal functions, Gaussian functions are identified as optimal for this specific task. The results underscore the effectiveness of ANFIS, leveraging the strengths of both artificial neural networks (ANNs) and fuzzy reasoning systems. ANFIS demonstrates superior capabilities in understanding nonlinear interaction patterns, adapting to evolving threats, and facilitating rapid learning in intrusion detection applications.

1. INTRODUCTION

In the current digitally connected era, where information technology is essential to nearly every aspect of our lives, ensuring the security of computer networks and systems has become a critical priority. The increase in advanced cyberattacks and intrusions has driven the research community to create robust and intelligent intrusion detection systems (IDSs) designed to protect sensitive data and critical infrastructure [1], [2]. This applies to all fields where misusing data by extruders can lead to disasters, such as healthcare, energy, autonomous vehicles, military, etc. [3, 4, 5, 6], and here, the importance of developing adaptive intrusion detection systems that can address the emerging challenges in the field of cybersecurity. Machine learning techniques have demonstrated their efficacy in successfully crafting intrusion detection systems with high levels of accuracy and precision [7] – [9]. A comprehensive review of various machine learning (ML) and deep learning (DL) methodologies employed in the development of network intrusion detection systems (NIDSs) can be found in [10][23]. Furthermore, in the context of wrappers, four distinct ML techniques—C4.5, naive Bayes (NB), random forest (RF), and the REP tree—have been employed. Specifically, focusing on Denial-of-Service (DoS) attacks, the outcomes exhibit exceptional performance,

Corresponding author. Email: karan.170987@gmail.com achieving false positive rates (FPRs) of 99.6%, 0.3%, 99.8%, and 2.7% for the respective methods. Among the various methodologies explored to address this pressing challenge, the integration of adaptive neuro-fuzzy inference systems (ANFISs) has emerged as a promising avenue because of its adaptability, self-learning capabilities, and ability to handle complex, nonlinear data patterns [11][12]. Traditional intrusion detection techniques, such as signature-based systems and anomaly detection, often struggle to keep pace with the ever-evolving attack landscape, leading to a high rate of false positives and false negatives [13]. The limitations of conventional methods have motivated researchers to seek more innovative and intelligent approaches for identifying and mitigating cyber threats effectively [14].

ANFIS is a hybrid model that merges the advantages of artificial neural networks and fuzzy logic systems, enabling the combination of precise reasoning with imprecise, human-like thinking. By blending the adaptability of neural networks with the interpretability of fuzzy logic, ANFIS excels in managing uncertain and dynamic network behaviors. It can learn from historical data, identify patterns, and generalize to detect new intrusions, making it a powerful tool for enhancing the security of modern IT infrastructures [15][32]. Toosi et al. employed an adaptive neuro fuzzy inference system (ANFIS) as a classifier for identifying intrusions in computer networks. The research assesses the classifier's performance both in binary and multiclass modes, distinguishing between regular and suspicious/intrusive system activities. The evaluation employs the KDD Cup 99 intrusion detection dataset, revealing that ANFIS demonstrates effectiveness in identifying diverse intrusion instances [16]. An IDS hybrid model comprises a cascade of self-organizing map (SOM) blocks interconnected with a fuzzy system that was proposed in [17]. The suggested hybrid framework undergoes training, testing, and validation by employing the KDD CUP 99 dataset. This paper conducts a comparative assessment against analogous solutions in the literature. Through this approach, a refined training dataset is generated, yielding improved classification outcomes, particularly for a single class, surpassing the best results from the KDD CUP 99 competition and more recent alternatives. The IDS was also employed to identify network or system abnormalities in [18][35]. However, owing to the considerable data volume, networks often face challenges such as elevated false alarm rates and decreased detection accuracy, particularly during novel attacks. The core objective is to increase accuracy and mitigate the false alarm rate (FAR). To overcome these obstacles, the proposed approach combines the crow search optimization algorithm with the adaptive neuro-fuzzy inference system (CSO-ANFIS). In this context, the crow search optimization algorithm optimizes the performance of the ANFIS model. Validation of this intrusion detection model leverages the NSL-KDD dataset. A comparative analysis against existing techniques demonstrated the superiority of the proposed approach. The intrusion detection accuracy when the NSL-KDD dataset is used is 95.80%, coupled with a notably low FAR of 3.45%. Rahman et al. [19] introduced an IDS designed for cyber-physical systems that employs an adaptive neuro-fuzzy inference system. This intelligent IDS acts as a security mechanism by analysing network traffic and historical data to permit authorized access to the system. To identify various intrusion patterns and attributes, the widely recognized KDD Cup 99 dataset is employed. The relevance of features is determined through chi-square testing and a correlation matrix, aiding in the classification of attack types. Through performance assessment, the study demonstrated enhanced accuracy in classifying diverse attack categories.

To understand the needs of today’s IT world, the main objective of this research is

- To present the utilization of ANFIS in intrusion detection systems to clearly differentiate between normal and malicious attacks.
- To understand the underlying principles of ANFIS, its architecture, and learning algorithms, as well as the challenges and limitations associated with its implementation in IDS, are needed.
- Different membership functions are used to obtain the best ANFIS model, which is then compared with other machine learning techniques.

To achieve the above objectives, the KDD99 dataset is used. The dataset has already been used by prominent researchers for IDS analysis, so its usage makes our work more useful and helps us analyse and highlight the practical benefits and effectiveness of ANFIS-based IDSs over other existing methods.

The remainder of this article is divided into 5 sections. Section 2 presents the literature review, followed by the proposed methodology in section 3. The results and discussion are given in section 3. Finally, the article is concluded in section 5.

2. LITERATURE REVIEW AND CONTEXTUAL BACKGROUND

2.1 ANFIS

An adaptive neuro-fuzzy inference system (ANFIS) is a hybrid computational model that combines the strengths of artificial neural networks and fuzzy logic systems [24, 25]. It is designed to perform pattern recognition, classification, and function approximation tasks by integrating the adaptability of neural networks and the interpretability of fuzzy logic. ANFIS is particularly effective in dealing with complex, nonlinear data patterns and handling uncertainty in data.

2.1.1 Fuzzy inference system (FIS) architecture

ANFIS is built upon the principles of fuzzy logic. A fuzzy inference system (FIS) comprises four key components:

a. Fuzzification: Convert crisp input data into fuzzy sets via membership functions to represent degrees of belonging.
b. Rule Base: This rule consists of a set of if-then rules, where the antecedents (input conditions) are represented via fuzzy sets, and the consequents (output actions) are expressed as fuzzy sets or linguistic variables.
c. Inference Engine: This engine applies fuzzy logic rules to make inferences about the system's behavior.
d. Defuzzification: Convert the fuzzy output of the inference engine back into crisp values for decision-making [29].

2.1.2 Layered ANFIS Architecture

ANFIS is constructed with a layered architecture, which consists of five layers, each serving a specific purpose:

a. Input Layer: Represents the input variables of the system, receiving crisp data as input.
b. Fuzzification Layer: This layer fuzzifies the crisp input data into fuzzy sets via predefined membership functions. Each node in this layer corresponds to a specific fuzzy set and computes the membership grade for the input data.
c. Rule Layer: Computes the firing strength of each rule by combining the membership grades of the fuzzified inputs via AND or OR operations, depending on the rule type (e.g., "AND" for conjunctive rules and "OR" for disjunctive rules).
d. Normalization Layer: This layer normalizes the firing strengths of the rules to ensure that their relative contributions remain consistent.
e. Output Layer: This layer combines the outputs of all the rules to obtain the final output of the ANFIS system. The output layer can have a single node (for scalar output) or multiple nodes (for vector output).

2.2 Learning algorithms

ANFIS uses supervised learning to determine the optimal parameters of its fuzzy inference system. Two popular learning algorithms for ANFIS are used during training [26,27]:

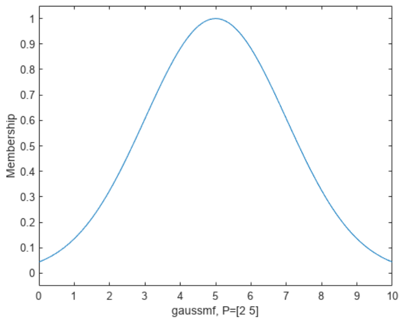
a. Backpropagation: The backpropagation algorithm, commonly used in neural networks, is employed to update the parameters of the consequent part of the fuzzy rules (e.g., the output fuzzy sets) on the basis of the error between the actual and desired outputs.
b. Gradient Descent: The gradient descent algorithm adjusts the parameters of the antecedent part of the fuzzy rules (e.g., the membership function parameters) to minimize the overall error between the predicted output and the actual output.

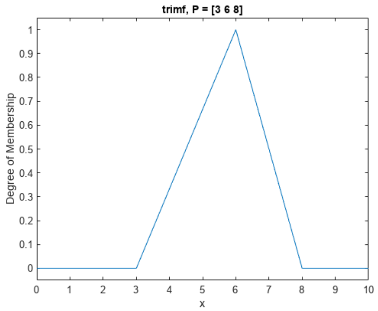
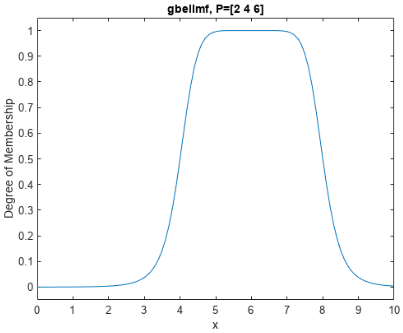
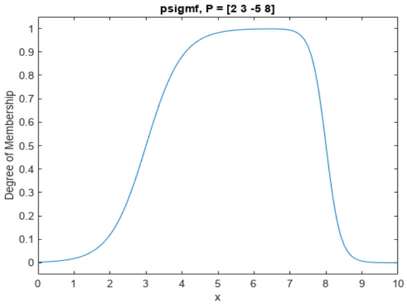
2.3 Hybrid Learning

The learning process in ANFIS is carried out in a hybrid manner. During training, the forward pass computes the output of the ANFIS system given the input data. Then, the backwards pass (using backpropagation and gradient descent) updates the parameters of the fuzzy inference system to minimize the error between the predicted output and the target output. This iterative process continues until the error converges to a satisfactory level.

In this study, many membership functions (MFs) are used to investigate the best MF for the IDS. The MFs used are Gaussian, triangular, bell-shaped, sigmoidal, and membership functions as shown in Table 1.

TABLE I. MEMBERSHIP FUNCTIONS USED [26]

MF	Equation	Shape
Gaussian	$f(x;\sigma,c) = e^{\frac{-(x-c)^2}{2\sigma^2}}$ Standard deviation, σ, and Mean c	

Triangular membership function (Trimf)	$f(x;a,b,c) = \max\left(\min\left(\frac{x-a}{b-a},\frac{c-x}{c-b}\right),0\right)$	
Generalized bell-shaped membership function (Gbellmf)	$f(x;a,b,c) = \frac{1}{1+\left\lvert\frac{x-c}{a}\right\rvert^{2b}}$	
Product of two sigmoidal membership functions (Psigmf)	$f(x;a_k,c_k) = \frac{1}{1+e^{-a_k(x-c_k)}}$	

3. METHODOLOGY

The methodology followed in this study is explained in this section, where it addresses the dataset used, reprocessing, deep neural networks and architecture optimization via the grey wolf optimizer.

3.1 KDD'99 Dataset

KDD'99 is used in this study for training and evaluating the model, as it is commonly used for IDSs. The network traffic data provided by DAPRA [20, 28] are published online for IDS studies. The file size is 4 GB of more than 5 million samples with 41 features labelled as normal or one of a set of 22 types of attacks. However, the attacks are regrouped into only 4 groups. To increase the likelihood of detecting new types of attacks, these groups are as follows:

- DoS (Denial of Service): sends much traffic to the server to slow or shut it down.
- R2L (Root to Local): Provides fraud access to a device locally through sending fraudulent packets.
- U2R (user-to-root): This provides access to the device as a normal user by exploiting the device vulnerability.
- Probe (Probing): collects data about the network to escape the security control systems.

3.2 Preprocessing

The data used are heterogeneous data that contain both categorical and numerical features, which require preprocessing to feed the DNN model. Many preprocessing operations are used for this purpose, and in this study, the following steps are followed:

3.2.1 Data conversion

All the techniques can transfer nominal data into numeric data, which are easier to handle. The categorical features in this dataset are distributed as follows: 3 categories of "Protocol Type", 70 categories of "Service" and 11 categories of "Flag". These columns are converted to numeric values by sorting them and then given one unique index for each category, which represents them numerically.

3.2.2 Data normalization

Normalization is vital in preprocessing any data before training because it has a major impact on model accuracy, as the dataset features should range from a similar scale, which is generally recommended to be between -3 and +3 [21, 30, 31]. In this study, the minimal-maximal normalization approach, which scales the data between 0 and 1, is used for all features as follows:

$$x_{scaled} = \frac{x - x_{min}}{x_{max} - x_{min}} \tag{1}$$

where x_{min} and x_{max} are the minimum and maximum values, respectively, of feature x.

3.2.3 Feature Selection

Feature selection (FS) plays a crucial and influential role in both the training and feature extraction processes, directly impacting the system's output. This task is instrumental in enhancing data pattern detection while simultaneously reducing the complexity and computational burden by eliminating less significant data features. Various FS techniques are employed, such as filter methods, which focus on identifying broad patterns within datasets, and wrapper methods, which utilize intelligent algorithms to assess feature importance, albeit at the cost of increased execution time. Commonly used classifiers for this purpose include RF, C4.5, NB, information gain (IG), (CFS), and REPTree, as well as hybrid models such as CAPPER.

In our study, Gini impurity [22, 33, 34] is utilized to assess node importance, assuming binary trees, where IG is computed as the reduction in entropy resulting from data splitting on a particular attribute. Feature importance is determined by measuring the decrease in node impurity, weighted by the likelihood of reaching that node. This probability is calculated as the number of data points reaching the node divided by the total number of samples. The higher the computed value is, the more valuable the corresponding feature. The best five features are chosen for training and testing the models.

3.3 Evaluation metrics

The most popular evaluation metrics for classification, given in Table 2, are used to assess the proposed model:

TABLE II. EVALUATION METRICS USED FOR EVALUATION [26]

Metric	Use	Equation
Precision (Pre)	which gives a clear observation of the cases that were classified in each class, and they are actually from this class	$Pre = \frac{TP}{TP + FP}$
Recall (Rec):	which gives a clear observation about cases where from a particular class and are predicted correctly.	$Rec = \frac{TP}{TP + FN}$
Accuracy (Acc)	It refers to the percentage of samples that were predicted correctly	$Acc = \frac{TP + TN}{TP + FP + TN + FN}$
F1-Score	It combines recall and precision and gives better observation when having uneven class distribution	$f1 - score = 2 \times \frac{precision \times recall}{precision + recall}$
Specificity	The percentage of the negative class has been predicted correctly	$Spec = \frac{TN}{TN + FP}$
AUC, Area Under Receiver Operating characteristic (ROC) Curve	It refers to the capability of the model to distinguish between classes	$TPR = \frac{TP}{TP + FN}$ $FPR = \frac{FP}{FP + TN}$

where TP: true positives, TN: true negatives, FP: false positives, FN: false negatives, TPR: true positive rate, and FPR: false positive rate.

4. EMPIRICAL RESULTS AND FINDINGS

In this study, the MATLAB 2023a version is used to implement and test the models. First, the data are undersampled, as ANFIS cannot be trained on a large number of inputs, as the number of membership functions increases and the computational cost becomes so high. Therefore, only the five most correlated features are selected for training. Three membership functions are used for each input, which is the maximum number that we can use. The dataset is split into 2 different sets for training and testing, where the results shown in this section are all based on the testing dataset. All the models are trained on the same dataset and tested on the same samples. The ANFIS model is trained with 4 different membership functions (Gaussian, triangular, bell-shaped, and sigmoidal), and the results derived from the different membership functions are shown in Table 3. Notably, the Gaussian MF achieves the best results, with an accuracy of 70%, whereas the triangular MF achieves the worst results. The ANFIS model with Gaussian MF was only able to distinguish between all the classes. Therefore, only the Gaussian MF is considered for further analysis.

TABLE III. ANFIS PERFORMANCE USING DIFFERENT MFS

MF	Gaussian	Trimf	gbellmf	psigmf
Acc	70%	56%	61%	59%
Pre	75	50	56	46
Rec	70	56	61	56
F1	69	50	57	47
Spec	92	89	90	89

The model is tested considering the evaluation metrics mentioned in section 2.4. The confusion matrix of the ANFIS model is shown in Figure 1, where it is noted that the model behaves slightly well except for the R2L class, where most of the cases were classified as U2R.

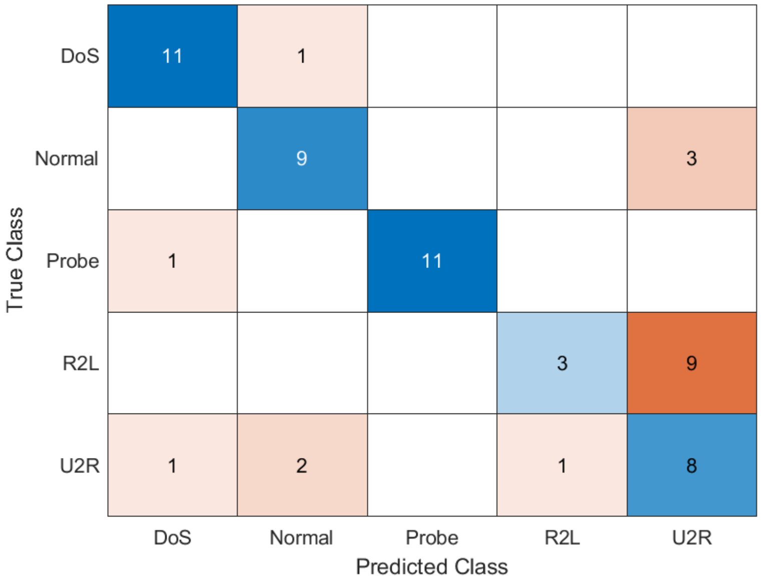


Fig. 1. Confusion matrix of an ANFIS model utilizing Gaussian membership functions

Figure 2 shows the different metrics of the model on the test set. The model accuracy is 70%. The total precision is found to be 75%, whereas the maximum precision is found for “Probe” attacks, which is 100%, with no false positive values, and the minimum precision is found for “U2R” attacks.

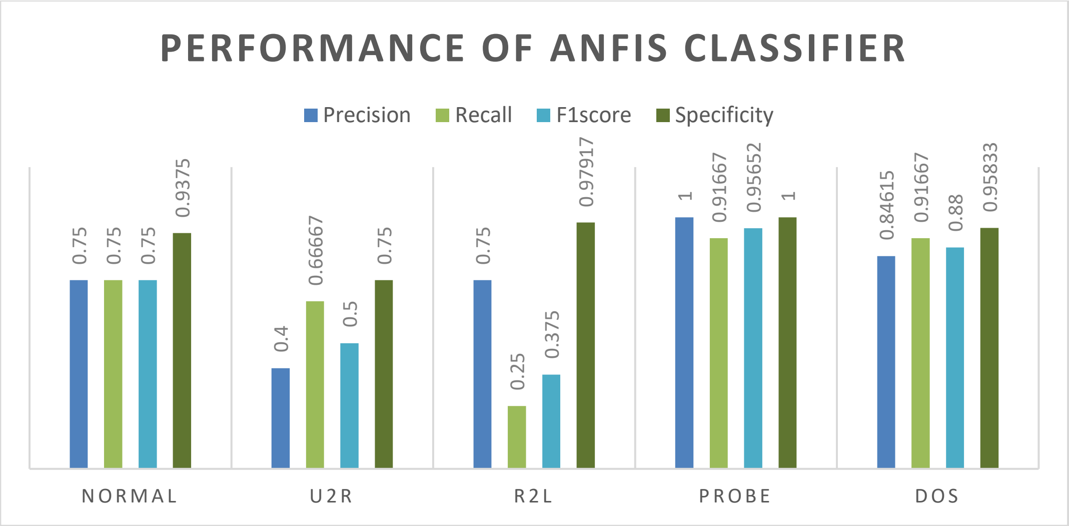
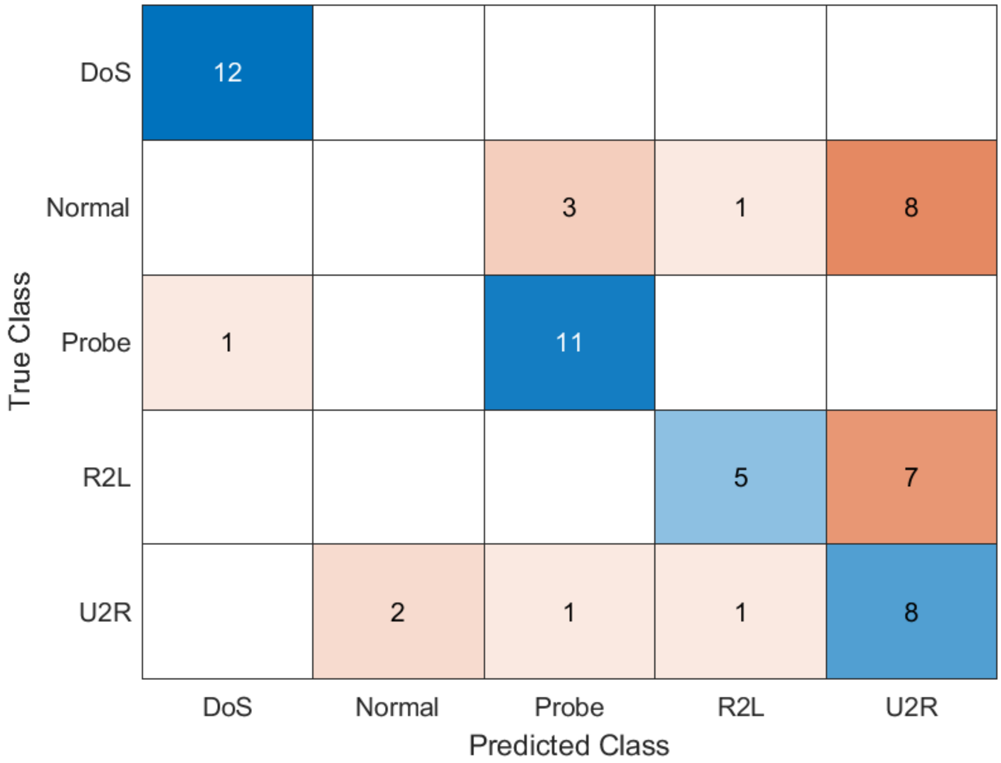


Fig. 2. The performance of the ANFIS model with Gaussian membership functions on the basis of evaluation metrics

On the other hand, the total recall value is 70%, with maximum recall for both the "DoS and Probe" attacks (91.7%) compared with 25% for the R2L attacks. Similarly, the total F1 score is 69%, with a maximum value of 95.6% for the Probe class and a minimum of 37.5% for R2L attacks. The model's specificity is 92.5%, with 100% and 75% specificity for Probe and U2R attacks, respectively.

To further analyse the performance of the ANFIS model, two machine learning models are trained using the same amount of data. Those models are multilayer perceptron and decision tree models. Compared with the ANFIS model, the two models have lower overall performance. The MLP has a total accuracy of 60%. The confusion matrix in Figure 3 shows that the model is not able to predict any "Normal" class correctly. However, it correctly predicted all DoS attacks with a 96% F1 score (92% precision and 100% recall), as shown in Figure 4.



	DoS	Normal	Probe	R2L	U2R
DoS	12				
Normal			3	1	8
Probe	1		11		
R2L				5	7
U2R		2	1	1	8

Fig. 3. MLP model confusion matrix

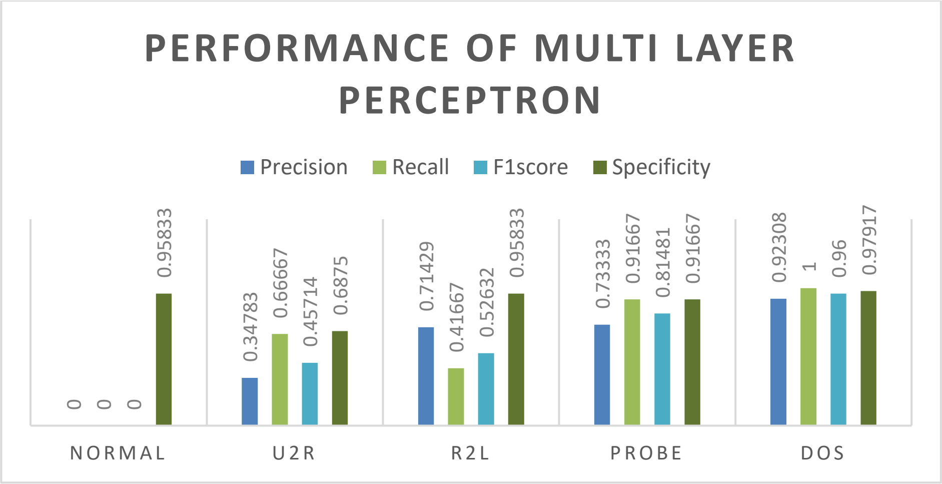
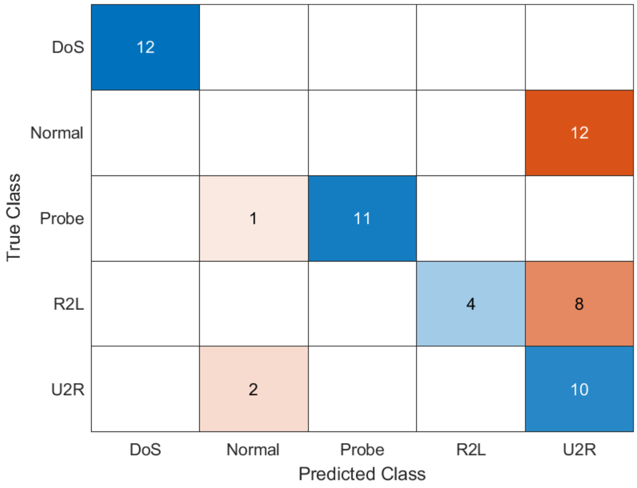


Fig. 4. MLP model evaluation metrics

Moreover, DTs have similar behaviours as those of the MLP, as shown in Figure 5 and Figure 6. However, DT predicted all the “Normal” attacks as U2R attacks. On the other hand, its performance in classifying the “DoS” attacks is the best, with no true negative false positive predictions. In addition, its ability to find “probe” attacks is also similar to that of ANFIS.



	DoS	Normal	Probe	R2L	U2R
DoS	12				
Normal					12
Probe		1	11		
R2L				4	8
U2R		2			10

Fig. 5. DT model confusion matrix

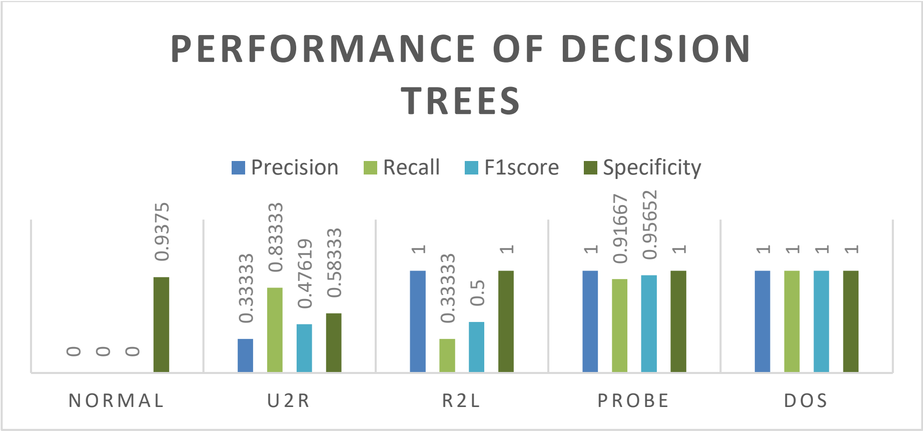


Fig. 6. DT model evaluation metrics

Notably, ANFIS outperforms the MLP and DT algorithms for this small amount of data, which is expected, as machine learning techniques are data hungry techniques, especially artificial neural networks and deep learning. Therefore, this result is valid only for small amounts of data and can be completely different when big data are used.

5. CONCLUSION

The present research integrates the ANFIS approach with an IDS, creating a perfect and more precise amalgam for network security. The developed system is evaluated on the KDD'99 dataset. This step started with feature selection, which was applied to identify the five most relevant inputs, reducing the computational cost and enabling efficient model training. Then, ANFIS is trained via different membership functions, such as Gaussian, triangular, bell-shaped, and sigmoidal functions, and the Gaussian MF is found to achieve the best results. Furthermore, this research proves useful in categorizing network data into malicious and normal data after the adaptive neuro-fuzzy inference system (ANFIS) is utilized as a classifier. Using the KDD99. Another objective has been fulfilled after comparing ANFIS with different approaches to machine learning. Here, ANFIS is compared with two different machine learning techniques, namely, decision tree and multilayer perceptron, and is found to outperform these techniques. On the basis of different evaluation metrics, ANFIS can detect all attack types with 70% accuracy, whereas the other ML techniques fail to classify the “normal” class. This work is important for developing efficient real-time intrusion detection systems, whereas machines with higher capacities can be utilized to train more complicated models with more data.

Funding

The authors had no institutional or sponsor support.

Data availability statement: KDD’99 is used in this study. It is available online. “KDD Cup 1999 Data.” http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed Jan. 04, 2023).

Conflicts of interest

The authors’ disclosure statement confirms the absence of any conflicts of interest.

References

[1] F. Ahmadi, Sonia, G. Gupta, S. R. Zahra, P. Baglat, and P. Thakur, “Multi-factor biometric authentication approach for fog computing to ensure security perspective,” In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development, INDIACom 2021, no. June, pp. 172–176, 2021.

[2] P. Tahiri, S. Sonia, P. Jain, G. Gupta, W. Salehi, and S. Tajjour, “An Estimation of Machine Learning Approaches for Intrusion Detection System,” In 2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), IEEE, Mar. 2021, pp. 343–348, 2021.

[3] F. Akram, D. Liu, P. Zhao, N. Kryvinska, S. Abbas, and M. Rizwan, “Trustworthy Intrusion Detection in E-Healthcare Systems,” Front Public Health, vol. 9, p. 788347, 2021.

[4] A. Alsharef, K. Aggarwal, Sonia, M. Kumar, and A. Mishra, “Review of ML and AutoML solutions to forecast time-series data,” *Archives of Computational Methods in Engineering*, vol. 29, no. 7, pp.5297-5311, 2022.

[5] B. A. Bensaber, C. G. P. Diaz, and Y. Lahrouni, “Design and modeling an Adaptive Neuro-Fuzzy Inference System (ANFIS) for the prediction of a security index in VANET,” *Journal of Computational Science*, vol.47, pp.101234, 2020.

[6] M. Bhakuni, K. Kumar, Sonia, C. Iwendi, and A. Singh, “Evolution and evaluation: Sarcasm analysis for twitter data using sentiment analysis,” *Journal of Sensors*, vol. 2022, no. 1, pp.6287559, 2022.

[7] I. Bala, I. A. Pindoo, M. M. Mijwil, M. Abotaleb, and W. Yundong, “Ensuring Security and Privacy in Healthcare Systems: A Review Exploring Challenges, Solutions, Future Trends, and the Practical Applications of Artificial Intelligence,” *Jordan Medical Journal*, vol.58, no.2, pp.250-270, 2024.

[8] A. Bashab, A.O. Ibrahim, I.A. Tarigo Hashem, K. Aggarwal, F. Mukhlif, F.A. Ghaleb, and A. Abdelmaboud, Optimization Techniques in University Timetabling Problem: Constraints, Methodologies, Benchmarks, and Open Issues. Computers, Materials & Continua, vol. 74, no. 3, 2023

[9] S. Gamage and J. Samarabandu, “Deep learning methods in network intrusion detection: A survey and an objective comparison,” *Journal of Network and Computer Applications*, vol. 169, p. 102767, 2020.

[10] Z. Ahmad, A. S. Khan, C. W. Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and deep learning approaches,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, pp. 1–29, 2021.

[11] H. I. H. Alsaadi, R. M. ALmuttari, O. N. Ucan, and O. Bayat, “An adapting soft computing model for intrusion detection system,” *Computational Intelligence*, vol. 38, no. 3, pp. 855–875, 2022.

[12] D. Karaboga and E. Kaya, “Adaptive network based fuzzy inference system (ANFIS) training approaches: a comprehensive survey,” *Artificial Intelligence Review*, vol.52, pp. 2263–2293, 2018

[13] Y. Zhang, W. Lee, and Y. A. Huang, “Intrusion detection techniques for mobile wireless networks,” *Wireless Networks*, vol. 9, no. 5, pp. 545–556, 2003

[14] C. Modi, D. Patel, B. Borisaniya, H. Patel, A. Patel, and M. Rajarajan, “A survey of intrusion detection techniques in Cloud,” *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 42–57, 2013

[15] N. S. M. Hassan, “Using Of Neuro-Fuzzy Classifier for Intrusion Detection Systems,” vol. 5, no. 2001963. C4I JOURNAL, pp. 46–61, Jan. 01, 2021. Accessed: Aug. 14, 2023. [Online]. Available: https://sid.ir/paper/954986/en

[16] A. N. Toosi, M. Kahani, and R. Monsefi, “Network intrusion detection based on Neuro-Fuzzy classification,” In 2006 International Conference on Computing and Informatics, ICOCI ’06, 2006.

[17] A. Midzic, Z. Avdagic, and S. Omanovic, “Intrusion detection system modeling based on neural networks and fuzzy logic,” In INES 2016 - 20th Jubilee IEEE International Conference on Intelligent Engineering Systems, Proceedings, pp. 189–194, 2016.

[18] S. Manimurugan, A. q. Majdi, M. Mohmmed, C. Narmatha, and R. Varatharajan, “Intrusion detection in networks using crow search optimization algorithm with adaptive neuro-fuzzy inference system,” *Microprocess Microsyst*, vol. 79, p. 103261, 2020

[19] S. Rahman, M. Ahmed, and M. S. Kaiser, “ANFIS based cyber physical attack detection system,” 2016 5th International Conference on Informatics, Electronics and Vision, ICIEV 2016, pp. 944–948,2016.

[20] “KDD Cup 1999 Data.” http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html (accessed Jan. 04, 2023).

[21] D.D.Solomon, Sonia, K. Kumar, K. Kanwar, S. Iyer, and M. Kumar, “Extensive review on the role of machine learning for multifactorial genetic disorders prediction,” *Archives of Computational Methods in Engineering*, vol. 31, no. 2, pp.623-640, 2024.

[22] R. Mehta, K. Aggarwal, D. Koundal, A. Alhudhaif, and K. Polat, “Markov features based DTCWS algorithm for online image forgery detection using ensemble classifier in the pandemic,” *Expert Systems with Applications*, vol.185, p.115630, 2021.

[23] D. Zaman and M. Mazinani, “Cybersecurity in Smart Grids: Protecting Critical Infrastructure from Cyber Attacks”, SHIFRA, vol. 2023, pp. 86–94, Aug. 2023, doi: 10.70470/SHIFRA/2023/010.

[24] J. S. R. Jang, “ANFIS: Adaptive-Network-Based Fuzzy Inference System,” *IEEE Transactions on Systems*, vol. 23, no. 3, pp.665–685, 1993.

[25] K. Aggarwal, M.S. Bhamrah, and H.S. Ryait, The identification of liver cirrhosis with modified LBP grayscaling and Otsu binarization. SpringerPlus, vol. 5, pp. 1-15, 2016.

[26] “MATLAB Documentation.” https://www.mathworks.com/help/matlab/ (accessed Aug. 14, 2023).

[27] S. Tajjour, S. Garg, S. S. Chandel, and D. Sharma, “A novel hybrid artificial neural network technique for the early skin cancer diagnosis using color space conversions of original images,” *International Journal of Imaging Systems and Technology*, vol. 33, no. 1, pp.276-286, 2023

[28] G. Ali, M. M. Mijwil, B. A. Buruga, and M. Abotaleb, “A Comprehensive Review on Cybersecurity Issues and Their Mitigation Measures in FinTech,” Iraqi Journal for Computer Science and Mathematics, vol.5, no.3, pp.45-91, 2024.

[29] A. Desai and M. Desai, “A Review of the State of Cybersecurity in the Healthcare Industry and Propose Security Controls,” *Mesopotamian Journal of Artificial Intelligence in Healthcare*, vol.2023, pp.82–84, 2023

[30] M. M. Mijwil, M. Gök, R. Doshi, K. K. Hiran, and I. Kösesoy, “Utilizing Artificial Intelligence Techniques to Improve the Performance of Wireless Nodes,” In Applications of Artificial Intelligence in Wireless Communication Systems,, pp.150-162, June 2023.

[31] A. Alsharef, Sonia, M. Arora, and K. Aggarwal, “Predicting time-series data using linear and deep learning models—an experimental study,” In Data, Engineering and Applications: Select Proceedings of IDEA 2021 (pp. 505-516). Singapore: Springer Nature Singapore

[32] A. I. Gide and A. A. Mu’azu, “A Real-Time Intrusion Detection System for DoS/DDoS Attack Classification in IoT Networks Using KNN-Neural Network Hybrid Technique ”, BJIoT, vol. 2024, pp. 60–69, Jul. 2024.

[33] A.M. Mahmood and I. Avcı, “Cybersecurity Defence Mechanism Against DDoS Attack with Explainability,” *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp.278-90, 2024.

[34] D.S. Ahmed, A.A. Abdulhameed and M.T. Gaata, “A Systematic Literature Review on Cyber Attack Detection in Software-Define Networking (SDN),” *Mesopotamian Journal of CyberSecurity*, vol. 4, no. 3, pp.86-135, 2024.

[35] G. Amirthayogam, N. Kumaran, S. Gopalakrishnan, K. Brito, S. RaviChand, and S. B. Choubey, “Integrating Behavioral Analytics and Intrusion Detection Systems to Protect Critical Infrastructure and Smart Cities”, BJN, vol. 2024, pp. 88–97, Jul. 2024.