Optimized Quantum Neural Networks for Anomaly Detection in Securities Transactions

Author: Geol Gladson Battu

Abstract: In financial systems, abnormal activities in securities transactions pose significant risks due to which there is a requirement of smart and accurate anomaly detection procedures. The presented work in this paper employs a Particle Swarm Optimization (PSO)-tuned Quantum Neural Network (QNN) for anomaly detection. The QNN proposed here is designed using variational quantum circuits to process PSO optimized features and utilises the quantum advantage in neural computing. Performance of the proposed system is evaluated by executing on the IEEE-CIS Fraud Detection dataset. QNN's weights and biases are optimized by using PSO to enhance capability of the designed network to escape from local optima and to enhance prediction accuracy. The results presented demonstrate the performance of proposed PSO-QNN model and these outcomes are compared with the conventional algorithms- Long Short-Term Memory (LSTM), k-Nearest Neighbours (KNN), and Support Vector Machines (SVM). The work proposed in this paper achieves a precision of 98.55% with improved sensitivity, specificity, recall and attained an impressive Matthews Correlation Coefficient (MCC) of 0.94. As presented in the results, reduced values of FP and FN rates, showcase the reliability of the proposed PSO-QNN model for anomaly detection. For anomaly detection, adopting QNN and optimising it by PSO, represents a significant advancement and this offers a progressive and functional solution for securities transactions in financial systems.

Keywords: Quantum Neural Networks (QNN), Particle Swarm Optimization (PSO), Anomaly Detection, Securities Transactions, Fraud Detection, IEEE-CIS Dataset

1. Introduction

The increasing complexity and volume of financial transactions in global securities markets have developed the need for advanced analytical techniques capable of detecting anomalies and irregular market behaviours. Traditional anomaly detection methods often struggle to remain effective amidst the evolving dynamics of financial fraud and market manipulation, particularly when analyzing nonlinear and high-dimensional datasets. These limitations have driven demand for more robust and adaptive solutions that offer improved accuracy, scalability, and responsiveness in financial surveillance systems [1,2]. In recent years, breakthroughs in artificial intelligence (AI) and quantum computing have opened new avenues for data analysis and pattern recognition. QNNs, which merge quantum computing principles with the adaptive learning mechanisms of neural networks, have demonstrated considerable promise in addressing the complexities inherent in large-scale financial data [3]. Unlike conventional models, QNNs combine quantum parallelism to evaluate multiple computational paths

simultaneously. This allows them to uncover refined relationships and delicate anomalies that may escape conventional deep learning techniques [4,5].

This study presents a novel QNN-based framework for anomaly detection in securities transaction data of financial systems. The proposed system utilizes the computational strengths of QNNs to analyse large financial datasets, identify latent structures, and detect potentially fraudulent or manipulative trading behaviours with enhanced speed and precision. By effectively modelling nonlinear dependencies and capturing hidden patterns within the data, the framework is well-suited for the early detection of financial misconduct such as fraud and anomaly. The remainder of this paper is structured as follows: Section 2 reviews related work in anomaly detection and quantum neural network applications. Section 3 outlines the proposed methodology and system architecture. Section 4 depicts the procedure of anomaly detection using PSO optimized QNN. Section 5 illustrates the results and their consequences. And Section 6 is for conclusion and future scope.

2. Recent Works

Anomaly detection has long been a crucial area of research in the financial sector, specifically for fraud detection, anti-money laundering (AML), and market surveillance. Traditional approaches frequently depend on guideline-oriented systems, statistical models, and ML algorithms such as decision tress, SVM and clustering procedures [6, 7]. While effective to a certain extent, these models typically depend on predefined thresholds or require large, labelled datasets, that cannot be available or appropriate for detecting intricate, evolving anomalies in real-time trading environments [8]. Amid the growing influence of deep learning, more advanced architectures such as CNNs, RNNs, and Autoencoders have been employed to financial anomaly detection [9]. These models have demonstrated improved performance by analysing complex structures directly on unprocessed data. For example, LSTM networks are employed widely in transaction sequences to capture sequential connections. Due to poor computational efficiency, reduced transparency and non-adaptability to varying financial systems, deep learning models are encountering limitations restrains [10].

Recent advances in quantum computing have introduced transformative paradigms for data analysis, particularly through the emerging field of Quantum Machine Learning (QML). Among the various models within this domain, QNNs represent a particularly promising class, utilizing quantum phenomena such as superposition and entanglement to perform complex computations concurrently [11]. These capabilities allow QNNs to process high-dimensional data more efficiently than conventional machine learning models, uncovering latent relationships that may remain undetected using traditional analytical approaches. While applications of QNNs in finance are still in their early stages, preliminary research has explored their utility in areas such as portfolio optimization, derivative pricing, and risk assessment. Nonetheless, the use of QNNs for anomaly detection remains relatively under-investigated, presenting a significant opportunity for innovation in financial analytics [12].

Early approaches to anomaly detection have relied heavily on statistical methodologies. For instance, the comprehensive review presented in [13] underscores the limitations of conventional techniques in managing the complexity of high-dimensional financial datasets.

The evolving characteristics of anomalous behaviours, particularly within dynamic and networked environments, have further emphasized the need for more flexible and resilient detection strategies, as discussed in [14]. In response, machine learning has gained prominence as a more adaptable approach to anomaly detection in financial systems. The Local Outlier Factor (LOF) method, explored in [15], exemplifies this shift by identifying data instances that diverge significantly from their local neighbourhoods, thereby laying the groundwork for unsupervised learning-based detection techniques. In [16], authors developed algorithms based on clustering and nearest neighbours, which were effective but struggled with scalability in large datasets. The introduction of deep learning marked a significant shift. In [17], authors demonstrated process of deep belief networks to learn compact representations of data, which later inspired autoencoder-based models for anomaly detection. A deep learning-based framework is explained in [18] that automatically learns feature representations for anomaly identification, improving performance on complex datasets.

Various deep learning models are employed by several researchers in literature for anomaly detection in securities transactions in financial systems. Recurrent neural networks (RNNs) are adopted in [19], exhibits better accuracy and recall compared to conventional approaches for anomaly detection in financial transactions. Future market behaviours and identification of deviations in transactions are performed using LSTM networks in [20]. Deep learning models like LSTM may exhibit high accuracy, but they require large datasets to train and involve considerable digital infrastructure. Because of its capacity to handle large dataset effectively quantum computing is emerging as a potential solution for anomaly detection. Theory of quantum machine learning is explained in detail in [21] and hybrid models which incorporates conventional, and quantum computing are proposed for solving complex tasks. Due to the ability of utilization of quantum parallelism, QNNs are gaining more attention compared to other networks. Using quantum learning models an algorithm called Quantum Approximate Optimization (QAOA) is proposed in [22] for solving combinatorial problems. By imitating the conventional neural networks quantum circuits are designed in [23] for pattern identification and classification.

For efficient search of anomalies in the data, a quantum inspired anomaly detection approach using Grover's algorithm is proposed in [24]. The results presented in this paper illustrate considerable enhancement in speed of the detection compared to conventional methods. Quantum Boltzmann machines are adopted in [25] to learn complex distributions and to identify irregularities in security transactions and results are compared with conventional ML models. To reduce dimensionality of large-scale transactional data in securities markets quantum principal component analysis (qPCA) is performed in [26]. The proposed approach in this paper assists QNN to concentrate on essential trends and anomalies without rise in computational overhead. In [27] introduced a hybrid quantum-conventional model that utilized quantum circuits for feature mapping and conventional neural networks for final categorization. Such models have shown promise in financial fraud detection, where feature interactions are often nonlinear and intricate.

Furthermore, recent work in [28] presented quantum-enhanced feature spaces that improve the separation of data classes, crucial for anomaly detection tasks where subtle deviations need to

be identified. Their variational quantum classifiers demonstrated improved generalization on small training sets, a notable advantage in financial anomaly detection where labelled data is scarce. On the practical implementation side, in [29] reviewed the challenges and prospects of deploying QNNs on near-term quantum hardware. They emphasized the need for noise-resilient architectures and optimization algorithms to ensure robust performance under real-world conditions. These insights are critical for developing deployable QNN-based anomaly detection systems. In [30], authors applied quantum machine learning to detect insider trading in securities markets. Their model utilized quantum kernel estimation to highlight hidden patterns indicative of fraudulent activities, achieving superior precision compared to classical models.

Quantum recommendation systems are explored in [31], which although primarily used in e-commerce, also demonstrated strong anomaly detection capabilities by identifying unusual user behaviors. Their findings contribute to cross-domain applications of QNNs, including finance. A quantum convolutional neural network (QCNN) is proposed in [32] for time-series anomaly detection, showing promising results in simulated stock market environments. QCNNs, with their hierarchical structure, are well-suited for capturing both short- and long-term patterns in transactional data. These advancements illustrate a growing interest in combining quantum computing with neural network architectures to enhance anomaly detection capabilities. Although the field is still in its infancy, preliminary results are encouraging and suggest that QNNs can overcome many of the limitations associated with traditional and deep learning models. However, challenges remain in terms of hardware scalability, noise tolerance, and integration into existing financial systems.

3. Problem Statement

With the exponential growth of digital finance and the increasing volume of securities transactions conducted through automated techniques, warranting the reliability and security of financial markets has become a critical challenge. Modern financial platforms process vast amount of sensitive transactional data in real time. This increases fraudulent activities and cyber threats. Conventional monitoring systems often lack required complexity to identify abnormalities within these large datasets with sensitive transactions. As financial systems are increasing their transactions density and velocity, malicious individuals are implementing more sophisticated methods to bypass conventional security protocols. Conventional anomaly detection approaches with rule-based systems or ML models often struggle to adapt to the changing circumstances of attackers. These methods often fall short in capturing nonlinear dependencies and detecting hidden relationships. This increases activities such as insider trading, market manipulation, or fraud. Although anomaly detection systems have been widely used in network security, their adaptation is limited in financial systems due to their intricate behaviour and high dimensional dynamics. Prior research has focussed on limited categories of anomalies, often overlooking the evolving nature of illicit activities within securities trading environments.

This paper proposes a Quantum Neural Network (QNN) model optimized through Particle Swarm Optimization (PSO) for anomaly detection in securities transactions. The incorporation

of quantum computational capabilities with PSO-optimization enhance the model's ability to recognise complex and irregular patterns while performing anomaly detection.

4. Proposed System using PSO-Optimized QNN

The anomaly detection approach using incorporation of PSO and QNN is proposed and developed particularly to identify fraudulent patterns within securities transactions of financial systems. Main disadvantages of conventional ML models are their inefficiency in handling nonlinear relationships in data sets and occasional abnormal behaviours within high-volume transactional data. The proposed approach contains three important steps including: data preprocessing, feature extraction by PSO optimization, and anomaly detection via PSO optimized QNN. Initially, the data are pre-processed by Min-Max normalization, for regulating the numerical features of the to a consistent range.

Then in the second step subset of features of the data are extracted by using PSO optimization. This will enhance the performance of QNN and generalization capability in anomaly detection. As the third step PSO is applied to optimize initial weights and biases of QNN for robust feature learning. This optimisation by PSO improves the convergence speed and generalization capability of the model. Optimized QNN uses quantum computation elements like quantum gates to identify the anomaly in securities transaction. Figure 1 presents the block diagram of the proposed PSO optimized QNN model.

Figure 1. Block diagram of the proposed PSO optimized QNN model

4.1. Dataset: IEEE-CIS Fraud Detection

An IEEE-CIS Fraud Detection dataset which is released by IEEE and Consumer Identity solutions (CIS) team is adopted to evaluate the efficacy of proposed PSO-QNN model. This dataset contains a rich, high dimensional data with 590,540 transaction records. Each record in marked with 434 obscured features including transaction metadata, identity and device/browser related variables. Even due to privacy considerations some features are hidden but the data represent the organizational and interactive particulars of real-world financial operations. One of the primary challenges in employing this dataset is its class imbalance. This data contains fraudulent transactions of 3.5% in the total observations. To mitigate the effect of this inequality, the proposed model contains applicable sampling approaches. Every record in this data is labelled as fraudulent or legitimate that allows semi supervised anomaly detection approach using PSO optimised QNN.

4.2. Preprocessing with Min-Max Normalization in PSO-Optimized QNN

For anomaly detection in securities transactions using PSO optimized QNN, preprocessing of the data plays a key role in assisting the training of the model. Min-Max normalization transforms the values of each input feature into a standardize range before incorporation of QNN. This normalization process improves the training dynamics of the model by making sure that all input features are contributed equally to the learning process. Min-Max normalization aids to numerical stability during the training procedure. This is important especially for optimization of QNN parameters using Particle Swarm Optimization (PSO).

Mathematically, Min-Max normalization transforms each original feature value m according to the following formula:

$$m' = min_{new} + (max_{new} - min_{new}).\frac{m - min_x}{max_x - min_x}$$

where:

- min_x, max_x are the lowest and highest values of the feature in the original data,
- min_{new}, max_{new} define the desired normalization range (typically 0 and 1),
- and m' is the normalized value.

Min-Max normalization presents a computationally efficient solution for normalization and this method is particularly advantageous with large dimensional dataset. T reduces the risk of distorting the statistical distribution of the input variables.

4.3. Feature Selection Using PSO for QNN

To enhance the operational efficiency of the QNN, Particle Swarm Optimization (PSO) is used to optimize the features of the data. This will enhance the performance of QNN and generalization capability in anomaly detection. As presented in figure 2 population of particles or subset of candidate features are initialised as binary vectors. A value of '1' indicates that a particular feature is included and '0' indicates that feature is excluded. These particles are initialised such that they should distributed randomly through out the feature search space. And for every iteration these particles are updated using particle velocity, best particle and global best particle. This procedure helps the model to explore the total search area and substantially converge to an optimal position which represent the best subset of candidate features.

Position of each particle represent a possible subset of features and fitness of each particle is calculated using accuracy of the QNN model of the validation set of the data. The PSO algorithm then iteratively updates each particle's velocity and position according to the equations:

Velocity Update:

$$v_i^{t+1} = w.v_i^t + c_1.r_1.\left(p_i^{best} - x_i^t\right) + c_2.r_2.(g^{best} - x_i^t)$$

Position Update:

$$x_i^{t+1} = x_i^t + v_i^{t+1}$$

Where:

- v_i^t is the velocity of particle i at iteration t,
- x_i^t is the position (feature subset) of particle i,
- p_i^{best} is the best position found by particle i so far,
- g^{best} is the global best position found among all particles,
- w is the inertia weight controlling exploration vs. exploitation,
- c_1 and c_2 are cognitive and social acceleration coefficients,
- r_1 and r_2 are random values uniformly distributed in $[0, 1]$.

As feature selection is a binary problem, the velocity is mapped to a binary decision using a sigmoid transfer function:

Binary Transformation (Sigmoid + Thresholding):

$$S(v_i^{t+1}) = \frac{1}{1 + e^{-v_i^{t+1}}}$$

$$x_i^{t+1} = \{1, \quad if\ S(v_i^{t+1}) > \theta\ 0, \qquad otherwise$$

Where θ is a predefined threshold (commonly set to 0.5).

Through iterative optimization, particles converge towards an optimal feature subset that maximizes the QNN's ability to detect fraudulent activities. The global best particle (i.e., the feature subset with the maximum classification performance) is picked as the final solution and is used as the input to train the final QNN model. This process effectively balances exploration (Exploring optimal feature collections) and exploitation (filtering good solutions), ensuring that the selected features enhance the QNN's detection capabilities without redundancy or overfitting. PSO serves as a powerful wrapper-based feature selection strategy that synergizes with QNNs to capture the most relevant attributes in deep-structured financial data, indicating to a more precise and computationally efficient anomaly detection system.

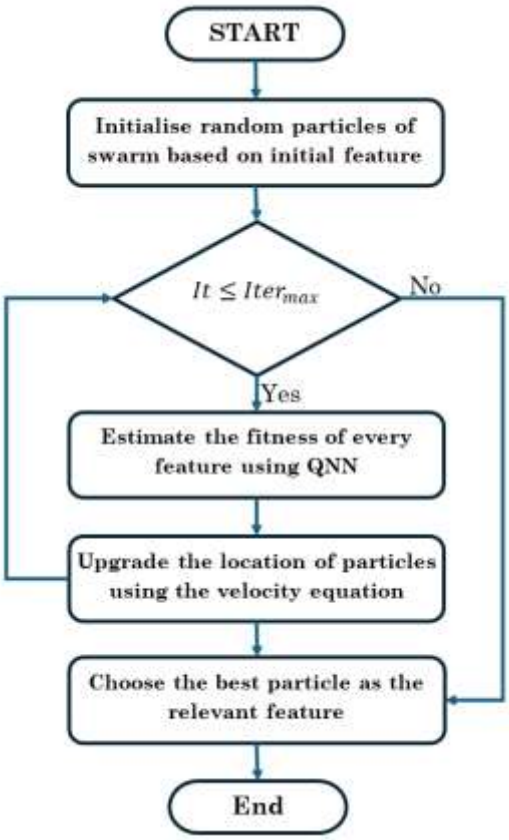

Figure 2. Flow chart for Feature Selection process using PSO.

4.4. Anomaly Detection Using PSO-Optimized QNN

QNNs employ the computational expertise of quantum mechanics to handle data encoded into qubit states. Each input vector is encoded into a set of qubits $|q\_1\rangle, |q\_2\rangle, \ldots, |q\_n\rangle$, which are manipulated using parameterized quantum gates (e.g., rotation and entangling gates).

The condition of a single qubit is denoted as:

$$|Q\rangle = x|0\rangle + y|1\rangle$$

$x, y \in C$ such that $|x|^2 + |y|^2 = 1$. This formulation is part of the Hilbert space as defined by Dirac notation.

For a system of n qubits, the quantum perceptron outputs the final state as:

$$|b\rangle = A\left(\sum_{j=1}^{n} h_j|Q_j\rangle\right)$$

Or, more specifically at time step s, the output can be written as:

$$|b(s)\rangle = A\left(\sum_{j=1}^{n} h_j(s)|q_j\rangle\right)$$

The weight update rule in the QNN (inspired by the perceptron learning algorithm) is given by:

$$h_j(s+1) = h_j(s) + \lambda(|b^*\rangle - |b(s)\rangle)\langle q_j|$$

Where λ is the learning rate, and $|b^*\rangle$ is the expected output state.

To optimize the QNN weights and biases, this work employs PSO. Each particle in the PSO represents a candidate solution (i.e., a set of QNN biases and weights), and the swarm iteratively searches for the optimal parameters that minimize the classification error.

Let:

- a: number of neurons in the hidden layer,
- b: number of input features,
- h: total number of parameters (weights and biases) in the QNN.

The total quantity of QNN parameters to be optimized is:

$$h = ab + 2a + 1$$

Each particle i in the swarm has a position $x_i \in R^h$, representing QNN weights/biases, and a velocity v_i. These are updated using the standard PSO equations:

Velocity Update Equation:

$$v_i(t+1) = w.\, v_i(t) + c_1.\, r_1.\left(p_i^{best} - x_i(t)\right) + c_2.\, r_2.\left(g^{best} - x_i(t)\right)$$

Position Update Equation:

$$x_i(t+1) = x_i(t) + v_i(t+1)$$

Where:

- w: inertia weight,
- c_1, c_2 : acceleration coefficients for cognitive and social components,
- $r_1, r_2 \sim U(0,1)$: random numbers,
- p_i^{best} : personal best solution of particle iii,
- g^{best}: global best solution among all particles.

The fitness of each particle is estimated depending on the classification accuracy or other performance metrics of the QNN model using that particle's weights. Over successive iterations, the PSO guides particles toward regions in the search space associated with better classification outcomes, thereby finding the optimal set of parameters for the QNN.

PSO-QNN Detection Flow

1. **Data Preprocessing**: Input data is first normalized using Min-Max normalization.
2. **Feature Selection**: PSO is applied to choose a best subset of features from the input.
3. **Weight Optimization**: PSO is again employed to optimize QNN weights and biases.
4. **QNN Training**: The QNN is trained using the optimal parameter set to learn the patterns in the data.
5. **Intrusion Detection**: The trained QNN detects anomalies based on the learned representations.

Flowchart for the PSO-QNN detection flow is illustrated in figure 3 and pseudocode is presented as follows.

Pseudocode: PSO-Optimized QNN for Anomaly Detection

BEGIN

1. Load and Preprocess Dataset

- Load IEEE-CIS Fraud Detection dataset
- Handle missing values (if any)
- Normalize or standardize the feature values
- Encode categorical variables
- Split data into Training and Testing sets

2. Feature Selection

- Apply PSO to select the most relevant features
- Reduce dimensionality of input features

3. Initialize QNN Structure

- Define number of input nodes (equal to selected features)
- Define number of hidden layer neurons
- Define number of output nodes (binary classification: fraud or not)
- Calculate total number of weights and biases (dimension of solution vector)

4. Initialize PSO Parameters

- Set number of particles
- Set maximum number of iterations
- Initialize particle positions randomly (each position encodes QNN weights and biases)

- Initialize velocities of all particles to zero
- Set inertia weight (w), cognitive (c1), and social (c2) coefficients

5. Optimization Loop (For each iteration)

FOR each iteration from 1 to Itermax DO

FOR each particle DO

- Decode the particle's position into QNN weight and bias matrices
- Evaluate fitness:
  - Run QNN forward pass with current weights
  - Compute classification accuracy or another metric on training data
- Update personal best position and fitness if current fitness is better
- Update global best position if current fitness is better than global best

END FOR

FOR each particle DO

- Update velocity using PSO update formula:

$$velocity = w * velocity + c1 * rand1 * (personalBest - currentPosition) + c2 * rand2 * (globalBest - currentPosition)$$

- Update position:

$$position = position + velocity$$

END FOR

END FOR

6. Evaluate Optimized QNN on Test Data

- Decode global best position into final QNN weights and biases
- Use final QNN to predict test data
- Calculate performance metrics:
  - Accuracy, Precision, Recall, F1-Score, Specificity, Sensitivity
  - False Positive Rate (FPR), False Negative Rate (FNR)
  - Matthews Correlation Coefficient (MCC)
  - Negative Predictive Value (NPV)

7. Output Final Results

- visualize performance metrics
- Compare results with standard models (LSTM, KNN, SVM)

END

5. Results and Discussions

The IEEE-CIS Fraud Detection dataset is adopted to evaluate the proposed QNN optimized by PSO for anomaly detection. The dataset contains a collection of identification related features and transaction related features that represent the real time scenarios for abnormalities in financial systems. Fo conventional ML models, adopting this dataset creates substantial difficulties due to its large dimensionality and imbalance. Hence this dataset is chosen for evaluating performance of proposed PSO-QNN. Using Min-Max normalization, initial data preprocessing is executed to systemize features of the data within a predefined range. This can improve the convergence speed while training the model. Then PSO is used to optimize the most informative features of the data. Subset of binary coded features of the data is represented as each particle and fitness of every particle can be assessed by evaluating the accuracy of the respective QNN configuration. After optimizing the most informative subset of features of the data, weights biases of the QNN can be adjusted by using PSO. This procedure increase the accuracy and reduces dimensionality of the data.

The data set is divided for training and testing by allocating 70% for training and 30% for testing. PSO optimized weights and biases are allotted for QNN as initialization for effectively explore through the solution area for identification of optimal parameter values. In PSO, maximum number of iterations are assigned as 100 and number of particles or population size is chosen as 50. Performance metrics like specificity, accuracy, precision, recall and F1-score are evaluated and compared with conventional ML models.

5.1. Performance Measures

Functioning of the proposed PSO optimized QNN is evaluated by comparing with conventional ML algorithms including LSTM, KNN and SVM in terms of performance metrics by using IEEE-CIS data. Performance metrics compared are given as follows:

- **Specificity** refers to the fraction of actual negative (legitimate) transactions which are correctly identified. It is calculated using the formula

$$Specificity(Spe) = \frac{TN}{TN + FP}$$

- **Sensitivity** (Recall) denotes the fraction of actual positive (fraudulent) transactions that are accurately identified. It is calculated as:

$$Sensitivity(Sen) = \frac{TP}{TP + FN}$$

- **Accuracy** indicates the overall fraction of correct estimates made by the model. It is computed using

$$Accuracy(Acc) = \frac{TP + TN}{TP + TN + FP + FN}$$

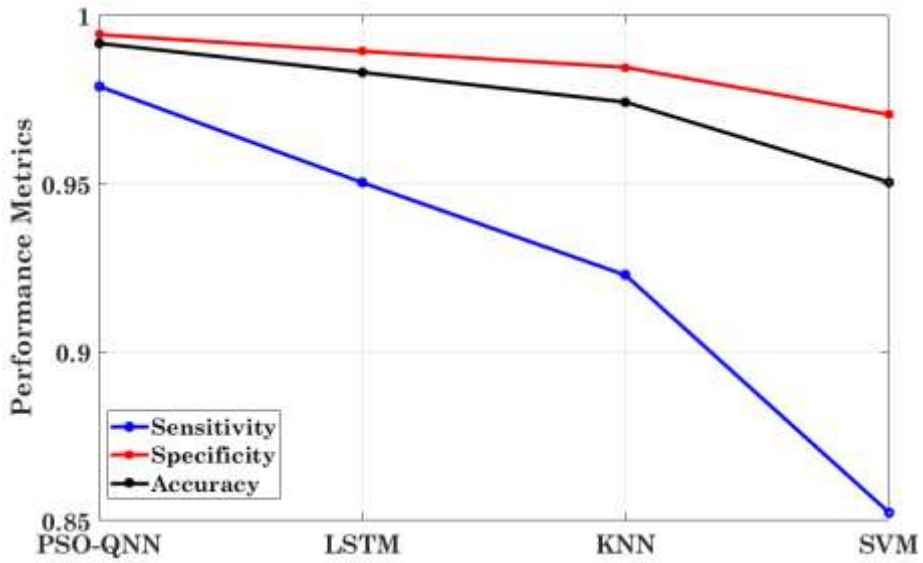

Figure 4. Comparison of performance metrics(Sen, Spe, Acc) between PSO-QNN and conventional methods

The graphical representation in Fig. 4 shows the comparison of Sensitivity, Specificity, and Accuracy between the proposed PSO-QNN model and existing classifiers. The results indicate that the PSO-QNN achieves superior performance, attaining an accuracy of 98.5%, which is higher than that of KNN, SVM, LSTM.

- **Precision** estimates the fraction of true positive estimates among all positive estimates attained by the model:

$$Precision = \frac{TP}{TP + FP}$$

- **Recall**, again calculated as Sensitivity, is reiterated here for consistency:

$$Recall = \frac{TP}{TP + FN}$$

- **F1-Score** is a harmonic mean of Precision and Recall, evaluating both metrics in a single score:

$$F1 - Score = \frac{2TP}{2TP + FP + FN}$$

As shown in Fig. 5, the PSO-QNN achieves significantly better Precision, Recall, and F1-Score than traditional models. This confirms its strength in identifying fraud with fewer misclassifications.

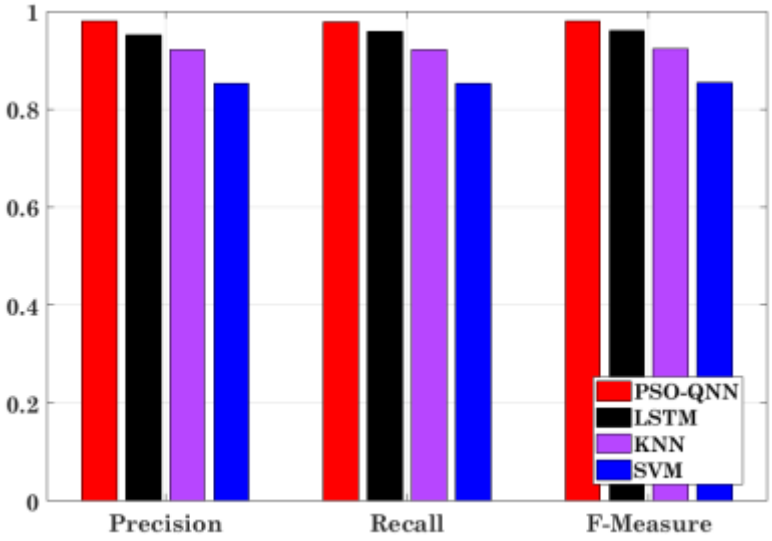

Figure 5. Comparison of performance metrics(Precision, Recall, F1 Score) between PSO-QNN and conventional methods

- **False Positive Rate (FPR)** measures the percentage of genuine transactions wrongly categorized as anomaly:

$$FPR = \frac{FP}{TN + FP}$$

- **False Negative Rate (FNR)** assesses the percentage of false transactions that were falsely predicted as genuine:

$$FNR = \frac{FN}{TP + FN}$$

As depicted in Fig. 6, the proposed PSO-QNN demonstrates a lower FPR and FNR compared to LSTM, KNN, and SVM, indicating its improved reliability and robustness in minimizing both false alarms and missed fraud detections.

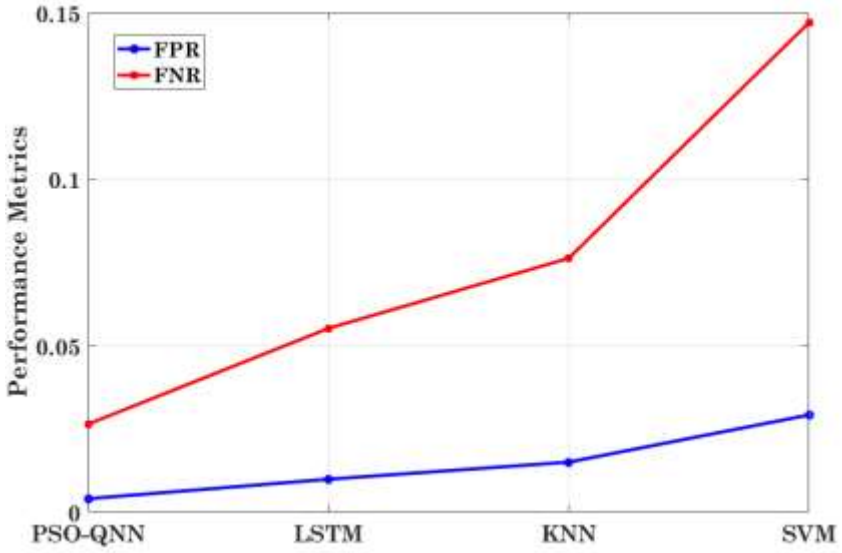

Figure 6. Comparison of FPR and FNR between PSO-QNN and conventional methods

These outcomes highlight the performance of the PSO-optimized QNN model in anomaly detection. The integration of PSO contributes to better weight and bias initialization, improving convergence and reducing overfitting — critical advantages when handling the composite and unnecessary data typical in financial fraud scenarios.

5.2. Matthews Correlation Coefficient (MCC)

The MCC is a widely recognized metric for evaluating performance of the model. MCC provides a reasonable evaluation that considers TP, TN and FP, FN, and it remains reliable even when class sizes are highly uneven.

The MCC is calculated applying the following formula:

$$MCC = \frac{(TP.TN) - (FP.FN)}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}}$$

The Negative Predictive Value (NPV) is used to measure the fraction of instances that were correctly predicted as negative (i.e., non-fraudulent transactions) among all predicted negatives. This metric is critical in anomaly detection, where minimizing the risk of missing fraudulent activities is essential. NPV is calculated as:

$$NPV = \frac{TN}{TN + FN}$$

The comparative results of the PSO-QNN model against traditional classifiers such as LSTM, KNN, and SVM are illustrated graphically in Fig. 7. These results indicate that the proposed PSO-QNN architecture yields higher MCC and NPV values, suggesting superior reliability and robustness in accurately classing both anomaly and non-anomaly transactions.

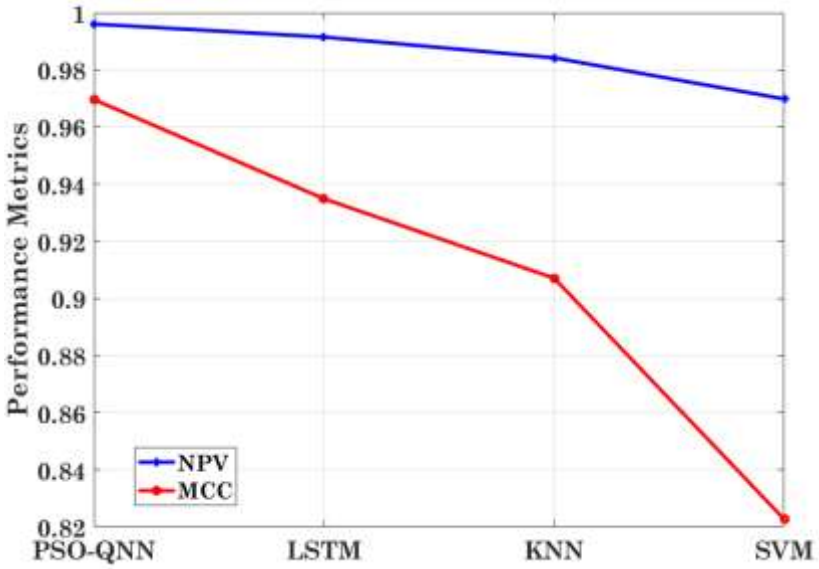

Figure 7. Comparison of NPV and MCC between PSO-QNN and conventional methods

The reliability of the proposed approach incorporating PSO and QNN for anomaly detection is illustrated in the simulation results. PSO is employed for optimizing the feature selection of the data set and weights and biases of QNN. The evaluation of optimal values for QNN increases the capacity of the model in anomaly detection for large data like IEEE-CIS dataset.

6. Conclusion

In this paper, Quantum Neural Networks (QNNs) is integrated with Particle Swarm Optimization (PSO) for anomaly detection in securities transactions of financial systems. PSO is employed for feature selection of dataset and for optimizing the weights and biases of QNN. An IEEE-CIS dataset is adopted to evaluate the performance of proposed model by detecting abnormalities or anomalies in securities transactions. As presented in results, compared to conventional ML models like LSTM, KNN and SVM, proposed PSO optimized QNN model demonstrates a considerable improvement. The evaluation of the effectiveness of the proposed model is performed by comparing performance metrics with conventional ML approaches. An accuracy of 98.55% is achieved by proposed PSO-QNN model than conventional models by exhibiting conceptual flexibility in anomaly detection. Optimization of features of dataset and optimization weights and biases of QNN by PSO explores the solution area efficiently and reduces the risk of local optima convergence. The capacity of the model further enhances due to quantum properties of QNN and design nonlinear relationships in high dimensional data. These nonlinear associations of data are essential to detect anomaly in securities transactions of financial systems. The results presented demonstrate that proposed PSO optimized QNN model efficiently detects anomaly in the data of financial transactions. This work can be extended by adopting federated learning enhanced by quantum networks and deploying in live financial transactions for practical threat mitigation.

References:

1. Atadoga, Akoh, Uchenna Joseph Umoga, Oluwaseun Augustine Lottu, and Enoch Oluwademilade Sodiya. "Evaluating the impact of cloud computing on accounting firms: A review of efficiency, scalability, and data security." *Global Journal of Engineering and Technology Advances* 18, no. 2 (2024): 065-074.
2. Bello, Halima Oluwabunmi, Adebimpe Bolatito Ige, and Maxwell Nana Ameyaw. "Adaptive machine learning models: concepts for real-time financial fraud prevention in dynamic environments." *World Journal of Advanced Engineering Technology and Sciences* 12, no. 02 (2024): 021-034.
3. Awujoola, J. Olalekan, T. Aniemeka Enem, J. Adeyemi Owolabi, O. Christiana Akusu, O. Abioye, E. AbidemiAwujoola, and R. OlayinkaAdelegan. "9 Exploring the Intersection of Quantum Neural Networks and Classical Neural Networks for Early Cancer Identification." *Quantum Computing: The Future of Information Processing* (2025): 147.
4. Hdaib, Moe, Sutharshan Rajasegarar, and Lei Pan. "Quantum deep learning-based anomaly detection for enhanced network security." *Quantum Machine Intelligence* 6, no. 1 (2024): 26.
5. Wang, Bingxing, Yuxin Dong, Jianhua Yao, Honglin Qin, and Jiajing Wang. "Exploring anomaly detection and risk assessment in financial markets using deep

neural networks." *International Journal of Innovative Research in Computer Science and Technology* 12, no. 4 (2024).

6. Khodabandehlou, Samira, and Alireza Hashemi Golpayegani. "FiFrauD: unsupervised financial fraud detection in dynamic graph streams." *ACM Transactions on Knowledge Discovery from Data* 18, no. 5 (2024): 1-29.
7. Hao, Jingwei, Senlin Luo, and Limin Pan. "Rule extraction from biased random forest and fuzzy support vector machine for early diagnosis of diabetes." *Scientific reports* 12, no. 1 (2022): 9858.
8. Xu, Yi, Lei Shang, Jinxing Ye, Qi Qian, Yu-Feng Li, Baigui Sun, Hao Li, and Rong Jin. "Dash: Semi-supervised learning with dynamic thresholding." In *International conference on machine learning*, pp. 11525-11536. PMLR, 2021.
9. Mienye, Ibomoiye Domor, and Theo G. Swart. "A comprehensive review of deep learning: Architectures, recent advances, and applications." *Information* 15, no. 12 (2024): 755.
10. Lisboa, Paulo JG, Sascha Saralajew, Alfredo Vellido, Ricardo Fernández-Domenech, and Thomas Villmann. "The coming of age of interpretable and explainable machine learning models." *Neurocomputing* 535 (2023): 25-39.
11. Chen, Linshu, Tao Li, Yuxiang Chen, Xiaoyan Chen, Marcin Wozniak, Neal Xiong, and Wei Liang. "Design and analysis of quantum machine learning: a survey." *Connection Science* 36, no. 1 (2024): 2312121.
12. Malempati, Murali. "Machine Learning and Generative Neural Networks in Adaptive Risk Management: Pioneering Secure Financial Frameworks." *Kurdish Studies. Green Publication. https://doi. org/10.53555/ks. v10i2* 3718 (2022).
13. Hilal, Waleed, S. Andrew Gadsden, and John Yawney. "Financial fraud: a review of anomaly detection techniques and recent advances." *Expert systems With applications* 193 (2022): 116429.
14. Liu, Jing, Yang Liu, Jieyu Lin, Jielin Li, Liang Cao, Peng Sun, Bo Hu, Liang Song, Azzedine Boukerche, and Victor CM Leung. "Networking systems for video anomaly detection: A tutorial and survey." *ACM Computing Surveys* 57, no. 10 (2025): 1-37.
15. Xu, He, Lin Zhang, Peng Li, and Feng Zhu. "Outlier detection algorithm based on k-nearest neighbors-local outlier factor." *Journal of Algorithms & Computational Technology* 16 (2022): 17483026221078111.
16. Fu, Yujian, Cheng Chen, Xiaohui Chen, Weng-Fai Wong, and Bingsheng He. "Optimizing the Number of Clusters for Billion-scale Quantization-based Nearest Neighbor Search." *IEEE Transactions on Knowledge and Data Engineering* (2024).
17. Mienye, Ibomoiye Domor, and Theo G. Swart. "Deep autoencoder neural networks: A comprehensive review and new perspectives." *Archives of computational methods in engineering* (2025): 1-20.
18. Alloqmani, Ahad, Yoosef B. Abushark, Asif Irshad Khan, and Fawaz Alsolami. "Deep learning based anomaly detection in images: insights, challenges and recommendations." *International Journal of Advanced Computer Science and Applications* 12, no. 4 (2021).
19. Khalid, Abdul Rehman, Nsikak Owoh, Omair Uthmani, Moses Ashawa, Jude Osamor, and John Adejoh. "Enhancing credit card fraud detection: an ensemble machine learning approach." *Big Data and Cognitive Computing* 8, no. 1 (2024): 6.

20. Duraj, Agnieszka, Piotr S. Szczepaniak, and Artur Sadok. "Detection of Anomalies in Data Streams Using the LSTM-CNN Model." *Sensors* 25, no. 5 (2025): 1610.
21. Nguyen, Thien, Tuomo Sipola, and Jari Hautamäki. "Machine learning applications of quantum computing: A review." *arXiv preprint arXiv:2406.13262* (2024).
22. Keller, Christo Meriwether, Satyajayant Misra, Andreas Bärtschi, and Stephan Eidenbenz. "Quantum approximate optimization: A computational intelligence perspective." *arXiv preprint arXiv:2407.07202* (2024).
23. Awujoola, J. Olalekan, T. Aniemeka Enem, J. Adeyemi Owolabi, O. Christiana Akusu, O. Abioye, E. AbidemiAwujoola, and R. OlayinkaAdelegan. "9 Exploring the Intersection of Quantum Neural Networks and Classical Neural Networks for Early Cancer Identification." *Quantum Computing: The Future of Information Processing* (2025): 147.
24. Naik, Abha Satyavan, Esra Yeniaras, Gerhard Hellstern, Grishma Prasad, and Sanjay Kumar Lalta Prasad Vishwakarma. "From portfolio optimization to quantum blockchain and security: A systematic review of quantum computing in finance." *Financial Innovation* 11, no. 1 (2025): 1-67.
25. Bhasin, Narinder Kumar, Sunil Kadyan, Kathari Santosh, Ramya HP, Ravindra Changala, and B. Kiran Bala. "Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management." In *2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS)*, pp. 1-7. IEEE, 2024.
26. Weinberg, Abraham Itzhak, and Alessio Faccia. "Quantum Algorithms: A New Frontier in Financial Crime Prevention." *arXiv preprint arXiv:2403.18322* (2024).
27. Dong, Yumin, Yanying Fu, Hengrui Liu, Xuanxuan Che, Lina Sun, and Yi Luo. "An improved hybrid quantum-classical convolutional neural network for multi-class brain tumor MRI classification." *Journal of Applied Physics* 133, no. 6 (2023).
28. Peng, Yifeng, Xinyi Li, Zhiding Liang, and Ying Wang. "Qsco: A quantum scoring module for open-set supervised anomaly detection." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 39, no. 19, pp. 19884-19894. 2025.
29. Lopez, Juan. "Quantum Machine Learning: Applications, Algorithms, and Hardware Challenges." *International Journal of AI, BigData, Computational and Management Studies* 5, no. 4 (2024): 1-13.
30. Mironowicz, Piotr, Antonio Mandarino, A. Yilmaz, and Thomas Ankenbrand. "Applications of quantum machine learning for quantitative finance." *arXiv preprint arXiv:2405.10119* (2024).
31. Sachdeva, Tamanna, Lalit Mohan Goyal, and Mamta Mittal. "Mapping the Landscape of Personalization: A Comprehensive Review of Prediction and Trends in Recommendation Systems." *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 15, no. 2 (2025): e70006.
32. Kea, Kimleang, Dongmin Kim, Chansreynich Huot, Tae-Kyung Kim, and Youngsun Han. "A Hybrid Quantum-Classical Model for Stock Price Prediction Using Quantum-Enhanced Long Short-Term Memory." *Entropy* 26, no. 11 (2024): 954.