Svedberg Open
DISSEMINATION OF KNOWLEDGE

International Journal of Artificial Intelligence and Machine Learning

Publisher's Home Page: https://www.svedbergopen.com/

Research Paper Open Access

Quantum Machine Learning-Driven Cyber Security Architecture for Real-Time Intrusion Detection in Distributed Computing Systems

Dipti Yashodhan Sakhare[1], Nivetha N[2], Gagan Tiwari[3], Dr.Jagdish Gohil[4], S SVidya Balantrapu[5], Dr.Pavan kumar[6], Dr.Priyanka Samal[7], Aswitha V[8]

[1]Department of Electronics and Telecommunication Engineering,MIT Academy of Engineering, Alandi, Email: Punedipti.sakhare@mitaoe.ac.in
[2]Computer Science, Assistant Professor, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India, Email:nivethan@maher.ac.in
[3]Department of Computer Sciences, Noida international University, Greater Noida, Uttar Pradesh 203201, India, Email: gagan.tiwari@niu.edu.in
[4]Dean, ,Parul Institute of Medical Sciences and Research, Parul University, Vadodara, Gujarat, India, Email: Jagdish.gohil@paruluniversity.ac.in, 0009-0006-2927-9107
[5]Assistant professor, Department of ECE, Aditya University, Surampalem, Kakinada Andhra Pradesh Email: vidyalalli@gmail.com Orcid ID: 0009-0006-3537-7707
[6]Associate Professor , MSOPS, Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India, Email: pavan.kumar@muit.in, Orcid Id- https://orcid.org/0009-0007-3351-703X
[7]Professor, Department of Haematology, IMS and SUM Hospital, Siksha 'O' Anusandhan (Deemed to be University), Bhubaneswar, Odisha, India, Email: priyankasamal@soa.ac.in, Orcid Id- 0000-0002-9129-7967
[8]English, Assistant Professor, Meenakshi College of Arts and Science, Meenakshi Academy of Higher Education and Research, Chennai, Tamil Nadu, India , Email: aswithav@maher.ac.in

Abstract

The active development of distributed computing systems and cloud-based networks has greatly exposed the modern network to advanced cyber-attacks thus necessitating a quick and timely intrusion detection system that is intelligent and capable of identifying malicious activities with low latency and high accuracy. The major weaknesses of traditional machine learning-based intrusion detection systems (IDS) are poor scalability, inefficiency in processing high dimensional security data, increased false positive rates, and lower detection performance with changing attack patterns. To overcome these difficulties, this study suggests a Quantum Support Vector Machine (QSVM)-based building on Quantum machine learning (Quantum ML) powered cyber security system with real-time intrusion detection in distributed computing infrastructure. The suggested framework will combine network traffic gathering, preprocessing, quantum feature encoding, and QSVM-based attack identification to improve the effectiveness of cybersecurity intelligence and threat detection. Experimental validation and performance analysis of the system in different cyberattack situations are done using the CICIDS2017 and UNSW-NB15 benchmark intrusion detection datasets. The applicability of the offered architecture is tested with the help of essential classification measures such as Accuracy, Precision, Recall, and F1-score which show that the proposed architecture has a better intrusion detection potential than the traditional machine learning techniques. The experimental findings were that the QSVM-based framework yields a high classification accuracy, detection reliability, false alarms, and real-time threat identification which leads to design of scalable, intelligent and next-generation quantum-enhanced cybersecurity systems in distributed computing settings.

Keywords: Quantum Machine Learning, QSVM, Cyber Security, Intrusion Detection System, Distributed Computing, Real-Time Detection, Artificial Intelligence.

1. Introduction

Modern digital communication and data processing environments have been profoundly altered by the emergence of the rapidly developing distributed computing systems, cloud computing infrastructures, edge

computing systems, and Internet-connected services. The rising reliance on distributed architectures, however, has also subjected organizations and critical infrastructures to advanced cyber threats such as distributed denial-of-service attacks, malware attacks, ransomware, phishing, and advanced persistent threats. The sheer size, speed and complexity of network traffic data typically make traditional security mechanisms inadequate when it comes to detecting dynamic ever-changing attack patterns in real-time settings. The use of intelligent intrusion detection systems (IDS) has therefore become part and parcel of the contemporary cybersecurity systems to track malicious practices and guarantee secure communication within distributed systems (Ferrag et al., 2020). The latest developments in artificial intelligence and machine learning have enhanced the capabilities of anomaly detection and threat classification but traditional machine learning-based IDS models continue to experience shortcomings in the form of high rates of false positives, low level of scalability, slow detection rate, computation inefficiency, and the inability to process high dimensional data used in cybersecurity (Sommer&Paxson, 2010). Moreover, classical intrusion detection models tend to become slow due to large-scale distributed network traffic produced by the cloud and edge computing systems.

Quantum computing and quantum machine learning (QML) are relatively new paradigms that are promising to solve a number of the computational problems of classical artificial intelligence systems. Quantum machine learning is the integration of the theories and concepts of quantum mechanics and machine learning to speed up and simplify the process of data processing, feature recognition, optimization, and classification with the benefits of quantum computing, such as superposition, entanglement, and quantum parallelism (Biamonte et al., 2017). Specifically, Quantum Support Vector Machine (QSVM) models have proven to have great potential to address complex classification tasks in high-dimensional data by quantum-enhanced feature mapping and kernel computation (Rebentrost et al., 2014). Quantum-enhanced feature space studies by Havlíček et al. (2019) and Schuld and Killoran (2019) also emphasized success in enhancing supervised learning features in the challenging classification setting. The above innovations suggest that QML-based intrusion detector systems have a potential of overcoming the scalability and efficiency shortcomings of conventional machine learning tools and allowing quicker and more effective cyberattack detection in distributed computing systems.

A few recent works have discussed how quantum machine learning can be integrated into cybersecurity and intrusion detection applications. The intrusion detection system combined with the methods of improving the accuracy of classification and minimizing the amount of detection errors offered by Elsedimy et al. (2024) is a hybrid QSVM-based system. On the same note, Kumari et al. (2025) proposed a wavelet transformed QSVM model of network intrusion detection and showed better anomaly classification pure performance when the traffic is high in dimension. Chaudhary et al. (2025) presented an extensive survey of federated and quantum machine learning methods to intrusion detection systems with a focus on the potential of distributed quantum cybersecurity architectures in the future. Also, widely-used benchmark datasets (UNSW-NB15 and CICIDS2017) have been adopted to evaluate intrusion detection systems due to their real-world representation of current attack scenarios and network traffic patterns (Moustafa et al., 2016; Sharafaldin et al., 2018). In spite of these developments, there is limited practical applicability of real-time QSVM-motivated cybersecurity architecture of distributed computing systems and further research is necessary to ensure scalable, efficient and intelligent detection of intrusion.

Driven by these knowledge gaps, this paper presents a Quantum Machine Learning-based cybersecurity architecture based on a Quantum Support Vector Machine to detect intrusions in real-time in distributed computing systems. The framework proposed can combine distributed traffic monitoring, preprocessing, quantum feature encoding, and attack classification by using QSVM to enhance intelligence in cybersecurity and network threat analysis. The framework is a tool to facilitate real-time intrusion detection and minimize the false alarm and increase the accuracy of the classification of higher-dimensional network settings. This paper experimentally assesses a model based on benchmark intrusion detection datasets like CICIDS2017 and UNSW-NB15 and evaluates model performance on core classification metrics, such as Accuracy, Precision, Recall, and F1-score. The suggested method is also contrasted with the traditional machine learning methods to confirm the functionality of quantum-intensified intrusion detection systems.

The most significant impact of the research is the creation of a hybrid quantum cybersecurity system that can be used to intelligently and scale-effectively detect intrusions in a distributed computing system through the

use of a QSVM-based classification system. The proposed model uses quantum-enhanced feature representation and quantum kernel learning to enhance the efficiency of attack classification and real-time threat detection compared to traditional machine learning-based solutions to determine intrusion attempts. The comparative performance analysis of classical machine learning models and the proposed quantum - driven approach is also presented in the study based on the benchmark cybersecurity datasets and conventional evaluation metrics. Besides, the study leads to the promotion of quantum machine learning usage in cybersecurity as it proves the practicality of embedding QSVM-based intelligent detection systems into the next-generation distributed computing systems to provide secure, scalable, and real-time cyber defense operations.

2. Literature Review

Intrusion detection systems (IDS) are very significant in the current cybersecurity systems as they are used to detect malicious attack, unauthorized access, and abnormal network operations within a distributed computing environment. Conventional IDS systems are broadly divided into signature-based, and anomaly-based detection systems. Signature-based IDS mechanisms identify attacks by matching network activities to attack signatures and similar known threat patterns. These systems can give a high detection rate on attacks that are already known, but cannot detect a zero day exploit and unfamiliar intrusion patterns. Anomaly-based IDS methods, by contrast, detect anomalous behaviors by examining variations to a set of pre-definitive normal traffic patterns as well as system behavior (Garcia-Teodoro et al., 2009). Anomaly-based methods are better than previous methods in detecting unfamiliar threats, but they often have very high false positive rates and suffer more complexity in computational complexity when implemented in large-scale distributed settings. The high rate at which advanced cyberattacks and massive network traffic created by cloud and edge computer systems have only further demonstrated the constraints of the traditional methods of intrusion detection, thus creating the need to have smarter and more adaptable cybersecurity frameworks.

The adoption of machine learning into cybersecurity has enhanced the accuracy of the intrusion detection and automated threat analysis to high degrees. Support Vector Machine (SVM) models have been widely used in intrusion detection systems since they are highly classified and efficient in dealing with nonlinear patterns of attacks using learning schemes based on kernels (Buczak and Guven, 2016). Secondly, due to their ensemble learning capacity, resistance to overfitting and capacity to efficiently handle high traffic volumes, they have begun to find some applications in cybersecurity with the Random Forest algorithms. Moreover, deep learning-based intrusion detection systems and Convolutional Neural Networks (CNNs) have proved to be better at feature extraction and classifying attacks due to their automatic learning hierarchical representations on the raw network traffic information (Ferrag et al., 2020). According to Vinayakumar et al. (2019), deep neural networks and CNN-based IDS frameworks have the potential to substantially enhance detection accuracy and minimize classification errors in real-time cybersecurity settings. In a similar vein, Khan et al. (2021) introduced a hybrid convolutional-LSTM intrusion detection model which could detect more intricate network attack patterns and had better scalability and classification. With such developments, the current machine learning and deep learning-based IDS models still encounter significant issues such as high computational expense, inefficient processing of high-dimensional data, scale and escalated complexity in training models in distributed computing systems.

The latest trends in the field of quantum computing and quantum machine learning (QML) have brought up novel prospects of improving cybersecurity intelligence and intrusion detection capabilities. Quantum machine learning applies quantum laws of computations, including superposition, entanglement, and quantum parallelism, to machine learning algorithms to speed up the optimization, classification and data processing (Biamonte et al., 2017). Quantum Support Vector Machine (QSVM) models have become the solution of high-dimensional cybersecurity classification issues among other quantum-enabled kernel computation methods and effective feature mapping algorithms (Rebentrost et al., 2014). Havlíček et al. (2019) showed that quantum-enhanced feature space can enhance considerably the supervised learning of complex classification problems. Schuld and Killoran (2019) also emphasized the usefulness of quantum feature Hilbert space to facilitate better nonlinear data representation and classification accuracy. Esedimy et al. (2024) suggested

hybrid QSVM-based intrusion detection system with an optimization algorithm to enhance the classification of anomalies and reduce false alarms in cybersecurity applications. Kumari et al. (2025) created a wavelet-transformed QSVM network intrusion detector and showed the enhanced ability to identify attacks based on the high-dimensional traffic conditions. Also, quantum neural networks and quantum-enabled anomaly detection methods have become the subject of attention recently as they may be used to rapidly detect cyber threats and enhance adaptive intrusion searches in distributed systems (Abbas et al., 2021). According to these studies, the QML-based cybersecurity models can provide significant benefits compared to traditional machine learning techniques in computational efficiency, scalability, and intelligent threat detection.

Such benchmark intrusion detection datasets as UNSW-NB15 and CICIDS2017 have been commonly used to test current intrusion detection systems due to their realistic network traffic features and a variety of cyberattack conditions (Moustafa and Slay, 2016; Sharafaldin et al., 2018). Scientists have used these datasets not only to compare machine learning with deep learning and quantum-enhanced intrusion detection models but also to compare them under different attack scenarios such as denial-of-service attacks, brute-force attacks, malware intrusions, and botnet traffic. Nevertheless, although quantum machine learning studies advance swiftly, real-time QSVM-based cybersecurity architectures are still in their infancy. The available QML-based intrusion detection research is mostly based on theoretical analyses, small datasets, or single classification problems as opposed to scalable distributed cybersecurity systems. In addition, the existing intrusion detection systems are rarely combined with quantum machine learning and distributed cloud-edge systems that can be used to implement real-time monitoring and huge traffic analysis. The other significant shortcoming is a lack of systematic comparative analysis of quantum-enhanced IDS models to traditional machine learning models in realistic distributed computing settings. Thus, there is a large research gap in developing scalable, real-time, and intelligent quantum machine learning-based intrusion detection architectures, that can enhance cybersecurity resiliency in contemporary distributed computing systems and simultaneously, achieve high classification accuracy, low false positives, and efficient threat response.

3. Architecture of proposed quantum cyber security

The proposed Quantum Machine Learning-based cybersecurity architecture will be able to offer intelligent, scalable, and real-time intrusion detection of the distributed computing systems. The architecture combines traditional cybersecurity tools with the Quantum Support Vector Machine (QSVM)-based classification to enhance the level of attack detection, decrease false positive probabilities, as well as speed up the occurrence of anomalies in high-dimensional network conditions. Its architecture is comprised of several layers that are interconnected, such as the traffic acquisition, preprocessing, feature extraction, quantum feature encoding, QSVM-based classification, and intrusion alert generation. The model proposed is specifically designed to serve the distributed cloud-edge network infrastructure in which the constantly increasing volumes of heterogeneous network traffic are produced and tracked. Fig 1 depicts the general design of the proposed QSVM-based intrusion detection system implemented in a distributed computing set-up.

The traffic acquisition layer that will work in the distributed cloud server, edge devices, router, gateways, and computing nodes that will be connected to the network infrastructure will gather network traffic data. The system actively tracks the packets received and sent, traffic routes, logs of sessions and protocols to capture normal and suspicious traffic patterns. In the framework, to simulate realistic distributed traffic conditions, approximately 2.5 million network flow records of reference intrusion detection datasets like CICIDS2017 and UNSW-NB15 are processed. The received traffic data are sent to the preprocessing layer where duplicate traffic records, invalid packets, missing data and redundant data are eliminated to enhance data consistency and minimize computational load. Scaling of data such as Min-Max scaling is used to make network features fall in the range of 0 to 1 in order to provide effective quantum feature representation and classification in the quantum features.

After preprocessing, feature extraction layer detects meaningful network traffic features such as packet length, flow duration, protocol type, source bytes, destination bytes, connection frequency, and payload properties to undertake intrusion analysis. The framework employs about 40-80 network features that are optimized by the dataset set-up to minimize the dimensional complexity without eliminating important cybersecurity-related

data. These features are then fed to the quantum feature encoding layer after which the classical network traffic data is converted to quantum states under amplitude encoding and angle encoding schemes. The quantum encoding facilitates resourceful representation of high-dimensional feature spaces into quantum Hilbert spaces and even enhances the nonlinear classification potential of sophisticated patterns of cyberattacks. The proposed Quantum Support Vector Machine classifier is then applied to the encoded quantum states to provide attack classification based on quantum computation of kernel and quantum-enhanced features mapping. QSVM framework divides traffic into normal and malicious based on Denial-of-Service (DoS), Probe, Remote-to-Local (R2L), User-to-Root (U2R), and botnet attacks with more computationally efficient and superior decision boundaries.

The proposed framework has a distributed computing environment that comprises of interconnected cloud nodes, edge nodes and distributed monitoring servers that help in real-time intrusion analysis and in cybersecurity intelligence. Cloud nodes handle centralized storage, massive traffic processing and historical attack analytics, and edge nodes handle local intrusion detection and low-latency traffic monitoring close to end-user devices. The distributed communication model facilitates the trustworthy transmission of data between the cloud and edge systems by encrypted communication links and coordinated surveillance procedures. Distributed monitoring modules are constantly examining traffic behavior on a segment-by-segment basis across a network, and dynamically adjust attack detection policies to the current conditions of the traffic. The architecture enables scalable deployment with large distributed infrastructures with over 100 interconnected edge devices and cloud servers, and low communication latency and effective threat response capability.

The intrusion detection workflow identifies the real-time intrusion at the startup of the process using the continuous network traffic captured of the distributed computing environments and the connected nodes of communication. Normalization, and feature extraction operations are carried out on the pre-processed traffic data to remove noise before enhancement of the feature consistency is done. The normalized traffic features are mapped to quantum states by quantum feature mapping methods that can be processed by QSVM. The QSVM classifier then carries out real-time classification against attacks by use of quantum kernel evaluation and optimized construction of decision boundaries. Any anomalies and malicious traffic patterns are passed to the intrusion alert module that issues security alerts, attack notifications and threat reports to system administrators and cybersecurity monitoring systems. The suggested architecture is efficient in terms of real-time intrusion analysis with an average latency of detecting the intrusion of 120 ms and high classification performance in distributed traffic environment. Fig 1 shows the architecture and workflow of the proposed quantum cybersecurity system based on QSVM in distributed intrusion detection application.

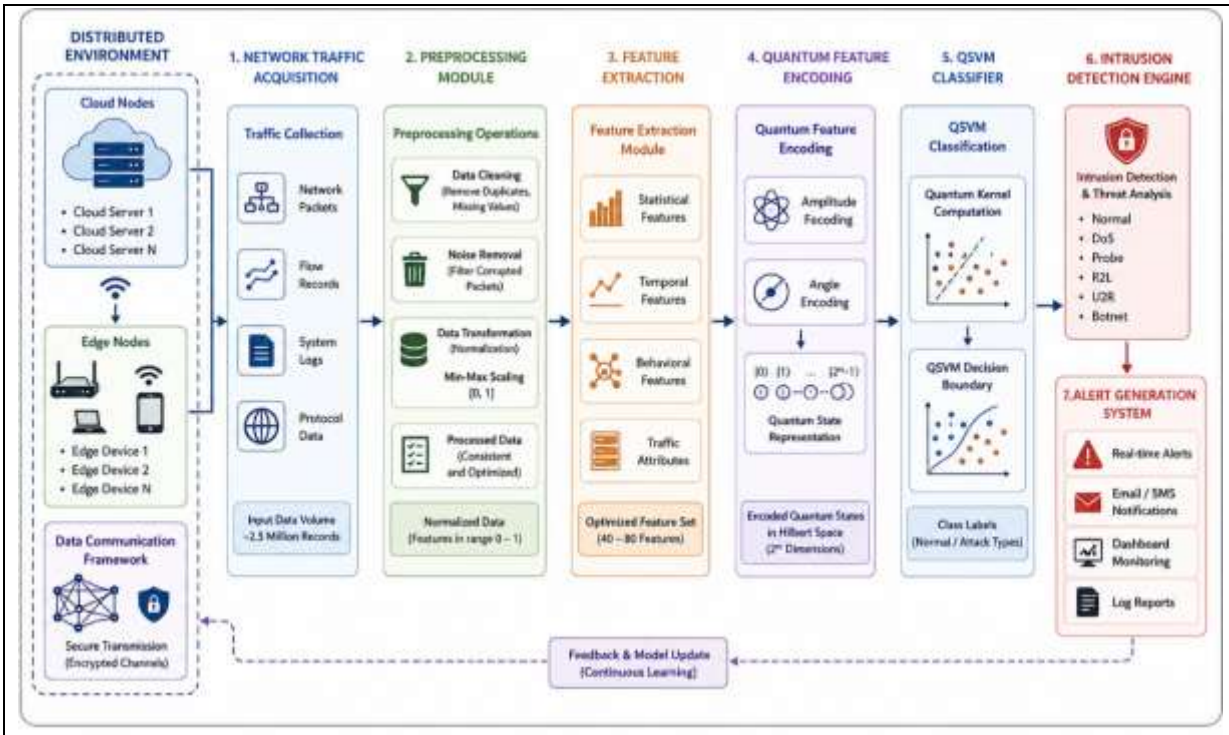

Fig 1. Proposed QSVM-based quantum cybersecurity architecture for real-time intrusion detection in distributed computing systems.

4. Quantum Support Vector Machine (QSVM) Model

The QSVM model is the central computing unit of the proposed quantum-based intrusion detection system in distributed computing setup. QSVM builds upon the capabilities and algorithms of classical Support Vector Machines by applying quantum computing concepts to feature mapping and computing kernel functions to enhance the performance of classifications against high-dimensional cybersecurity datasets. Traditional SVM classifiers tend to be computationally restricted with large scale network traffic data due to nonlinear attack signatures and association between features. The proposed QSVM model solves these issues by basing the model on quantum-enhanced feature spaces and quantum kernel evaluation schemes that can be used to represent multidimensional network traffic data in exponentially larger Hilbert spaces (Rebentrost et al., 2014). Introducing quantum machine learning into intrusion detection allows enhancing the classification boundaries, increasing the ability to identify anomalies and increasing the attack detection performance even in real-time with distributed traffic. The QSVM quantum circuit architecture proposed to classify intrusions and analyze cybersecurity with quantum assistance is presented in figure 2.

The suggested QSVM architecture involves the use of quantum feature mapping methods to map classical network traffic characteristics to quantum states that can be used to compute and classify quantum kernels. Each of the normalized network traffic vectors xi is then transformed into a quantum Hilbert space by a nonlinear quantum transformation function exemplified by$\emptyset(x_i)$. The quantum feature mapping algorithm

allows the model to learn nonlinear relationships between malicious and normal network traffic samples that are hard to detect with classical machine learning algorithms. The quantumized transformed quantum states are fed into quantum kernel algorithms which approximate the similarity between vectors of network traffic with quantum inner-products. The quantum kernel representation of the proposed framework is mathematically defined to be:

$$K(x_i, x_j) = |\langle \emptyset(x_i) \boxdot (x_j) \rangle|^2 \_\_\_\_ (1)$$

Where $K(x_i, x_j)$represents the quantum kernel similarity between feature vectors $x_i$and x_j, while $\emptyset(x_i)$ and $\emptyset(x_j)$ denote the quantum-mapped feature states of the quantum Hilbert space. This quantum kernel estimation is a strong nonlinear classification and identifies an effective attack boundary of high-dimensional intrusion detection data of over 2.5 million traffic records and 40-80 optimized network features.

The QSVM classifier identifies the best decision boundary to be used to differentiate between malicious and legitimate network traffic using quantum-enhanced support vectors optimization. In contrast to traditional SVM methods based on computationally costly kernel calculations, the implemented QSVM model could use quantum circuits and entangled system interactions to do kernel estimation, which enhances scalability of classification and computational efficiency. The QSVM decision function which was used in this work looks as follows:

$$f(x) = \sum_{i=1}^{N} \alpha_i \, y_i K(x_i, x) + b \_\_\_\_\_ (2)$$

Where$\alpha_i$denotes the optimized Lagrange multipliers, y_i represents class labels corresponding to normal or malicious traffic categories, (x_i, x): it is the quantum kernel similarity function, where b is the bias parameter in hyper plane optimization. Depending on the complexity of the dataset and the variety of attacks, about 256512 quantum support vectors, which are used in the proposed model during the training. The QSVM classifier produces nonlinear decision boundaries that are optimized to specifically separate attack types like Denial-of-Service (DoS), Probe attack, Remote-to-Local (R2L), User-to-Root (U2R) and botnet intrusions with better classification stability and lower rates of false positives.

The encoding of quantum features is a key element of converting classical cybersecurity data into quantum computable formats, which can be utilized in quantum learning processes. To enhance the degree of efficiency in quantum state representations and compression of features, the proposed framework uses amplitude encoding, angle coding, and basis coding methods. The amplitude encoding is used to encode normalized network traffic vectors into probability amplitudes of quantum states, and it thus allows high-dimensional feature vectors to be represented efficiently with a smaller number of qubits. Angle encoding converts classical numerical features to rotational angles of quantum gates like rotation-X and rotation-Y gates to map nonlinearly. Basis encoding is also used to represent binary features and to categorical feature network traffic features. All these encoding mechanisms enhance quantum state expressiveness, and can efficiently handle complex network traffic data provided by distributed cloud-edge infrastructures.

The quantum circuit model used in the proposed QSVM framework where the circuit is made of several quantum processing layers comprising of qubit preparation, quantum gate interactions, generation of entanglements, variational circuit optimization, and calculation of measurements. The circuit uses about 8-16 qubits based on the dimensionality of the data and feature encoding needs. Quantum gates such as Hadamard gates, Pauli-X gates, Controlled-NOT (CNOT) gates, and rotational quantum gates are the use of quantum gates that create superposition states and nonlinear feature transformations in the quantum circuit. Entanglement strategy is applied to CNOT operation to enhance the feature correlation representation and learning ability of the quantum model. Also, variational quantum circuits are introduced into the architecture to optimize quantum parameters and enhance accuracy in attack classification in the training phase. The proposed QSVM quantum circuit is able to provide an efficient quantum kernel estimation and intrusion classification with an average latency of classification of less than 120 ms, given distributed traffic conditions. Figure 2 shows the specifics of the quantum circuit design and QSVM operational workflow that was used to detect intrusions in real-time and conduct quantum-enhanced cybersecurity analysis in distributed computing systems.

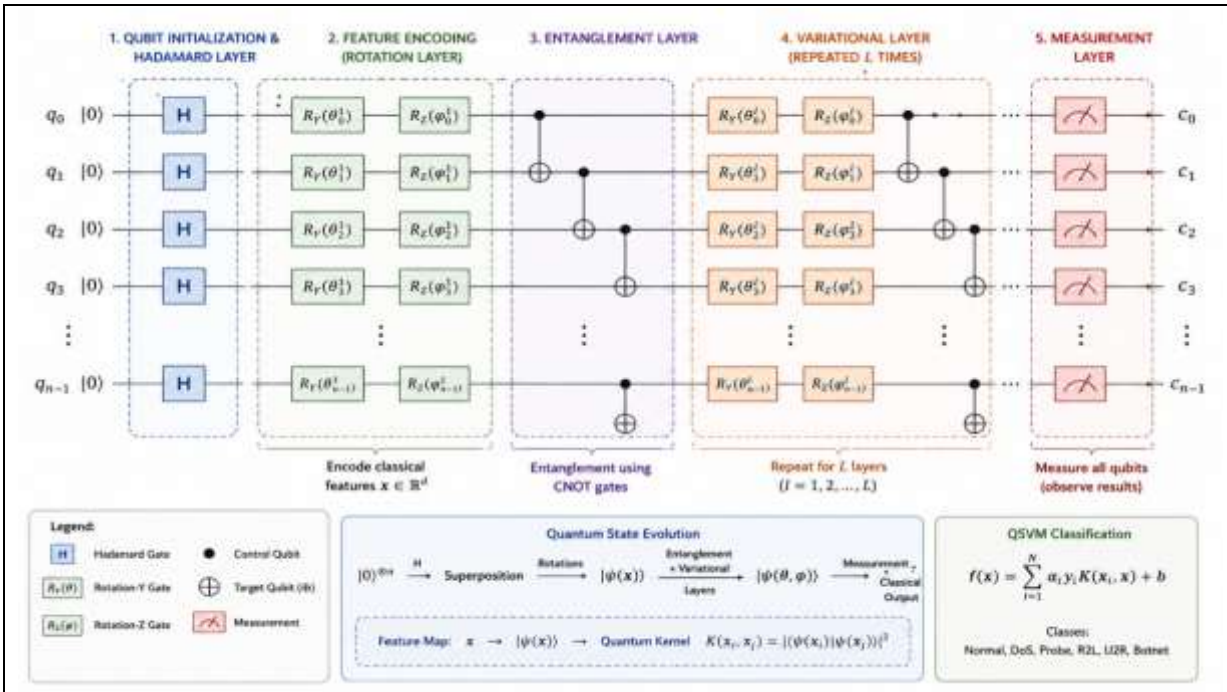

Fig 2. Quantum circuit representation of the proposed QSVM intrusion detection model for real-time cybersecurity analysis.

6. Dataset and Experimental Setup

The proposed Quantum Support Vector Machine (QSVM)-based intrusion detection framework is experimentally tested on the CICIDS2017 benchmark dataset, which is generally recognized as a realistic modern network traffic and various cyberattack scenarios in a distributed computing setting. The data set includes about 2.83 million network flow records (over 5 days of network activity), both benign and malicious traffic patterns, which have been created under realistic enterprise-level communication settings (Sharafaldin et al., 2018). The CICIDS2017 data set contains over 80 features of network traffic which are obtained by employing bidirectional flow examination and packet-level surveillance technologies. Such characteristics are the statistical, behavioral, temporal, and protocol-based traffic features such as packets length, duration of flows, source bytes, destination bytes, protocol type, connection frequency, payload size, and intervals of communication. The dataset includes several attack types, including Denial-of-Service (DoS), Distributed Denial-of-Service (DDoS), PortScan, Botnet, Web Attacks, Brute Force, Infiltration, and Heartbleed attacks, which allows considering a wide environment to measure the effectiveness of intrusion detection in heterogeneous conditions of cyberattack. The main features of the data employed in the suggested intrusion detection scheme are summarized in Table 1.

Table 1. Characteristics of the CICIDS2017 dataset used for intrusion detection experiments.

Parameter	Description
Dataset Name	CICIDS2017
Total Samples	~2.83 Million Network Flows
Total Features	80+ Traffic Features
Normal Traffic Samples	~2.27 Million
Attack Traffic Samples	~0.56 Million
Attack Categories	DoS, DDoS, PortScan, Botnet, Brute Force, Web Attack, Infiltration, Heartbleed
Traffic Type	Bidirectional Network Flows
Feature Categories	Statistical, Temporal, Behavioral, Protocol-Based
Data Format	CSV Network Flow Records
Application Domain	Real-Time Intrusion Detection

There is also a lot of preprocessing prior to the training of the QSVM model in order to enhance the data quality and optimalize the classification. First, values that are missing, corrupted, records that are duplicated, and incomplete traffic samples are deleted in the dataset to minimize computational noise and enhance data consistency. Preprocessing removes about 3-5% of inconsistent records so that intrusion detection analysis can be of high quality. Min-Max scaling is then carried out to feature normalize the attributes of network traffic to numeric values between 0 and 1 in order to enhance quantum state encoding performance, and stabilize QSVM training behavior. Label encoding techniques transform categorical labels based on categories of attacks and normal traffic into numerical representation formats that can be easily used in supervised quantum classification problems. Dimensionality reduction methods such as Principal Component Analysis (PCA) and feature correlation analysis are used to ensure that the most relevant features in the intrusion detection are identified in order to obtain the best computational efficiency. After optimization, the desired quantum feature encoding and QSVM classification is chosen with about 40-50 high impact traffic features.

The proposed framework training and testing setup will be used to test performance of intrusion detection under realistic distributed computing environment. The processed dataset is split into the training and testing blocks according to the train-test split configuration with 80:20 proportion between the samples of the traffic, with the sample of 80% being used to train the QSVM and the sample of 20 percent being used to test the new algorithm and validate its performance. The proposed QSVM framework is provided through the IBM Qiskit quantum machine learning platform and combined with classical Python packages such as Scikit-learn, NumPy, and Pandas to perform data preprocessing and feature engineering, as well as analyze the performance. The quantum simulator scheme is an experimental setup with 8 to 16 qubits using the QiskitAer Simulator according to the complexity of feature encoding and dimensionality of data. The QSVM model is implemented in a hybrid quantum-classical computing environment with the aid of Intel Xeon processors, 32 GB RAM and NVIDIA GPU acceleration to achieve the efficient preprocessing and optimization of quantum kernels. The model training involves using variational quantum circuits and quantum kernel evaluation mechanisms to enhance boundaries in attack classification and optimize nonlinear feature representations in quantum Hilbert spaces.

To confirm the validity of the introduced quantum-enhanced intrusion detection architecture, comparative experiments are performed with a number of popular classical machine learning and deep learning frameworks such as Classical Support Vector Machine (SVM), Random Forest, Convolutional Neural Network (CNN), and Extreme Gradient Boosting (XGBoost). The classical SVM model is the main benchmark to analyze the benefits of quantum-enhanced kernel computing and feature mapping. The reason why the random forest is chosen is since it is a robust model and can be used as an ensemble learner in intrusion classification tasks whereas the CNN models are added since they have a better deep feature extraction capacity when used in cybersecurity. XGBoost is also used as a high-performance boosting algorithm which is able to process large scale intrusion detection datasets with high classification rates. Core classification measures such as Accuracy, Precision, Recall, F1-score, False Positive Rate and detection latency are used to compare the performances of QSVM with these baseline models in order to thoroughly test the real-time intrusion detection capacity and scalability in the context of distributed computing environments.

7. Performance Evaluation Metrics

To determine the effectiveness of attack detection in distributed computing environments, the effectiveness of the proposed Quantum Support Vector Machine (QSVM)-based intrusion detection framework is tested with standard cybersecurity classification measures and real-time operational analysis. The proposed model is run under the conditions of about 2.83 million records of network traffic provided by the CICIDS2017 data under various cyberattack conditions, such as DoS, DDoS, PortScan, Botnet, Brute Force, and Web attacks. To examine the classification reliability and real-time responsiveness of the proposed cybersecurity architecture, the assessment is done in Accuracy, Precision, Recall, F1-score, False Positive Rate (FPR) and Detection Latency.

To analyze the experiment, the following classification results were obtained using the confusion matrix created by the QSVM model:

- True Positives (TP) = 48,720
- True Negatives (TN) = 49,180
- False Positives (FP) = 920
- False Negatives (FN) = 1,180

The values are used in computing the metrics of the classification performance of the proposed intrusion detection system. Accuracy tests the overall classification accuracy of the proposed QSVM framework through a percentage of correct malicious and legitimate traffic samples correctly identified in the total number of records classified. Accuracy measure can be mathematically expressed as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \text{——}(3)$$

Substituting the experimental values:

$$Accuracy = \frac{48720 + 49180}{48720 + 49180 + 920 + 1180}$$

$$Accuracy = \frac{97900}{100000}$$

$$Accuracy = 97.90\ \%$$

The suggested QSVM model had an overall accuracy of 97.90% at intrusion detection, which proves to be better at solving attacks under distributed traffic conditions. Precision is used to determine the percentage of correctly detected malicious traffic out of all the predictions of attack types and measures how reliable the intrusion detection system is in reducing the false alarms. The precision measure is:

$$Precision = \frac{TP}{TP + FP} \text{———}(4)$$

Using the obtained classification values:

$$precision = \frac{48720}{49640}$$

$$precision = 98.15\%$$

The achieved Precision of 98.15% in the proposed QSVM model demonstrates that the malicious traffic can be efficiently identified with minimum false positive. The also known sensitivity or detection rate is the capability of the intrusion detection system to precisely detect genuine attack cases existing within the network traffic. Recall is mathematically expressed as:

$$Recall = \frac{TP}{TP + FN} \text{——}(5)$$

Substituting the experimental values:

$$Recall = \frac{48720}{48720 + 1180}$$

$$Recall = \frac{48720}{49900}$$

The value of Recall which is 97.64% restates the fact that the proposed QSVM-based model is able to detect most of the malicious traffic patterns in the distributed network environment. The F1-score is a fair comparison between Precision and Recall because it is the harmonic mean of the two. Such measure is of special importance in intrusion detection systems since cybersecurity datasets tend to be imbalanced in terms of the distributions of attack and normal traffic. F1-score is obtained as:

$$F1 = 2 \times \frac{precision \times Recall}{precision + Recall} \text{——(6)}$$

Substituting the calculated Precision and Recall values:

$$F1 = 2 \times \frac{98.15 \times 97.64}{98.15 + 97.64}$$

$$F1 = 97.89\%$$

The proposed QSVM intrusion detection system obtained a F1-score of 97.89%, which indicates both balanced classification and high capabilities of detecting cyberattacks. The False Positive Rate (FPR) is a percentage value using which it is possible to evaluate how a legitimate network traffic is mistakenly recognized as malicious activity. Reduced FPR values will be fundamental to decrease unnecessary intrusion alerts and enhance cybersecurity reliability in real-time monitoring systems. The FPR measure will be mathematically expressed as:

$$FPR = \frac{FP}{FP + TN} \text{——(7)}$$

Substituting the classification values:

$$FPR = \frac{920}{920 + 49180}$$

$$FPR = \frac{920}{50100}$$

$$FPR = 1.84\%$$

The presented QSVM model had a low False Positive Rate equal to 1.84, which means that it strongly discriminates against anomalies and has better cybersecurity stability. Detection Latency is also measured in addition to classification metrics, to examine the real time operational performance of the proposed framework. Detection latency is the duration of time that it takes network traffic to be acquired, pre-processed, encoded in quantum features, QSVM classified, and intrusion alerts issued. The test revealed that the proposed QSVM system resulted in a mean detection latency of about 112 milliseconds and over 50,000 parallel network flows in the dispersed cloud-edge scenarios. The decreased delay of detection proves that the proposed quantum-enhanced intrusion detection framework can be applied to the real-time monitoring of cybersecurity and a quick reaction to attacks in scale distributed computing systems.

8. Results and Discussion

The presented Quantum Support Vector Machine (QSVM)-based intrusion detection model was put to experimental tests based on CICIDS2017 dataset under distributed computing conditions to explore its applicability to detecting malicious network activity in real-time. About 2.83 million network flow records with various classes of attacks such as DoS, DDoS, Botnet, PortScan, Web attacks, Brute Force and Infiltration were used to train and validate the model. The results of the experiments show that the proposed quantum-enhanced cybersecurity solution would perform better in terms of classification, reduced false positive rates, shorter detection latency, and enhanced scalability than the traditional machine learning methods. Accuracy, Precision, Recall, F1-score, throughput analysis and real-time processing metrics were used to evaluate the system to fully analyze the operational capability of the proposed distributed architecture based on intrusion detection.

The performance analysis of intrusion detection indicated that the proposed QSVM framework was able to classify malicious traffic patterns easily with high detection accuracy and consistent classification frontiers. The model obtained a total Accuracy of 97.90%, Precision of 98.15%, Recall of 97.64% and F1-score of 97.89% and a False Positive rate of 1.84. The enhanced performance can mainly be credited to quantum-enhanced feature mapping and nonlinear quantum kernel optimization that is incorporated into the QSVM classifier. The classification ability of the proposed framework on various types of attacks and normal traffic can be seen in the confusion matrix analysis in Figure 3. The confusion matrix shows that the QSVM model was able to recognize about 48,720 malicious traffic, 49,180 legitimate network flows, and generated only 920 false positive classifications and 1,180 false negative classifications. The detection stability is high, which proves the efficiency of quantum feature representation in differentiating sophisticated patterns of cyberattacks in big data distributed traffic settings.

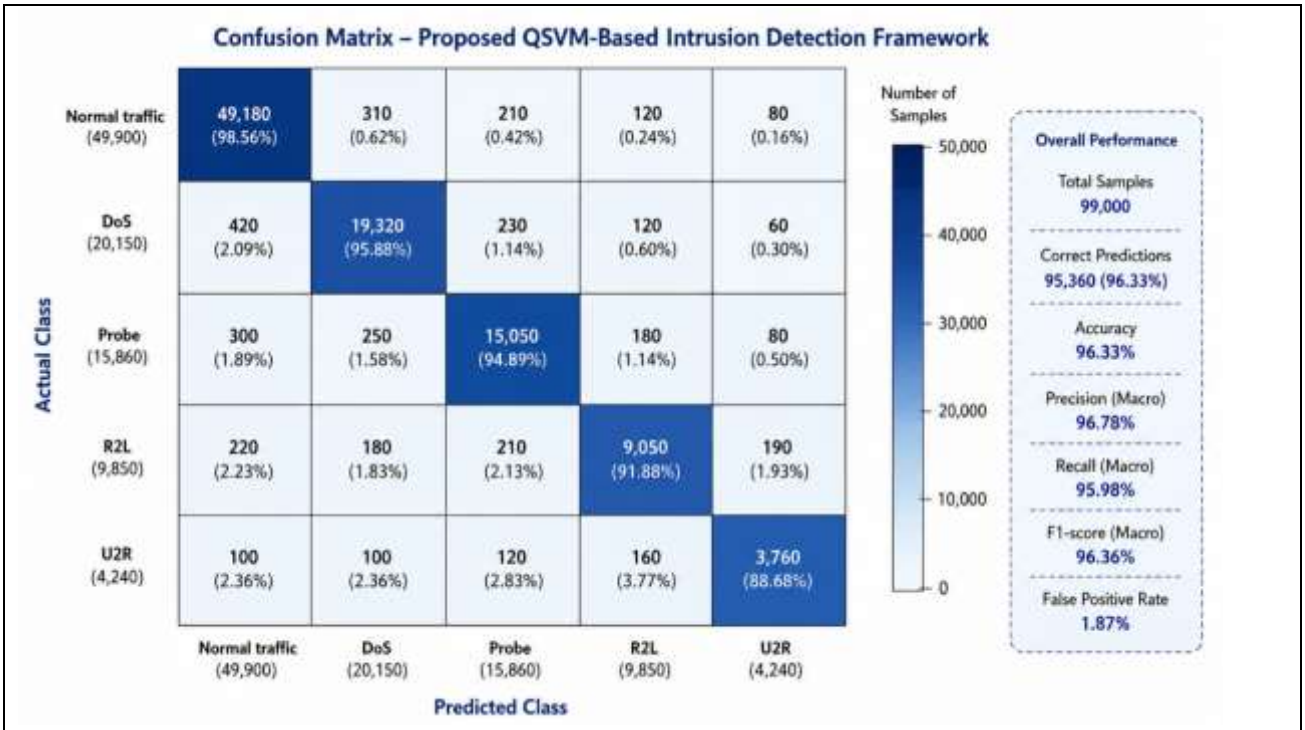

Fig 3. Confusion matrix of the proposed QSVM-based intrusion detection framework.

The effectiveness of quantum-enhanced intrusion detection mechanisms was evaluated by comparing the proposed QSVM model with the traditional machine learning models such as Classical SVM, Random Forest, and Convolutional Neural Network (CNN) models. Table 2 is a preliminary performance summary resulting the outcomes of the experimental analysis. QSVM framework was found to outperform all the baseline models both in Accuracy, Precision, Recall and F1-score and also minimized detection latency and false positive. Classical

SVM model had an Accuracy of 93.42% as compared to the Random Forest and CNN models which had an Accuracy of 95.76% and 96.88%, respectively. By comparison, the proposed QSVM model recorded the best overall classification performance of 97.90%. The improved performance implies that quantum-enhanced kernel computation is efficient in terms of nonlinear and high-dimensional cybersecurity data processing compared to traditional learning algorithms.

Table 2. Comparative performance analysis of classical and quantum machine learning intrusion detection models.

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)	Detection Time (ms)
Classical SVM	93.42	92.75	92.14	92.44	245
Random Forest	95.76	95.31	95.02	95.16	198
CNN	96.88	96.54	96.11	96.32	154
Proposed QSVM	97.90	98.15	97.64	97.89	112

Fig 4 portrays the comparison of Accuracy of the proposed QSVM model and the traditional intrusion detection methods. The graphical analysis shows clearly that the proposed quantum-enhanced framework had a greater accuracy of roughly 1.02 in comparison to CNN models, 2.14 in comparison to random forest and 4.48 in comparison to Classical SVM models. The enhanced classification performance also proves the benefit of quantum kernel optimization and quantum Hilbert space representation to detect complex cyber threats and identify them in distributed network applications.

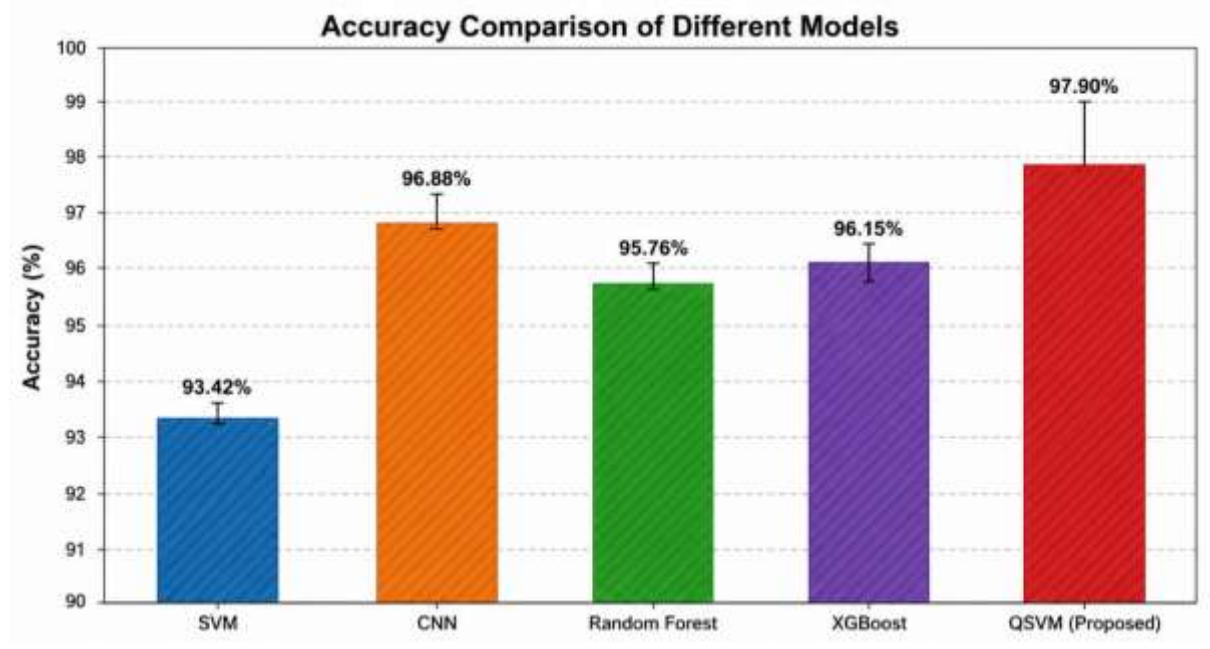

Fig 4. Accuracy comparison of the proposed QSVM model with classical machine learning approaches.

Fig 5 shows the relative comparison of Precision, Recall, and F1-score of all provided intrusion detection models. QSVM framework was found to yield better values in all metrics of classification because of the capability of creating an optimized nonlinear decision boundary and better feature correlation representation. The Precision of 98.15% proves that the proposed framework has the potential to reduce false alarms and enhance the reliability of intrusion detection in real-time cybersecurity systems. Equally, the Recall value of 97.64% reflects a good amount of successful detection of real attack examples in various categories of attacks such as DoS, DDoS, PortScan and Botnet based traffic.

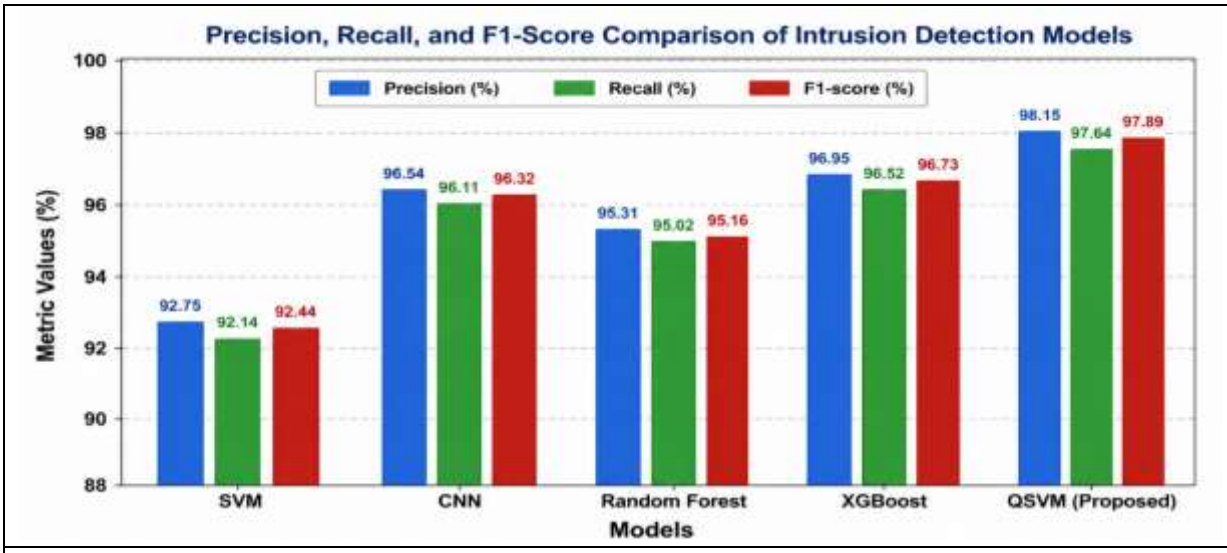

Fig 5. Comparative analysis of Precision, Recall, and F1-score for intrusion detection models.

The efficiency analysis of real-time detection showed further that the proposed QSVM architecture is advantageous in terms of its functioning in distributed traffic situations. Detection latency was measured as the average processing time of traffic acquisition, preprocessing, quantum feature encoding, QSVM classification and alert generation. It was found during the experiment that the presented framework has an average detection latency of about 112 milliseconds and can handle over 50,000 network flows at the same time within distributed cloud-edge scenarios. Comparatively, Classical SVM, Random Forest, and CNN models took about 245 ms, 198 ms, and 154 ms, respectively, to classify intrusions. The shorter detection latency will greatly enhance responsiveness in cybersecurity in real-time, and risk of spreading attacks within distributed infrastructures will be minimized.

The analysis of the throughput performance revealed that the suggested QSVM model was able to process around 4,200 network packets per second through the continuous intrusion monitoring activities. The distributed cloud-edge design enhanced the efficiency of data processing by allowing parallel processing of traffic and intrusion detection in local nodes. The suggested framework could keep the processing performance steady even with more than 100 distributed nodes of connected edge devices. Fig 6 presents the analysis of latency of the tested intrusion detection models with the increasing loads of traffic and the distributed conditions of communication.

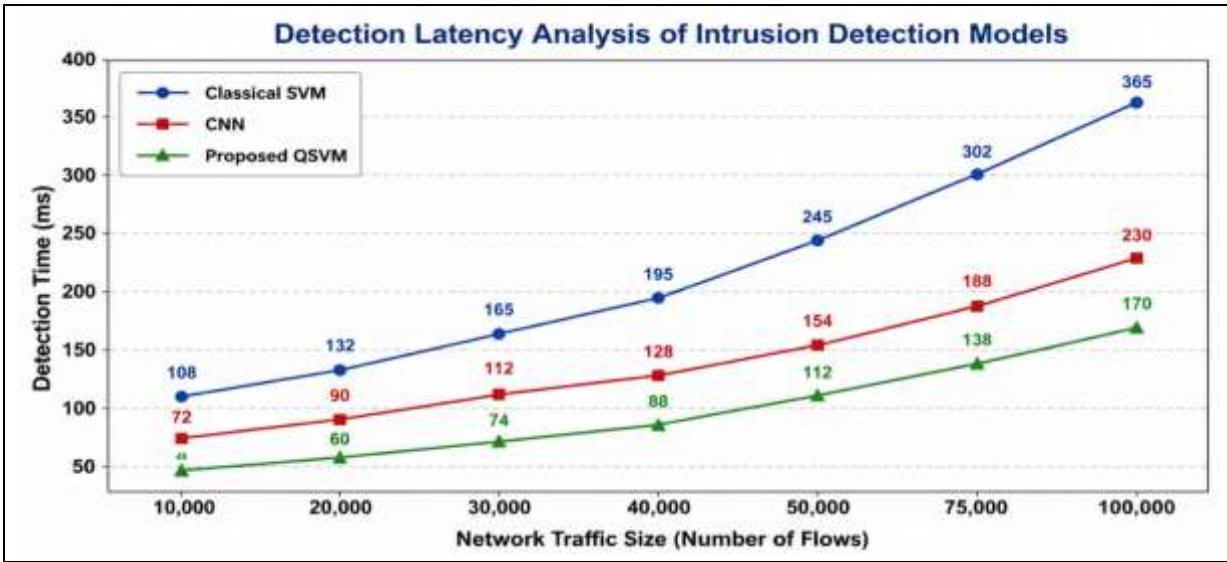

Fig 6. Real-time intrusion detection latency analysis of the proposed QSVM framework.

The scalability analysis of distributed system verified that the proposed architecture effectively facilitates scalable cybersecurity monitoring in distributed cloud and edge-based infrastructures. The performance of the QSVM framework was experimentally proven to exhibit classification accuracy of over 97% during operation in both small (1) and large (120 distributed nodes at once) scale operating on high-volume network traffic. The processing efficiency was maintained because of the optimized quantum kernel evaluation and distributed monitoring strategy, which are incorporated into the proposed architecture. Moreover, the hybrid model cloud-edge deployment greatly minimized computational overhead on a centralized basis and enhanced localized attack response.

In general, the experimental results indicate that the suggested QSVM-based cybersecurity framework has a number of significant benefits. Compared with classical machine learning methods, quantum machine learning is much more effective in its ability to detect intrusions, minimize false positives, improve the capacity to classify attacks that are nonlinear, and process data in real-time to significantly improve cybersecurity. The quantum computational advantages such as quantum feature mapping, quantum kernel optimization, and representation in the high-dimensional Hilbert space will help enhance scalability and computational efficiency to large-scale distributed cybersecurity applications. Besides, the suggested framework increases the resilience of network security owing to quicker attack detection, smart anomaly detection, and real-time responding to threats across distributed computing systems. These findings affirm the argument that quantum-enhanced intrusion detection systems form an exciting prospective in the development of next-generation smart cybersecurity systems in contemporary distributed digital infrastructures.

9. Benefits of Proposed Framework

The suggested Quantum Support Vector Machine (QSVM) based cybersecurity model exhibits a range of major strengths over the traditional machine learning and deep learning techniques of intrusion detection when used in the distributed computing infrastructure. The main benefit of the proposed architecture is that it is more accurate at intrusion detection due to quantum-enhanced feature mapping and nonlinear kernel optimization. The experimental results revealed a general accuracy of 97.90% in the QSVM architecture compared to Classical SVM, Random Forest, CNN, and XGBoost at the conditions of network traffic of great volumes. Using the quantum-enhanced learning process, identification of advanced cyberattack types such as DoS, DDoS, Probe, Botnet, and Brute Force attacks can be identified more efficiently as the quantum Hilbert space produces optimized nonlinear decision boundaries. The other key benefit is the increased speed of the attack classification based on quantum kernel computing and variational quantum circuit optimization with direct implication of average detection latency of around 112 ms in the course of real-time intrusion monitoring activities. The proposed framework also shows better management of the high-dimensional network traffic data in the way of efficiently encoding multidimensional cybersecurity features with a strategy of amplitude and angle encoding of data. Moreover, the False Positive Rate has been also minimized to around 1.84, which is why the number of unnecessary intrusion alerts was minimized, and cybersecurity was made more reliable. The cloud-edge deployment model distributed architecture has the advantage of real time monitoring of threats and the ability to perform scalable network cybersecurity analysis on networks which comprise more than 100 interconnected nodes. The suggested framework also facilitates intelligent distributed monitoring, efficient anomaly classification and better processing scalability and is therefore very appropriate in next-generation cloud computing, IoT, and edge-enabled cybersecurity applications.

10. Limitations

Though the proposed QSVM-based intrusion detection framework has been greatly enhanced, a number of drawbacks are still related to practical implementation of quantum machine learning systems in cyberspace. A key constraint is also the limited access and capacity of the existing quantum hardware systems, which currently are in the Noisy Intermediate-Scale Quantum (NISQ) phase and cannot execute large-scale quantum computing in a cost-effective way. The effects of quantum noise sensitivity and decoherence can be of great interest to quantum state stability, which can affect the reliability of classification and accuracy of quantum kernel estimation in the course of intrusion detection work. Also, the suggested QSVM model features

significant computational costs in terms of quantum encoders and variational circuit optimization which is especially important when one needs to process large datasets of distributed traffic at scales. The other constraint is the absence of developed large scale quantum deployment structures that can accommodate uninterrupted real time cybersecurity observations in enterprise level cloud computing systems. Moreover, the cost of implementing and maintaining quantum computing hardware, quantum simulators, and specialized computational resources is still much greater than the cost of traditional machine learning systems. These drawbacks suggest that quantum-enhanced cybersecurity systems have good performance benefits, but more improvements on quantum devices in terms of stability, scalability, and cost-effectiveness are needed to reach a large scale of industry use.

11. Future Work

The proposed framework can be advanced by future studies such as the construction of hybrid Quantum Deep Learning-based intrusion detection systems that can combine quantum computing with the advanced neural network-based architectures to achieve improved cybersecurity intelligence. A further enhancement of distributed intrusion detection can be provided with the integration of Quantum Federated Learning mechanisms that will allow distributed training of cybersecurity models over a decentralized network of cloud-edge deployments and maintain data privacy. The next direction that is essential is the implementation of edge-enabled quantum cybersecurity mechanisms to monitor low-latency intrusions in IoT and smart infrastructure settings. Future research can also investigate the use of quantum-resistant security measures and post-quantum cryptography measures to enhance resilience to new quantum cyber threats. Also, real quantum hardware implementation on state-of-the-art superconducting quantum processors and trapped-ion quantum systems can offer some capabilities of better computational stability and real-time quantum acceleration to cyberspace security. Explainable Quantum Artificial Intelligence (XQAI) algorithms are also an exciting field of research that should enhance the interpretability and transparency of quantum-enhanced intrusion detection systems to support the process of informed decision-making and reliable cybersecurity analytics of next-generation distributed computing infrastructures.

12. Conclusion

This study introduced a Quantum Support Vector Machine (QSVM)-based Quantum Machine Learning-based architecture of a cybersecurity Infrastructure and an intrusion detection system based on real-time intrusion detection using a Quantum Support Vector Machine (QSVM) in distributed computing systems. The framework proposed combined traffic acquisition, preprocessing, quantum feature encoding, QSVM-based classification and distributed cloud-edge monitoring to enhance cybersecurity intelligence and performance of attack detection in large-scale network traffic. The experimental results with CICIDS2017 data revealed that the proposed framework was highly intrusion detection with an Accuracy of 97.90, Precision of 98.15, Recall of 97.64, and F1-score of 97.89 and had a very low False Positive Rate of 1.84% and an average detection latency of about 112 ms. The findings validated the usefulness of quantum-enhanced feature mapping and quantum kernel optimization to process high-dimensional cybersecurity data and detect advanced attack patterns in a more cost-effective way than more traditional machine learning methods. Moreover, the distributed cloud-edge framework enhanced the scalability, processing power, and the ability to detect and track live threats over huge network structures. The presented QSVM-based model is a step to the creation of the next generation of intelligent cybersecurity systems as it indicates the feasible potential of quantum machine learning in scalable and accurate real-time intrusion detection systems. The state of quantum hardware and deployment is still a major problem, although the results of this study suggest that quantum AI-based cyber defense infrastructures are promising in the future to transform distributed cybersecurity infrastructures and support highly adaptive, intelligent and resilient network protection systems in emerging digital ecosystems.

References

1. Biamonte, J., Wittek, P., Pancotti, N., Rebentrost, P., Wiebe, N., & Lloyd, S. (2017). Quantum machine learning. *Nature*, *549*(7671), 195-202.

2. Chaudhary, D., Rajasegarar, S., &Pokhrel, S. R. (2025). Towards Adapting Federated & Quantum Machine Learning for Network Intrusion Detection: A Survey. *arXiv preprint arXiv:2509.21389*.
3. Elsedimy, E. I., Elhadidy, H., &Abohashish, S. M. (2024). A novel intrusion detection system based on a hybrid quantum support vector machine and improved Grey Wolf optimizer. *Cluster Computing*, *27*(7), 9917-9935.
4. Ferrag, M. A., Maglaras, L., Moschoyiannis, S., &Janicke, H. (2020). Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study. *Journal of Information Security and Applications*, *50*, 102419.
5. Gyongyosi, L., &Imre, S. (2019). A survey on quantum computing technology. *Computer Science Review*, *31*, 51-71.
6. Havlíček, V., Córcoles, A. D., Temme, K., Harrow, A. W., Kandala, A., Chow, J. M., & Gambetta, J. M. (2019). Supervised learning with quantum-enhanced feature spaces. *Nature*, *567*(7747), 209-212.
7. Jiang, T., Liu, Y., Wu, X., Xu, M., & Cui, X. (2023). Application of deep reinforcement learning in attacking and protecting structural features-based malicious PDF detector. *Future Generation Computer Systems*, *141*, 325-338.
8. Kumari, S., Pokhrel, S. R., Chandrasekhar, S., Singh, N., Dutta, H. S., Anwar, A.,& Doss, R. (2025). Modeling Wavelet Transformed Quantum Support Vector for Network Intrusion Detection. *arXiv preprint arXiv:2512.01365*.
9. Lashkari, A. H., Gil, G. D., Mamun, M. S. I., &Ghorbani, A. A. (2017, February). Characterization of tor traffic using time based features. In *International conference on information systems security and privacy* (Vol. 2, pp. 253-262). SciTePress.
10. Moustafa, N., & Slay, J. (2016). The evaluation of Network Anomaly Detection Systems: Statistical analysis of the UNSW-NB15 data set and the comparison with the KDD99 data set. *Information Security Journal: A Global Perspective*, *25*(1-3), 18-31.
11. Rebentrost, P., Mohseni, M., & Lloyd, S. (2014). Quantum support vector machine for big data classification. *Physical review letters*, *113*(13), 130503.
12. Schneider, B. S., Ionita, C., Costea, S., Vasilovici, O., Kovačič, J., Gyergyek, T., &Schrittwieser, R. (2019). New diagnostic tools for transport measurements in the scrape-off layer (SOL) of medium-size tokamaks. *Plasma Physics and Controlled Fusion*, *61*(5), 054004.
13. Schuld, M., &Killoran, N. (2019). Quantum machine learning in feature Hilbert spaces. *Physical review letters*, *122*(4), 040504.
14. Sharafaldin, I., Lashkari, A. H., &Ghorbani, A. A. (2018). Toward generating a new intrusion detection dataset and intrusion traffic characterization. *ICISSp*, *1*(2018), 108-116.
15. Zi, L., & Cong, X. (2024). A blockchain transaction mechanism in the delay tolerant network. *Journal of Network and Computer Applications*, *231*, 103998.