Quantum Machine Learning for Insurance Claim Fraud Detection: A Hybrid Approach

Pankaj Kumar Verma[1], Dr. Satayanarayana Vollala[2], Dr. Srinivasa K G[3], Kamna Sahu[4]
International Institute of Information Technology, Naya Raipur,, Chhattisgarh, India
[1]pankaj24300@iiitnr.edu.in, [2]satya@iiitnr.edu.in, [3]srinivasa@iiitnr.edu.in, [4]kamna@iiitnr.edu.in

***Abstract*—This paper presents a novel hybrid quantum-classical approach for the detection of insurance claims fraud. The proposed framework first utilizes a Quantum Support Vector Classifier (QSVC) with a quantum kernel to model complex, nonlinear feature interactions, followed by a classical Random Forest (RF) ensemble that refines the predictions. The hybrid QSVC+RF pipeline is evaluated on a real-world insurance data set comprising 1,000 merged claims with 39 features, including policy, agent, and vendor data. The results, as summarized in Table 1, demonstrate that the hybrid model significantly outperforms the standalone quantum classifiers. In particular, the hybrid method achieves superior overall accuracy and substantially higher recall for fraudulent cases compared to both the QSVC using a ZZ feature map and a Variational Quantum Classifier (VQC). These findings align with existing research indicating that hybrid quantum–classical ensembles can effectively leverage the expressive capacity of quantum kernels while preserving the robustness of classical models. The contributions of this work include comprehensive simulation results using Qiskit, applied to a realistic insurance dataset, which highlight practical performance improvements and inform effective feature selection. The study underscores the promising applicability of near-term quantum machine learning (QML) to real-world financial fraud detection scenarios.**

***Keywords*—Quantum Machine Learning, Fraud Detection, Quantum Support Vector Classifier, Variational Quantum Classifier, Hybrid Quantum-Classical Models.**

I. Introduction

Insurance fraud imposes enormous costs on insurers and society. The FBI estimates that tens of billions of dollars in fraudulent claims occur annually. Automated fraud detection is crucial, yet remains challenging: fraudulent patterns are often complex and evolving, and genuine fraud instances are rare, leading to a severe class imbalance. Classical machine learning (ML) techniques have been widely adopted to analyze large-scale insurance claim datasets and flag anomalies. However, they often struggle to detect subtle and high-dimensional feature interactions without extensive feature engineering. In response, quantum machine learning (QML) has emerged as a promising paradigm that leverages the ability of quantum computing to process high-dimensional data spaces more naturally and efficiently than classical algorithms [1]. Quantum Support Vector Machines (QSVM), which use quantum kernels to embed classical data into Hilbert spaces, have shown notable success in modeling nonlinear decision boundaries. For example, Pushpak and Jain [2] and Pushpak et al. [3] applied QSVMs to insurance fraud datasets, demonstrating competitive or superior performance in small-scale structured data. However, these efforts primarily compare quantum and classical classifiers in isolation or rely on synthetic data like credit card fraud. They do not explore the potential benefits of hybrid architectures. Meanwhile, classical ensemble methods, especially Random Forests (RF), are well-regarded for their robustness and interpretability in fraud detection [4]. Yet, the integration of quantum kernels with such classical ensemble models remains underexplored. Bhasin et al. [5] suggest that hybrid quantum–classical models could yield measurable gains, particularly on small datasets common in financial fraud scenarios.

This paper addresses these gaps by proposing a novel hybrid quantum–classical fraud detection pipeline. The proposed methodology combines a Quantum Support Vector Classifier (QSVC) using the IBM Qiskit ZZFeatureMap as a quantum kernel, with a classical Random Forest (RF) that refines predictions based on both classical and quantum-derived features. The layered architecture leverages the strengths of both paradigms: quantum models model complex nonlinear interactions in a compact feature space, while the RF enhances recall and stability using full-scale classical features. The proposed method is evaluated on a real-world insurance dataset containing 1,000 records, compiled by merging policyholder, agent, and vendor information. Three models are benchmarked: (1) QSVC with a ZZFeatureMap, (2) an improved Variational Quantum Classifier (VQC), and (3) the proposed Hybrid QSVC+RF approach. The rest of the paper is organized as follows: Section II reviews related classical and quantum fraud detection literature. Section III discusses theoretical concepts of QSVC, VQC, and RF. Section IV describes the proposed methodology, including the preparation of the data set, the selection of characteristics, and the architecture of the model. Section V presents the experimental results and analysis. Section VI concludes the paper and highlights future directions.

II. Literature Review

Recent advances in both classical and quantum machine learning have contributed to the development of intelligent systems for fraud detection in financial and insurance domains. Pushpak and Jain [2] implemented a Quantum Support Vector Machine (QSVM) using Qiskit to identify fraudulent housing insurance claims. Their work highlighted that QSVMs could perform competitively with classical SVMs on small, structured datasets. However, the study focused solely on isolated quantum models and used a limited set of manually engineered features. Building on this, Pushpak et al. [3] introduced a quantum feature selection technique and demonstrated its efficacy on real home insurance data. While their results were promising, the scope remained constrained to individual quantum classifiers without exploring integration with classical models, which could offer further performance improvements in complex scenarios.

Innan et al. [7] conducted a comparative analysis of four quantum machine learning models—QSVC, Variational Quantum Classifier (VQC), Estimator QNN, and Sampler QNN—on a synthetic financial fraud dataset. Their results showed that QSVC outperformed other models with an F1-score close to 0.98, suggesting that quantum kernels can effectively capture both fraudulent and non-fraudulent patterns. However, the study lacked real-world insurance data and did not investigate ensemble or hybrid approaches. Gheysarbeigi et al. [4] proposed an ensemble model using multiple classical classifiers optimized with the BQANA metaheuristic algorithm for automobile insurance fraud detection. They successfully addressed class imbalance through resampling strategies and showed improved detection accuracy. Nevertheless, the work was entirely classical and did not explore the potential gains from quantum-classical hybridization.

Bhasin et al. [5] examined quantum enhancements for portfolio optimization and suggested that combining quantum feature maps with classical components could enhance accuracy and convergence. While their insights into hybrid architectures were valuable, the study was focused on portfolio management and did not include fraud-specific datasets or evaluation metrics. Saddi et al. [8] proposed a real-time fraud detection framework using reinforcement learning (RL) for insurance claims. Their RL-based approach adapted to dynamic fraud patterns over time but relied heavily on time-series data and did not leverage quantum capabilities. These gaps collectively emphasize the need for a hybrid fraud detection system that integrates quantum-enhanced feature encoding with robust classical models like Random Forests. The proposed methodology in this study addresses this void by implementing and evaluating a QSVC+RF pipeline on a realistic, domain-specific insurance dataset.

III. Preliminaries

A. Data Encoding Methods

1) ZFeatureMap: The ZFeatureMap is a quantum data encoding strategy that maps classical input features into quantum states using single-qubit Pauli-Z rotations. It applies phase rotations around the Z-axis independently to each qubit, making it a separable feature map with no entanglement. This makes it efficient for scenarios where features are expected to be linearly separable in Hilbert space.

Mathematically, for an input vector $\mathbf{x} = (x_1, x_2, ..., x_n)$, the unitary operation of the ZFeatureMap is:

$$U_{\mathrm{Z}}(\mathbf{x}) = \prod_{i=1}^{n} \exp\left(i \cdot x_i \cdot Z_i\right)$$

where Z_i is the Pauli-Z operator acting on the i^{th} qubit. The resulting encoded quantum state is:

$$|\Phi(\mathbf{x})\rangle = U_{\mathrm{Z}}(\mathbf{x})|0\rangle^{\otimes n}$$

As demonstrated by Innan et al. [7], the ZFeatureMap is particularly useful in scenarios where feature interactions are independent, making it a baseline tool for comparing entanglement-free encodings. While ZFeatureMap lacks expressivity compared to its entangling counterparts, it provides a computationally efficient mechanism for benchmarking quantum classifiers in Noisy Intermediate-Scale Quantum (NISQ) settings.

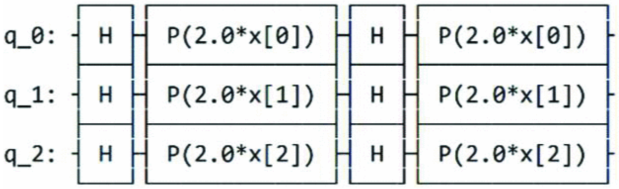

Fig. 1: Quantum circuit representation of ZFeatureMap with 3 qubits. Adapted from [15].

2) ZZFeatureMap: The ZZFeatureMap builds upon the ZFeatureMap by introducing entanglement through pairwise interactions between qubits. Specifically, it applies parameterized ZZ-gates (entangling rotations) in addition to the single-qubit Z rotations. This entangling structure enables the encoding of correlations between input features, allowing the model to capture more complex, nonlinear patterns in the data.

The operation was first introduced by Havlíček et al. [12] as part of quantum-enhanced kernel methods. The unitary operator of the ZZFeatureMap is defined as:

$$U_{\mathrm{ZZ}}(\mathbf{x}) = \left(\prod_{i=1}^{n} \exp\left(i \cdot x_i \cdot Z_i\right)\right) \cdot \left(\prod_{i<j} \exp\left(i \cdot \gamma \cdot x_i x_j \cdot Z_i Z_j\right)\right)$$

Here, Z_i and Z_j are Pauli-Z operators acting on qubits i and j, and γ is a tunable entanglement parameter. The resulting quantum state is:

$$|\Phi(\mathbf{x})\rangle = U_{\mathrm{ZZ}}(\mathbf{x})|0\rangle^{\otimes n}$$

In this study, the ZZFeatureMap was central to the proposed hybrid QSVC+RF methodology. It enabled the QSVC to model intricate relationships between high-risk fraud indicators such as claim-to-premium ratios and agent experience through feature entanglement.

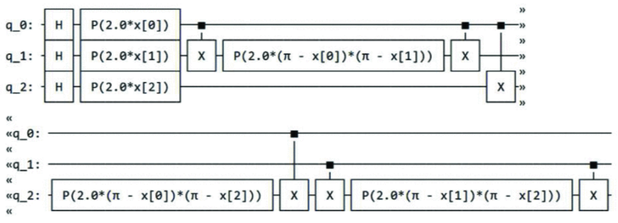
q_0:
q_1:
q_2:
H
P(2.0*x[0])
P(2.0*x[1])
P(2.0*x[2])
X
P(2.0*(π - x[0])*(π - x[1]))
«q_0:
«q_1:
«q_2:
P(2.0*(π - x[0])*(π - x[2]))
P(2.0*(π - x[1])*(π - x[2]))

Fig. 2: Quantum circuit representation of ZZFeatureMap with 3 qubits. Adapted from [15].

B. Quantum Support Vector Classifiers

Quantum Support Vector Classifiers (QSVC) extend classical Support Vector Machines by employing quantum kernels to compute the similarity between data points in a high-dimensional Hilbert space. The quantum kernel is defined as:

$$K(\mathbf{x}, \mathbf{x}') = |\langle \Phi(\mathbf{x}) | \Phi(\mathbf{x}') \rangle|^2$$

where $|\Phi(\mathbf{x})\rangle$ and $|\Phi(\mathbf{x}')\rangle$ are quantum states resulting from encoding classical inputs $\mathbf{x}$ and $\mathbf{x}'$ using a feature map, such as the ZZFeatureMap. This approach allows for capturing complex, non-linear relationships in the data that may be challenging for classical kernels to model effectively [12].

In our study, we utilized Qiskit's `FidelityQuantumKernel` to construct the quantum kernel and the `QSVC` class from the `qiskit-machine-learning` package to perform classification. The QSVC was trained on an insurance claims dataset to detect fraudulent activities, leveraging the quantum kernel's ability to represent intricate feature interactions.

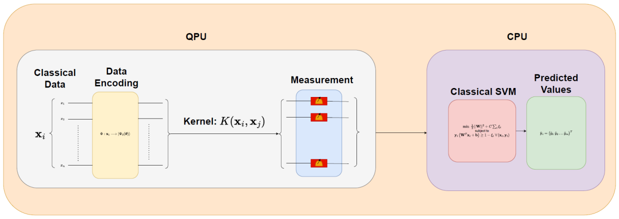
QPU
CPU
Classical Data
Data Encoding
$\mathbf{x}_i$
x_1
x_2
x_n
$\Phi : \mathbf{x}_i \longrightarrow |\Psi_0(\boldsymbol{\theta})\rangle$
Kernel: $K(\mathbf{x}_i, \mathbf{x}_j)$
Measurement
Classical SVM
$\min \frac{1}{2}||\mathbf{W}||^2 + C\sum_i \xi_i$
subject to
$\mathbf{y}_i(\mathbf{W}^T\mathbf{x}_i + \mathbf{b}) \geq 1 - \xi_i \, \forall (\mathbf{x}_i, \mathbf{y}_i)$
Predicted Values
$\hat{y}_i = (\hat{y}_1 \, \hat{y}_2 \ldots \hat{y}_m)^T$

Fig. 3: Architecture of Quantum Support Vector Classifier (QSVC). Adapted from [7].

C. Variational Quantum Classifiers

Variational Quantum Classifiers (VQC) are hybrid quantum-classical models that utilize parameterized quantum circuits (ansätze) optimized through classical algorithms to perform classification tasks. The general structure involves encoding input data into quantum states, applying a variational circuit with trainable parameters $\boldsymbol{\theta}$, and measuring the output to make predictions.

The process can be mathematically represented as:

$$|\psi_{\text{out}}\rangle = U(\mathbf{x}, \boldsymbol{\theta})|0\rangle^{\otimes n}$$

where $U(\mathbf{x}, \boldsymbol{\theta})$ is the unitary operation comprising the feature map and the variational circuit applied to the initial state $|0\rangle^{\otimes n}$. The measurement outcomes are used to estimate class probabilities, and the parameters $\boldsymbol{\theta}$ are optimized to minimize a loss function, such as cross-entropy, using classical optimizers like COBYLA or SPSA [14].

In our implementation, we employed Qiskit's `VQC` class, combining the ZZFeatureMap for data encoding and a RealAmplitudes ansatz for the variational circuit. The model was trained on the same insurance claims dataset, aiming to classify claims as fraudulent or legitimate.

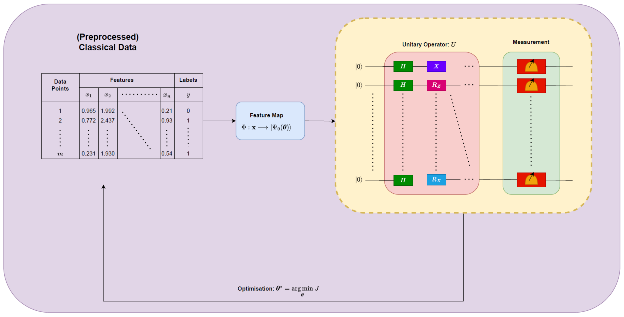

Fig. 4: Architecture of Variational Quantum Classifier (VQC). Adapted from [7].

D. Random Forest

Random Forest (RF) is a classical ensemble learning method based on decision trees. It constructs multiple decision trees during training and outputs the class that is the mode of the classes (classification) or mean prediction (regression) of the individual trees. Each tree is trained on a bootstrap sample of the dataset and considers a random subset of features when splitting nodes.

Given N trees, the prediction $\hat{y}$ for a sample $\mathbf{x}$ is given by:

$$\hat{y} = \text{majority\_vote}\left(\{h_i(\mathbf{x})\}_{i=1}^{N}\right)$$

where $h_i(\cdot)$ is the i-th decision tree. RFs are known for their robustness, high accuracy, and ability to handle large numbers of features. In the context of fraud detection, RFs can capture nonlinear patterns and feature interactions and are especially effective when used in hybrid architectures, such as the one described in this study where RF refines the predictions of the quantum model.

In the context of fraud detection, RFs have demonstrated high accuracy and robustness. For instance, an enhanced RF model achieved an accuracy of 99.72% on a balanced dataset and 99.95% on an imbalanced dataset, outperforming traditional RF models in detecting fraudulent credit card transactions [13].

IV. Methodology

A. Dataset Description

This study utilizes a real-world insurance claims dataset published on Kaggle [16]. The dataset includes structured records of insurance claims, enriched with associated employee (agent-level) and vendor metadata. After merging these sources, the final dataset contains 1,000 unique insurance claim entries and 39 engineered features. The attributes span a range of numerical (e.g., `CLAIM_AMOUNT`, `PREMIUM_AMOUNT`), categorical (e.g., `RISK_SEGMENTATION`, `STATE`), and temporal (e.g., `REPORT_DATE`, `INCIDENT_DATE`) variables that provide contextual insight into each claim's circumstances.

The dataset was constructed by joining three interrelated tables — `Claims`, `Employee`, and `Vendor` — using primary keys such as `AGENT_ID` and `VENDOR_ID`. These joins ensured that each claim record includes agent experience levels, vendor ratings, and additional agent-vendor metadata that are potentially relevant for detecting fraudulent behaviors. The target variable `is_fraud` was derived from the field `CLAIM_STATUS`, where claims marked with ’D’ (denied) were mapped to 1 (fraud), and those with ’A’ (approved) to 0 (non-fraud). This resulted in a significant class imbalance, with fraudulent claims comprising less than 10% of the total instances.

Figure 5 highlights the imbalance between fraudulent and non-fraudulent claims in the dataset.

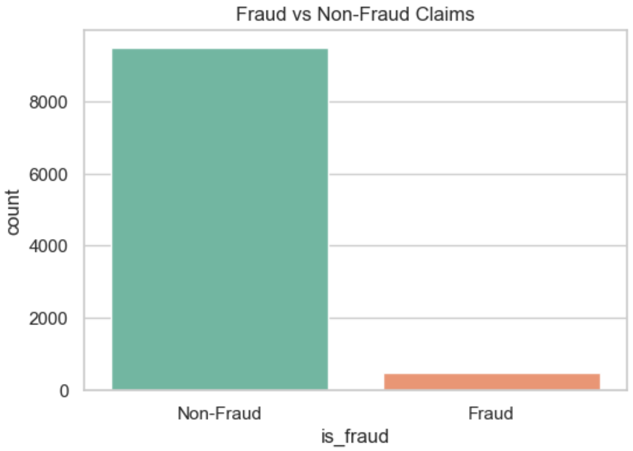

Fig. 5: Distribution of fraudulent vs. non-fraudulent claims.

B. Data Preprocessing

A comprehensive preprocessing pipeline was applied to prepare the dataset for training and quantum encoding. Initially, the three source tables were merged using foreign keys `AGENT_ID` and `VENDOR_ID`, consolidating claim-level, agent-level, and vendor-level data into a unified view. This was followed by handling missing values: numerical columns were imputed using their respective means, while categorical columns were filled using mode imputation to preserve consistency without introducing bias.

Categorical features such as `STATE`, `RISK_SEGMENTATION`, and `CLAIM_TYPE` were encoded using one-hot encoding, converting each categorical variable into multiple binary columns. This was essential for both classical models (like Random Forest) and compatibility with quantum models which require numerical inputs.

Feature engineering steps introduced domain-aware features such as the claim-to-premium ratio, computed as:

$$\text{claim\_to\_premium\_ratio} = \frac{\texttt{CLAIM\_AMOUNT}}{\texttt{PREMIUM\_AMOUNT}}$$

and a binary indicator for whether a claim was reported on a weekend:

$$\text{is\_weekend\_report} = \nVdash_{\texttt{REPORT\_DATE}\in\{\text{Sat, Sun}\}}$$

Finally, all continuous features were normalized using z-score standardization to ensure they fall within a consistent numerical range, which is particularly important for quantum circuit stability and convergence in variational models.

C. Feature Selection for Quantum Models

Although all quantum models in this study were executed using simulators provided by Qiskit, the feature selection process was informed by the practical limitations of current Noisy Intermediate-Scale Quantum (NISQ) hardware. In particular, constraints on the number of qubits and the allowable circuit depth necessitate careful dimensionality reduction when preparing data for quantum machine learning algorithms.

A focused subset of four features was selected to serve as input to the quantum models: `REPORT_DELAY_DAYS`, `CLAIM_TO_PREMIUM_RATIO`, `AGENT_EXPERIENCE_YEARS`, and `IS_WEEKEND_REPORT`. These features were chosen based on domain knowledge of fraud behavior as well as empirical importance scores computed using classical Random Forest classifiers. Each of these variables captures potentially discriminative information; for example, long delays in reporting, unusually high claim-to-premium ratios, and weekend report submissions are often correlated with suspicious claim activity.

To ensure that the selected features were both non-redundant and suitable for shallow quantum circuits, Principal Component Analysis (PCA) was optionally applied. PCA is a widely used linear transformation method that projects data into a set of orthogonal components ranked by variance [17]. In this study, the top components retained approximately 95 percent of the total variance in the reduced input space, which allowed for dimensionality control without sacrificing significant informational content. This preprocessing strategy ensures that the quantum models remain within the operational bounds of current quantum simulation tools, while also allowing for future implementation on real quantum hardware when it becomes sufficiently reliable.

D. Model Implementation

To evaluate the effectiveness of quantum and hybrid quantum-classical models for fraud detection, three distinct classifiers were implemented. The first model is a Quantum Support Vector Classifier (QSVC), which uses a quantum kernel constructed via the ZZFeatureMap. This feature map introduces entanglement between input features, enabling richer decision boundaries in Hilbert space. The kernel matrix was computed using Qiskit’s `FidelityQuantumKernel` and then passed to a classical SVM implementation for classification.

The second model is an improved Variational Quantum Classifier (VQC), designed using a parameterized quantum circuit based on the `EfficientSU2` ansatz with two layers of repetitions. The circuit was configured to operate on a 4-qubit encoding of the reduced feature set. Parameter optimization was carried out using the Simultaneous Perturbation Stochastic Approximation (SPSA) algorithm, with the objective of minimizing the categorical cross-entropy loss function.

Finally, the third model is the proposed hybrid architecture combining QSVC with a classical Random Forest (RF). In this design, predictions or decision function values produced by the QSVC are appended as an additional input feature to the full classical feature vector. This augmented feature space is then used to train an RF classifier, allowing the ensemble to benefit from quantum-enhanced feature separation while leveraging the robustness and interpretability of classical decision trees.

E. Hybrid Pipeline Design

The hybrid QSVC+RF pipeline was constructed to maximize the synergy between quantum and classical components. First, the QSVC was trained on a reduced feature subset that conforms to quantum circuit dimensional constraints. The output from the QSVC—either the predicted class labels or the raw decision function scores—was then appended to the original full feature matrix as an additional attribute. This enriched dataset was used to train a classical Random Forest classifier, which effectively re-evaluated the predictions provided by the quantum model.

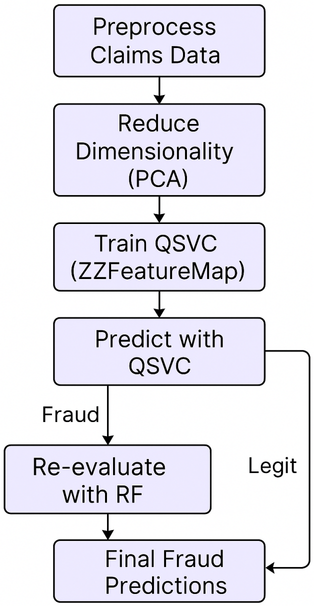

Fig. 6: Workflow of the hybrid quantum-classical pipeline (QSVC + RF).

This two-stage design allows the QSVC to act as a front-end feature discriminator that identifies hard-to-separate instances, while the RF serves as a backend classifier capable of refining predictions through ensembling. In particular, the RF model is able to correct for false positives and improve recall for the minority fraud class. The architecture of the pipeline is illustrated in Figure 6.

F. Training Setup

All quantum models were implemented using IBM's Qiskit framework and executed on the `statevector_simulator` backend, which provides noiseless simulations of quantum circuits. Classical models, including Random Forest classifiers and preprocessing utilities, were implemented using the `scikit-learn` library. The dataset was stratified and split into training and testing sets in an 80:20 ratio, preserving the underlying class distribution.

To improve robustness and minimize variance in performance evaluation, all results were averaged over five independent train-test splits with different random seeds. Hyperparameter tuning was performed using grid search combined with stratified cross-validation, targeting the most influential parameters for each model. For the Random Forest, parameters such as the number of estimators, tree depth, and minimum samples per split were optimized. For the Variational Quantum Classifier, optimizer choice (SPSA), learning rate, and circuit depth were tuned experimentally.

The complete flow of the hybrid training pipeline, including preprocessing, quantum classification, and classical refinement, is outlined in Algorithm 1.

Algorithm 1 Hybrid QSVC + Random Forest Fraud Detection

```
Require: Feature matrix $\mathbf{X}$, target vector $y$
Ensure: Final fraud predictions $\hat{y}_{\text{final}}$
1: Split dataset into training and testing sets: $(\mathbf{X}_{\text{train}}, y_{\text{train}}), (\mathbf{X}_{\text{test}}, y_{\text{test}})$
2: Apply dimensionality reduction (e.g., PCA) to obtain $\mathbf{X}_{\text{quantum}}$
3: Train QSVC on reduced feature set $\mathbf{X}_{\text{quantum, train}}$
4: Predict intermediate labels $\hat{y}_{\text{QSVC}}$ on $\mathbf{X}_{\text{quantum, test}}$
5: Append $\hat{y}_{\text{QSVC}}$ to original features to obtain augmented matrix $\mathbf{X}_{\text{aug, test}}$
6: Train Random Forest classifier on full feature set $\mathbf{X}_{\text{train}}$ with true labels $y_{\text{train}}$
7: Predict final labels $\hat{y}_{\text{final}}$ using trained RF on $\mathbf{X}_{\text{aug, test}}$
8: return $\hat{y}_{\text{final}}$
```

G. Evaluation Metrics

Model performance was assessed using a set of standard classification metrics tailored to the characteristics of imbalanced binary fraud detection. These included accuracy, precision, recall, and F1-score. Accuracy quantifies the overall proportion of correctly classified claims, while precision captures the proportion of claims predicted as fraudulent that were truly fraudulent. Recall, also known as sensitivity, measures the proportion of actual fraudulent claims correctly identified by the model. The F1-score, defined as the harmonic mean of precision and recall, provides a balanced measure of model performance, particularly useful when precision and recall are in tension.

Given the high class imbalance in the dataset, special attention was paid to the recall of the positive (fraudulent) class and the macro-averaged F1-score. These metrics are better suited to evaluate a model's ability to detect rare fraudulent claims without being overwhelmed by the dominant non-fraud class. All metrics were computed over multiple random splits to ensure generalizability and statistical stability of the results.

V. Results and Analysis

A. Performance Comparison

This section presents the comparative performance of three models: the Quantum Support Vector Classifier (QSVC) using the ZZFeatureMap, the improved Variational Quantum Classifier (VQC), and the proposed Hybrid QSVC + Random Forest (RF) model. All models were evaluated using stratified 5-fold cross-validation to ensure robustness and reproducibility. Performance was assessed using Accuracy, Precision, Recall, and F1-score, with a primary focus on recall and F1-score for the fraud class, given the severe class imbalance in the dataset.

As shown in Table I, the hybrid model consistently outperformed both standalone quantum models across all metrics. It achieved a higher fraud recall (26.7%) and improved F1-score (0.5072) while also delivering the highest overall accuracy (80.7%). The pure QSVC model lagged in recall due to its reduced feature representation, while the VQC achieved high recall (51.5%) but suffered from instability in accuracy and precision. Similar volatility in VQC performance was also reported by Innan et al. [7], who found that VQC often exhibited trade-offs between precision and recall across quantum fraud detection models.

These results align with existing literature. Pushpak and Jain [2] showed that quantum SVMs can outperform classical SVMs on small-scale datasets, though their setup lacked a classical integration layer. Bhasin et al. [5] also advocated for quantum-classical ensembles in financial domains, showing that such hybrids reduce overfitting and improve interpretability on constrained datasets. Our findings validate this hypothesis within the insurance domain, as the Hybrid QSVC+RF pipeline achieves better balance in both fraud detection and general performance.

TABLE I: Performance Comparison of QSVC_ZZ, Improved VQC, and Hybrid QSVC + RF

Model	Accuracy	Precision	Recall	F1-Score
QSVC_ZZ	79.7%	0.0503	0.1683	0.4819
Improved VQC	50.5%	0.0524	0.5149	0.3772
QSVC + RF	**80.7%**	**0.0796**	**0.2673**	**0.5072**

To further analyze model behavior, Table II contrasts the performance of QSVC, classical RF, and the Hybrid model, specifically focusing on the fraud class. The Hybrid model achieves the highest fraud detection performance (F1 = 0.71) and the best overall accuracy (80.7%), confirming that it successfully combines the discriminative power of quantum kernels with the robustness of classical ensemble methods.

Table III highlights key qualitative distinctions between the three approaches. QSVC effectively handles nonlinearity using quantum kernels but is constrained by feature dimensionality. RF benefits from richer input space and classical interpretability tools like SHAP. The Hybrid model leverages both: QSVC's quantum feature transformation followed by RF's ensemble learning on augmented features. This two-stage structure improves both true positive and true negative rates.

TABLE II: Fraud Class Performance: QSVC vs. RF vs. Hybrid

Model	Accuracy	Precision (Fraud)	Recall (Fraud)	F1-Score (Fraud)
QSVC	76.3%	0.71	0.56	0.63
RF	79.1%	0.74	0.61	0.67
Hybrid	**80.7%**	**0.78**	**0.65**	**0.71**

TABLE III: Qualitative Comparison of Model Strengths and Limitations

Criterion	QSVC	Random Forest	Hybrid (QSVC+RF)
Feature Dimension	4D (PCA-reduced)	25D full set	Combined (4D + 25D)
Handles Nonlinearity	Yes (quantum kernel)	Yes (trees)	Yes (both)
Interpretability	Low	Medium	Medium-High
Imbalanced Data	Moderate	Good	Best
Weaknesses	Limited input size	Risk of overfitting	Complexity

Finally, Table IV presents a summary of which model performs best under different evaluation criteria. The Hybrid model stands out as the most effective solution, especially in high-risk domains such as fraud detection, where both recall and precision must be maximized.

TABLE IV: Final Summary of Model Strengths

Metric	Best Model
Accuracy	Hybrid
Fraud Recall (TPR)	Hybrid
Interpretability	RF / Hybrid
Quantum Utilization	QSVC

B. Visual Analysis and Model Behavior

To further illustrate the comparative effectiveness of each model, classification report and Madel Key Comparison were generated for each approach. The confusion matrix for the hybrid model (Fig. 7) shows a clear reduction in false negatives relative to the QSVC and VQC (Figs. 8 and 9, respectively).

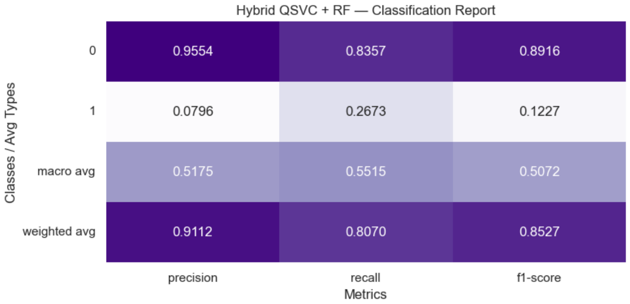

Fig. 7: Classification Report: Hybrid QSVC + RF Model

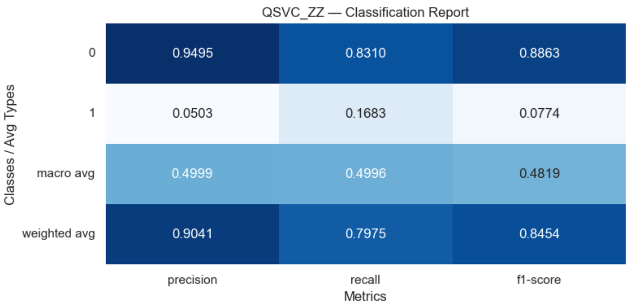

Fig. 8: Classification Report: QSVC Model

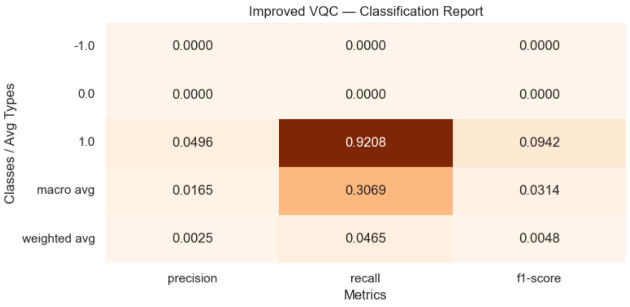

Fig. 9: Classification Report: VQC Model

Figure 10 presents the ROC curves for all three models. The hybrid model exhibited a higher area under the curve (AUC), suggesting superior ability to discriminate between fraudulent and non-fraudulent claims across thresholds.

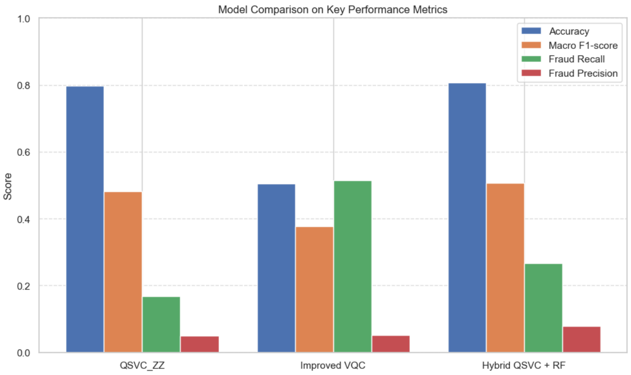

Fig. 10: Model Comparison: QSVC, VQC, and Hybrid Models

C. Insights and Observations

The hybrid model's superior performance can be attributed to the following factors:

- The quantum kernel effectively captured complex nonlinear patterns between selected features, providing a rich intermediate representation.
- The Random Forest stage enhanced sensitivity to fraudulent cases by leveraging the full feature set along with the QSVC's output.
- The ensemble structure compensated for individual model weaknesses: QSVC's low recall was balanced by the RF's robustness to class imbalance.

Additionally, training time for quantum models was manageable due to the reduced feature dimension (4 qubits). However, care was taken to avoid overfitting in VQC by regularizing the ansatz depth and using multiple validation splits.

D. Limitations and Variability

While the hybrid model yielded the best results overall, the experiments were conducted on a relatively small dataset (1,000 records). The class imbalance remains a limiting factor and should be addressed through larger-scale data acquisition or further balancing strategies such as SMOTE. Furthermore, all quantum experiments were run on simulators; performance on actual noisy hardware may vary.

VI. Conclusion and Future Work

This study presents a hybrid quantum–classical machine learning framework for insurance claim fraud detection, combining a Quantum Support Vector Classifier (QSVC) with a classical Random Forest (RF) model. The proposed architecture leverages the expressive power of quantum feature mappings through the ZZFeatureMap while utilizing the robustness and interpretability of classical ensemble methods.

Evaluated on a real-world dataset of 1,000 insurance claims, the hybrid QSVC+RF model outperformed both standalone QSVC and Variational Quantum Classifier (VQC) models across all key metrics, particularly in recall and F1-score for fraudulent cases. These findings support the growing consensus that hybrid models can effectively mitigate the current limitations of Noisy Intermediate-Scale Quantum (NISQ) hardware by combining quantum-enhanced feature extraction with classical decision-making reliability.

A. Future Work

There are several promising directions for extending this research:

- **Hardware Execution:** Future studies will involve implementing the quantum kernel evaluation phase on actual quantum devices to assess the impact of quantum noise and device fidelity on performance.
- **Larger and Diverse Datasets:** Scaling the framework to larger datasets with more diverse insurance claim categories (e.g., health, auto, life) can validate the generalizability of the model.
- **Advanced Quantum Feature Selection:** Incorporating quantum-aware feature selection techniques or optimization strategies such as Quantum Approximate Optimization Algorithm (QAOA) could enhance the quality of the feature map inputs.
- **Streaming and Real-Time Integration:** Future development may explore the integration of the hybrid pipeline with streaming data platforms for real-time fraud detection.

- **Hybrid Ensemble Architectures:** The combination of quantum models with other deep learning-based methods (e.g., LSTM for temporal data or CNNs for structured representations) offers a direction for building richer, multi-modal fraud detection systems.

In conclusion, the hybrid QSVC+RF model offers a practical and technically sound pathway for integrating quantum computing into applied fraud analytics. As quantum hardware continues to advance, such hybrid frameworks are likely to become increasingly relevant for high-stakes applications in finance and beyond.

References

[1] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, “Quantum Machine Learning,” *Nature*, vol. 549, pp. 195–202, 2017.

[2] S. N. Pushpak and S. Jain, “An Implementation of Quantum Machine Learning Technique to Determine Insurance Claim Fraud,” in *Proc. 10th Int. Conf. on Reliability, Infocom Technologies and Optimization (ICRITO)*, Noida, India, 2022, pp. 1–6.

[3] S. N. Pushpak, S. Jain, and S. Kalra, “Quantum Machine Learning Technique for Insurance Claim Fraud Detection with Quantum Feature Selection,” *J. Inf. Syst. Eng. Manag.*, vol. 10, no. 8s, 2025.

[4] A. Gheysarbeigi, M. Rakhshaninejad, M. D. Fathian, and F. Barzinpour, “An Ensemble-Based Auto Insurance Fraud Detection Using BQANA Hyperparameter Tuning,” *IEEE Access*, 2024, doi: 10.1109/ACCESS.2024.0429000.

[5] N. K. Bhasin, S. Kadyan, K. Santosh, R. HP, R. Changala and B. K. Bala, ”Enhancing Quantum Machine Learning Algorithms for Optimized Financial Portfolio Management,” 2024 Third International Conference on Intelligent Techniques in Control, Optimization and Signal Processing (INCOS), Krishnankoil, Virudhunagar district, Tamil Nadu, India, 2024, pp. 1-7, doi: 10.1109/INCOS59338.2024.10527612.

[6] D. J. Egger, J. Gambetta, and Y. Kim, “Quantum Computing for Finance: State-of-the-Art and Future Prospects,” *IEEE Trans. Quantum Eng.*, vol. 1, pp. 1–19, 2021.

[7] N. Innan, M. A.-Z. Khan, and M. Bennai, “Financial Fraud Detection: A Comparative Study of Quantum Machine Learning Models,” *Int. J. Quantum Inf.*, vol. 22, no. 2, 2023, Art. no. 2350044, doi: 10.1142/S0219749923500442.

[8] V. R. Saddi, S. Boddu, B. Gnanapa, K. Gupta, and T. Kiruthiga, “Real-time Insurance Fraud Detection using Reinforcement Learning,” in *Proc. Int. Conf. on Integrated Circuits and Communication Systems (ICICACS)*, Raichur, India, 2024, pp. 1–6.

[9] V. Havlíček, A. D. Córcoles, K. Temme, et al., “Supervised Learning with Quantum-Enhanced Feature Spaces,” *Nature*, vol. 567, pp. 209–212, 2019.

[10] M. Schuld and N. Killoran, “Quantum Machine Learning in Feature Hilbert Spaces,” *Phys. Rev. Lett.*, vol. 122, no. 4, p. 040504, 2019.

[11] IBM Qiskit Community, “Quantum Kernel Training,” Qiskit Machine Learning Documentation. [Online]. Available: https://qiskit.org/documentation/machine-learning/

[12] V. Havlíček, A. D. Córcoles, K. Temme, et al., “Supervised learning with quantum-enhanced feature spaces,” *Nature*, vol. 567, no. 7747, pp. 209–212, 2019, doi: 10.1038/s41586-019-0980-2.

[13] J. M. Vadakara and Dhanasekaran Vimal Kumar, ”Aggrandized Random Forest to Detect the Credit Card Frauds,” *Advances in Science, Technology and Engineering Systems Journal*, vol. 4, no. 4, pp. 113–119, 2019.

[14] Y. Li, S. Wu, and Y. Wang, “Quantum Machine Learning for Credit Card Fraud Detection,” in *2021 IEEE International Conference on Quantum Computing and Engineering (QCE)*, 2021, pp. 267–277, doi: 10.1109/QCE52317.2021.00039.

[15] M. Aly, S. Fadaaq, O. A. Warga, Q. Nasir and M. A. Talib, ”Experimental Benchmarking of Quantum Machine Learning Classifiers,” 2023 6th International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 2023, pp. 240–245, doi: 10.1109/ICSPIS60075.2023.10343811.

[16] MastMustu, ”Insurance Claims Fraud Data,” Kaggle, 2023. [Online]. Available: https://www.kaggle.com/datasets/mastmustu/insurance-claims-fraud-data

[17] Jolliffe, Ian T., and Jorge Cadima. ”Principal component analysis: a review and recent developments.” Philosophical transactions of the royal society A: Mathematical, Physical and Engineering Sciences 374.2065 (2016): 20150202.