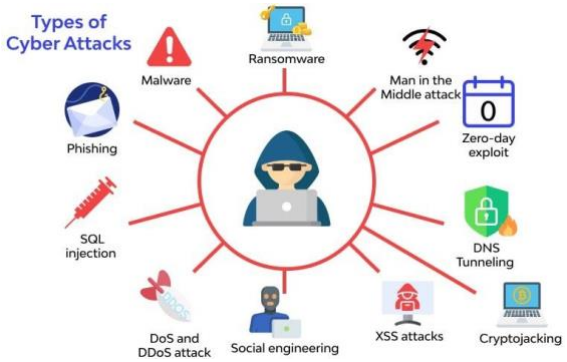
IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 26, Issue 1, Ser. 2 (Jan. – Feb. 2024), PP 16-24
www.iosrjournals.org

Detection Of Cyber-Attacks And Anomalies In Cyber System

Annem Shivaji
Integrated M.Tech Computer Science Engineering Vellore Institue Of Technology Vellore, India

Abstract
As more and more sensitive information is kept and communicated online, cyber attacks and abnormalities in cyber systems have grown to be a major issue for businesses and individuals. Cyber systems are becoming more complicated and interconnected, which leaves them open to a variety of attacks and abnormalities that could seriously harm their reputation and finances.
It's critical to establish reliable techniques for spotting cyberattacks and anomalies in order to reduce these dangers.
This study investigates the detection and analysis of network cyberattacks using soft computing approaches. It examines several strategies, including network traffic detection, classification, clustering, and anomaly analysis, as well as the data sets and methods used in various studies.



Keywords
ANN (Artificial neural network) Fuzzy Logic
Genetic Algorithm Information Security
Automated Process Control Systems Fuzzy rule based system
Epoch Anomalies
Mean Squared Error (MSE)

Date of Submission: 08-01-2024 Date of Acceptance: 18-01-2024

I. Introduction:

This report stresses how new and different cyber threats have emerged as a result of the extensive use of the internet and its integration into vital infrastructure. It highlights how crucial it is for network traffic to be monitored for these dangers by cyber security. This study includes the literature reviews of the studies that we used as references.

In this article, neural networks and fuzzy logic—two commonly used techniques for identifying cyberattacks and anomalies—are discussed. We also go over the drawbacks of each of these approaches and suggest a brand-new model dubbed the AFG model.

The model's MATLAB implementation follows, which demonstrates why it is superior than the alternatives.This study also contain Challenges, recommendations and future research directions for the detection of cyber attacks and anomalies.

II. Literature Review :

1. Soft computing for anomaly detection and prediction to mitigate IoT-based real-time abuse : To recognise and stop potential security threats or resource misuse, anomaly detection and prediction in IoT systems is a crucial responsibility. Using soft computing approaches, which are a collection of computational methods created to approximatively or model complicated and uncertain systems, is one way to deal with these problems.

The application of soft computing approaches for anomaly detection and prediction in IoT systems will be the main topic of the literature review.

IoT systems frequently use artificial neural networks (ANNs) for anomaly detection. For instance, the authors of [1] presented an ANN-based anomaly detection solution for Internet of Things systems by combining an extreme learning machine and an adaptive network-based fuzzy inference system.

The suggested strategy produced a low percentage of false alarms and a high detection accuracy. The authors of [2] suggested a deep belief network-based ANN-based anomaly detection solution for industrial control systems. The suggested strategy produced a low percentage of false alarms and a high detection accuracy.

The suggested strategy produced a low percentage of false alarms and a high detection accuracy.

In [5], the authors proposed a hybrid approach that combines fuzzy logic with ANN for anomaly detection in IoT systems. The suggested strategy produced a low percentage of false alarms and a high detection accuracy.

In [6], the authors proposed a hybrid approach that combines fuzzy logic with ANN for anomaly detection in IoT systems. The suggested strategy produced a low percentage of false alarms and a high detection accuracy.

ANNs and fuzzy logic, in particular, have been extensively used for anomaly detection and prediction in IoT systems, according to the literature. These techniques have demonstrated great detection precision and minimal false alarm occurrence. Additionally proposed and demonstrated to enhance the efficacy of anomaly detection and prediction in IoT systems are hybrid approaches that combine ANNs and fuzzy logic. Identification and prevention of security threats and resource misuse in IoT systems depend on anomaly detection and prediction. Artificial neural networks (ANNs), a type of soft computing approach, are frequently employed for this task and have been found to produce excellent detection accuracy and a low false alarm rate. Performance has also been demonstrated to be enhanced by hybrid approaches combining ANNs.

2. Information security technology for computer networks through classification of cyber-attacks using soft computing algorithms : Network information security technology is a crucial topic of study that has attracted a lot of attention recently. Traditional security measures are showing to be unable to defend networks from these threats as cyberattacks get more complex. The use of soft computing algorithms for the classification of cyber-attacks is one of the solutions that have been suggested to deal with this problem.

A group of computer methods known as "soft computing" includes evolutionary algorithms, artificial neural networks, and fuzzy logic. These strategies work well for tackling issues like uncertainty, imperfect knowledge, and non-linearity that are challenging to solve with conventional strategies.

The use of soft computing techniques for the classification of cyberattacks has been the subject of numerous studies. For instance, one study classified network attacks based on characteristics of network traffic by combining fuzzy logic and artificial neural networks. The findings of this investigation demonstrated that the suggested strategy was highly accurate at identifying various sorts of attacks.

Another study put up an evolutionary algorithm- based classification scheme for cyberattacks.

The framework was put to the test on a dataset of network traffic, and the findings revealed that it was able to detect various sorts of assaults with high accuracy.

In other instances, the use of genetic algorithms for intrusion detection has also been suggested. The outcomes of these experiments have demonstrated that very accurate genetic algorithms can be used to identify and categorise various kinds of cyber- attacks.

The majority of the research points to soft computing techniques as a useful tool for classifying computer network cyberattacks. These algorithms are highly suited for dealing with the complex and dynamic nature of cyber-attacks because they can handle uncertainty, incomplete information, and non- linearity. However, additional investigation is required to assess how well these algorithms operate in practical settings and to create more reliable defences against cyberattacks.

Information security technology for computer networks is a vital area of research that has recently generated a lot of interest due to the increasingly sophisticated cyber-attacks. For the classification of cyberattacks, the use of soft computing techniques has been proposed as a solution. Soft computing, which is ideally suited for dealing with non-linear, uncertain, and incomplete data problems, is a category of computer techniques that includes fuzzy logic, artificial neural networks, and evolutionary algorithms. Studies have shown that these techniques can classify cyber-attacks with a high degree of accuracy. To determine how well these algorithms perform in real-world scenarios and to develop more dependable defences against cyberattacks, more research is necessary.

3. Using GRU neural network for cyber-attack detection in automated process control systems : Automated Process Control Systems (APCS) are widely utilised in many different sectors, including manufacturing, transportation, and energy. These systems' internet integration has nevertheless also rendered them susceptible to

cyber-attacks, which can result in serious malfunctions and safety risks. Therefore, it is essential to create efficient techniques for APCS cyberattack detection.

The use of Gated Recurrent Unit (GRU) neural networks for cyber-attack detection in APCS has been suggested as a solution to this problem. In order to handle sequential data, such as network traffic, which is frequently utilised in cyber-attack detection, GRU is a form of Recurrent Neural Network (RNN) architecture.

Another study put forth a GRU neural network-based approach for APCS cyberattack detection. The framework was put to the test on an artificial power system, and the findings showed that it was successful in identifying and categorising cyberattacks there.

Additionally, some studies have suggested using GRU neural networks for anomaly detection in SCADA systems. The outcomes of these studies have shown that these networks can be used to accurately identify and categorise various cyberattack types while also offering a quick way to spot attacks.

Overall, the research points to GRU neural networks as a promising method for detecting cyberattacks in APCS. These neural networks operate well with sequential data, like network traffic, which is frequently used to identify cyberattacks. However, additional investigation is required to assess how well GRU neural networks perform in practical situations and to create more reliable defences against cyber- attacks. Automated Process Control Systems (APCS) are vulnerable to cyber assaults since they are used extensively across many industries. This issue has been addressed by the use of Gated Recurrent Unit (GRU) neural networks in APCS for cyber-attack detection. GRU is a type of recurrent neural network (RNN) architecture designed to handle sequential input, such as network traffic, which is widely used in cyber-attack detection. Research has shown that GRU neural networks are capable of correctly identifying and classifying a variety of cyber-attacks in APCS.

4. Evaluation of Cybersecurity Data Set Characteristics for Their Applicability to Neural Networks Algorithms Detecting Cybersecurity Anomalies : Since they have proven to be successful in spotting patterns and abnormalities in huge datasets, neural network algorithms have drawn a lot of attention in recent years as a means of detecting cybersecurity anomalies. The quality and characteristics of the cybersecurity dataset used for training and testing, however, affect how effective these algorithms are.

As a result, a crucial area of research is the evaluation of cybersecurity dataset properties for their application to neural network methods.

Another study has forward a strategy for assessing the cybersecurity datasets' applicability to neural network algorithms and their representativeness. The framework was put to the test on a dataset of network traffic, and the findings revealed that the dataset's representativeness had a big impact on how well the neural network algorithms performed. Furthermore, several research have suggested employing metrics like class imbalance, feature relevance, and feature redundancy to assess the properties of cybersecurity datasets. These research' findings have demonstrated that these measures can be used to assess the dataset's quality and applicability for neural network algorithms.

In conclusion, the research points to a substantial relationship between the effectiveness of neural network algorithms for identifying cybersecurity anomalies and the properties of the cybersecurity dataset utilised for training and testing. In order to make sure that the neural network algorithms are capable of accurately identifying patterns and abnormalities in the data, it is crucial to assess the quality and representativeness of the dataset.

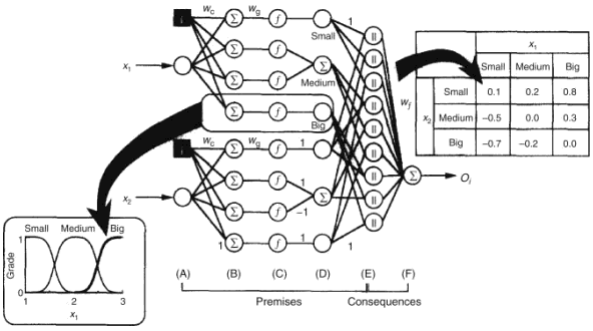
Neural network algorithms have received a lot of interest recently as a way of detecting cybersecurity anomalies since they have shown to be effective in spotting trends and abnormalities in large datasets. But the performance of these algorithms depends on the nature and characteristics of the cybersecurity dataset used for training and testing. It is necessary to evaluate the cybersecurity dataset's characteristics in order to apply them to neural network.

More research is needed to improve the efficiency of neural network algorithms for identifying cybersecurity anomalies and to create more dependable techniques for evaluating cybersecurity dataset features.

III. Detection of cyber attacks

A. Using neural networks :

By identifying patterns and abnormalities in massive datasets, neural networks are able to identify cyberattacks. This is accomplished by teaching the neural network on a dataset of well-known assaults, enabling the network to discover the traits and properties of various attacks. After being taught, the neural network can be used to examine fresh data, such network traffic, to find possible intrusions.A possible attack will be flagged by the neural network if it notices any similarities between the incoming data and the patterns and features it learned during training. The neural network is finding data that is different from what it has previously seen, which could suggest a cyberattack. This process is known as anomaly detection.

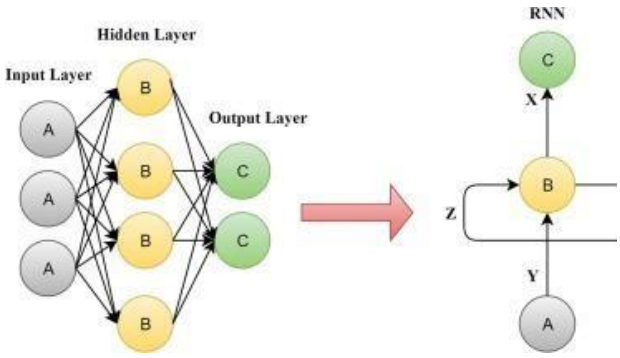


B. Using fuzzy logic :

By defining a set of rules for what defines a cyberattack, fuzzy logic can be used to detect them. These guidelines are based on the traits and characteristics of recognised cyberattacks, like certain patterns in network traffic or peculiar actions from a device. These rules are used by the fuzzy logic system to analyse fresh data, like network traffic, and compare it to the set of rules to see whether any patterns or features of a cyberattack are present.

In order to group similar data together, fuzzy logic systems can also use clustering techniques like the Fuzzy C-Means (FCM) method. Using this, it is possible to spot trends or anomalies in the data that might point to a cyberattack.

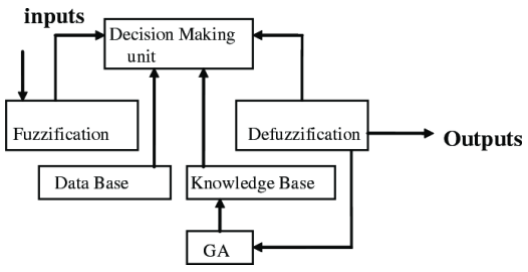
A fuzzy rule-based system (FRBS) can be used by fuzzy logic systems to make judgements based on the data they are fed. The FRBS decides whether the data it receives qualifies as a cyberattack or not using a series of if-then criteria.



In conclusion, fuzzy logic systems determine whether data represents a cyberattack or not by analysing it, comparing it to a set of predefined rules and patterns that are characteristic of known cyberattacks, and using clustering algorithms and fuzzy rule-based systems.decisions about whether the data constitutes a cyberattack or not.

IV. Proposed model

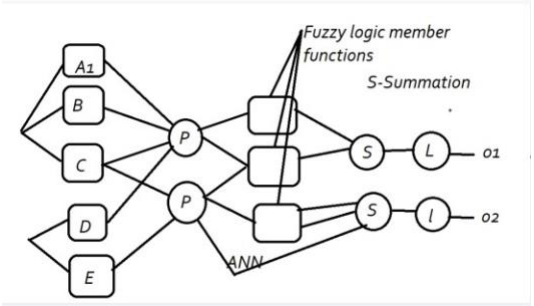
AFG model is a combination of ANN , Fuzzy logic and GA to detect anamolies.
In this model ANN is used to calculate rules in the fuzzy logic.



Genetic algorithms (GAs) can be used to optimize the parameters of a fuzzy logic system. The goal is to find the best set of parameter values that produce the best results for a specific problem.

In a typical implementation, the parameters of the fuzzy logic system are represented as a set of genes in a chromosome. The GA then uses evolutionary operations, such as **selection, crossover, and mutation**, to evolve a population of chromosomes towards a solution that optimizes a specific performance criterion.
Here's a high-level outline of the steps involved in using a GA to optimize a fuzzy logic system:

1) Define the fuzzy logic system, including the inputs, outputs, and rules.
2) Define the performance criterion that the GA will optimize. This could be a measure of the accuracy of the system, a measure of the interpretability of the system, or a trade- off between accuracy and interpretability.
3) Encode the parameters of the fuzzy logic system as a set of genes in a chromosome.
4) Create an initial population of chromosomes.
5) Evaluate the performance of each chromosome in the population using the performance criterion.
6) Apply evolutionary operations, such as selection, crossover, and mutation, to evolve the population towards a better solution.
7) Repeat steps 5-6 until the stopping criteria are met, such as a maximum number of generations or a satisfactory solution is found.
8) Extract the best set of parameter values from the final population and use them to configure the fuzzy logic system.
9) By using a GA to optimize the parameters of a fuzzy logic system, it is possible to improve the accuracy and interpretability of the system, as well as its ability to handle complex, real-world problems.



V. Results and Discussion With the help of : (Reference)

Mehdi Ghasri (2023). Hybrid Artificial Neural Network with Genetic Algorithm (https://www.mathworks.com/matlabcent ral/fileexchange/124600-hybrid-artificial-neural- network-with-genetic-algorithm), MATLAB Central File Exchange. Retrieved February 14, 2023.

We implemented our ANN-fuzzy-GA model with the help of matlab

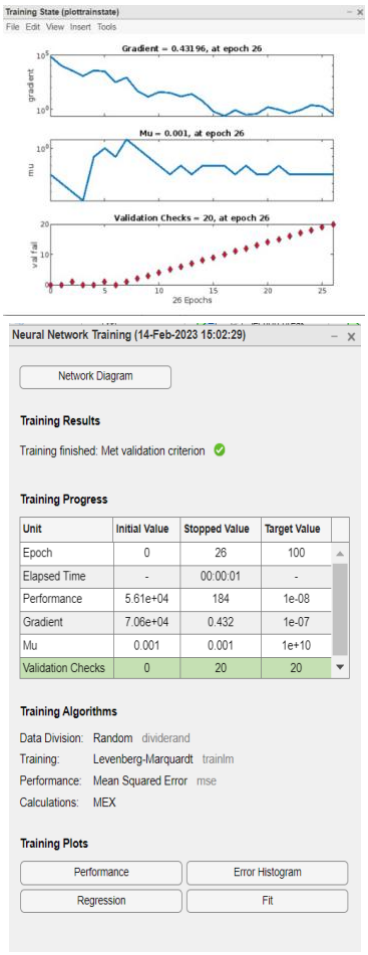
Hybrid ANN and fuzzy provides the search space and utilizes GA to find the best solution by tuning the weights and biases required to achieve lower error rates. The error between the model output and the exact training data can reach a minimum value by iterating the GA until the desired error is met.

Input

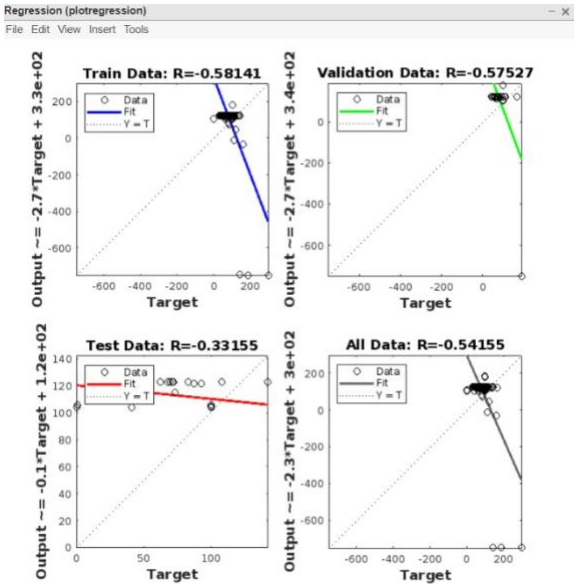
Number of hidden layers : 2
Maxit for GA : 20
Npop for GA : 10
Method : Roulette wheel Selection **Cross over percentage :** 0.8 **Mutation percentage :** 0.2

```
          ...
%%%%% Hybrid ANN-GA %%%%%
          ...
Iteration 1Best Cost = 262.1701
Iteration 2Best Cost = 262.1701
Iteration 3Best Cost = 237.4165
Iteration 4Best Cost = 237.4165
Iteration 5Best Cost = 205.1309
Iteration 6Best Cost = 172.7996
Iteration 7Best Cost = 172.7996
Iteration 8Best Cost = 172.7996
Iteration 9Best Cost = 162.8571
Iteration 10Best Cost = 146.7667
Iteration 11Best Cost = 146.7667
Iteration 12Best Cost = 146.7667
Iteration 13Best Cost = 142.6069
Iteration 14Best Cost = 142.3673
Iteration 15Best Cost = 142.3673
Iteration 16Best Cost = 142.3673
Iteration 17Best Cost = 141.9059
Iteration 18Best Cost = 141.8225
Iteration 19Best Cost = 141.8225
Iteration 20Best Cost = 141.8225
Calculation mode: MEX
```

Target epoch value was 100 but we stopped at 26 as we got a good result and the training is completed
20 Validation checks completed. We got values of gradient, mu

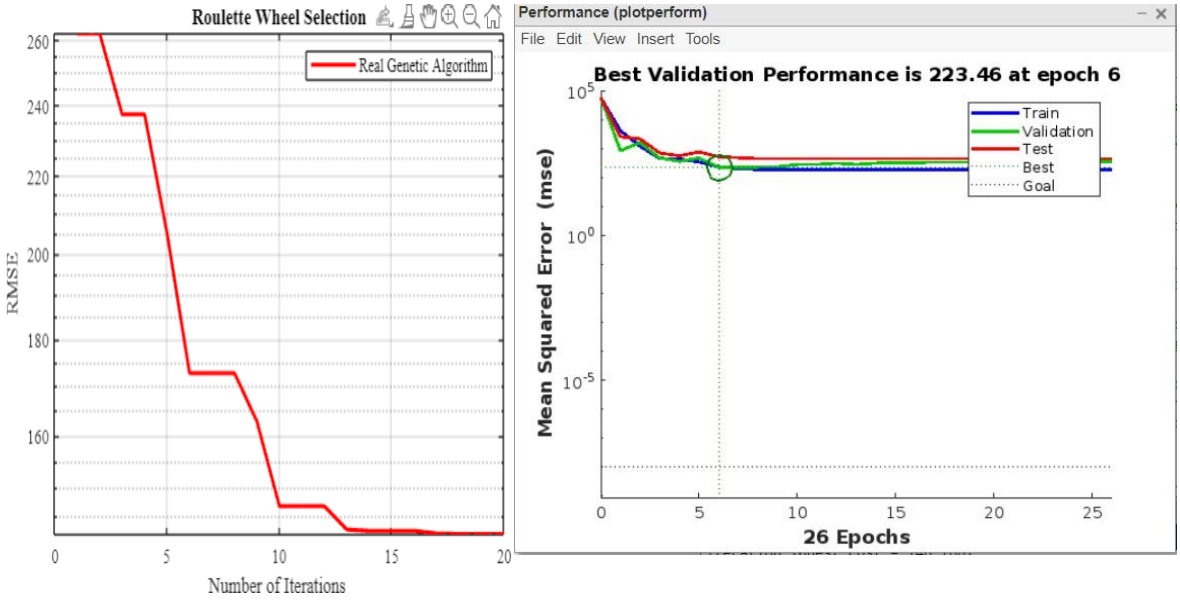


We got regression values for all data



When comparing the values of a dependent variable's anticipated and actual values, regression analysis frequently uses the metric known as root mean squared error (RMSE).

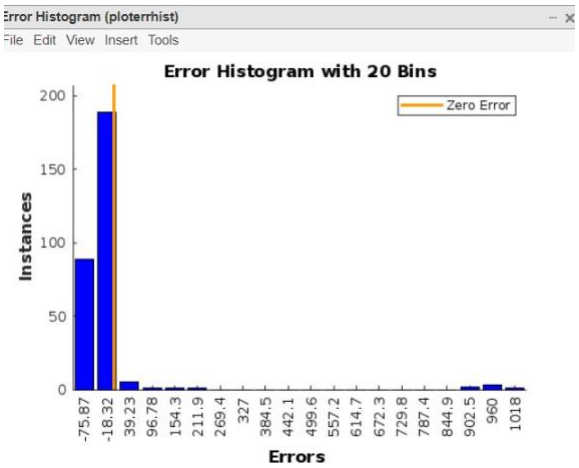
$$RMSE = \sqrt{\sum_{i=1}^{n} \frac{(\hat{y}_i - y_i)^2}{n}}$$



Notice how the RMSE value decreased as the number of iterations increased indicating the difference between predicted values and actual values decreased over the time.

A. Error Histogram

The distribution of errors between anticipated and actual values in a model is shown visually in an error histogram.

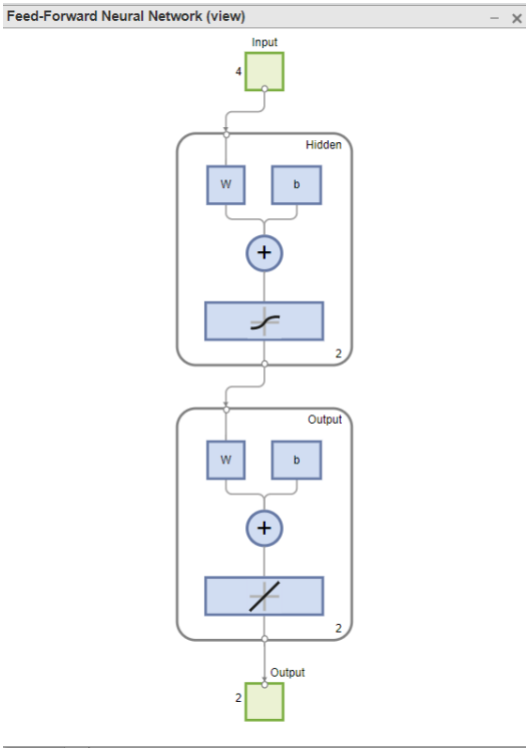


As you can see, we got zero error during the second bin.

B. Performance

The average squared difference between the anticipated and actual values of a dependent variable is measured by the mean squared error (MSE), which is a commonly used metric in regression analysis.
This is used as a model evaluation measure for regression models and **the lower value indicates a better fit.**
We got best validation performance of value 223.46 (lowest MSE among all epochs) at epoch 6.

C. Network diagram



VI. Challenges, recommendations and future research directions

a. Adapting to a remote workforce
b. Emerging 5G applications
c. Blockchain and cryptocurrency attacks
d. Ransomware evolution
e. IoT attacks
f. Cloud attacks
g. Phishing and spear-phishing attacks
h. Software vulnerabilities
i. Machine learning and AI attacks Each challenge is explained in detail, and some solutions are provided for each.

The main solutions include cloud-based cybersecurity solutions, robust technical infrastructure, anti-malware and anti-phishing solutions, encryption, security analysis, anti-phishing tools, and software vulnerability management. The article also emphasizes the importance of employee training, and being aware of the fundamentals of security to reduce the risk of falling victim to cyber attacks.

Artificial intelligence (AI) and machine learning (ML) are also expected to play a significant role in the future of cybersecurity.

Another important area of focus will be the protection of personal data and privacy. With the increasing amount of data that organizations collect, store and process, there will be a greater need for data protection measures such as encryption, and for compliance with data protection regulations, such as the General Data Protection Regulation (GDPR).

In addition, blockchain technology and quantum computing are likely to have a big impact on cyber security in the future. Blockchain's decentralized nature will provide a new layer of security to various industries, while quantum computing will bring new challenges in encryption, which will require new security protocols to be developed. Overall, the future direction of cybersecurity is likely to involve a continued focus on protecting against new and evolving threats, and the use of advanced technologies to improve the efficiency and effectiveness of security solutions.

VII. Conclusion

In this research ,we discussed about cyber security attacks and anamolies, types of cyber attacks, machine learning methods to detect anamolies.

We also discussed about challenges recommendations and future research directions.

We also implemented a Hybrid ANN- fuzzy logic and GA model with matlab tools and we also best validation performance.

Acknowledgement

Mehdi Ghasri (2024). Hybrid Artificial Neural Network with Genetic Algorithm (https://www.mathworks.com/matlabcentral/fileexchange/124600-hybrid-artificial-neural-network-with-genetic-algorithm), MATLAB Central File Exchange. Retrieved January 19, 2024.

References

[1] J. G. Mcquaid, And S. Nixon, "A Survey Of Intrusion Detection Techniques," Journal Of Network And Computer Applications, Vol. 27, Pp. 2-23, 2004.

[2] R. A. Kemmerer, "A Taxonomy Of Computer Program Security Flaws," Ieee Transactions On Software Engineering, Vol. 18, Pp. 733-746, 1992.

[3] M. A. Kaafar, And R. S. Sandhu, "Anomaly Detection In Computer Networks: A Survey," Ieee Communications Surveys And Tutorials, Vol. 12, Pp. 34-55, 2010.

[4] Lee.S And Kim.J, Warning Bird: A Near Real- Time Detection System For Suspicious Urls In Twitter Stream Ieee Transactions On Secure Computing, Vol 10,No.3,May/June 2013.