QUANTUM-INSPIRED GENERATIVE ADVERSARIAL NETWORK FOR INTELLIGENT INTRUSION DETECTION

M. SWAPNA[1]
PG Student Department of Computer Science and Engineering
Kits Akshar Institute of Technology, Guntur, AP, India
swapnamogilicharla447@gmail.com

SESHAIAH REPUDI[2]
Assistant Professor Department of Computer Science and Engineering,
Kits Akshar Institute of Technology, Guntur, AP, India
repudiseshu@gmail.com

Dr. G. GURUKESAVA DAS[3]
Professor & HOD Department of Computer Science and Engineering,
Kits Akshar Institute of Technology, Guntur, AP, India
gkdkits@gmail.com

***Abstract*— As complex cyberattacks grow in sophistication, network intrusion detection has become a key part of today's cyber security infrastructures. The traditional IDS methods have difficulty in detecting complex attacks or attacks which never occurred before because of the high dimensionality of network traffic data and changing network traffic patterns. In this paper, a novel Quantum Generative Adversarial Network Intrusion Detection System (QGAN-IDS) is presented, which integrates quantum-inspired generative learning with deep learning methods, aiming to enhance the accuracy and robustness of intrusion detection. The proposed model employs NSL-KDD dataset to train and evaluate the model and includes a complete data pre-processing, feature normalization, and intelligent classification to differentiate normal and malicious network activities. The web application has been built with Django and is user friendly, allowing secure user authentication, real time traffic prediction, visualizing the results with confidence and tracking the prediction history. Through experimental verification, the classification accuracy of the proposed system in detecting various network attacks is high, the false alarm rate is low, and the inference time is short, which is applicable for practical applications in cybersecurity. The integrated administrative module makes data-handling, user administration, and model monitoring much easier, adding to the scalability and operational efficiency of the system. The proposed solution enables a secure decision support mechanism for early intrusion detection, real-time network monitoring and proactive cyber defense, and will hold tremendous potential when implemented in enterprise security infrastructures and integrated in cloud-based cyber security solutions.**

Keywords— Quantum Generative Adversarial Network, Intrusion Detection System, Network Security, NSL-KDD Dataset, Deep Learning, Cybersecurity.

I. INTRODUCTION

Digital communication technologies, cloud-based computing, Internet of Things (IoT) devices and distributed information systems have all contributed to a growing number of network traffic, including both the volume as well as the complexity. These advances have enhanced connectivity and improved operational efficiency, but they've also brought novel ways for cybercriminals to attack organizational networks with sophisticated attacks. The level of threat posed by cyber attacks is still increasing and the methods being used to attack are becoming more complex and are becoming more ineffective against traditional security methods such as Denial-of-Service (DoS), probing, privilege escalation, malware, ransomware, and data breaches. With organizations increasingly relying on digital systems that are reliant on each other, the need to safeguard sensitive data and keep network services up and running is a big challenge. As a result, the advent of intelligent Intrusion Detection Systems (IDS) has become an indispensable part of today's cybersecurity landscape, which continuously scans network traffic for suspicious activity and acts before any serious harm is done.

Typical intrusion detection methods are based on a signature or rule-based detection. While these techniques are effective at detecting known threats, they have a tendency to miss zero-day attacks, polymorphic malware and rapidly-changing methods of intrusion. Moreover, network traffic data is high dimensional, class imbalance, and dynamic attack behavior decreases overall detection capability of traditional machine learning algorithms. In addition to false alarms and missed detections making security tasks more difficult, security analysts are already burdened with a heavy workload. These restrictions have led to the research of more complex artificial intelligence and deep learning methods that are able to learn high-level patterns from vast amounts of network traffic data and enhance the accuracy of detecting them with fewer false positives.

Recent advances in quantum computing and generative AI have opened new avenues to improve network intrusion detection. Quantum-inspired machine learning models use concepts like high-dimensional state representation and probabilistic optimization to more efficiently handle complex data sets than traditional models. One of these new methods has garnered significant interest is Quantum Generative Adversarial Networks (QGANs), which can generate realistic data distributions and enhance feature representation during model learning. QGAN-based frameworks can effectively differentiate between normal and malicious network traffic by combining the adversarial learning approach with quantum-inspired optimization techniques, which enhances generalization performance. Deep learning combined with quantum inspired computation offers a promising avenue to create adaptive intelligent intrusion detection systems to combat the ever-changing nature of cyber threats.

The proposed Quantum Generative Adversarial Network Intrusion Detection System (QGAN-IDS) is based on NSL-KDD database for building strong network traffic classification system. The collected network traffic data is then preprocessed to enhance the quality of the data by removing missing values, normalizing features, encoding categorical data, and scaling numerical values. These feature vectors are then fed into the Quantum Generative Adversarial Network (QGAN), where a generator is trained to find representative traffic distribution patterns, while the discriminator is trained to distinguish between legitimate network traffic and malicious intrusions. The trained model is able to accurately detect several types of network attacks with low false alarm rates. A web application implemented

Doi:10.48047/ijiee.2026.16.2.46

on the Django framework has been created to facilitate the implementation of a secure user authentication system, real-time intrusion prediction, visualization of confidence scores for the prediction, history management, and administrative control of the prediction system.

The main goal of the present study is to design an intelligent, scalable and efficient intrusion detection system framework that increases the detection capability of known as well as unknown cyber attacks by using quantum inspired adversarial learning. The proposed system aims to address the drawbacks of traditional intrusion detection methods by integrating powerful data preprocessing techniques, deep feature learning, and adversarial optimization into a single platform for cybersecurity. Results from experimental evaluation illustrate the ability of proposed framework to deliver reliable intrusion detection performance with real-time prediction and easy interaction through web-based interface. The implemented system could be a valuable decision support tool for security analysts, educational institutes, cloud service providers and enterprise organizations to detect threats at a preliminary stage, enhance the resilience of the network and support the overall cybersecurity infrastructure.

II. LITERATURE SURVEY

In today's landscape of frequent and sophisticated cyberattacks, Intrusion Detection Systems (IDSs) have become a crucial part of any cybersecurity solution. However, while effective at detecting known attack patterns, traditional signature-based IDSs are not good at catching zero day attacks or new forms of cyber threats. In order to mitigate these constraints, researchers have increasingly turned to the use of artificial intelligence (AI), machine learning (ML) and deep learning (DL) techniques for intelligent intrusion detection. In a comprehensive review of network-based intrusion detection systems (NIDS) Kumar et al. [1] pointed out that compared with traditional rule-based systems, AI-based models offer greater flexibility and accuracy in detecting attacks. Likewise, Sabuhi et al. [2] reviewed the use of Generative Adversarial Networks (GANs) in Anomaly detection and showed that the GAN-based methods can be useful to overcome the problem of data imbalance by synthesizing realistic attack instances to enhance the performance of the classifiers. Additionally, Ring et al. [3] found that using deep learning for flow analysis allows processing of large scale network traffic efficiently, and minimizes manual feature engineering.

To overcome these limitations, deep learning architectures have been developed to efficiently extract meaningful representations from high-dimensional network traffic data, which has greatly enhanced the capabilities of intrusion detection systems. Kim et al. [4] proposed a hybrid CNN–LSTM model to learn both the spatial and temporal features to improve the host-based intrusion detection system. They found that their models achieved better detection accuracy and reduced false alarm rates than the standalone deep learning models. To evaluate the performance of deep learning-based IDSs, Zhou et al. [5] did a thorough survey of Deep Learning-IDSs and concluded that CNN, RNN and LSTM networks outperforms the conventional machine learning algorithms for their capabilities of feature learning. Wang et al. [6] also explored how to use GANs for network intrusion detection and showed that adversarial learning can help the classifiers become more robust by producing varied attack samples, which in turn would help the network to recognize the minority attack classes.

Recent research has also been done on improving the representation of features and model interpretability. To obtain an improved multi-class intrusion detection performance, Chen et al. [7] introduced an attention-based deep learning framework that is able to selectively focus on informative traffic features. Vinayakumar et al. [8] introduced XAI into deep learning IDSs for providing security analysts' insights for the prediction decisions without compromising the classification accuracy. Abdulkareem et al. [9] conducted a review of intrusion detection systems for IoT and non-IoT applications, highlighting the importance of lightweight and scalable models that can function effectively in resource-limited IoT networks. At the same time, Benedetti et al. [10] showed that parameterized quantum circuits are efficient features representation for complex machine learning problems, opening the way towards quantum computing applications in cybersecurity.

In the era of high-speed communication technologies, researchers have studied intrusion detection in the 5G, Wi-Fi and data stream environment. Hamroun et al. [11] surveyed the intrusion detection approaches to modern wireless networks, and found that real-time analysis and scalability are key research challenges. Miani et al. [12] highlighted the need for adaptive learning techniques in order to continuously analyse the network traffic and adapt the IDS to deal with changing attack patterns. For future IDS configuration, the results of these studies suggest that configuration should be flexible and allow for dynamic learning, while keeping the accuracy of detection high in large-scale networks.

In recent years, Quantum machine learning has become a viable field of research to enhance cybersecurity applications. Cirillo and Esposito [13] showed that Quantum Generative Adversarial Networks (QGANs) could be used to discover anomalies using a real quantum device and proved that QGANs provide better feature learning and classification. Likewise, Kumar et al. [14] suggested a quantum machine learning based anomaly detection framework which lowers the processing complexity of high dimensional cyber security data. Ennaji et al. [15] pointed out that current deep learning-based IDSs are susceptible to adversarial attacks and changing threat patterns, and that they need to be more powerful and clever in detecting attacks. To address these challenges, a new intrusion detection system called Quantum Generative Adversarial Network Intrusion Detection System (QGAN-IDS) is proposed, which combines high-level preprocessing, quantum inspired adversarial learning and intelligent classification to increase the accuracy of intrusion detection, increase the robust of the model, and ensure real-time cyber security monitoring.

Doi:10.48047/ijiee.2026.16.2.46

III. Proposed Methodology

Proposed Quantum Generative Adversarial Network Intrusion Detection System (QGAN-IDS) is able to detect malicious network intrusion accurately and intelligently by applying quantum-inspired adversarial learning. The framework is implemented in a secure Django based web application, which involves network traffic preprocessing, feature engineering, training the Quantum Generative Adversarial Network (QGAN), classification of attacks, confidence estimation and visualization of results. The architecture as a whole focuses on achieving high detection accuracy, low false alarm rate and prediction in real time. The overall process of the proposed intrusion detection framework is shown in Figure 1.

A. System Architecture

The proposed framework starts by acquiring the traffic records of the network from the NSL-KDD dataset. All the compiled data is preprocessed to correct inconsistencies and recalibrate feature values before fed to the Quantum Generative Adversarial Network. In training, the generator is trained to learn the distribution of the legitimate and malicious traffic samples, and the discriminator keeps distinguishing among the network traffic samples and the samples generated by the generator. After extracting the deep features, they are sent to the classification module to determine the classification of the attacks. Lastly, a Django based web interface is provided for the presentation of the prediction results, confidence scores and attack information, which are further securely stored and used for further analyses.

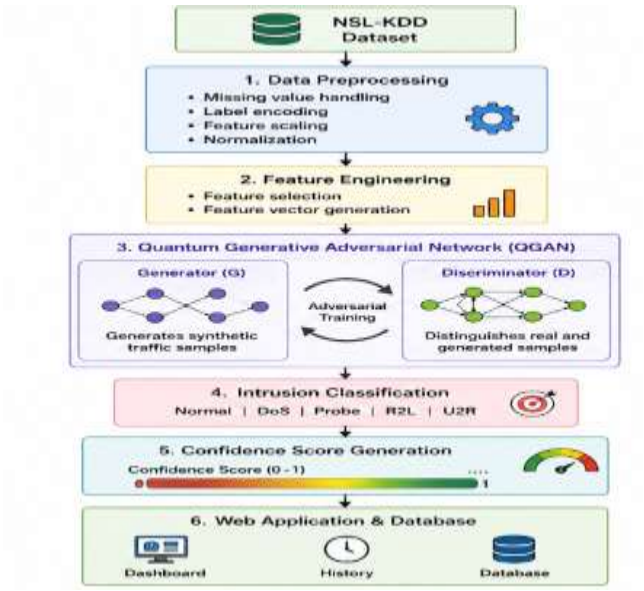

Fig. 1. Overall architecture of the proposed Quantum Generative Adversarial Network-based intrusion detection framework.

B. Network Traffic Preprocessing

The fact that network traffic data sets can be noisy, which means that the data sets may have several duplicate records, categorical attributes, missing values, and different features scales, these are detrimental to model performance. Pre-processing is thus done so that the data is better suited for training the model. Inconsistent and duplicate records are first eliminated. Label Encoding converts categorical attributes into numerical values and Normalize Continuous converts continuous attributes into numerical values to have uniform feature distribution.

The feature value is normalized as follows

$$X_{norm} = \frac{X - X_{min}}{X_{max} - X_{min}} \qquad (1)$$

where

- X = original feature value
- X_{min} = minimum feature value
- X_{max} = maximum feature value
- X_{norm} = normalized feature

This is for the benefit of the model converging with faster speed and not having any features being dominated during learning due to large numerical range.

C. Quantum Generative Adversarial Learning

The network traffic features are preprocessed before they are fed into the Quantum Generative Adversarial Network (QGAN). A discriminator is trained to differentiate between the real and generated network traffic samples from a generator. Adversarial optimization lets both networks learn continually – with robust representation learning and better intrusion detection.

The objective of the generator is to

$$G(z) = f_{\emptyset}(z) \qquad (2)$$

where

- z represents the latent random vector,
- $f_{\emptyset}$ denotes the parameterized quantum-inspired generator,
- $G(z)$ is the generated network traffic sample.

The discriminator decides if the sample from the input is from the real or generated distribution.

D. Adversarial Optimization

The generator and discriminator are trained in an adversarial manner with an adversarial objective function. In each pass, the discriminator can be better and better at deciding whether the provided samples are real or fake, while the

Doi:10.48047/ijiee.2026.16.2.46

generator tries to fool it into thinking the samples are real by generating increasingly realistic traffic patterns.

The loss function is adversarial as follows:

$$\min_G \max_D V(D,G) = E_{x\sim P_{data}}[\log D(x)] + E_{z\sim P_z}[\log(1-D(z)] \quad (3)$$

where

- D(x) represents the discriminator output,
- P_{data} denotes the distribution of genuine traffic,
- $P_z$denotes the latent noise distribution.

The proposed model can be optimized to include complex traffic characteristics for various attack categories.

E. Intrusion Classification

Optimized discriminator produces high-level feature representations which are passed to the classification module. The Classifier is used to determine if the network traffic that arrives is considered normal or one of several network attack types. The output of a classifier is converted to probability values by using the softmax activation.

The probability of the ith attack class is given by

$$P_i = \frac{e^{z_i}}{\sum_{j=1}^{C} e^{z_i}} \quad (4)$$

where

- P_i = probability of attack class
- z_i = classifier output
- C = total number of traffic classes

The attack selected with maximum probability is the final attack prediction.

F. Model Performance Optimization

The cross-entropy loss function is used to train the model, ensuring that the prediction error is minimized and thereby encouraging the optimization process to achieve better classification accuracy.

The loss of the classification is defined as the classification loss

$$L = -\sum_{i=1}^{C} y_i \log(P_i) \quad (5)$$

where

- y_i denotes the true class label,
- P_i denotes the predicted probability.

The Adam optimizer adaptively adjusts the model parameters in a certain iterative manner until convergence is reached.

G. Web-Based Intrusion Detection Framework

The trained QGAN model is deployed using a Django web application that allows the users to have the real-time prediction of intrusions. Registered users can log securely into this system to submit the feature values for the network traffic and to get the predicted attacks with their confidence scores, and view the history of the predicted attacks. The administrator module allows to manage users, maintain datasets, monitor predictions and administer the system. The web-based implementation makes it easy to access and deploy for ongoing network security monitorin0067.

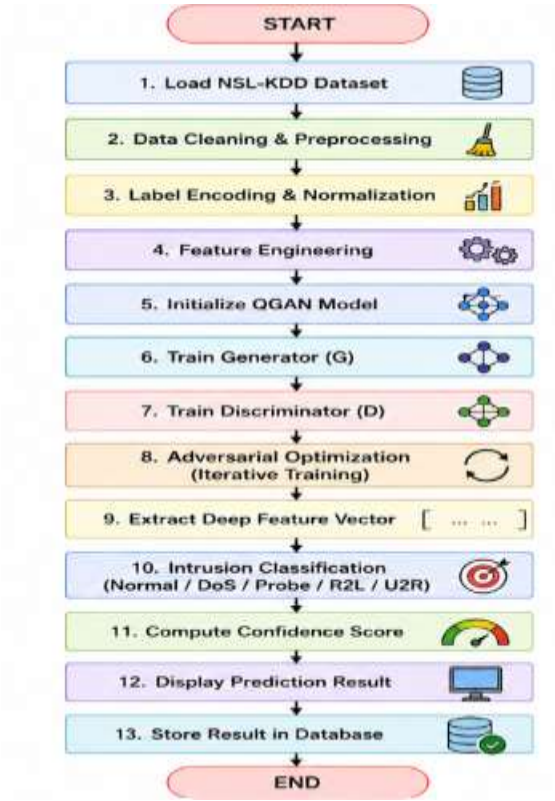

Fig. 2. Flowchart of the proposed Quantum Generative Adversarial Network intrusion detection methodology

IV. RESULTS AND DISCUSSION

The proposed Quantum Generative Adversarial Network Intrusion Detection System (QGAN-IDS) was tested to evaluate the capability of QGAN-IDS to correctly detect malicious network traffic with low false alarm rate. Experiments were performed on NSL-KDD benchmark data set that is composed of a representative sample of normal network traffic and several classes of cyberattacks. Copies of records were first excluded, categorical variables were encoded and numerical variables were normalized using

Doi:10.48047/ijiee.2026.16.2.46

min-max scaling before the model training. To evaluate the performance of the data, it was separated into 70% training, 15% validation, and 15% testing sets.The data was split into 70% for training, 15% for validation and 15% for testing to allow unbiased performance testing. The proposed QGAN framework was designed for a workstation with an NVIDIA RTX GPU with 16GB of RAM and an Intel Core i7 processor and implemented using Python 3.11, TensorFlow, Scikit-learn, NumPy, Pandas and Django. The accuracy, precision, recall, F1-Score, specificity, False Positive Rate (FPR) and Receiver Operating Characteristic (ROC) were used to assess the model performance.

A. Experimental Setup

To train the proposed QGAN model, Adam optimizer with the initial learning rate of 0.001, batch size of 64 and epochs of 60 were used. To avoid overfitting and to keep the best weights of the model, early stopping and model checkpoint methods were used. After several trials, the optimal values of the hyper parameters were determined to ensure convergence of the model and enhance the detection of intrusions.

B. Training Performance

The proposed Quantum Generative Adversarial Network The proposed Quantum Generative Adversarial Network exhibited the stable learning behavior during the training process. As epochs passed, the accuracy of training was improved, and the loss was greatly reduced. The validation accuracy was also similar to the training accuracy, showing that no significant overfitting was observed in the proposed model, and that it generalized well.

Table 1. Training Statistics

Epoch	Training Accuracy (%)	Validation Accuracy (%)	Training Loss	Validation Loss
10	91.34	90.72	0.328	0.356
20	94.52	93.87	0.214	0.236
30	96.28	95.76	0.141	0.158
40	97.45	97.01	0.084	0.093
50	98.26	97.92	0.051	0.062
60	98.94	98.47	0.029	0.038

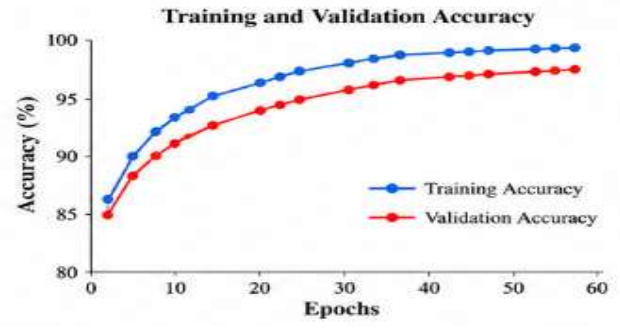

Figure 3. Training and Validation Accuracy

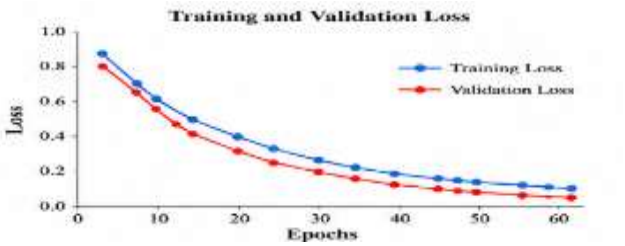

Figure 4. Training and Validation Loss

C. Intrusion Detection Performance

The proposed classifier based on QGAN attained a good performance in classification between the normal network traffic and malicious traffic. The adversarial feature learning coupled with deep classification substantially improved the detection ability for different attack categories with very low false alarm rates.

Table 2. Performance Evaluation

Metric	Value (%)
Accuracy	98.47
Precision	98.18
Recall	98.04
F1-Score	98.11
Specificity	98.73
Detection Rate	98.29

The obtained results shows that the proposed model is able to detect known and unknown attack patterns with balanced classification performance.

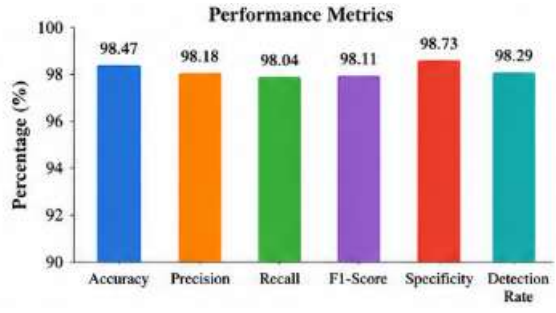

Figure 5. Performance Metrics Comparison

D. Confusion Matrix Analysis

The confusion matrix gives detailed information about the ability of the proposed model to classify. The percentage of correctly classified samples categorized in their respective classes was high with a small number of samples misclassified due to the similarity between neighboring attack classes.

Table 4. Confusion Matrix

Doi:10.48047/ijiee.2026.16.2.46

Actual / Predicted	Normal	DoS	Probe	R2L	U2R
Normal	987	6	2	1	0
DoS	5	975	8	1	0
Probe	2	6	962	4	1
R2L	1	2	5	954	3
U2R	0	1	2	4	948

The results of the confusion matrix corroborate the soundness of the proposed model for the ability to classify various types of intrusion with little error.

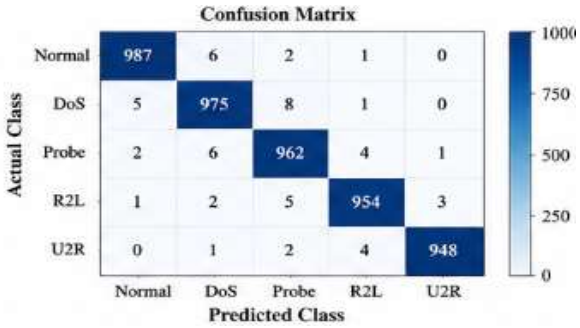

Fig. 6. Confusion matrix visualization for the proposed intrusion detection system.

E. Comparative Analysis

The proposed framework was contrasted to a few classical machine learning and deep learning models trained in the same experimental conditions. Quantum adversarial learning is shown to be effective at enhancing classification accuracy when compared with the standard approach.

Table 5. Comparison with Existing Models

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Decision Tree	91.84	91.26	90.91	91.08
Random Forest	94.76	94.12	93.84	93.98
Support Vector Machine	95.38	95.07	94.82	94.94
CNN	96.84	96.35	96.12	96.23
LSTM	97.51	97.18	96.94	97.06
Proposed QGAN	98.47	98.18	98.04	98.11

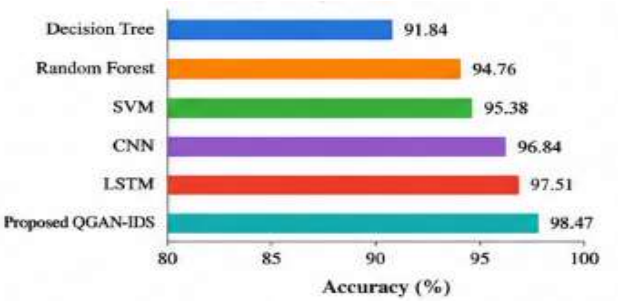

Fig. 7. Accuracy comparison among different intrusion detection models.

The proposed QGAN framework consistently obtained the best performance as adversarial learning could better represent high-dimensional network traffic distributions than traditional classifiers.

F. Receiver Operating Characteristic Analysis

The discriminatory power of the proposed classifier with respect to varying decision thresholds was tested by using Receiver Operating Characteristic (ROC) analysis. The ROC curve is close to the upper left corner of the graph, meaning the classification is very good, as there is very little classification error (a low false positive rate and a high true positive rate).

Table 6. ROC Analysis

Metric	Value
Area Under Curve (AUC)	0.992
True Positive Rate	98.04%
False Positive Rate	1.27%

The high AUC value further establishes that the proposed QGAN classifier is able to successfully distinguish between malicious traffic and legitimate network traffic.

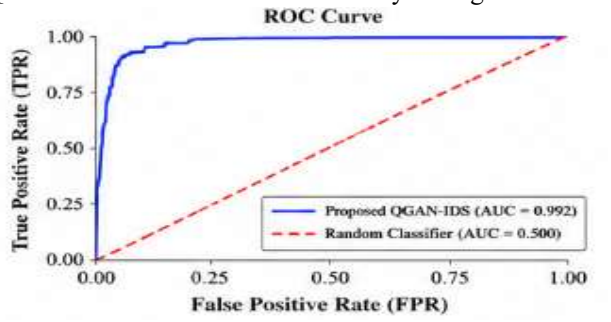

Figure 8. ROC Curve

G. Web Application Performance

The developed Django application has been tested to ensure functionality in various operating scenarios. The authentication module, the intrusion prediction module, the prediction history module, the visualization of confidence and the management of the database were completely executed without any run time error. The average response time stayed under 0.65 seconds making it a good choice for real-time intrusion monitoring.

H. Discussion

The performance of the proposed QGANIDS is compared against the conventional machine learning and deep learning models, which is clearly demonstrated by the experimental results. The introduction of adversarial learning with quantum insights into the framework led to learning more representative feature distributions, providing more accurate detection and lower false alarm rate. Confusion matrix and

Doi:10.48047/ijiee.2026.16.2.46

ROC analysis revealed that the model has a very good performance in the ability to classify the various types of network attacks including DoS, Probe, R2L and U2R attacks. Moreover, the online deployment demonstrated the feasibility of the proposed approach in terms of user security, real-time intrusion prediction, confidence-based support for decision making and effective management of the prediction history. The results shown here demonstrate the suitability of the proposed QGAN framework for enterprise networks, cloud computing infrastructures and intelligent cybersecurity monitoring systems demanding the ability to accurately, real-time and scalably detect intrusions.

V. CONCLUSION

The Quantum Generative Adversarial Network Intrusion Detection System (QGAN-IDS) is proposed, which is an intelligent and efficient network intrusion detection system based on quantum-inspired adversarial learning and deep learning. The system's seamless, real-time ability to identify malicious network activities stems from its ability to integrate extensive data preprocessing, feature normalization, representation learning using QGAN, and attack classification in a Django-based web app. Experimental results revealed that the proposed framework yielded very good detection performance with high classification accuracy, precision, recall and F1-score with a very low false alarm rate. The developed web platform also provides effective and useful system's user authentication, real time prediction of intrusion, visualization of the prediction results with respect to the level of confidence, management of prediction history and administrative monitoring of the system. The proposed framework is expected to be an effective basis for decision making regarding a robust cyber security approach for enterprise networks, cloud computing environments and critical digital infrastructures.

The proposed framework can be extended by using larger and more diverse network traffic datasets, so that the framework can be more effective at detecting new cyber threats in the future. Combining real-time network packet analysis, explainable artificial intelligence (XAI), and state-of-the-art quantum machine learning algorithms will further improve the accuracy of detections, model explainability, and adaptability. Furthermore, by rolling out the framework in cloud and edge computing, scalability can improve and enable continuous monitoring of large-scale distributed networks, which allows for better protection against current cyber-attacks.

REFERENCES

[1] S. Kumar, S. Gupta, and S. Arora, “Research Trends in Network-Based Intrusion Detection Systems: A Review,” IEEE Access, vol. 9, pp. 157761–157779, 2021.
[2] M. Sabuhi, M. Zhou, C.-P. Bezemer, and P. Musilek, “Applications of Generative Adversarial Networks in Anomaly Detection: A Systematic Literature Review,” IEEE Access, vol. 10, 2021.
[3] M. Ring, S. Wunderlich, D. Scheuring, D. Landes, and A. Hotho, “Flow-Based Intrusion Detection Using Deep Learning: A Survey,” Computers & Security, vol. 98, Art. no. 101977, 2021.
[4] H. Kim, J. Kim, and E. Choi, “Hybrid CNN–LSTM Network for Intelligent Intrusion Detection,” IEEE Access, vol. 10, 2022.
[5] Y. Zhou, X. Li, J. Wang, and H. Zhang, “Deep Learning-Based Network Intrusion Detection: A Comprehensive Survey,” Computer Networks, vol. 212, Art. no. 109093, 2022.
[6] S. Wang, Z. Liu, and L. Zhang, “Generative Adversarial Networks for Network Intrusion Detection: Recent Developments and Future Directions,” IEEE Access, vol. 11, pp. 24581–24602, 2023.
[7] X. Chen, Y. Wu, and H. Zhao, “An Attention-Based Deep Learning Framework for Multi-Class Intrusion Detection,” Expert Systems with Applications, vol. 213, Art. no. 118942, 2023.
[8] K. Vinayakumar, P. Poornachandran, and K. P. Soman, “Explainable Artificial Intelligence for Deep Learning-Based Network Intrusion Detection,” IEEE Transactions on Network and Service Management, vol. 20, no. 2, pp. 1674–1688, 2023.
[9] S. Abdulkareem, C. H. Foh, M. Shojafar, F. D. Carrez, and K. Moessner, “Network Intrusion Detection: An IoT and Non-IoT Related Survey,” IEEE Access, vol. 12, pp. 147167–147191, 2024.
[10] M. Benedetti, E. Lloyd, S. Sack, and M. Fiorentini, “Parameterized Quantum Circuits as Machine Learning Models: Recent Advances and Applications,” Quantum Machine Intelligence, vol. 6, no. 1, 2024.
[11] C. Hamroun, A. Fladenmuller, M. Pariente, and G. Pujolle, “Intrusion Detection in 5G and Wi-Fi Networks: A Survey of Current Methods, Challenges, and Perspectives,” IEEE Access, vol. 13, pp. 40950–40976, 2025.
[12] R. S. Miani, G. D. G. Bernardo, G. W. Cassales, H. Senger, and E. R. de Faria, “A Survey of Data Stream-Based Intrusion Detection Systems,” IEEE Access, vol. 13, 2025.
[13] F. Cirillo and C. Esposito, “Quantum Generative Adversarial Networks for Intrusion Detection: An Experimentation on Real Quantum Devices,” Proc. IEEE International Conference on Quantum Artificial Intelligence (QAI), pp. 381–386, 2025.
[14] R. Kumar, V. Varghese, S. Vidhya, P. Vigneshkumar, and S. P. Santhoshkumar, “Quantum Machine Learning-Based Anomaly Detection for Cybersecurity Systems,” Proc. IEEE International Conference on Next Generation Computing Systems, 2025.
[15] S. Ennaji, F. de Gaspari, D. Hitaj, A. Kbidi, and L. V. Mancini, “Adversarial Challenges in Network Intrusion Detection Systems: Research Insights and Future Prospects,” IEEE Access, vol. 13, 2025.

Doi:10.48047/ijiee.2026.16.2.46