Hybrid Quantum-Classical Intrusion Detection System for Next-Gen Networks

Appadi Geethika[1], Ashamolla Harshika[2], Vippari Neha[3], Dr. Potu Narayana[4]
[1,2,3] *Department of Computer Science and Engineering Stanley College of Engineering & Technology for Women Hyderabad, India.*
[4]*Associate Professor, Department of Computer Science and Engineering Stanley College of Engineering and Technology for Women Hyderabad, India*

***Abstract*—The current state of computer networks today experiences severe cybersecurity threats which include unauthorized access and malware attacks and data breaches. The detection of complex patterns through traditional intrusion detection systems faces challenges because they cannot handle the detection process which needs to analyze network traffic in modern network environments. The proposed research solution establishes a Quantum– Classical Intrusion Detection System which the researchers designed for next-gen network systems. The system uses network flow data to implement feature extraction and classification mechanisms which identify malicious traffic patterns. The hybrid quantum–classical model improves detection capability by combining the efficiency of algorithms with the advanced potential of quantum methods. The proposed system protects environments through enhanced security measures which increase threat detection accuracy and establish a dependable protection system for next-gen network environments against emerging cyber threats.**

***Index Terms*—Intrusion Detection System, QuantumClassical Computing, Network Security, Cyber Attack Detection, UNSW-NB15 Dataset, Machine Learning, Network Traffic Analysis, Cybersecurity Monitoring, Anomaly Detection, Artificial Intelligence, Distributed Systems, Next-Generation Networks.**

I. INTRODUCTION

Modern computer networks are becoming more complicated because they face multiple cybersecurity threats which include malware attacks and unauthorized access and denial-of-service attacks and data breaches. Traditional intrusion detection systems face three major difficulties which include limited accuracy for detecting threats and challenges in detecting advanced attack techniques and their struggle to process substantial network traffic. The increasing need for intelligent intrusion detection solutions has become essential because advanced networking technologies and digital communication systems continue to grow. The recent developments in artificial intelligence and machine learning and quantum computing have created fresh possibilities to enhance cybersecurity methods. Quantum-classical hybrid approaches enable the combination of traditional machine learning methods with the new computational power that quantum technologies bring. The combination of these methods allows intrusion detection systems to enhance their ability to monitor intricate network traffic patterns while achieving better results for finding both existing and new cyber threats. The proposed Quantum–Classical Intrusion Detection System architecture for next-generation networks collects network traffic data and extracts features and conducts hybrid quantum-classical processing and displays intrusion detection results. The system uses advanced computational techniques to analyze network traffic features which it then classifies into normal and malicious categories. The proposed quantum-classical intrusion detection framework enhances cybersecurity monitoring capabilities while detecting attacks more effectively and delivering an efficient solution to protect next-generation systems.

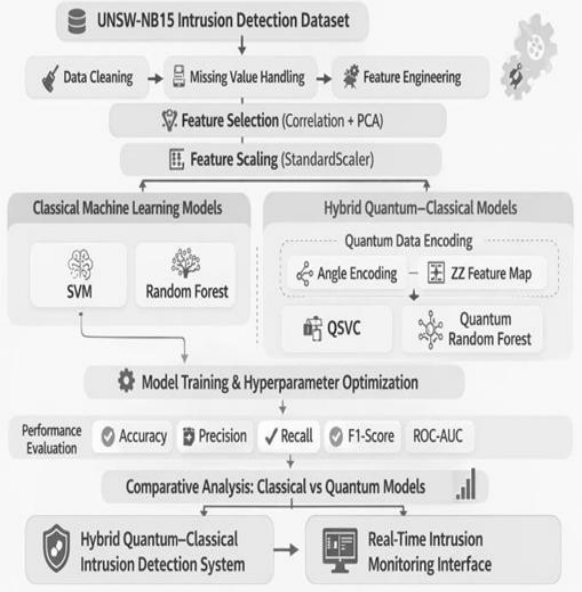


Figure 1: System architecture of Hybrid Quantum-Classical Intrusion Detection System

II. LITERATURE REVIEW

The recent development of quantum computing together with machine learning technologies has enhanced the functioning of modern computer network intrusion detection systems. The traditional intrusion detection systems fail to identify sophisticated cyberattacks which operate in high-dimensional space because they depend on standard rule-based systems and traditional machine learning methods. The research shows that using quantum computing together with classical systems leads to better results when tracking advanced network attacks. The researchers studied different methods for quantum to classical encoding which demonstrated that hybrid intrusion detection systems could successfully process high-dimensional attack data through variational quantum circuits while different encoding methods including Amplitude Angle IQP and QAOA affected their detection ability [1]. The researchers introduced quantum-based outlier analysis methods which use quantum state fidelity and entropy-based anomaly detection to enhance detection abilities for distributed denial-of-service and zero-day attacks. The research community has studied machine learning methods that combine hybrid quantum and classical methods to create network intrusion detection systems which function in multiple settings. Researchers have developed quantum- based outlier detection methods which enhance their ability to identify distributed denial-of-service attacks and zero-day attacks through their usage of quantum state fidelity and entropy-based anomaly detection systems [2].

Different researchers have studied how to use hybrid quantum–classical machine learning methods for network intrusion detection in various environments. Quantum Support Vector Classifiers and Quantum Random Forest models have demonstrated superior performance compared to classical algorithms when applied to IoT and network security datasets such as UNSW-NB15 [3]. The combination of classical neural networks with quantum processing layers has been developed in hybrid frameworks to improve threat detection in distributed systems. Hybrid quantum– classical neural network models which combine wavelet transforms with convolutional neural networks and quantum layers have demonstrated better capabilities to identify distributed denial-of-service attacks and malware threats in software-defined networks [6]. The research work studied quantum machine learning-based intrusion detection models which operate on new network infrastructure systems. The study found that quantum machine learning-based intrusion detection systems which employ variational quantum circuits achieve effective results in detecting both binary and multiclass security threats [5]. Researchers developed feature optimization methods which work with quantum support vector machines to decrease false positive rates while enhancing detection accuracy in intrusion detection systems [8]. Quantum security systems which combine quantum key distribution and intrusion detection systems have been developed to strengthen IoT networks and smart city systems against cyber threats [4].

Research efforts investigate how machine learning and quantum technologies affect cybersecurity through their various applications. The systematic review of anomaly detection methods shows that quantum machine learning techniques have become essential for enhancing both intrusion detection accuracy and scalability in IoT networks[7]. Explainable artificial intelligence research shows that using SHAP, LIME, and ELI5 systems to enhance machine learning-based intrusion detection system transparency will help cybersecurity professionals understand how models reach their decisions [9]. The

research study proved that organizations can use quantum machine learning systems for intrusion detection because they can successfully operate on existing quantum hardware despite current equipment limitations [10].

III. PROPOSED METHODOLOGY

The Quantum–Classical Intrusion Detection System which has been proposed will use classical machine learning methods together with quantum-inspired models to identify security threats in future networks. The system analyzes network traffic data through multiple stages including dataset preparation, feature engineering, hybrid quantum– classical classification, and intrusion monitoring.

A. Dataset and Data Preprocessing

The proposed system starts its first stage by collecting network traffic data from the UNSW-NB15 dataset which contains both normal network activities and multiple types of cyber attacks. The dataset provides various network flow features that help the model understand different traffic patterns. The preprocessing of data creates a prepared dataset which enables subsequent model training. The process involves three main tasks which include data cleaning, elimination of duplicate features, and processing of absent data, while the dataset gets converted into a machine learning compatible structured format.

B. Feature Engineering and Scaling

The researchers choose appropriate network traffic features after preprocessing because these features will enhance model performance while decreasing the time needed for computations. Feature engineering helps identify the most important attributes that contribute to intrusion detection. The dataset undergoes feature scaling procedures which standardize its various attributes to a consistent measurement scale. The step establishes a model training performance which will maintain stability throughout its training process.

C. Hybrid Quantum–Classical Classification

The researchers conduct their analysis of the processed data through a hybrid quantum–classical learning framework. The initial pattern analysis uses classical machine learning techniques while the classification process receives enhancement from quantum-inspired models. The Quantum Support Vector Classifier (QSVC) identifies network traffic patterns which it categorizes into normal and malicious traffic. The hybrid method combines classical algorithms' efficient performance with quantum computing concepts' advanced pattern recognition skills.

D. Intrusion Detection and Monitoring

The system uses model training results to determine whether incoming network traffic demonstrates standard behavior or indicates a cyber attack. The monitoring interface displays detection results through a web-based dashboard which shows the results to users. This interface allows users to visualize prediction results analyze network behavior and monitor intrusion detection logs for effective cybersecurity monitoring in next-generation network environments. The hybrid system uses classical algorithms for efficient processing while it implements quantum computing concepts to achieve advanced pattern detection capabilities.

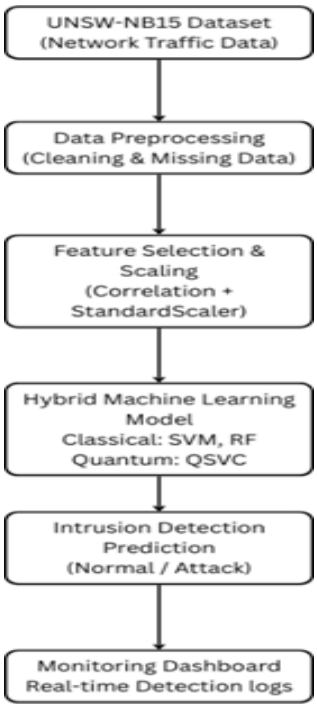


Figure 2. Workflow of Hybrid Quantum-Classical Intrusion Detection System

III. RESULTS AND DISCUSSION

The Hybrid Quantum–Classical Intrusion Detection System . (HQ-IDS) was developed as a software solution that engineers built with Python to operate in high- performance computing systems. The experimental platform used an Intel i7 processor together with 16 GB RAM and SSD storage to achieve effective model training and inference. The system uses classical machine learning algorithms together with quantum-enhanced models to achieve better intrusion detection performance in modern network environments. The development team created a Streamlit-based web monitoring interface that shows real-time results while continuously tracking intrusion detection activities. The evaluation of performance used two types of metrics which included model-level metrics and system-level metrics. The proposed framework functions as a machine learning-based intrusion detection system which requires standard classification metrics for evaluation. The system-level performance assessment

A. Performance Metrics and Evaluation

The researchers used the entire UNSW-NB15 dataset to train their classical machine learning models, which they tested to create their most accurate baseline results.

1) Random Forest Classifier

The Random Forest model achieved an accuracy of 90.46%, demonstrating strong capability in distinguishing between malicious and normal network traffic. The ensemble learning framework uses multiple decision trees to create a stable prediction model which decreases the chances of overfitting because it combines the predictions of various tree-based models.

The system achieved high precision and high recall results, which demonstrated trustworthy intrusion detection capabilities that produced few false alerts and failed to catch only a small number of attacks. The Random Forest algorithm functions effectively in large cybersecurity systems.

2) Linear Support Vector Machine

The Linear SVM model achieved an accuracy of 82.74%. The Linear SVM algorithm enables quick classification of extensive data sets, making it valuable in situations where organizations require swift results instead of achieving the highest accuracy.

B. Quantum Model Performance

The researchers selected the top eight features because the feature count determines the number of qubits needed for the system. 7) System Stability Under Continuous Monitoring System stability evaluates reliability during prolonged monitoring sessions. The system received 500 continuous detection requests which it successfully detected 500 times. The system maintained consistent performance throughout its operation without experiencing crashes or memory overflow or execution interruptions.

C. Intrusion Detection Output Validation

The trained hybrid model classified generated traffic samples into two categories which were Normal Traffic and Intrusion Attack. The system monitoring interface displayed prediction results together with network traffic feature logs to provide transparent access to network activity information.

Example Outputs:

- Traffic Sample 1 → Normal Traffic
- Traffic Sample 2 →Intrusion Detected
- Traffic Sample 3 →Normal Traffic
- Traffic Sample 4 →Intrusion Detected

The outputs demonstrate that the detection system operates according to its intended functions.

TABLE 1: PERFORMANCE EVALUATION SUMMARY OF PROPOSED SYSTEM

S.No	Performance Metric	Formula Used	Observed Value
1	Accuracy (ACC)	(TP+TN)/(TP+TN+FP+FN)	90.46%
2	Precision (PR)	TP/(TP+FP)	98.73%
3	Recall	TP/(TP+FN)	87.10%
4	F1-Score	2(PR×RC)/(PR+RC)	92.55%
5	Detection Processing Time	T_pre + T_pred	1.28sec

6	Real-Time Detection Rate	Success/Total ×100	100%
7	System Stability Rate	Success/Total ×100	100%

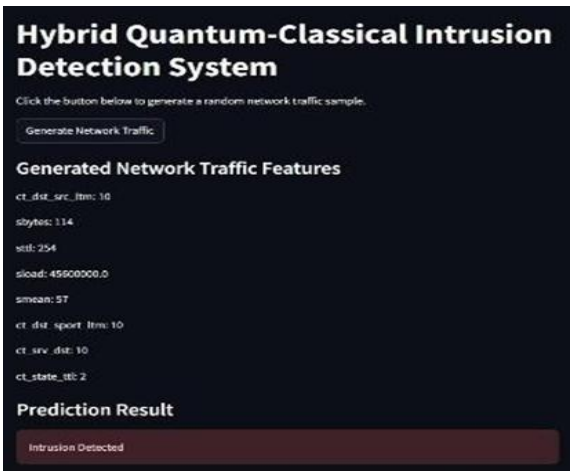
The Hybrid Quantum–Classical Intrusion Detection System which we developed demonstrates three main performance areas and two additional benefits, which together produce system performance excellence. The system detects security threats with high accuracy because it processes security events with fast response times while maintaining its ability to function in real time. The system maintains its stable performance through its ability to monitor operations at all times. The system achieves better classification results through the combination of quantum machine learning and classical machine learning methods which maintain the system's ability to perform in real time. The monitoring dashboard which we developed, allows users to operate, because it shows active security threats through its complete detection system.

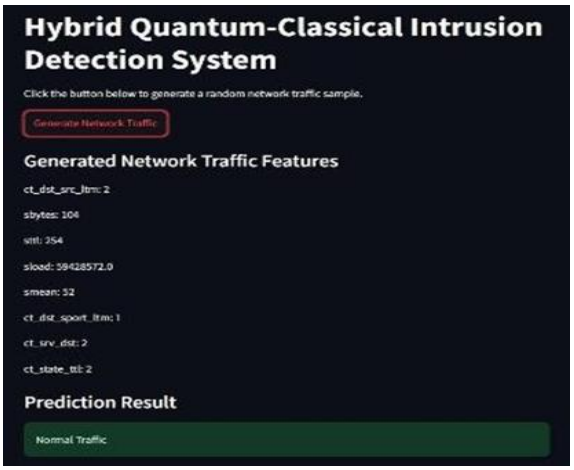
V. CONCLUSION

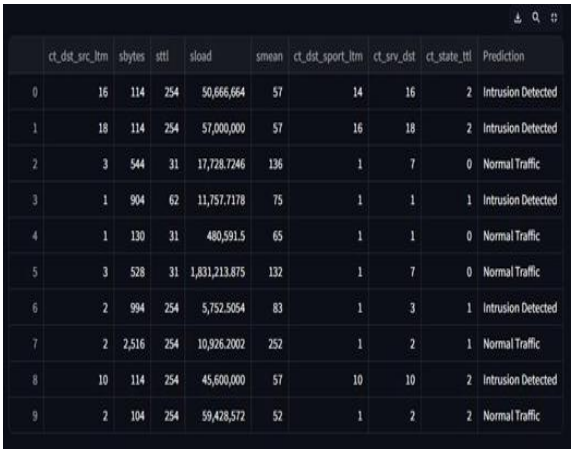
The research presents a Hybrid Quantum-Classical Intrusion Detection System, which improves network security protection for future network systems. Cyberattack detection through traditional intrusion detection systems becomes impossible because network traffic patterns and attack methodologies have become more intricate. The proposed system uses classical machine learning methods together with quantum machine learning methods to boost its ability to detect intrusions. The system uses classical algorithms to select features and preprocess data, while quantum classification models evaluate network traffic patterns through high-dimensional quantum feature space analysis.

The hybrid approach successfully detects malicious network traffic through its experimental evaluation which shows better detection results than traditional methods. The combination of quantum computing technologies with cybersecurity applications develops into a research area which holds great potential for future progress.

The evolution of quantum computing technologies will establish hybrid quantum-classical systems as key components which protect modern network systems against new cyber threats while enhancing cybersecurity infrastructure defense.







	ct_dst_src_ltm	sbytes	sttl	sload	smean	ct_dst_sport_ltm	ct_srv_dst	ct_state_ttl	Prediction
0	16	114	254	50,666,664	57	14	16	2	Intrusion Detected
1	18	114	254	57,000,000	57	16	18	2	Intrusion Detected
2	3	544	31	17,728.7246	136	1	7	0	Normal Traffic
3	1	904	62	11,757.7178	75	1	1	1	Intrusion Detected
4	1	130	31	480,591.5	65	1	1	0	Normal Traffic
5	3	528	31	1,831,213.875	132	1	7	0	Normal Traffic
6	2	994	254	5,752.5054	83	1	3	1	Intrusion Detected
7	2	2,516	254	10,926.2002	252	1	2	1	Normal Traffic
8	10	114	254	45,600,000	57	10	10	2	Intrusion Detected
9	2	104	254	59,428,572	52	1	2	2	Normal Traffic

REFERENCES

[1] B. Kadi, M. A. Ferrag, L. Shu and X. Yang, "An In-Depth Comparative Study of Quantum–Classical Encoding Methods for Network Intrusion Detection," IEEE Open Journal of the Communications Society, vol. 6, pp. 1–17, 2025.

[2] S. Kim and R. Madhavi, "Quantum Intrusion Detection System Using Outlier Analysis," Scientific Reports (Nature), vol. 14, no. 11265, pp. 1–14, 2024.

[3] R. Singh, P. Narang and D. Sharma, "Internet of Things Network Intrusion Detection Using Quantum and Classical Machine Learning," IET Quantum Communication, vol. 3, no. 1, pp. 25–40, 2025.

[4] M. Al-Khalili, A. Rahman and Y. Chen, "QESIF: A Lightweight Quantum Enhanced IoT Security Framework for Smart Cities," Smart Cities (MDPI), vol. 8, no. 2, pp. 45–63, 2025.

[5] J. Marques, L. Souza and F. Costa, "QML-IDS: Quantum Machine Learning Based Intrusion Detection System," Proc. IEEE SISY International Conference on Intelligent Systems and Informatics, 2025, pp. 122–129.

[6] Z. Abbas, T. Ahmed and S. Khan, "Unified Hybrid Quantum–Classical Neural Network Framework for Detecting Distributed Denial of Service and Android Malware Attacks," EPJ Quantum Technology (Springer), vol. 12, no. 6, pp. 1–22, 2025.

[7] R. Aparcana-Tasayco and J. Luna, "A Systematic Review of Anomaly Detection in IoT Security: Towards Quantum Machine Learning Approach," EPJ Quantum Technology (Springer), vol. 11, no. 4, pp. 1–36, 2025.

[8] A. El-Sayed, M. M. Hassan and K. Li, "A Novel Intrusion Detection System Based on a Hybrid Quantum Support Vector Machine and Improved Grey Wolf Optimizer Algorithm," Cluster Computing (Springer), vol. 27, no. 3, pp. 1455 1472, 2024.

[9] Y. Hussein, F. Omar and S. Abdulrahman, "Evaluating Machine Learning Based Intrusion Detection Systems With Explainable AI: Enhancing Transparency and Interpretability," Frontiers in Computer Science, vol. 6, pp. 1 14, 2025.

[10] T. Martins and A. Ribeiro, "Quantum Machine Learning- Based Intrusion Detection: A Comparative Study on Real Quantum Hardware," Proc. IEEE SISY International Symposium on Intelligent Systems and Informatics, 2025, pp. 210 217.