Journal of Information Systems Engineering and Management
2025, 10(27s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Security Evaluation of Soft Computing Intrusion Detection Systems (Ids) with Neural Networks

Osamah Kareem Hadi[1], Alharith A. Abdullah[2]
University of Babylon . College of Information Technology , Information Networks [1,2]
Osamah.hadi@student.uobabylon.edu.iq , alharith@uobabylon.edu.iq

ARTICLE INFO

Received: 23 Dec 2024

Revised: 20 Feb 2025

Accepted:26 Feb 2025

ABSTRACT

With the advancement of computer communication technology and the emergence of soft computing networks, many defense strategies have emerged to enhance network security and improve the effectiveness of intrusion detection systems (IDS) against cyber-attacks, including distributed denial of service (DDoS) attacks. This research aims to propose artificial neural network technology as a tool for network security assessment, which contributes to reducing human intervention and increasing the efficiency of detection processes to achieve accurate and fast results. Two data sets were used to train and test the proposed model, and the results showed that the model achieves a detection accuracy of up to 98.194%, with a mean square error (MSE) of 0.161%. These results confirm the effectiveness and efficiency of the technology in quickly detecting and responding to threats, which enhances network security and increases the ability of systems to face cyber challenges.

Keywords: soft computing, Cyber-security, Intrusion Detection Systems (IDSs), Artificial Neural Networks (ANNs), Distributed Denial of Service (DDoS).

INTRODUCTION

Soft computing is a fundamental branch of computing science that focuses on solving complex and traditional problems through models that mimic the workings of the human brain[1]. Soft computing relies on a variety of techniques, such as artificial neural networks (ANN), fuzzy logic, and evolutionary algorithms, making it an effective tool for dealing with uncertainty and complexity in data. With the increasing complexity and sophistication of cyber-attacks in the modern era, the importance of soft computing emerges as a means of enhancing the security of information systems[2].

Distributed denial of service (DDoS) attacks is one of the common cyber threats that negatively affect many systems and networks. These attacks rely on exploiting weaknesses in the system by sending huge amounts of requests, which leads to a disruption of service. In this context, the importance of soft computing becomes clear, as neural networks can be used to enhance the ability of intrusion detection systems (IDS) to recognize attack behaviors[3].

ANNs are characterized by their ability to learn from historical data and detect abnormal behavioral patterns, enabling them to distinguish normal behavior from malicious behavior. With these capabilities, neural networks can adapt to rapid changes in user behavior and the evolution of attack methods, enhancing the ability to detect threats, such as DDoS attacks, early and effectively counter them. In fact, ANNs algorithm consist of several layers and components as shown in the Figure1 [4] .

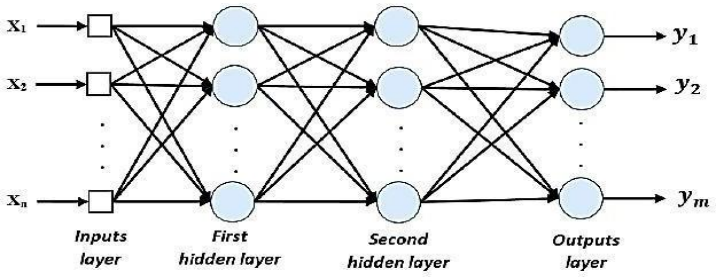


Figure 1: ANNs layers and main components [5].

The details of the ANN algorithm layers are demonstrated as follows:

- Input Layer: Receives input data from the surrounding environment.
- Hidden Layers: Process information through a set of neurons, where each cell processes the data and outputs it to the next cell. The work of these neurons depends on specific weights, allowing them to learn from the input data and adjust the weights based on the calculated errors.
- Output Layer: Provides the final results after processing the data[6].

This architecture is effective in tackling complex problems, such as detecting cyber-attacks, as it contributes to improving the accuracy and efficiency of intrusion detection systems (IDS) by recognizing unusual patterns [7]. In this paper, we propose an ANN architecture specifically designed for detecting DDoS attacks in a soft computing environment. Two datasets are used to build and test the model, allowing for comprehensive performance evaluation.

This research consists of several main components, as the section 2 reviews the literature related to intrusion detection systems and soft computing, and analyzes the performance of neural networks in detecting attacks. In the section 3, the proposed methodology will be presented, while the section 4 discusses the results and recommendations drawn, and the research concludes with conclusions in the section 5.

LITERATURE REVIEW

By reviewing previous studies and the latest scientific articles that addressed the topic of this study, we can summarize some of the researchers' contributions and their prominent methods as follows:

(Eissa Alreshidi et al., 2019) [8] analyzed a group of prominent cloud service providers that were used to support this evaluation. This study aims to summarize the prominent cloud service providers taking into account the following criteria: a) structure and architecture, b) technological developments, c) developer environment and support, d) security, and e) costs and pricing plans. In addition to collecting information, the study provided a summary of the prominent cloud service providers. The results showed that there are differences between service providers regarding the aforementioned considerations, but they adopt different strategies in the services they provide to their customers.

(Dheyab Salman Ibrahim et al., 2019) [9] Studied methods to prevent unauthorized access to data. This solution relies on hiding sensitive encrypted data within images and storing them in cloud data centers as needed. The main challenge in cloud computing is data protection as this data can be accessed, retrieved or modified by unauthorized individuals or devices. Therefore, data protection is of utmost importance. To increase data security in cloud data centers, plans have been developed to ensure security by using multi-stage encryption techniques (DES and RSA) in addition to using steganography techniques using LSB.

(Hussam Alhadawi et al., 2019) [10] Reviewed a research paper that addressed the challenges related to cloud computing security with a focus on the security requirements in different types of cloud computing (SaaS, PaaS, IaaS). While (Jaydip Kumar et al., 2020) [11] proposed a project based on robust algorithms to protect data in cloud computing. This research emphasized that cloud computing is affected by major challenges related to managing huge amounts of data (text, audio, video, etc.), which necessitates the need to protect data using multiple techniques.

For his part, (Intisar Salem Hamed Al-Mandhari et al., 2020)[12]explained through a detailed study the main reasons for the noticeable shortcomings of some popular classifiers in detecting weak classes of attacks. The study indicated that the KDD Cup '99 dataset suffers from an increase in some types of data due to the diverse nature of the domain, while some attacks remain very frequent and others are rare, leading to an imbalance in the distribution of data. The problem of the study or research gap lies in the absence of a specific technique for detecting counterattacks in networks that rely on soft computing, which makes it difficult to improve IDS and ensure network security. The multiplicity and diversity of attack methods also represent an additional challenge that makes it difficult to find a comprehensive defense technique. This study aims to use ANN techniques as an effective means of detecting and deterring random attacks, given the ability of neural network algorithms to train and analyze the input data.

In 2023, M. Sunil Kumar, et., al.[13], analyzed a weight optimized deep learning model for cluster-based intrusion detection system. This study discusses the optimization concept that optimally tunes the weight of DBN by introducing a new hybrid optimization algorithm called Cuckoo Insisted Lion Algorithm, which is a combination of Cuckoo Search and Lion Algorithm. The overall performance of this recommended model is verified in relation to certain prediction parameters in comparison to the other modernization models. In wireless sensor networks (WSNs), the implemented conventional intrusion detection frameworks require more energy and computation time,

which affects the lifespan of the WSN. Additionally, a few of these models generate a significant volume of IDS traffic, which causes congestion and restricts the bandwidth of the WSN. This paper presents a new hierarchical type intrusion detection system for identifying the malicious sensor nodes.

In 2023, Aman Goyal, et., al.[14], presented a study that employed dense artificial neural networks (Deep-ANN) to create deep learning (DL) algorithms for IDS in wireless sensor networks (WSNs). The development of new concepts and techniques is required to increase the overall security of WSNs. The primary concern with WSNs is intrusion prevention. The accuracy of the model created using Ann was the greatest, at 96.45 percent, when comparing the findings of this study with those of earlier models. The ANN model performs better than other machine learning models that are currently on the market because to its higher recall accuracy and F1 scores of 96.38, 98.94, and 97.64.

METHODOLOGY

In this Part, the proposed model of the soft computer security architecture of IDS will be evaluated to identify digital malware and identify attack flows. Distributed Denial of Service (DDoS) execution flows will be re-analyzed with the help of AI techniques (PC-based intelligence), using Artificial

Neural Network ANN algorithms by training the inputs to achieve the best detection of malicious attack models. A pivotal simulation of the soft computing network architecture will be designed through information sets that must handle dual and basic types of data, which are information (valid) data sets, and also auxiliary are intrusion (malware) data sets. Different network simulators provide many types of required data. For this work, the required data for sent information and attack flows will be prepared through two accredited global data sites, namely (kaggle.com and github.com), in addition to the possibility of processing the uploaded data using MATLAB application tools and services efficient software.

1.1 Methodology Steps

Through the proposed model, the soft PC security engineering of IDS will be assessed to distinguish advanced malware and recognize assault streams. Distributed Denial of Service (DDoS) execution streams will be re-dissected with the assistance of computer-based intelligence methods (PC-based intelligence), utilizing ANN algorithms via preparing the contributions to accomplish the best detection of noxious assault models. The methodology flow chart of the proposed model is shown in Figure 2.

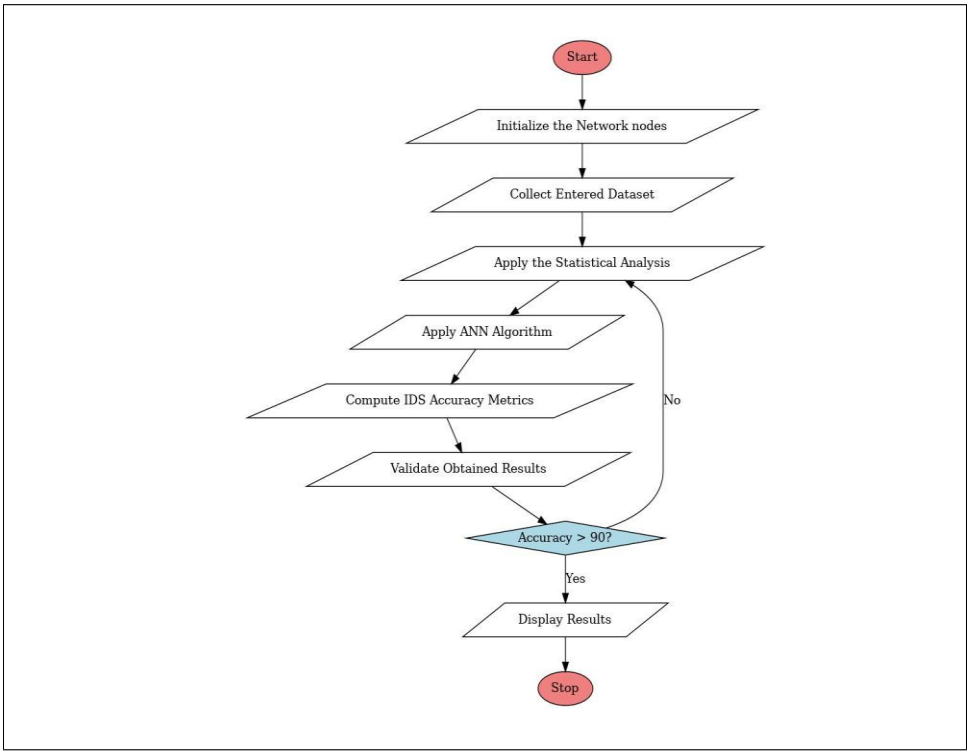


Figure 2: The proposed soft computing cloud detection and attacks prevention IDS system flow chart.

As one might observe through the proposed model flow diagram presented in Figure 2, the executed model will enter the needed (TCP/IP) dataset stream. There will be a checkup to choose if such flood is the referenced dataset stream (non-burden); in the event that it isn't, route will be dismissed; expecting it is, the input info stream will be delivered

off the model (i.e., it will not be obstructed). The recorded dataset stream will be inhibited in the going with move to check whether they include an assault stream. The recorded info will be taken care of, and distinct as intrusion info, also entrance will be dismissed in the event that there is a positive assault trajectory control. The model will be finished with pure info also outdoors assault samples if

this isn't true. The data streams will then, at that point, be stood out from other generally average activities for extra affirmation. The data that went into the model will similarly be analyzed subsequent to beginning affirmation using statistical assessment units (autocorrelation check, and so on) and a while later passing questionable data to the artificial intelligence algorithm to get ready it and limit threatening and bothersome streams.

1.2 The Proposed ANN Architecture

The proposed neural model will exhibit the arrangement cycle of the Artificial Neural Network (ANN) calculation on the information bundle tests (n = 300 examples) so it tends to be contrasted and the first preparation concentrate on as far as progression rates as well as MSE boundaries. To make sense of the instrument of ANN calculation, the information data is the first data, which is well defined for the communicated data stream. This information is instated by arranging it in the principal layer of the ANN calculation with the goal that it is prepared for preparing. Figure 3 presents the last construction of the planned ANN technique.

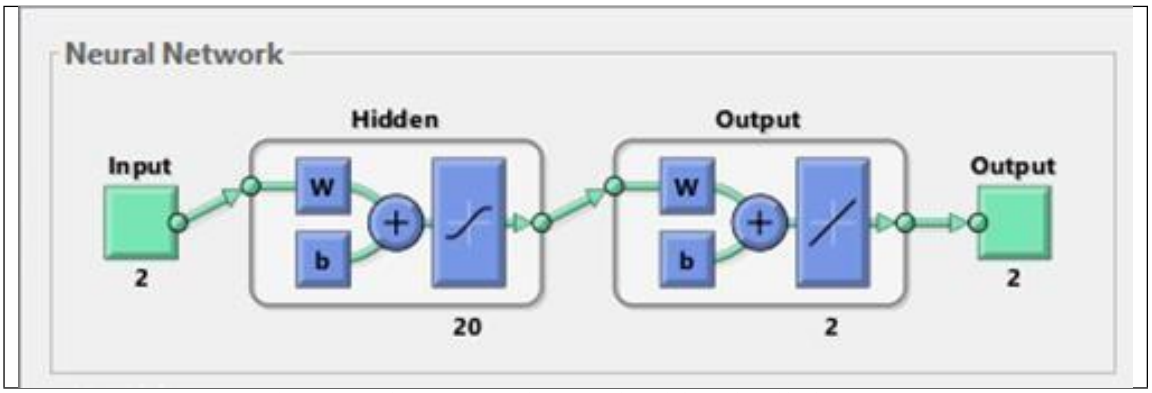


Figure 3: The proposed ANN algorithm detailed structure.

After giving it an underlying name, this data is entered into the appropriate ANN computation, and it is then enhanced by adding additional encoding that depends on the underlying mark to increase the characterization accuracy. Here, feature filters are incorporated into the convolutional neural network computation, which use unique, sophisticated characteristics to represent each emphasis's form or image. Therefore, based on the degree of proximity, the number of filters, and the precision of the mathematical attributes assigned to them, we collect comparative frequencies with at least one filter. After passing through the Relu layer, the feature filters' numerical upsides are reduced, and these features are then collected into the pooling layer. In order to prepare the calculation and concentrate the results that can be compared and the required classifiers, the data is given the inward weight layers after these methods. The incorrect results are then added up, and the weights and preparation interaction are rehashed several times until convergence occurs and the best match and the fewest errors exist.

Later being assigned an underlying mark between 0 and 1, this data is entered into the order algorithms. In order to improve the correctness of the arrangement, it is then redesigned by adding more code that depends on the underlying name. By separating the important comments separately in one group and the irrelevant comments in another, the order algorithms operate according to their expertise and the arrangement component is delegated to them. For example, feature filters that use the shape or value of each information test to display it with unique numerical features are integrated into the convolutional neural network computation. Therefore, based on the degree of similarity, the number of filters, and the precision of the computerized attributes assigned to them, we compile similar samples with at least one filter. After passing through the Relu Layer, the number of upsides of the feature filters is reduced. These features are then

compiled in the pooling layer. Following these methods, layers of inner weights are applied to the data in order to prepare the calculation, concentrate the results that can be measured by the required classifiers, and determine how much error to make when updating the weights and repeating the preparation cycle a few times until convergence occurs and the best match and the fewest errors are obtained.

1.3 The Employed Dataset

In this study, various network simulators produce numerous kinds of needed dataset, in which the required dataset for sent information and attack flows will be prepared through two accredited global data sites, namely (kaggle.com

and github.com).[15][16][17] Also, there will be a possibility of processing the uploaded data using MATLAB application tools and services with efficient software.

SIMULATION RESULTS

In this section, the proposed soft computing technique for IDS is implemented and simulated using MATLAB 2020b. The m-file scripts are utilized to identify and detect network intrusions, with a particular focus on DDoS flood attacks. The technique relies on artificial intelligence (AI) methods to illustrate the impact of a DDoS attack on a TCP packet dataset, and explore ways to identify and mitigate such attacks using statistical methods such as skewness, drift, and autocorrelation function (ACF). In addition, ANN are used to improve the detection capability of the system.

The proposed framework is simulated and applied to 1000-part TCP/IP datasets, which are regularized and weighted using MATLAB scripts. Figure 4 shows the TCP/IP datasets loaded into the IDS simulator, where the peaks of the TCP/IP sample flow appear as multiple mixed sinusoidal functions, depicted in a bar stream. The effect of arbitrary assault stream is also simulated utilizing MATLAB built in functions.

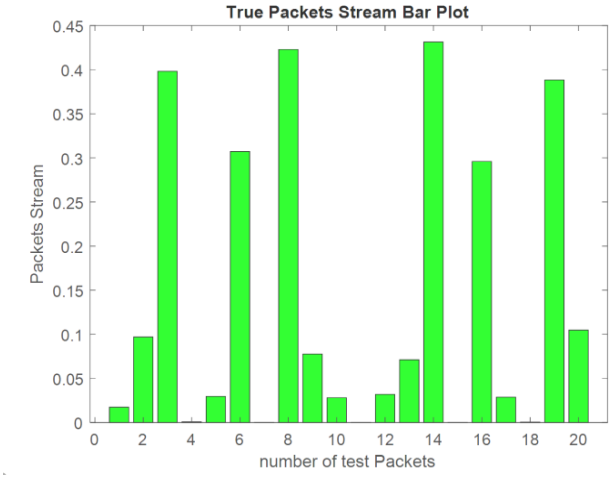


Figure 4: The TCP/IP info packets employed to the simulated IDS software

In Figure 5, the random attack stream is distributed over time using the same number of packet samples, N = 1000. The figure shows the random attack stream as a bar graph, which illustrates how random intrusion attack streams are added to the dataset. This allows us to better understand the impact of these attacks on the data flow.

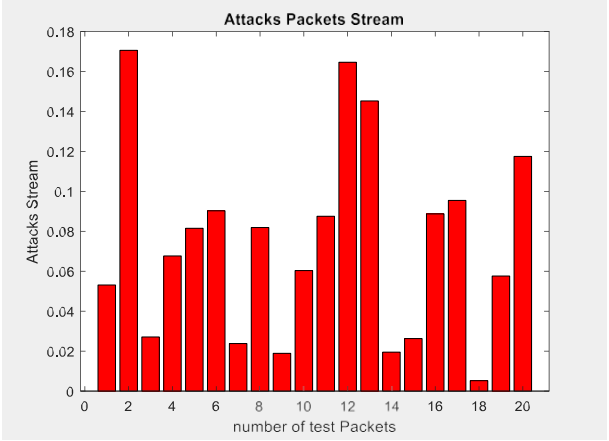


Figure 5: The random attack stream packets employed in the simulated IDS software

Figure 6 shows that randomly generated intrusion packet streams, represented by red bars, significantly distort the original data flow, represented by green. This interaction reflects the behavior of a DDoS attack, emphasizing the need to analyze the combined dataset and intrusion stream. The developed hybrid model uses statistical methods and artificial neural networks to detect malware, where the statistical analysis involves measuring the autocorrelation function, skewness (S), and skewness (K) for each input stream, dataset, intrusion, and corrupted DDoS stream.

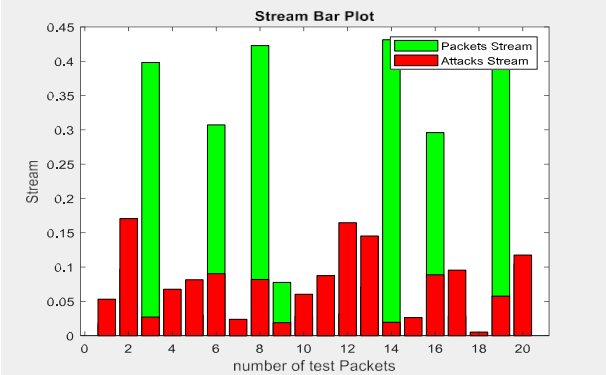
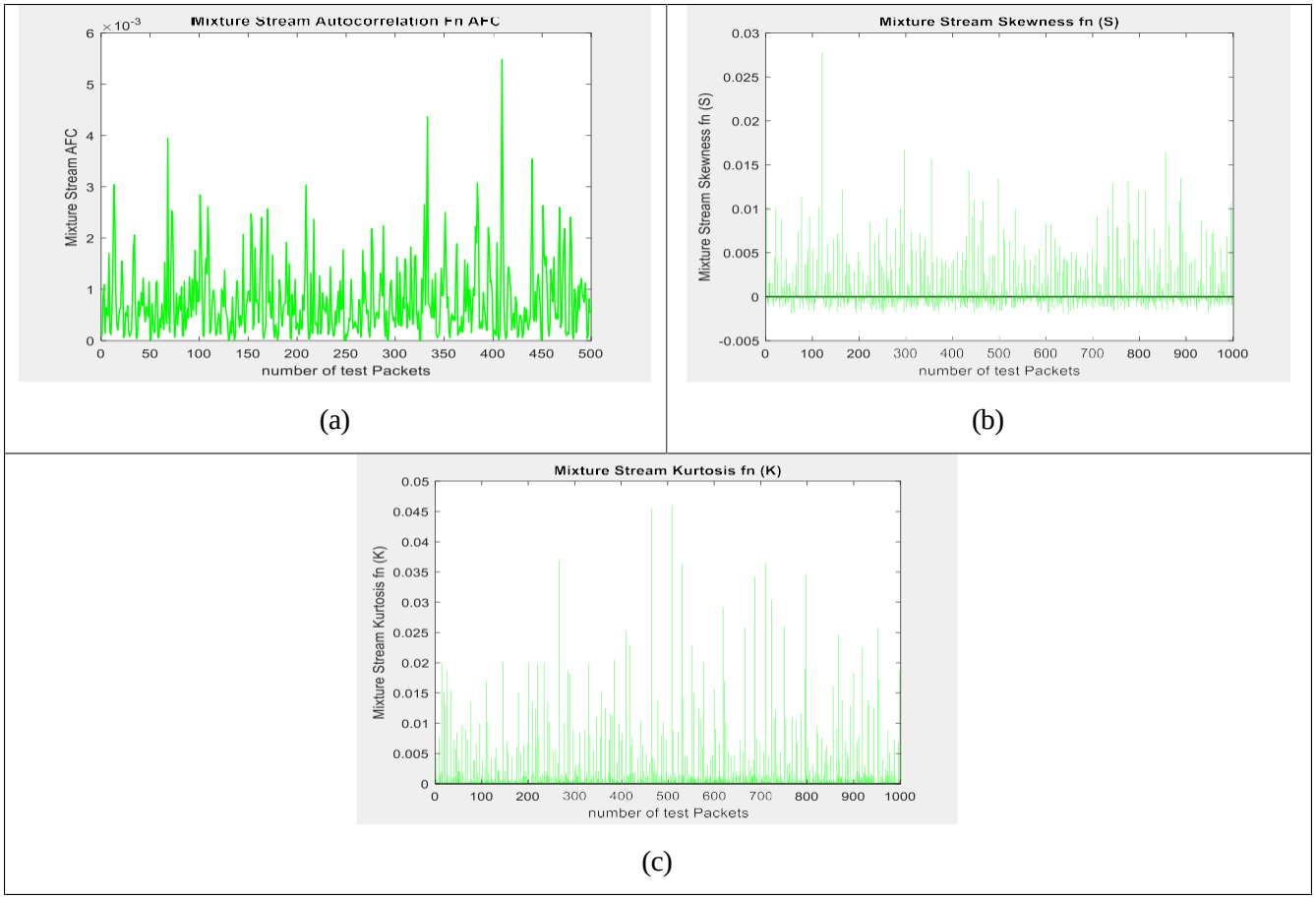


Figure 6: The mixed data with random attack stream packets employed in the simulated IDS software

Figure 7 (a-c) presents the results of statistical tests applied to the hybrid DDoS model with data: (a) autocorrelation function (ACF), (b) skewness (S), and (c) skewness (K). Skewness is specifically used to measure the similarity of recurring patterns within a dataset. As Figure (c) highlights, the combined flood (info + assault) skewness is identical to the malware flood skewness, indicating the presence of a cyberattack. This integration of statistical results enhances the robustness of the proposed model for intrusion detection.

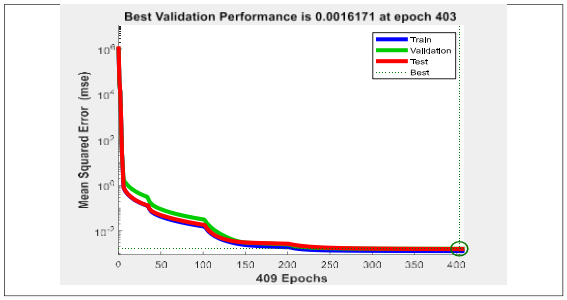


Figures 7: Results of statistical tests of mixed DDoS models with data, (a) Autocorrelation Function (ACF) measure (b) Skewness (S) measure, (c) Kurtosis (K) measure.

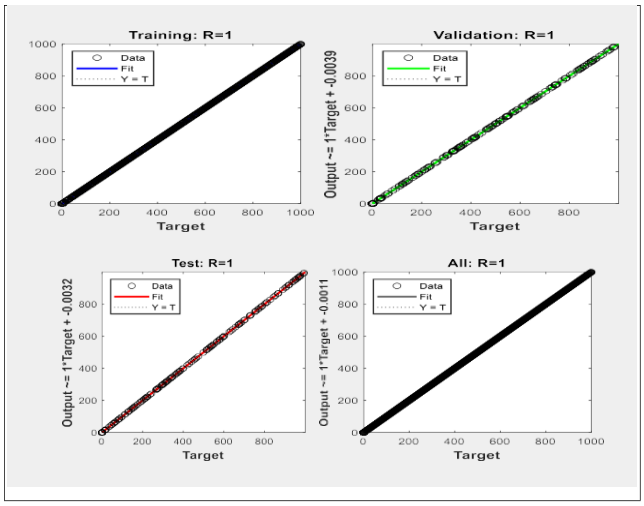
To complete this process, Figure 8 presents the design details of the ANN algorithm, including the training interface (a) and the ANN interface (b). The designed ANN consists of several internal layers with up to 30 neurons, using binary vectors for input and output.

Figure 8: The design details of the ANN algorithm training process interface.

The results presented in Figure 9 (a-b) illustrate the validation metrics of the forward neural network, where a low square error value of 0.00161 was achieved after 403 training epochs, demonstrating the efficiency in detecting and eliminating stealth packets. The forward neural network achieved a gradient of 0.04702 at 409 training epochs, reflecting the effectiveness of training. Moreover, the error graph shows minimal error values, highlighting the ability of the artificial neural network to distinguish between real data and intrusion packets.



(a)



(b)

Figure 9: The measuring metrics of the validation, training, and testing samples obtained from the ANN technique examination program, (a) MSE, (b) Regression (ROC).

Finally, Figure 10 shows the results of the ANN in detecting attack packets. The attack packets, shown in blue, closely match the original data stream, shown in green, confirming the success of the ANN in identifying and blocking attack packets. The error samples, shown in red, also confirm the accuracy and efficiency of the network in detecting and dealing with attack floods.

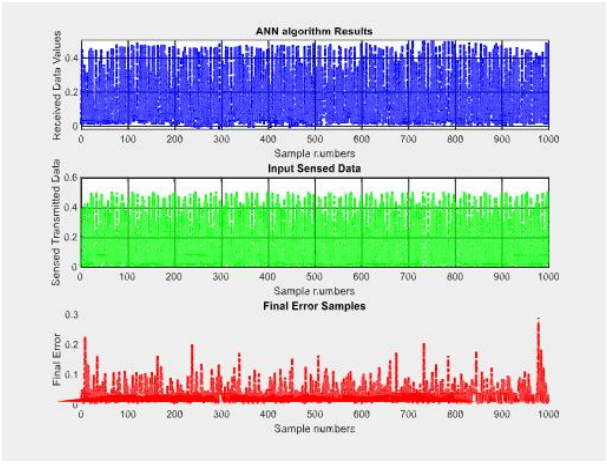


Figure 10: The final achieved results using the ANN attacks detection strategy, (a) ANN resulting data, (b) Input sensed data,

(c) Error samples.

The performance metrics of the ANN algorithm are summarized in Table 1, which lists metrics such as accuracy, privacy, sensitivity, precision, and F-score.

Table 1: The performance measures of the proposed ANN model.

Metric Values		*Accuracy*	*Specificity*	*Sensitivity*	*Precision*	*F score*
TP	0.96758	99.23%	97.94%	97.98%	98.17%	98.25%
TN	0.97478					
FP	0.01901					
FN	0.01971					

In conclusion, the ANN algorithm showed strong performance in the intrusion detection protocol, as shown in Table 2. The performance metrics indicate the success of the proposed soft computing model in detecting and mitigating DDoS attacks and other cyber-attacks.

Table 2: Performance results of the IDS soft computing ANN model.

Measurements Type	**ANN Algorithm** At (407) epoch
Mean Square Error (MSE) Performance	0.161 % (403) epoch
Training States	0.04702
Error Histogram	0.00732 at 700 samples
Regression (ROC)	100%

CONCLUSION

In this paper, we present a comprehensive framework for soft processing network improvements to enhance network security and develop IDS. We adopt a hybrid approach that combines statistical analysis and ANN algorithm to address the challenges associated with cybersecurity. The effectiveness of neural networks in countering attacks is analyzed, with a focus on the statistical analysis tool. The developed detection systems showed excellent results, with the ANN algorithm achieving MSE value of 0.00161 and a slope of 0.04702 after 409 training epochs on a dataset of 1000 samples. The ROC curve also showed a good balance between target values and results, reflecting the effectiveness of the system in dealing with DoS attack flows.

REFERENCES

[1] J. Fei, and H. Xu, "Assessing computer network security with fuzzy analytic hierarchy process." 2010 2nd International Conference on Advanced Computer Control. Vol. 5. IEEE, 2010.

[2] M. Andre, and R. Astudillo, "From softmax to sparsemax: A sparse model of attention and multi-label classification." International Conference on Machine Learning. 2016.

[3] MM. Zahra, MH. Essai, and ARA. Ellah, "Performance functions alternatives of MSE for neural networks learning." International Journal of Engineering Research & Technology (IJERT) 3.1 (2014): 967- 970.

[4] S. Ming, "Computer network security evaluation based on intelligent algorithm." 2017 Sixth International Conference on Future Generation Communication Technologies (FGCT). IEEE, 2017.

[5] S. Liu, and Y. Fang, "Application research in computer network security evaluation based on genetic algorithm." 2012 International Symposium on Instrumentation & Measurement, Sensor Network and Automation (IMSNA). Vol. 2. IEEE, 2012.

[6] R. K. Vigneswaran, R. Vinayakumar, K. P. Soman and P. Poornachandran, "Evaluating Shallow and Deep Neural Networks for Network Intrusion Detection Systems in Cyber Security," *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, Bengaluru, India, 2018, pp. 1-6, doi: 10.1109/ICCCNT.2018.8494096.

[7] Q. Hao, and Y. Xu, "Application Analysis of Neural Network in Computer Network Security Evaluation." system 5.3 (2019).

[8] Eissa Alreshidi, " COMPARATIVE REVIEW OF WELL-KNOWN CLOUD SERVICE PROVIDERS (CSPS)",

Sci.Int.(Lahore),31(1)B,165-170,2019 ISSN 1013-5316; CODEN: SINTE 8 165, January- February.

[9] Dheyab Salman Ibrahim, "Enhancing Cloud Computing Security using Cryptography & Steganography", Iraqi Journal of Information Technology. V.9 N.3. 2019.

[10] Hussam Alhadawi, et. al., " A Review of Challenges and Security Risks of Cloud Computing", Article · March 2017.

[11] Jaydip Kumar, "Cloud Computing Security Issues and Its Challenges": International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-8, Issue-1S4, June 2019.

[12] Oya, S. and F. Kerschbaum. (2021). “Hiding the Access Pattern is Not Enough: Exploiting Search Pattern Leakage in Searchable Encryption”. In: Proceedings of the 30th USENIX Security Symposium (USENIX Security 21).

[13] Sravanthi Godala, M. Sunil Kumar, “A weight optimized deep learning model for cluster-based intrusion detection system”, Optical and Quantum Electronics (2023) 55:1224, https://doi.org/10.1007/s11082-023-05509-x.

[14] Aman Goyal, Sourav Mishra, Dr. Vijay K Chaurasiya, “Intrusion Detection in Wireless Sensor Networks Using Deep Learning”, 2023 4th International Conference for Emerging Technology (INCET) Belgaum, India. May 26-28, 2023

[15] https://www.kaggle.com/code/abhaymudgal/intrusion-detection-system

[16] https://www.kaggle.com/code/girgismicheal/network-intrusion-detection-using-deep-learning\

[17] https://www.kaggle.com/code/dhirajchandak04/network-intrusion-detection