Volume 3, Issue X, October 2024, No. 49, pp. 628-643
Submitted 3/10/2024; Final peer review 30/10/2024
Online Publication 3/11/2024
Available Online at http://www.ijortacs.com

# DEVELOPMENT OF AN INTELLIGENT AND SECURED MODEL FOR A CLOUD-BASED DETECTION OF ADVERSARIAL ATTACKS USING ARTIFICIAL NEURAL NETWORK

[1*]Okonkwo Chinonso J. [2]Ogochukwu C. Okeke
[1,2]Department of Computer Science, Faculty of Physical Sciences,
Chukwuemeka Odumegwu Ojukwu University, Anambra State
Author Email: [1]nsojoe@gmail.com, [2]cj.okonkwo@coou.edu.ng.com

**Abstract**

To identify and mitigate adversarial attacks, this paper explores the development of a intelligent and secure model for a 5G cloud-based facility utilising Artificial Neural Networks (ANN) and sophisticated statistical approaches. The research uses the Structured System Analysis and Create Methodology (SSADM) to analyse and create the suggested solution. Principal Component Analysis (PCA) and Mahalanobis distance were used in conjunction with a multi-layered neural network model to detect unusual packet behaviour and facilitate effective threat identification. The study makes use of an actual 5G cloud dataset with many traffic types, and pre-processes the data using techniques like feature extraction and imputation. Achieving an exceptional ROC score of 0.98673 and a detection accuracy of 99.6%, the detection model was assessed utilising critical performance indicators including Positive Predictive Value (PPV), False Discovery Rate (FDR), accuracy, and Receiver Operating Characteristic (ROC) analysis. The suggested ANN-based model outperformed the state-of-the-art algorithms in a comparative analysis, showing a 98.67% detection rate. The results demonstrate how well the approach works to improve cybersecurity for 5G cloud networks by offering a strong defence against hostile attacks.

**Keywords: 5G Cloud; Adversarial Attacks; Artificial Neural Network; Mahalanobis Distance; Principal Component Analysis.**

## 1. INTRODUCTION

The advent of the Fifth-Generation (5G) network has brought about significant improvements in the field of information and telecommunication technology. In many developing and even developed countries, this technology has been embraced, and it has triggered great advancements in big data management for both the public and private sectors. Unlike the conventional Fourth Generation (4G), the 5G offers numerous benefits in the overall quality of service characterization and has facilitated advanced data management technologies like cloud computing (Zolotukhin et al., 2023).

In Suryateja (2022), cloud computing is a virtual network made up of three main services: Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), and used for data management. Each of these services offers different levels of support for the management of various Information Technology (IT) infrastructures. SaaS for instance enables users to access data from the cloud through software networking. IaaS offers virtualized computing resources, including storage, networking, and servers, to customers over the Internet. PaaS provides the framework for the development, deployment, and management of software applications (Al-Jumaili et al., 2023).

Overall, cloud computing has become an essential tool for organizations to manage their IT infrastructure more efficiently, and the availability of 5G networks has further enhanced its capabilities. Today as a result companies are transferring their data from the conventional enterprise server to the cloud-based platform for easy storage, flexibility, and management. However, one major issue that remains the center of attraction today is the security vulnerability in the 5G network infrastructure (Duddu, 2015). These security vulnerabilities are attributed to various factors which include seamless access to data through software-defined networking, the shared infrastructure by the network, and wrong security configurations, which make the network prone to security risks and susceptible to different types of attacks, such as man-in-the-middle, denial of service, wormhole, blackhole, and most recently the adversarial attack model.

In Ibitoye et al. (2020), the adversarial attack model has gained dominance in recent studies on cybersecurity due to its high success rate in penetrating the network. This attack model involves the crafting of specially designed input that causes the Machine Learning Model (MLM) to make incorrect decisions. This is achieved by manipulating the input data, which slightly alters the feature vectors from the originally trained vectors, deceiving the security model to gain access to the network. The adversarial attack approach can be classified into three methods, which include the poisoning, evasion, and oracle methods (Akhtar and Mian, 2018). The poisoning method injects false data into the original data to corrupt the security model, while the evasion method misleads the ML security model during the testing process using the gradient-free technique. The oracle method involves stealing the security algorithm, duplicating the ML model, and using it to attack the network.

Recent studies by Papernot et al. (2017), Akhtar and Mian (2018), and Zhang et al. (2020) have focused on the adversarial attack model due to its prevalence and success rate in penetrating wireless networks. Countermeasures to the adversarial threats include Benaddi et al. (2022), who compared several machine learning algorithms, including linear regression, decision tree, random forest, support vector machine, and deep learning algorithms for the detection of adversarial attacks. The classifiers were trained using benchmark datasets such as NSL-KDD and UNSW-NB 15. These data were augmented with Gaussian data augmentation techniques, before training the model. The result reported an average accuracy of 76% for all the classifiers, while the deep learning algorithm recorded the best accuracy of 77.68% for NSL-KDD and 78.56% for UNSW-NB15 datasets. Another approach to adversarial attack detection in 5G was proposed by Guangquan et al. (2021), who developed the Red Green Blue (RGB) stream and the Spatial Rich

Model (SRM). The RGB model captures differences in adversarial samples, while the SRM serves as a filter to generate noise features that provide evidence of attack detection. The results of the experiment showed a detection rate of 91.3%. Liang et al. (2018) applied an adaptive Denoising approach, while Lui et al. (2019) proposed a steg-analysis approach. These studies have contributed significantly to the field of wireless network security, however, solutions have not been obtained for a security model which is adaptive enough to detect future adversarial threats to the wireless network. Most of the studies were able to detect and classify adversarial attacks; however, their reliability to detect future attacks was never mentioned and has remained a major challenge. This is because features of adversarial attacks In Ibitoye et al. (2020) are been modified by hackers on several occasions to deceive the security model and penetrate the network. Hence developing a solution that considers these uncertainties in future attacks is the "Holy Grail", because it will ensure that the 5G network architectures are secured irrespective of the dynamics of future attack models. To this end, this study therefore proposes the development of an intelligent and secured model for a 5G cloud-based facility against adversarial penetration using Artificial Neural Network algorithm. To achieve this, data of normal packets will be collected, processed and trained to generate a baseline model for the classification of adversarial threats.

## 2. RESEARCH METHODOLOGY

The methodology adopted for the study is the Structured System Analysis and Design Methodology (SSADM). This is a systematic methodology for the design and analysis of information systems. It involved seven key steps which are a phased approach, logical and physical views, data modeling, system analysis, prototyping, and documentation and user involvement. The proposed system to address the problem was also analyzed and justified. The research design applied necessary diagrams in line with the methodology, such as data flow diagrams, entity relationship diagrams, flow charts, block diagrams, high-level models and architectural diagrams. The system implementation utilized Matlab programming and packet tracker as the tools, while the testing and validation were done using simulation, deduction and comparative analysis techniques respectively.

## 3. RESEARCH METHODS

The neural network type proposed is the multi layered neural network. First the data collection and preparation step was also applied in this detection model, however during the training process, a neural network algorithm with three hidden layers was selected and then trained with Stochastic Gradient Descent (SGD) to generate the model for the detection of adversarial network. The system workflow diagram was presented in the figure 1;

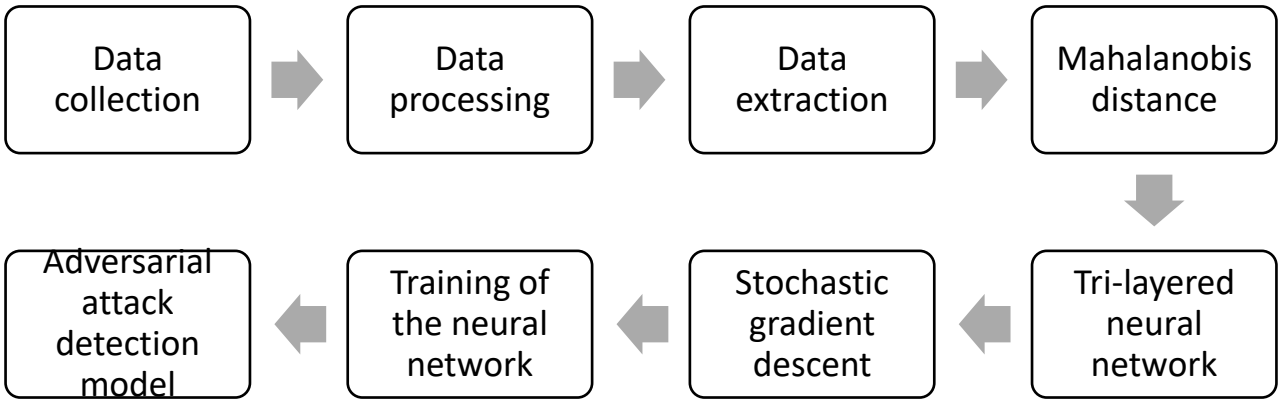


Figure 1: Workflow of the neural network-based model for adversarial attack detection

**3.1 Data collection**

The dataset used for the study was 5G normal cloud data published by the Czech researchers focuses on HTTPS traffic classification and provides valuable insights into various traffic categories. The data collection process primarily involved capturing traffic from the real backbone network, omitting IP addresses and ports for privacy and security reasons. The datasets were generated using a flow probe called Ipifixprobe, which exports bidirectional flows along with sequences of packet lengths, times, and bursts. The data size is 1048578 features and span across 24 attributes which include packet lengths, times, bursts, and traffic categories. The structure of the dataset revolves around the classification of HTTPS traffic into five distinct categories of Live Video Streaming, Video Player, Music Player, File Upload/Download, and Website/Other Traffic.

**3.2 Data processing**

The data processing method utilized is the imputation method. The approach searches for duplicate values and fixes using the Excel toolbox. Secondly, the mean imputation method was applied to search for and replace missing values using the MATLAB programming environment. The processed data was then applied for feature selection discussed in the next section.

**3.3 Feature selection**

The feature selection method was applied to selection automatically the normal packet features of the 5G network according to their most important vectors. The method applied for this process is the fisher test approach (Gianluca, 2021). It selected the features by adding a penalty term to the linear regression objective function, which encourages some feature coefficients to become exactly zero, effectively selecting a subset of the most important features and achieving feature selection and regularization simultaneously. These selected features were fed to the data extraction model for further processing steps.

**3.4 Data extraction**

The data extraction is a process applied to the selected features to retrieve its information and convert it to a compact feature vector for each identification by the Mahalanobis distance model. The technique applied for the data extraction process is the Principal Component Analysis

(PCA). The PCA is a statistical method of feature extraction which applies mathematical computation of the covariance matrix for the data features points, then the engine value and eigenvectors for each of the features are determined and used to create a new vector in which the new extracted features

### 3.5 Mahalanobis distance

The Mahalanobis distance is a statistical method used for the quantification of the dissimilarity between feature points, considering covariance. This was applied in this work to measure the Mahalanobis distance of every feature vector extracted by the PCA. The Mahalanobis distance used the covariance value of the PCA output in the feature extraction to determine the Mahalanobis distance through the correlation between the different features and then set as the threshold for the detection of abnormal feature deviation from the normal packet.

## 4. SYSTEM ALGORITHM

The algorithms used in this work are the PCA algorithm, the stochastic gradient descent algorithm and neural network algorithm for adversarial attack detection algorithm for threat detection.

**Algorithm 1: The PCA algorithm**

1. Start
2. Standardize data (optional).
3. Calculate covariance matrix ($\Sigma$).
4. Perform eigen-value decomposition of $\Sigma$ to get eigenvectors (w) and eigen-values ($\lambda$).
5. Choose a subset of eigenvectors with highest eigen-values.
6. Project data points (x) onto principal components using eigenvectors
7. End

**Algorithm 2: Stochastic gradient descent**

1. Start
2. Initialize weights and biases
3. Randomly initialize weights and biases for each layer
4. for epoch in range(num_epochs):
5. Forward propagation
6. Compute the output of the network given the input data
7. Compute loss
8. Compute the loss function
9. Back-propagation
10. Compute gradients of the loss function with respect to weights and biases
11. Update weights and biases using gradient descent or other optimization algorithm
12. After training, the weights and biases of the network have been adjusted to minimize the loss function
13. End

**Algorithm 3: Adversarial threat detection model with ANN**

1. Start
2. Load network data % Adversarial attack or normal packet
3. Load adversarial attack classifier% trained ANN
4. Extract packet data features % with PCA
5. Identify changes in covariance% with mahalanobis

6. Classification process % pattern matching
7. If
   Threat detection
   "flag packet as threat"
8. Else if
   Normal packet detected
   "flag as normal user"
9. Initialize decision based access control algorithm
10. Return
11. End

### 4.1 Control Center

The control center was used to model the overall system structure, showing how data will flow in relation with the proposed security solution against adversarial attack in the cloud based network. The access to the to the proposed network facility is software as a service which utilized the power of Software Defined Network (SDN) to allows used access to the cloud network infrastructure for various activities. In the control center diagram of figure 2, the network users are the attackers and also the normal users. These users respectively generates packet and upload on the cloud platform through the SDN. In the gateway, the Adversarial Attack Detection Model (AADM) identified the packet features from the mahalanobis distance and PCA, then perform classification process to detect normal packet or adversarial threats. The detection output is feed as input to the access control algorithm which now decides if the isolate the user from the network or all the user access to the cloud in the case of normal packet.

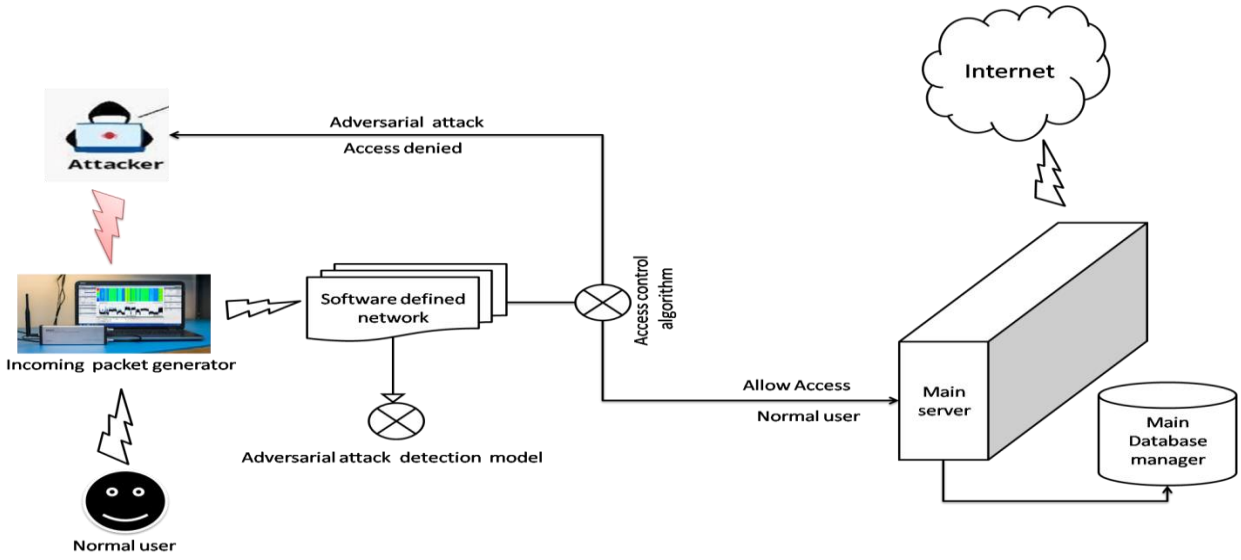


Figure 2: The control system architecture

## 5. SYSTEM IMPLEMENTATION

To implement the access control algorithm in MATLAB, we begin by initializing the system variables and defining the necessary functions. The system initialization phase involves setting up the environment and allocating memory for variables. The access protocol is initialized to establish rules governing access to server resources. Once the system is prepared, input is received from an adversarial attack detection model to assess potential threats. In the main loop

of the algorithm, the system continuously monitors for threats while processing incoming data. If a threat is detected based on the input from the attack detection model, access to the server is promptly denied to prevent unauthorized access attempts. Conversely, if a normal packet is detected, indicating legitimate access, the system allows access to the server. This conditional decision-making process ensures that the system dynamically adapts its access permissions based on the presence or absence of threats. Throughout the implementation process, attention is given to optimizing the efficiency and accuracy of threat detection and access control mechanisms. MATLAB's capabilities in data analysis and signal processing can be leveraged to enhance the system's ability to detect and respond to potential threats effectively. Regular testing and validation are essential to ensure the reliability and robustness of the implemented system, helping to mitigate security risks and maintain the integrity of the server environment. The generated adversarial threat detection model was integrated on a 5G based cloud network using virtual box, packet tracker and Wireshark before testing with adversarial attack features. The virtual box was sued to simulate the network threat, the packet tracker was applied to model the network topology for the attack while the Wireshark was used for the network analysis.

### 5.1 Performance evaluation metrics for the AADM

The parameters utilized for the AADM model assessment are positive predictive value, false discovery rate, accuracy, true positive rate and area under curve.

**1. Positive Predictive Value (PPV)**: PPV measures the accuracy of positive predictions:

$$PPV = TP / (TP + FP) \quad (1)$$

Where: TP: True Positives; FP: False Positives

**2. False Discovery Rate (FDR)**: FDR quantifies the proportion of false positives among all positive predictions:

$$FDR = FP / (TP + FP) \quad (2)$$

Where: FP: False Positives

**3. Accuracy**: Accuracy measures the overall correct predictions, both true positives and true negatives, relative to all predictions:

$$Accuracy = (TP + TN) / (TP + TN + FP + FN) \quad (3)$$

Where: TP: True Positives; TN: True Negatives; FP: False Positives; FN: False Negatives

**4. True Positive Rate (TPR)**: TPR calculates the proportion of actual positives correctly predicted:

$$TPR = TP / (TP + FN) \quad (4)$$

**5. False Negative Rate (FNR)**: FNR represents the proportion of actual positives that were incorrectly predicted as negatives:

$$FNR = FN / (TP + FN) \quad (5)$$

## 6. RESULTS OF THE ANN ADVERSARIAL THREAT DETECTION MODEL

In this section, the performance of the adversarial threat detection model developed with neural network was considered and reported in the considering similar performance evaluation metrics. From the results, it was observed that the neural network algorithm reported values for PPV

FDR, TPR, FNR but diverse in the ROC analysis. The PPV reported 99.5%, FDR was 0.5%, TPR was 100% and TNR was 100%, while the ROC reported 0.9830. all results are in figure 3-5.

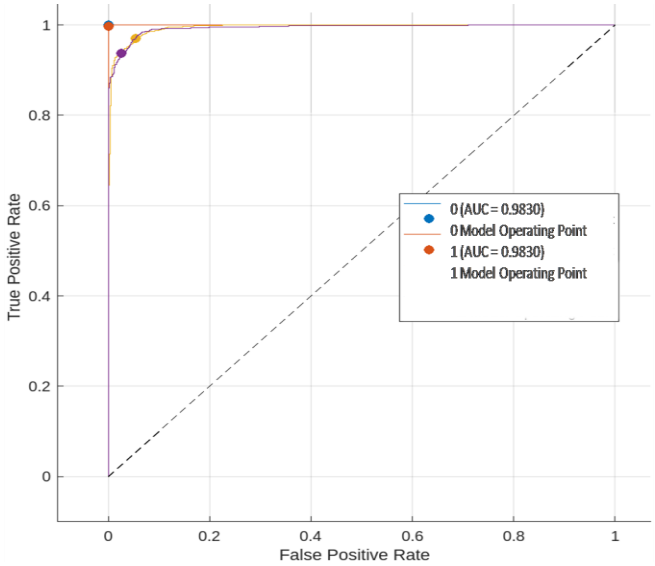


Figure 3: ROC analysis of the adversarial model

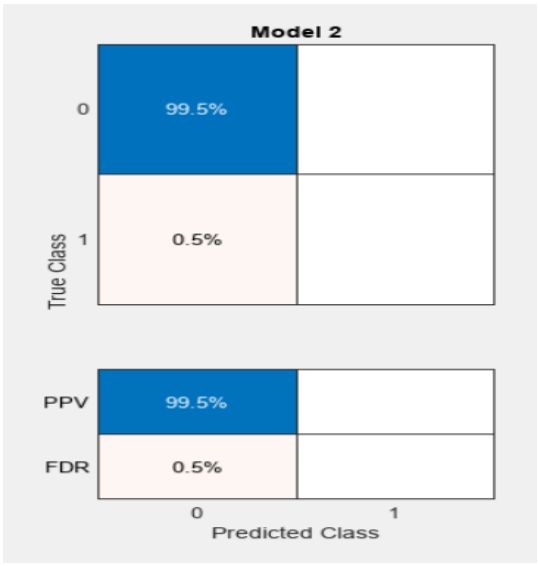


Figure 4: PPV/FDR result of the adversarial model

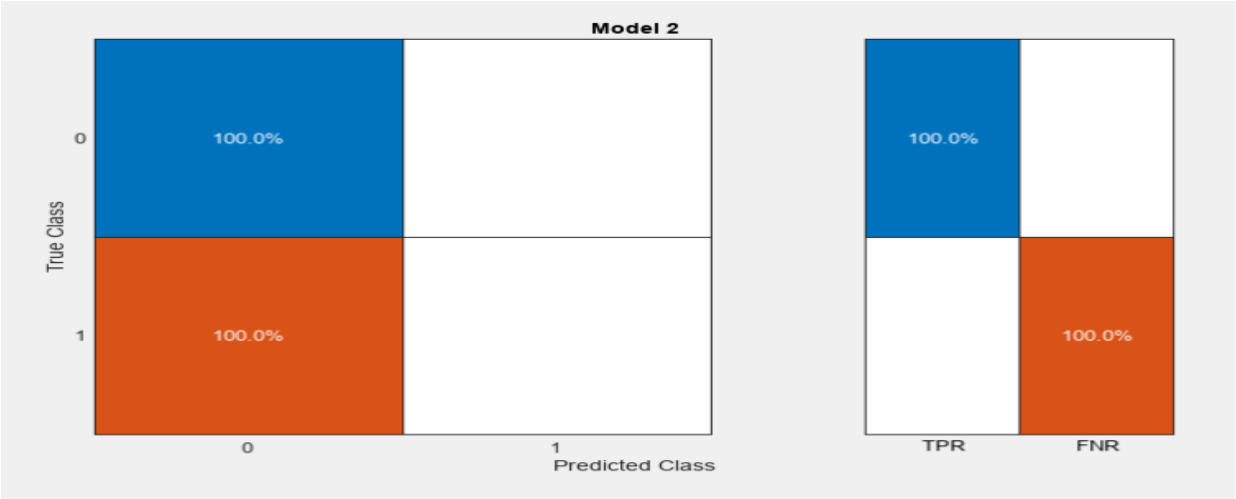


Figure 5: The TPR/FNR of the adversarial model

Figure 3 showcased the ROC analysis of the neural network-based adversarial attack detection model, considering the relationship between TPR and FPR respectively. From the results, it was observed that when the model was evaluated with threat (1) and without threat class (0), the recorded 0.9830 as the ROC values for the two classes. The implication is that the model was able to correctly classify positive threat features and also correctly classify positively normal packet features. The reason why the ANN demonstrated the best performance, especially on the ROC which measured how reliable the new system is was due to the data process technique, specifically the application of the Mahalanobis distance model which was able to identify packet features, despite the dynamic covariance matrix, and hence address the issues of false alarm as shown in figure 4 and 5.

### 6.1 Cross-Validation of the Models

The cross-validation of the ANN and SVM models considered the k-fold validation approach, where the k value is 10 and the results were reported in Table 1 for SVM and Table 2 for ANN.

**Table 1: CROSS-VALIDATION RESULTS OF ADVERSARIAL ATTACK DETECTION MODEL**

| S/N | TPR (%) | FNR (%) | PPV (%) | FDR (%) | ACC (%) | ROC |
|---|---|---|---|---|---|---|
| 1 | 100 | 100 | 99.5 | 0.5 | 99.5 | 0.9830 |
| 2 | 100 | 100 | 99.5 | 0.5 | 99.5 | 0.9847 |
| 3 | 99.7 | 99.8 | 99.3 | 0.7 | 99.8 | 0.9837 |
| 4 | 100 | 100 | 99.5 | 0.5 | 99.5 | 1.0000 |
| 5 | 100 | 99.6 | 99.6 | 0.4 | 99.7 | 0.9792 |
| 6 | 100 | 100 | 99.5 | 0.5 | 99.5 | 0.9886 |
| 7 | 100 | 99.6 | 99.7 | 0.3 | 99.6 | 0.9790 |
| 8 | 100 | 100 | 99.5 | 0.5 | 99.8 | 1.0000 |
| 9 | 99.7 | 100 | 99.8 | 0.2 | 99.6 | 0.9834 |
| 10 | 100 | 100 | 99.7 | 0.3 | 99.5 | 0.9857 |
| Avg. | 99.94 | 99.9 | 99.56 | 0.44 | 99.6 | 0.98673 |

The ANN adversarial attack detection model performs well across important metrics, according to the cross-validation findings shown in Table 1. With an astounding True Positive Rate (TPR) of 99.94%, the model demonstrated its capacity to reliably identify hostile attempts. Furthermore, a low False Negative Rate (FNR) of 99.9% implies a low rate of missed detections, demonstrating the sensitivity of the model in detecting real threats. The model exhibits great precision in its predictions, as evidenced by its Positive Predictive Value (PPV) of 99.56%. This means that in the majority of cases, when it flags an adversarial attack, it is correct.

Moreover, the artificial neural network model demonstrated an exceptionally low erroneous Discovery Rate (FDR) of 0.44%, signifying a negligible incidence of erroneous positive predictions. This low false alarm rate (FDR) increases the model's dependability by reducing the number of pointless or false alarms. The model's robust performance in threat detection is demonstrated by its high overall Accuracy (ACC) of 99.6%, which highlights its effectiveness in correctly categorizing adversarial attacks and non-attacks. Furthermore, the model's high capacity to distinguish between true and false positives is demonstrated by its Receiver Operating Characteristic (ROC) value of 0.98673, which approaches an optimal performance level close to 1, confirming its effectiveness in detecting adversarial attacks. It can be concluded that the ANN adversarial attack detection model performs exceptionally well based on its near-optimal ROC value, high PPV, low FDR, high ACC, and low FNR. The reason why the ANN demonstrated the best performance, especially on the ROC which measured how reliable the new system is was due to the data process technique, specifically the application of the Mahalanobis distance model which was able to identify packet features, despite the dynamic covariance matrix, and hence address the issues of false alarm. Together, these findings demonstrate the model's efficacy and dependability in precisely recognizing and categorizing hostile threats, demonstrating its value as an adjunct to cybersecurity defenses. The model's excellent

performance on a variety of assessment measures highlights its potential to improve threat detection capabilities and make a substantial contribution to cybersecurity initiatives aimed at thwarting hostile attacks.

### 6.2 Comparative Analysis

In the comparative analysis, the performance of the model developed for adversarial attack detection was performed using the data presentation in the Table 1, then Table 2 presented the comparative analysis with other state of the art algorithms for adversarial attack detection alongside the techniques applied and the average detection rates achieved for the operation.

**TABLE 2: COMPARATIVE ANALYSIS WITH EXISTING ALGORITHMS**

| Author | Technique | Threat detection rate (%) |
|---|---|---|
| Guangquan et al. (2021) | Two stream networks | 91.23 |
| Aiken and Scott Hayward (2020) | KNN | 95.00 |
| Apruzzese et al. (2019) | KNN | 97.11 |
| | RF | 97.11 |
| | MLP | 98.16 |
| Sharma et al. (2019) | RNN-LSTM | 82.66 |
| | K-NN | 94.25 |
| | RF | 95.02 |
| Ghanem (2017) | SVM | 93.67 |
| Xu et al. (2021) | Spatial rich model | 91.30 |
| Alshahrami et al. (2022) | Generative adversarial network | 85.92 |
| Restuccia et al. (2022) | Generalized adversarial machine learning | 97.00 |
| Proposed | New ANN model | 98.67 |

The table 2 presented the comparative analysis of the new ANN model for adversarial attack detection with other state of the art algorithms considering their detection rate. The data presentation table was graphically analyzed in figure 6.

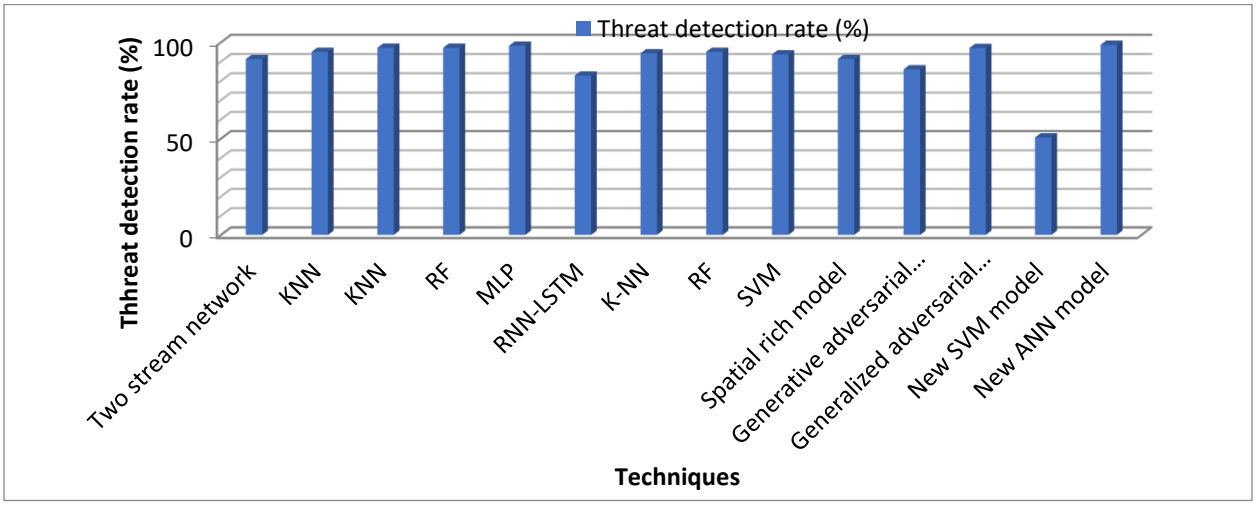


Figure 6: Comparative adversarial attack detection models performance

From Figure 4, it was observed that while the existing model all reported high detection rates for adversarial attack penetration, the new ANN-based model was able to record the best results, with 0.52% improvement against the closest rival which was MLP by Apruzzese et al. (2019) who recorded 98.16% detection rate.

**Result of Model Integration on Cloud Network**

In the system integration, the neural network based attack was integrated on a 5G network routing device and tested with denial of service attack with adversarial features as the threat vector. The network topology for the attack was presented in the figure 7.

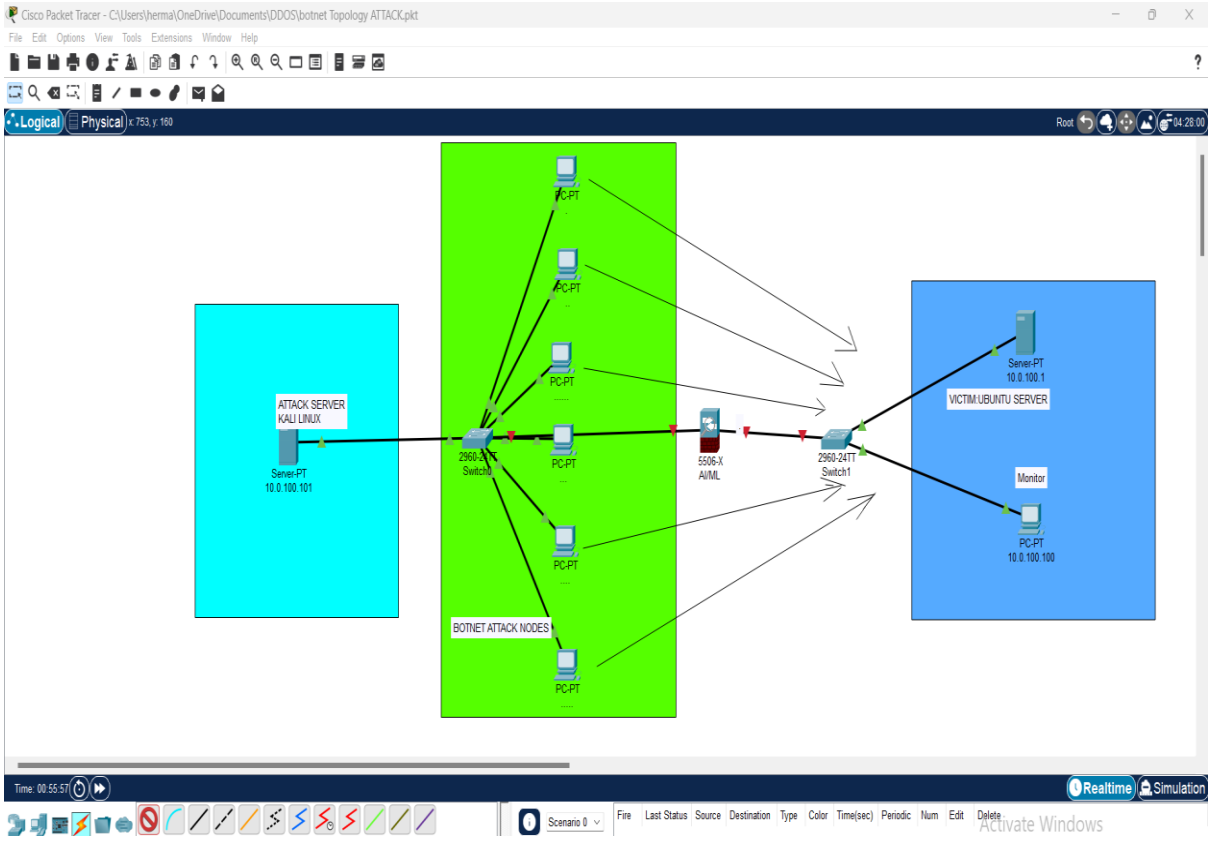


Figure 7: Packet tracer model of the network topology for attack test

The figure 7 presented a DDOS attack model with six nodes with Attacker IP: 10.0.100.101 VICTIM IP: 10.0.100.1 and MONITOR IP: 10.0.100.100 respectively. The performance of the network was measured with wireshark software considering throughput, latency and packet loss. These parameters were employed to access the impacts of the threat penetration and how reliable the new security solution presented was able to detect and isolate the threat from the network facility. The DDOS attack features used to test the network is a pertubated rootkif vector as shown in the figure 8, while the visual analysis of the threat by the routing system was presented in the figure 9;

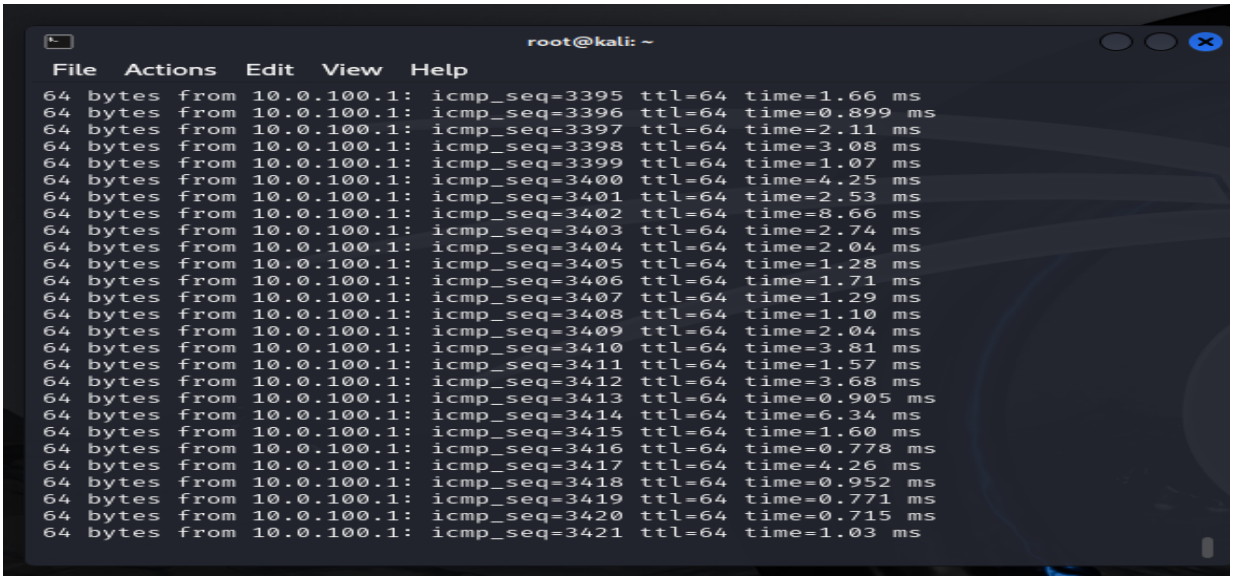


Figure 8: The adversarial threat on the network

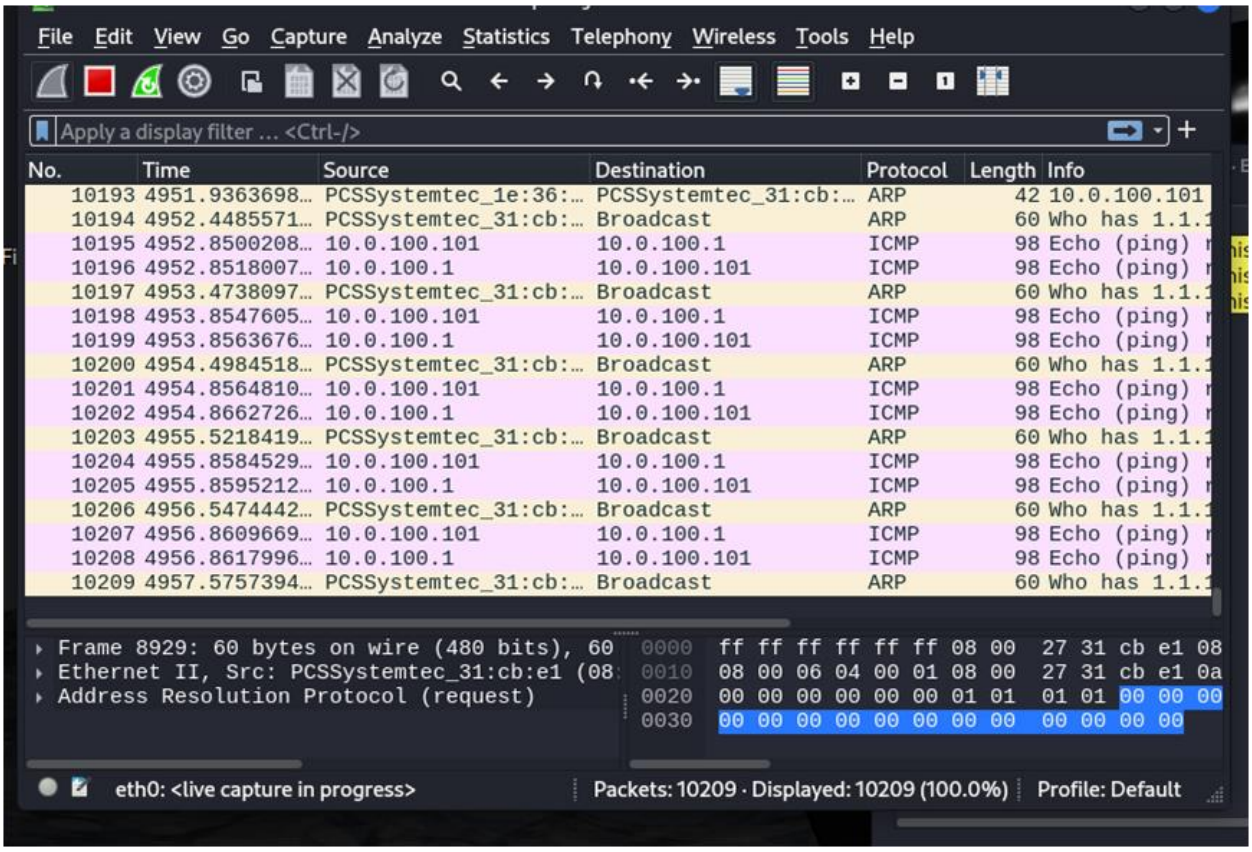


Figure 9: The network analysis of packet by the routing system with ANN based model

In the figure 8-9, it was observed that the rootkit packet transmitted on the network was detected with the 10.0.100.1 IP address as shown multiple times on the network. These packets features were extracted with the PCA algorithm and then the covariance analyzed with the mahalanobis distance before classification with the trained ANN model to detect threat and isolate from the network with the decision based algorithm to ensure quality of service on the network, while

denying access to adversarial threat features. In the figure 10, the network throughput was measured under threat condition and reported as follow;

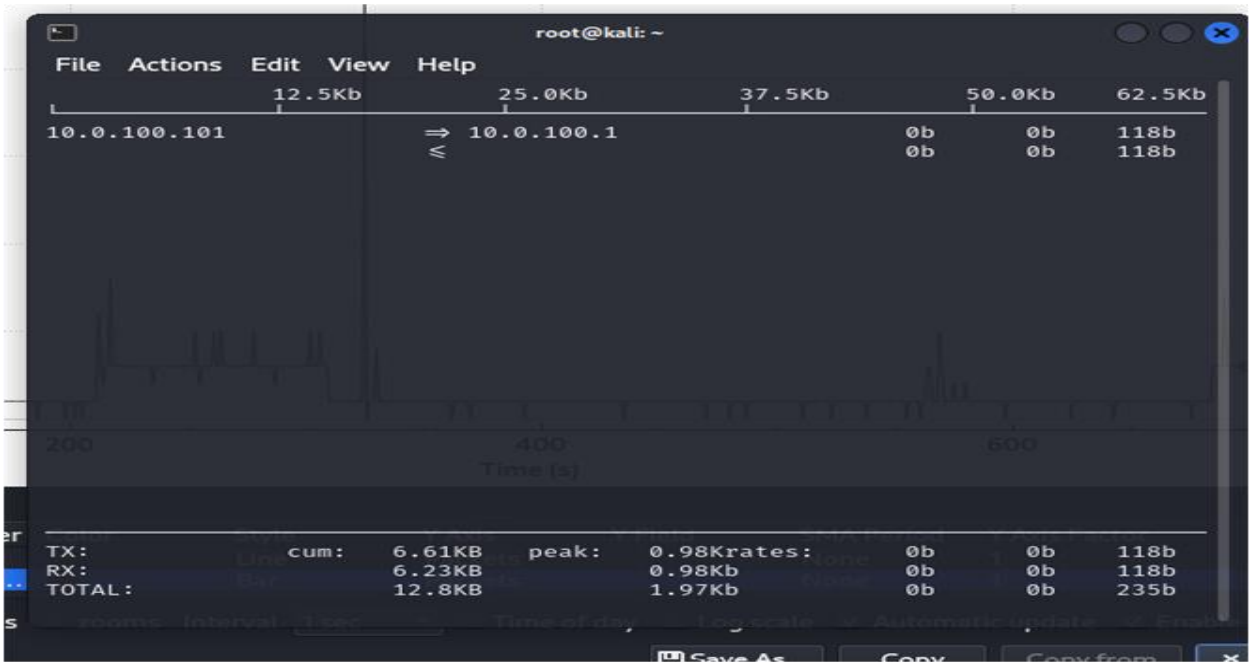


Figure 10: Result of throughput during threat on the protected network

From the results in the figure 10, it was observed that when 6.61kB of data was transmitted from normal user, 6.23kb was allowed access and received, which gives 94.25% throughput, while simultaneously denying access to packet which are adversarial threats to the network. Also when 0.98kb of packet was transmitted, 0.98 kb was received which is 100% throughput in another instance when 118.6kb of packet was transmitted, 118kb was received which is 100% throughput. Overall it was observed that during the testing process, when the adversarial threat was penetrated during the network operation, it was observed that the ANN based adversarial attack detection model was able to capture the dynamic characteristics of the threats with the help of the mahalanobis distance model and then correctly classify the threats features and isolate them from the network with the decision based algorithm. Hence the attack was not allowed to penetrate the network and caused poor quality of service, which resulted in the very high throughput recorded for all packet transmitted. This result suggested that the ANN based model for adversarial attack detection was very efficient, able to classify the features of malicious packets and isolate from the network, while allowing normal packet to flow. In the figure 11, the latency of the network was measured.

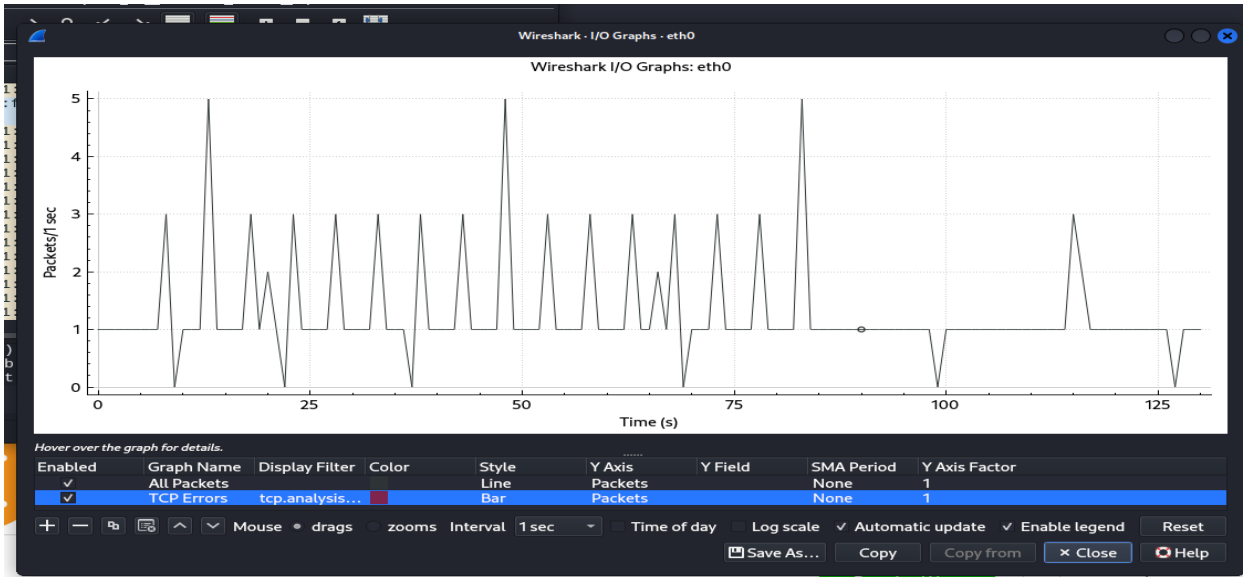


Figure 11: Latency during threat on the protected network

From the result of figure 11, the latency of the network was analyzed over 125secs of evaluation with DDOS attack penetration. From the results, it was observed that averagely the latency on the network is 2.48secs. This latency suggested that the routing speed on the network is very good for HTPP packet and hence implied that the new security model was able to isolate all threats tailored towards the network and ensure quality of service. To evaluate the decision based algorithm, the figure 12 was applied.

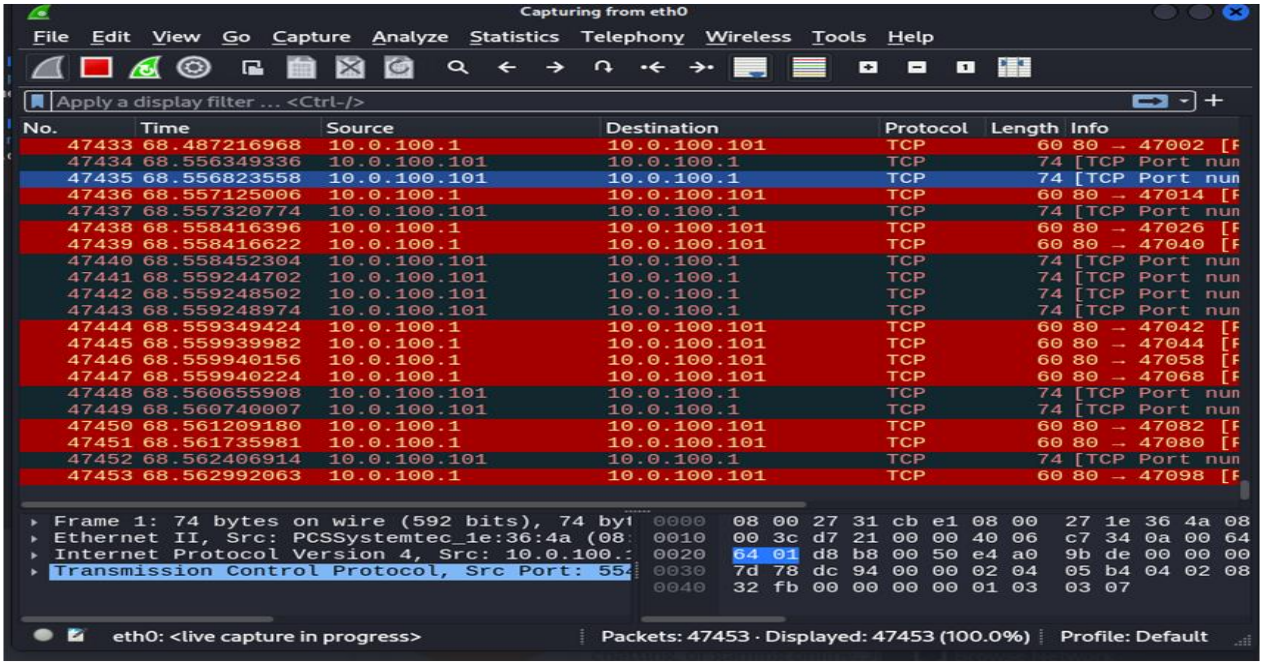


Figure 12: Result of the decision based algorithm

The figure 12 was used to demonstrate the performance of the decision based algorithm after the classification of threat by the ANN based adversarial attack detection model. From the results, it was observed that the entire suspicious packet IP was identified and flag off as threat, before

isolation from the server. The time of the attack, the source, IP address, destination and protocol were identified by the decision based algorithm and then deny access to the server, thereby protecting the network.

## 7. CONCLUSION

Over the years, the evolution of cloud computing has attracted massive upload of data to the cloud, thus making it a hotspot for storage of massive data and critical organization information, hence making it also the centre of attention for cyber criminals. Several studies to arrest the penetration of threat into cloud environments despite their success are not able to provide reliable security solution due to the diversity of cyber threats. This research by the virtual of the performance evaluation analysis has presented a reliable security models, leveraging the power of artificial intelligence. To achieve this, data of normal packet was collected and then processed for integrity. PCA was applied for feature extraction, while mahalanobis distance model was used to capture the dynamic characteristics of packet features covariance. ANN was adapted and trained with the data to develop two models for adversarial threat detection. Comparative analysis of the model showed that the ANN was the best in real time detection of adversarial attack, due to its ability to correct extract and identify the intricate feature of the threat and recognize those not normal packet data as threats.

## 8. REFERENCES

Aiken, J., & Scott-Hayward, S. (2020). Investigating adversarial attacks against network intrusion detection systems in SDNs. In IEEE Conference on Network Functions Virtualization and Software Defined Networks (pp. 12–14). IEEE. https://doi.org/10.1109/NFV-SDN47374.2019.9040101

Akhtar, N., & Mian, A. (2018). Threat of adversarial attacks on deep learning in computer vision: A survey. arXiv preprint, arXiv:1801.00553.

Al-Jumaili, A., Muniyandi, R., Hasan, M., Paw, J., & Singh, M. (2023). Big data analytics using cloud computing based frameworks for power management systems: Status, constraints, and future recommendations. Sensors, 23(2952). https://doi.org/10.3390/s23062952

Alshahrani, E., Alghazzawi, D., Alotaibi, R., & Rabie, O. (2022). Adversarial attacks against supervised machine learning-based network intrusion detection systems. PLOS ONE. https://doi.org/10.1371/journal.pone.0275971

Apruzzese, G., Colajanni, M., Ferretti, L., & Marchetti, M. (2019). Addressing adversarial attacks against security systems based on machine learning. In 2019 11th International Conference on Cyber Conflict: Silent Battle (Eds.). NATO CCD COE Publications, Tallinn.

Benaddi, H., Jouhari, M., Ibrahimi, K., Othman, J. B., & Amhoud, E. M. (2022). Anomaly detection in industrial IoT using distributional reinforcement learning and generative adversarial networks. Sensors, 22(8085). https://doi.org/10.3390/s22218085

Dudu, B., Luis, M., Yoram, H., Ariel, A., & Carlos, B. (2015). Software-defined wireless transport networks for flexible mobile backhaul in 5G systems. Mobile Networks and Applications, 20(6), 793–801. https://doi.org/10.1007/s11036-015-0635-y

Ghanem, K., Aparicio-Navarro, F., Kyriakopoulos, K., Lambotharan, S., & Chambers, J. (2017). Support vector machine for network intrusion and cyber-attack detection. IEEE SSPD, 1-5. https://doi.org/10.1109/SSPD.2017.8233268

Guangquan, X., Guofeng, F., Litao, J., Meiqi, F., Xi, Z., & Jian, L. (2021). FNet: A two-stream model for detecting adversarial attacks against 5G-based deep learning services. Wiley Online Library. https://doi.org/10.1155/2021/5395705

Ibitoye, O., Abou-Khamis, R., Matrawy, A., & Shafiq, O. (2020). The threat of adversarial attacks against machine learning in network security: A survey. ArXiv:1911.02621v2.

Liang, B., Li, H., Su, M., Li, X., Shi, W., & Wang, X. (2018). Detecting adversarial image examples in deep neural networks with adaptive noise reduction. IEEE Transactions on Dependable and Secure Computing, 18.

Liu, J., Zhang, W., & Zhang, Y. (2019). Detection-based defense against adversarial examples from the steganalysis point of view. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 4825–4834). IEEE.

Papernot, N., McDaniel, P., Goodfellow, I., Jha, S., Celik, Z., & Swami, A. (2017). Practical black-box attacks against machine learning. arXiv:1602.02697v4 [cs.CR]. https://doi.org/10.1145/3052973.3053009

Restuccia, F., D'oro, S., Al-Shawabka, A., Rendon, B., Chowdhury, K., Ioannidis, S., & Melodia, T. (2020). Generalized wireless adversarial deep learning. Proceedings of the 18th ACM International Conference on Mobile Systems, Applications, and Services, 49–54. https://doi.org/10.1145/3395352.3402625

Sharma, P., Austin, D., & Liu, H. (2019). Attacks on machine learning: Adversarial examples in connected and autonomous vehicles. IEEE HST, 1-7. https://doi.org/10.1109/HST47167.2019.9032989

Suryateja, P. (2023). Cloud computing threats, vulnerabilities and countermeasures: A state-of-the-art. iSecure, 1-58. https://doi.org/10.22042/isecure.2022.312328.718

Xu, G., Feng, G., Jiao, L., Feng, M., Zheng, X., & Liu, J. (2021). FNet: A two-stream model for detecting adversarial attacks against 5G-based deep learning services. Security Threats to Artificial Intelligence-Driven Wireless Communication System, Article ID 5395705. https://doi.org/10.1155/2021/5395705

Zhang, W., Sheng, Q., Alhazmi, A., & Li, C. (2020). Adversarial attacks on deep-learning models in natural language processing: A survey. ACM Transactions on Intelligent Systems and Technology (TIST), 11(3), Article 24, 1–41. https://doi.org/10.1145/3374217

Zolotukhin, M., Zhang, D., Hämäläinen, T., & Miraghaei, P. (2023). On attacking future 5G networks with adversarial examples: Survey. Network, 3, 39–90.