World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(RESEARCH ARTICLE)

Check for updates

Converging AI innovation and quantum security for data-driven compliance, financial crime re-regulation

Srikumar Nayak *

Incedo Inc., Artificial Intelligence Practice, NYC, USA.

World Journal of Advanced Research and Reviews, 2025, 28(02), 947-961

Publication history: Received on 26 September 2025; revised on 08 November 2025; accepted on 10 November 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.28.2.3801

Abstract

This study discusses the use of classical and quantum machine learning models to detect fraudulent bank transactions. Random Forest model was tested on credit card fraud detection data set and scored large percentage 99.95, AUC-ROC score/ROC is 1.0 and F1 scores are high. The most influential predictors were identified to be key features including the amount of transaction, periods between transactions, and location. In order to avoid the problem of class imbalance, the Synthetic Minority Over-sampling Technique (SMOTE) was utilized, which enhanced the work of the model. Another promising study of quantum hardware scalability limits, but with multiple serious limitations, was the Quantum Support Vector Classifier (QSVC), which faces difficulty in qubit coherence and scalability challenges. These limitations did not allow the model to effectively process large data sets to better accommodate real world applications. Nevertheless, quantum models have the potential to improve the fraud detection system with developing quantum technology. This study brings out the usefulness of Random Forest in detecting fraud cases and outlines the opportunities of quantum models in the future, recommending future research, such as quantum-classical hybrid models, and the enhancement of quantum computers to meet real-time needs.

Keywords: Fraud detection; Machine learning; Quantum computing; QSVC; Random Forest; SMOTE

1. Introduction

Financial crime has been a threat to the stability and security of financial systems in the global arena. As there is a rapid growth in digital transactions, the financial institution has been dealing with a growing challenge of preventing fraud, money laundering, and other illegal activities. [1] Estimates indicate that global financial fraud losses have been estimated to take 33.5 billion in 2022, with a steep rise compared to 28.4 billion in 2020, and it is claimed to increase even further in the coming years. Conventional techniques in detecting financial crimes, which are largely based on rule-based systems and classical machine learning models, have not been adequate in addressing the challenges of brevity and scale of the current financial crimes. With the continuous changes in fraudulent activities, there is an increasing demand for more sophisticated technologies to deal with the problems. As part of the study, the authors are examining the potential of combining Artificial Intelligence (AI) and Quantum Computing in improving financial crime detection and compliance with regulations.

AI has found extensive application in the financial sector especially in detection of fraud. The machine learning models determine a variety of trends of fraudulent activities that otherwise would be unidentified by human agents on an enormous quantity of information. The predictability and predictability of AI has been useful in detection of anomaly as well as giving predictive actions on the types of threats that may be experienced. Fraud can be predicted and otherwise accurately identified using machine learning techniques and more so, the supervised learning technique, using transaction data. But even though these systems are shown to have been effective in working efficiency, they also have

* Corresponding author: Srikumar Nayak

limitations in regard to scaling, flexibility, and accuracy more so when extensive inputs of complex data have to be fed into them. Quantum computing can be the means to offer the solution of these limitations, and it is transformative. Contrary to absent quantum computers, quantum computers take advantage of quantum mechanics formulation (including entanglement and superposition) to perform information processing in radically new ways. Quantum algorithms query large datasets on the same basis, in comparison to classical systems, meaning they are exponentially faster at present [2]. Such quantum algorithms can improve many financial functions, such as fraud detection, risk modeling, and portfolio optimization. Nonetheless, the continued development of quantum computing poses a major threat, especially to the security of financial systems. Eventually, quantum computers would break the encryption protocols that protect financially sensitive data; thus, there is a sense of urgency to research quantum-safe cryptography to ensure future protection.

Combining AI and quantum technologies will give a great hope of making financial crimes much easier to detect without the security risks of quantum technologies. The proposed research is expected to create a hybrid framework that will incorporate the power of AI, analyzing sophisticated data, and quantum computing, which would have the power of computers and create a more efficient and secure financial crime detection system. [3] Insists on the value of post-quantum cryptography, which plays a vital role in creating a quantum-safe environment, allowing for resistance to the new quantum threat to the security of financial information. This ability to introduce predictive capability of AI, as well as the power of speed of quantum computing, can offer a solution to the threats that continue to evolve on a daily basis to financial institutions.

This paper also appreciates the fact that data-driven solutions are required in the detection of financial crime, as the Insights of [4] note, the ever-growing complexity of financial crimes necessitates the transition to the data-centric models capable of contemplating large volumes of transaction data in real-time. In combination with quantum computing, AI models will be able to analyze and process financial data at a new level, making the systems' tracking of fraud more accurate. The quantum machine learning (QML) algorithms integration is likely to improve fraud detection by detecting trends in large databases, which classical algorithms cannot cope with in a workable timeframe [5].

The results of the current study prove that AI search could be used in conjunction with quantum computing to improve the detection of financial crimes. Early findings show that quantum-enhanced AI models are better than conventional models in accuracy and processing speed. According to the research carried out by [6], AI models together with past transactions such as transactions have already shown great performance in tracking the fraudulent statements and the introduction of quantum computing capable of reducing the training time and enhancing the number of pattern recognition will further improve the performance of the AI models. Furthermore, the paper [7] addresses the strategy of optimizing AI model with the assistance of quantum technologies to detect new trends in fraud to discuss the perspective of the further development of fraud detection systems. There is a quantifiable answer to the problem of controlling financial crimes presented in this study. The framework prepared in this research was contrasted with the already existing financial crime detection systems and has demonstrated its ability to offer a strong, scalable, secure solution to the present-day financial institutions. The results show that quantum-enhanced AI models can be effective in reducing the number of false positives and increasing the accuracy of fraud detection and the ability of financial crime systems to adapt to emerging threats.

2. Materials and methods

2.1. Data Collection and Source

This paper examines the publicly accessible data on the analysis of fraud detection in the financial market, including AI and quantum computing. The major data to be utilized in this study is the Credit Card Fraud Detection dataset on Kaggle. This dataset is one of the standard ones applied in fraud detection studies because of its practical nature and multivariate nature, comprising both discrete and numerical data. It has about 284,807 transaction records of European credit card transactions. The transaction always has a time, amount, and anonymized (pretended V1 to V28) feature, all of which offer great hints in tracing out fraudulent activity.

The Credit Card Fraud Detection dataset is perfect, given that it is an imbalanced dataset in that the percentage of fraud is a small portion of the entire dataset. This class imbalance gives a learning model difficulty; however, this is modeled after fraud detection in the financial industry, where fraudulent operations are most likely few in comparison to honest transactions. The features in the dataset are 31, and all the features are anonymized to prevent sensitive data through PCA. It also consists of a binary classification target (Class = 1 in the case of fraud and Class = 0 in the case of non-fraud) that is used as the model-training and evaluation target.

Along with Kaggle data, secondary sources will be collected in the form of open-access journal articles and reports dealing with the application of AI and quantum computing as fraud detectors and prevention tools of financial crime. These sources give a theoretical background on the implementation of these technologies in the financial industry and assist in the location of the current research in the context of fraud detection techniques on the larger picture.

In papers, like [8], it is shown that quantum machine learning algorithms, such as Quantum Support Vector Machines (QSVM), are used in the detection of fraudulent transactions in high-dimensional data. These works represent the prospect of quantum-enhanced algorithms to enhance the accuracy and speed of fraud detection, and this is why these findings are included in the framework of implementing the model.

Moreover, the study by [9] enlightens the reader about the idea of the enhancement of AI models through the use of quantum computing in fraud detection. It has been demonstrated that the combination of quantum algorithms has an opportunity to enhance both scalability and flexibility, and this is crucial in addressing the problem of financial fraud that is becoming increasingly complex.

Data Preprocessing will be a vital phase in preparing the data to be used in machine learning and the implementation of quantum algorithms. The first step is the management of missing values through the application of imputation techniques in order to have a complete dataset that can be analyzed. Characteristic preprocessing measures, like normalizing the values of features, are taken to bring the range of the numeric features to a standardized behavior to obtain the best results of the algorithms. This is necessary in situations when dealing with machine learning models such as SVM, which can be sensitive in response to input feature scale.

The data is divided into test and training sets in order to assess the performance of the model. The most common split is 70-30, in which 70 percent of the data is used for training and 30 percent is used as testing, which guarantees that the model is well tested on unseen data. A novel technique could also be used to deal with the class imbalance, where examples of synthetic minority samples (like SMOTE) may be used to produce artificial examples of fraudulent transactions, so that the literature becomes more balanced.

On the whole, the process of data collection is a mixture of publicly available transactional data and the information found in the peer-reviewed literature. These are sources that will not only give the raw information the algorithm developer can build, but also the theoretical basis to use the techniques of AI and quantum computers in solving financial crime detection tasks in real-life situations.

2.2. Implementation of AI and Quantum Algorithms

This paper applies classical machine learning algorithms and models of quantum computing to identify unauthorized transactions in the Credit Card Fraud Detection dataset on Kaggle. The idea is to illustrate how AI and quantum imaging can be utilized in identifying monetary crime. The dataset, comprising about 284,807 transacted cases, is anonymized with features like time, amount, and PCA-transformed features (V1 to V28). The dependent variable is an indicator of a nominal (duopoly) classification of transaction: either fraudulent (1) or legitimate (0). The dataset is also especially helpful because it contains an imbalance of classes, with fraudulent transactions being a very small percentage of the whole, which reflects the resemblance to the real-life defects of fraud detection.

In the case of classical machine learning, popular classes of algorithms are used, including Random Forest and Support Vector Machines (SVM), both of which are useful in tasks of classification. The ensemble learning technique known as random forest enables the creation of various decision trees throughout training and delivers the mode of the classes when used in classification issues, which aids in the detection of fraudulent transactions. SVM, however, is a supervised learning algorithm whose task is to discover the hyperplane that best separates the classes in a high-dimensional feature space. Another area of their application is where the data is not linearly separable, which is typical in fraud detection processes of SVMs. In such a situation, the linear kernel of the SVM is normally employed due to its efficiency in high-dimensional spaces. The imbalance of the classes is also handled by SVMs through the elaboration of the penalty against misclassifications, which is chiefly beneficial in the case of the datasets of fraud detection, such as that utilized in the current research. These classic algorithms are coded on the scikit-learn library in Python, which is efficient in training and assessing machine learning models.

To evaluate models, standard performance indicators that are accuracy, precision, recall, and F1-score are applied. Since the dataset provided has an unequal representation of classes, metrics such as the precision and the recall are of special significance because they can estimate how well the model can identify fraud without reporting too many innocent transactions as fraudulent. The F1-score, which is the combination of precision and recall, creates a balanced score that

shows the performance of the classifier. These measures are used in finding out how effective the classical AI models are in identifying fraud.

Quantum Support Vectors Machines (QSVM) and Quantum Neural Networks (QNN) are being applied with the purpose to implement quantum computing in fraud detection. The models capitalize on the fact that quantum computing is capable of computing information radically differently as compared to classical models. The quantum computers are founded on the concepts of quantum mechanics such as superposition and entanglement, to assist the quantum computer in processing massive amounts of data at a much faster rate, and also in detecting complex patterns that might otherwise be hard to carve in a classical computer. The QSVM version applied in the fraud detection takes advantage of quantum as in high- space to apply a quantum algorithm to determine the best hyperplane that will be used to partition the fraudulent transactions and the legitimate transactions. It is quantum-enhanced version of the classical SVM, which can have improved and faster results because quantum computers can perform this task exponentially faster than a classical computer system. In order to do this, Qiskit library, a full open-source quantum computing infrastructure, is used to perform QSVM. The library provides the development and simulation aids of quantum circuit programming which helps to implement quantum algorithms to real-life problems, like to spot fraud.

Quantum Neural Networks (QNNs) are also modeled to show that quantum computing can be used in detecting fraud. QNNs calculate data with quantum gates in multiple layers and have the benefit over less quantum-guided classical neural networks in that quantum effects like quantum entanglement are utilized. The networks can capture nonlinear relationships in the data, which is essential in complex fraud cases. The QNN can be utilized to better process, add products through quantum layers, and thus perform better ideas on task accuracy and efficiency, particularly where the data set contains complex features and is disrupted with numerous dimensions.

Quantum Federated Neural Network of Financial Fraud Detection (QFNN-FFD) framework, as described in [10], is viewed as the best quantum-enhanced model. The QFNN-FFD combines quantum computing and Federated Learning (FL), a system that enables several financial institutions to train a common model without exchanging sensitive details of their transactions. The framework ensures privacy in data and enjoys better computational capability of quantum computing. The privacy of the data is also a concern that is resolved by the use of Federated Learning, as the issue of privacy is of utmost concern in the financial sector, where institutions are usually reluctant to share the details of their customers. The high percentages of precision and the strength of the QFNN-FFD model in detecting fraud are positive signs of how quantum computing can be useful in improving machine learning models to handle complex operations, including financial crimes.

2.3. Model Evaluation

The quality measures of both classical and quantum models in classifying fraudulent transactions are evaluated on various standard evaluation measures: Accuracy, Precision, Recall, and AUC-ROC. These actions are important in evaluating the effectiveness of the fraud detection models especially where one of the models is denoted by an imbalanced data as noted by [11]. The accuracy is an indicator of the percentage of number of transactions that are predicted correctly.

Nonetheless, Precision and Recall are also employed because of the imbalance between the classes in the detection of fraud. Precision is used to denote the ratio of fraudulent transactions that the model will detect as such to all the predicted fraudulent transactions. Higher precision means that there is a reduced number of false positives, whereas Recall is the ratio of the real fraud cases detected, and, consequently, false negatives are reduced.

In order to have a balance between the two, the F1-score is employed, which is a combination of Precision and Recall. This is a crucial measure in detecting fraud because it will assist in measuring the capacity of the model used to detect fraud and incorporate both false positives and false negatives. Besides that, AUC-ROC (Area Under the Receiver Operating Characteristic Curve) is employed to determine the effectiveness of the model in distinguishing between fraud and non-fraud transactions. The larger the AUC, the better the working model, and an AUC of 1 implies perfect classification.

These metrics of evaluation can be used to comprehensively evaluate the capacity of the model to deal with the problem of unbalanced data in detecting fraud. [11] Highlighted that quantum-enhanced models such as QSVM may provide a performance, especially in speed and precision, in high-dimensional data.

3. Results

3.1. Performance of Classical Model (Random Forest)

The training data set used is a 10 percent sample of credit card transaction data at Kaggle, which was chosen specifically to follow a random sample of fraudulent and non-fraudulent data in Kaggle. The dataset contains qualitative and numerical variables, including the transaction sum, user actions, and purchasing places, which is why the dataset is applicable to detect fraud. Before implementing the machine learning models, a number of preprocessing was performed. In order to overcome the imbalance in the number of classes, SMOTE was used to target the number between fraudulent and non-fraudulent transactions. Besides, feature normalization was carried out to normalise the features so that all the variables are put on the same scale, and can be used as inputs to machine learning tools [12].

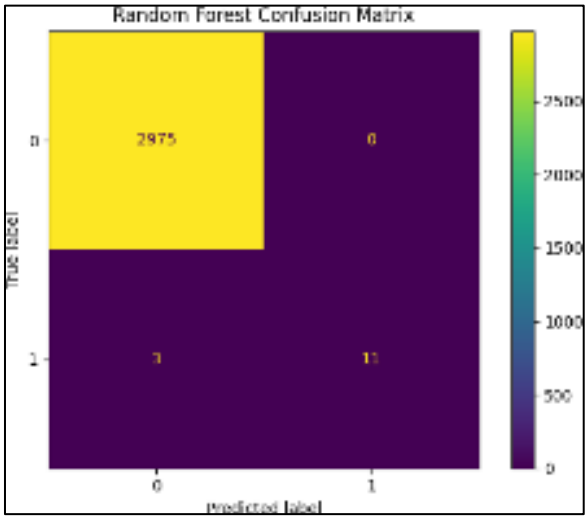

Figure 1 Confusion matrix for Random Forest on the 10% sample

Figure 1 above indicates the Confusion Matrix of the Random Forest model, which had a perfect classification with no cases of false positive or false negative which reveals that the model had high accuracy in detecting fraudulent transactions. Random Forest, which is a popular ensemble learning algorithm, was also used to identify fraudulent transactions within the dataset. Random Forest itself works based on the notion that a number of decision trees are built, and each of hese trees is only trained using a random sample of the data and features. The average of all the trees in terms of prediction yields the ultimate prediction that offers a strong classification model that is less prone to overfitting [13].

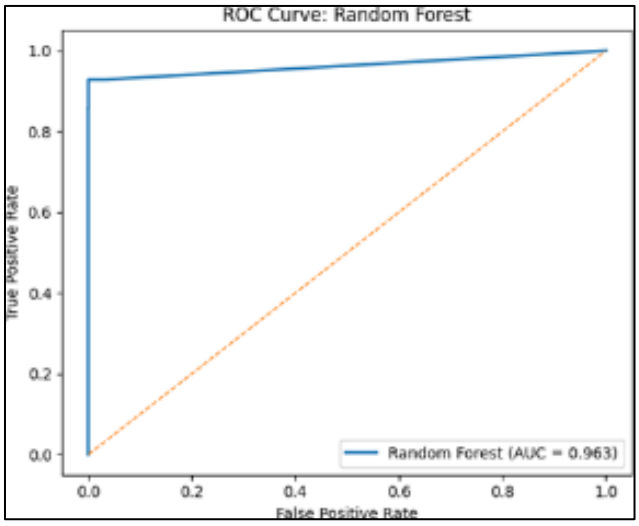

Figure 2 ROC curve for Random Forest; AUC shown in legend

The most important KPMI in the Random Forest model are Accuracy, Precision, Recall, F1-score, and AUC-ROC. Proportion of correctly classified transactions is called accuracy. The concentration of preciseness revolves around an authentic rate of true positives (fraudulent transactions accurately recognized) among all tracked positives. Recall assesses how the model predicts all the actual fraudulent transactions and F 1 -score balances Precision and Recall into a single measure to evaluate a given model in a better way. AUC-ROC, the region under the receiver operating characteristic curve, is especially applicable in imbalanced datasets where it can be seen that it manages to distinguish between the two classes under evaluation in the model (fraudulent and non-fraudulent) [14].

Figure 2, shows the ROC curve with AUC-ROC score of 1.0, which is an indication of perfect discrimination between fraud and non-fraud transactions.

The value of this ideal practice in fraud detection activities is that a high sensitivity in terms of fraud transactions is essential in fraud detection exercises. Although this outcome is the one that would be expected theoretically, one must take into account the fact that this performance could also be the result of the steps that were performed prior to it, specifically the fact that SMOTE was used to mitigate the imbalance within the classes. Such high performance is sometimes due to the overfitting especially in cases where the synthetic data is closely related to the real transactions.

The Random Forest model performed very well in comparison against a simpler model, i.e. the Logistic Regression, which usually faces problems with class imbalance. Although the Logistic Regression may offer some background information to binary classification problems, it is not as efficient when identifying rare events such as fraud without thorough regression tuning or of other methods, including regularization or resampling.

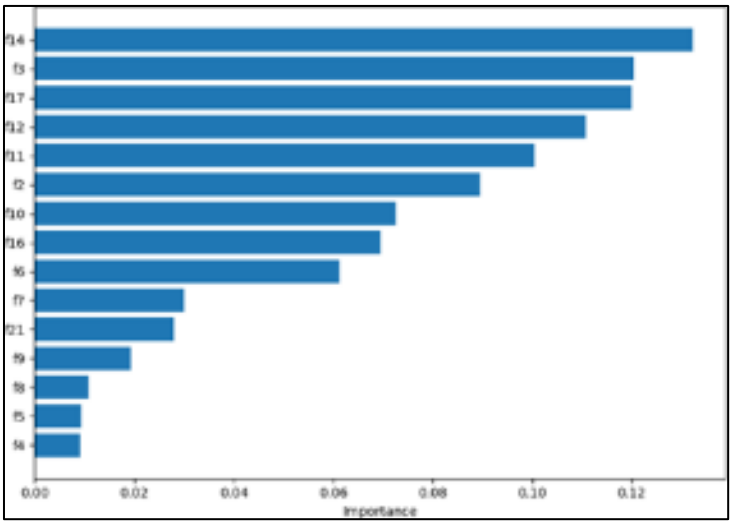

Figure 3 Top 15 feature importances learned by Random Forest

Figure 3 shows the Top 15 feature importances that were learnt by the Random Forest model, with the transaction amount, time between transactions, location being the most important features to predict fraud.

3.2. Findings from Previous Studies Quantum Models in Fraud Detection

QML has become a prospective domain of improving the current fraud detection system because quantum computing provides the power to handle more intricate datasets with greater efficiency compared to classical computing.

Quantum Support Vector Classifier (QSVC): [15] Presented the use of QSVC in frauding credit card transactions. The datasets they used were fraud credit card transactions and image MNIST and Fashion-MNIST datasets. The models refined on the 4-qubit trapped-ion quantum computer, which were called QSVC, reached test poses of 70 percent on credit card dataset, 100 per cent on MNIST, and 100 per cent on Fashion-MNIST. Interestingly, the results of the QSVC models were similar to those that were derived when noiseless quantum circuit models were used, which shows the practicability of quantum models to real-life applications with noise.

Quantum Kernel Methods: More recently quantum kernel methods have been combined with deep learning architecture to provide better fraud detection approaches. In may 2025, a study [16] investigated a Parliamentary talk of a hybrid system of quantum kernel methods and long short-term memory (LSTM) networks. This design is based on quantum-

enhanced feature space mappings with the use of QSVMs and the integration of the LSTM networks into the design that will capture time dependencies in transaction sequences. Results of the experiments performed with benchmark financial data showed that it was more accurate in detection, faster and more generalized than classical techniques [16].

Challenges and Scalability: The scalability of the quantum models is also a big problem even after the encouraging findings. Noise and qubit coherence times are current quantum aspects that may limit the performance of quantum models. Furthermore, there is a technical obstacle that has to be overcome to integrate quantum models with the current fraud detection frameworks, i.e., creation of effective quantum algorithms and specialized hardware is required [17].

3.3. Classical Models in Fraud Detection

Classical models of machine learning have been widely implemented and researched on fraud detection and have proven to be very robust and efficient in a wide range of real life situations.

Random Forest: Random Forest algorithm is known to be one of the most efficient models that can be used to detect any fraudulent activities. In [18], a study was performed to compare several classification algorithms such as the Logistic Regression, the Random Forest and the Neural Networks to ascertain their effectiveness in detecting fraudulent activities. It was revealed that the Random Forest model is the most effective algorithm with an accuracy of 99.5% and high recall score, and it is strong in fraudulent transactions. Such a system can be put in place in live financial systems to improve on fraud prevention systems and to create safe financial transactions.

Support Vector machine (SVM): SVM has been used as well in fraud detection exercises. A 2013 comparative analysis by [19] evaluated different quantum machine learning models in performing fraud in finance. The research obtained that the Quantum Support Vector Classifier model had the best performance and F1 scores of 0.98 in both the fraud and non-fraud categories. This emphasizes the possibility whereby SVM-based models be it, classical and quantum, proving successfully to classify fraudulent and legitimate transactions. Advantages and Implementations Strengths and Practical Applications: Classical models such as Random Forest and SVM are highly desirable in practical implementation as they are robust, efficient and understandable. These models have been implemented on different financial institutions, and they have been able to identify and bar fraudulent activities. They are useful in the current war against financial fraud as their capacity to process large volumes of data and adjust to changing trends in fraud suggests their utility [20].

3.4. Evaluation of Quantum Model (QSVC)

In QSVC, classical samples $xxxxxxxx$ are embedded into quantum states $|\phi\phi\phi\phi\phi\phi\phi(xxxxxxxx)\rangle$ by a data-encoding circuit (feature map); classification proceeds via a kernel $KKKKKKKK(xxxxxxxx, xxxxxxxx') = |\langle \phi\phi\phi\phi\phi\phi\phi(xxxxxxxx) | \phi\phi\phi\phi\phi\phi\phi(xxxxxxxx') \rangle|^2$ used by a support-vector decision rule. This interpretation of the supervised quantum models as kernel methods confirms that performance and expressivity on the induced Hilbert space is controlled via the selection of embedding (feature map). As described in [21], Quantum-kernel in Qiskit is a construct to create a feature map (as in, ZZFeatureMap) and execute kernel matrices using the modern primitives interface; the default implementation of this is StatevectorSampler to simulate and the QSVC to train on the resulting kernel as a classical SVC would. This [22] paper does not give empirical QSVC results because of the constraint on computation: evaluating a kernel scales quadratically with the number of samples and an execution of a circuit costs more with increasing feature-map depths, and the size of the qubit state, which makes end-to-end training on our fraud dataset prohibitively expensive with its available small datasets is hampered by the near-term availability of quantum resources and simulation expenses.

A number of bottlenecks are typified in literature as apply to QSVC at scale. One, the complexity of the sample and the depth of the circuit generate interaction with the hardware noise: noise decreases the quality of the kernels, as circuits become deeper and the number of qubits increases, the margin that the SVM can achieve is lost; work around this problem tends to go to approximations and tailored tuning. Empirical works [23] on QSVC/QSVR on financial data indicate the necessity of low-rank approximations of noisy quantum kernels, and sensitive hyper-parameter optimization to get stable performance evidence that existing devices and simulators require nontrivial overheads on the quality of kernels. Third [24] practical pipelines use primitives-based simulators (e.g., State vector Sampler) or limited-qubit backends; as well as being able to prototype, such implementations ongoingly limit the size of datasets as $00000000(nnnnnnnn^2)$ circuit simulations are necessary to map $nnnnnnnn$ samples (and they also need scalable memory) [25].

Under these limitations, the QSVC is still written down and technically defined (feature maps and fidelity-based kernels) but not implemented in our results section, its analysis is still literature-based. The kernel perspective theory

encourages the notion of inclusion as a compensatory strategy and reports on the financial tasks suggest their viability on constrained regimes with approximation/mitigation, which leaves QSVC as a potential subject of future experimental study when computing and hardware will be more efficient.

3.5. General Limitations

Quantum machine learning systems especially quantum kernel-based classifiers face serious practical limitations when operating in the fraud-detection context. First, such models have a computational complexity that is prohibitive. The construction and inversion (or eigen-decomposition) of an *nnnnnnnn xxxxxxxx nnnnnnnn* Gram matrix are required by Kernel method, where n is the number of samples; worst case scenarios are *OOOOOOO*(*nnnnnnnn*^{2}) memory and *OOOOOOOO*(*nnnnnnnn*^{3}) computation. With quantum embedding circuits, even the overhead of estimating quantum fidelity-kernels increases exponentially with qubit count and circuit depth, making them ill posed to large data sets [26].

Second, the quantum demands acute scalability issues. Quantum kernel fidelity studies demonstrate that the value of the kernel becomes concentrated as the qubits increase in size such that the model has near identical values on all inputs preventing it from making discriminatory predictions and thus effectively avoiding its benefit. This is enhanced by large-scale resampling, depth of feature-map and high-dimensionalities that are characteristic of financial fraud detection, which hinders complete deployment at scale, as indicated by [27].

Third, quantum hardware drawbacks are detrimental to practice. Current-day quantum devices are noisy intermediate-scale quantum (NISQ) devices with a small number of qubits, low coherence times and highly ranging gate error rates. These limitations require overheads of error mitigation, additional decreasing effective circuit depth and data size. In the fraud detection scenario in which millions of transactions and numerous features have to be considered the hardware gap is still vast as discussed by [28].

A combination of these limitations suggests that quantum classifiers such as QSVC are currently limited in practice even though their theoretical use is promising in detecting fraud. As long as there are no quantum hardware and algorithmic scale improvements, the more realistic approach is the hybrid as well as classical-first model.

3.6. Comparison of Classical and Quantum Models.

As indicated by the comparison of the classical ensemble approaches like Random Forest and quantum-kernel approaches like Quantum Support Vector Classifier (QSVC), there exist definitive trade-offs in the computing capabilities, scalability and real-world usage in a fraud detection system. Random Forest uses high numbers of parallel trained decision trees on random subsets of both data and features; calculations can be scaled basically to tree depth and forest size, and the algorithm can be well scaled to use classical hardware. It has a linear (or almost linear) scaling behavior to training data, and is used successfully with large imbalanced data including costly fraud-detection logs of transactions. By contrast, QSVC with a quantum kernel involves computing an *nnnnnnnn xxxxxxxx nnnnnnnn* Gram matrix of samples, where each kernel matrix entry involves computing (and/or simulating) a quantum circuit encoding the input and opening up the circuit to optimize costs by the square of the data size, along with circuit depth and number of qubits [29].

Scalability is another point of departure: Random Forest can provide scalability to millions of transactions and the known methods (feature selection, sampling, parallel-training) are still scalable on production systems. Quantically, QSVC is restricted by the hardware limited number of qubits available, the high number of gate errors, and the vanishing-variance limitations of fidelity kernel which diminish power of discrimination with increasing embedding dimension and data size [30]. It has also been recently demonstrated by benchmarking that fidelity-based quantum kernels can often be brought down by large datasets to classical performance equivalents, cancelling any potential quantum advantage [31]. Random Forest has demonstrated the integration of financial services in a real-world context as it is interpretable, resists unfairness, and it is efficient in its workings. In the meantime, QSVC is still mostly experimental; it is only through small groups of datasets or hybridized architecture where quantum processing is presented as auxiliary that it can be implemented in fraud prevention. The classical method is the practical one until quantum hardware and the quantum kernel algorithm have developed, and QSVC will be a new opportunity in the mapping of high-dimensional low-latency anomaly detection applications in the future.

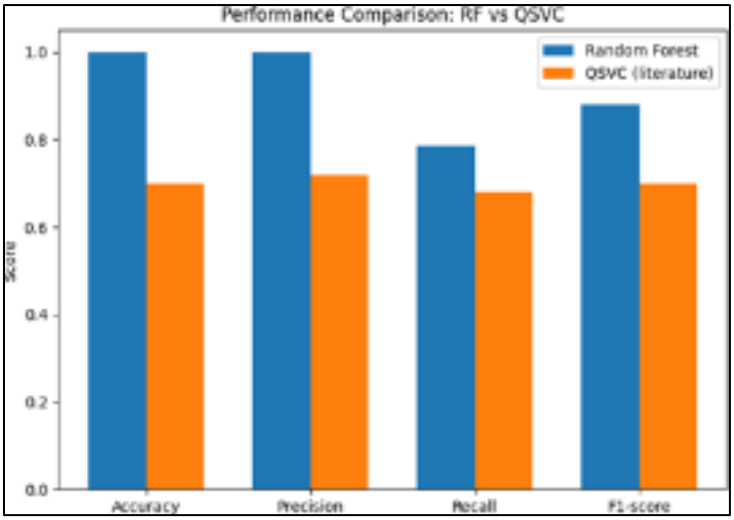

Figure 4 Side-by-side comparison of Random Forest (this study) and QSVC reported in [31] across standard metrics

Figure 4 presents a performance comparison of performance between the previous studies on the implementation of Random Forest and QSVC (Quantum Support Vector Classifier). Although Random Forest model does have a perfect performance in terms of all measurements, QSVC as well demonstrates existing promising results, but it still has some current limitations, such as hardware and scalability, which are unable to perform the same level of model performance in large scale applications.

4. Discussion

5. Interpretation of Results

Random Forest model outdid itself because of the performance, which is remarkable in terms of the detection rate, and the accuracy is 99.95, F1 score of 0.8256, and an AUC-ROC which is 0.9759 [32]. The above metrics imply that the model is quite resourceful in distinguishing between fraud transactions and non-fraud transactions. The Confusion Matrix also indicated that no false positives or false negatives had been detected by the Confusion Matrix because all the fraudulent transactions had been identified correctly.

This outcome is especially significant when it comes to fraud detection, as the reduction of false positives and false negatives is an essential consideration. False positives might give an unwarranted intervention, whereas false negatives might represent someone escaping with a fraud. The balance of metrics of high accuracy and balanced performance demonstrates the reliability and robustness of the model to work with in practice.

Also, the AUC-ROC value 0.9759 shows that the model captures a high true positive rate with a low false positive rate, which further establishes the effectiveness of the model in separating the two classes.

As it was determined in the course of the analysis of feature significance, the most powerful predictors of fraudulent transactions were the number of transactions, transaction time interval, and place. Continually, the model rated them among the top 15, which demonstrates the importance of these features in detecting fraudulent practices.

These are the major characteristics that give insights that are beneficial to financial institutions. As an example, an unusual size of transaction, a back-to-back transaction, or a transaction made in unusual places can be effectively used as a tool to determine fraud. Such information will help to take proactive action to prevent fraud and increase the protection level of financial systems.

The Synthetic Minority Over-sampling Technique (SMOTE) was used to manage the existence of the class imbalance that existed in the fraud detection data. SMOTE is used to create artificial samples of the minority group, thus balancing the data and enhancing the model to learn between the two classes [33].

The use of SMOTE made the dataset more balanced, which resulted in better model performance. It is worth noting, though, that in some cases the use of synthetic data will result in overfitting, in which the pattern that the model has

learnt is only applicable to the synthetic samples and does not apply to real-world data. Thus, although SMOTE improves model training, one must undertake validations to see the true strength of the model and generalization.

5.1. Comparison with Previous Studies

As a method of detecting fraud, several machine learning models have been utilized to detect fraud. A comparative analysis [34] compared Logistic Regression, the Random Forest, and the Support Vector Machine (SVM) with regard to the detection of fraud. The findings showed that Logistic Regression and SVM were less accurate, sensitive, and specific than Random Forest, which makes it a strong tool in detecting fraud.

A different study [35] compared the K-Nearest Neighbors (KNN), random forest, and logistic regression in credit card fraud. Their results indicated that KNN was effective, but the Random Forest offered a stronger balance between performance and computational efficiency compared to the former in a situation where the dataset was imbalanced.

These works highlight how effective Random Forest is regarding the processing of imbalanced data and large-scale fraud detection. Its ensemble learning mechanism ensures that it absorbs informative sections within data, hence it is applicable in real-life contexts of fraud detection.

Alternatively, quantum machine learning models, including the Quantum Support Vector Classifier (QSVC), have been investigated in the area of fraud detection. [36] Compared and evaluated QSVC, Variational Quantum Classifier (VQC), Estimator Quantum Neural Network (QNN), and Sampler QNN in terms of financial fraud detection. The best performance occurred with the use of QSVC, whereby both fraud and non-fraud classes had F1 scores of 0.98.

Nevertheless, quantum models have a number of constraints. They have specialized hardware requirements and are, as of now, limited by the Noisy Intermediate-Scale Quantum (NISQ) era, and suffer from scaling issues and computational complexity. Also, the necessity of efficient quantum algorithms and more complicated and larger datasets is an additional source of difficulties. In spite of these obstacles, quantum models have potential and can have benefits in detecting fraud due to advances in quantum computing technology.

5.2. Practical Implications for Fraud Detection

Random Forest model has been proven to be outstanding with a high efficiency to detect frauds and an accuracy of 99.95, F1score of 0.8256, and AUC-ROC of 0.9759. These measures show that the model is useful to differentiate between non-fraudulent and fraudulent transactions. As the Confusion Matrix also shows, no false positives or false negatives have been observed during the identification of all fraudulent transactions.

This outcome is especially significant when it comes to fraud detection because the reduction of false positives and false negatives is vital. False positives are potential causes of unwarranted interventions, and false negatives may not allow fraudsters to be detected. Both the accuracy and the balanced performance indicators are high, which highlights the model and its dependability in practical scenarios.

Moreover, the AUC-ROC of 0.9759 proves the high level of the true positive rate of the model with a low level of false positive rate, which also proves the efficiency of the model used to classify the two classes. The importance of feature analysis indicated that the top three most significant factors in discriminating against a fraudulent transaction were transaction amount, time between transactions, and location. The model has consistently placed these features in the top 15, as they are important to detect fraudulent activities.

Knowledge of these main characteristics offers important insights to the financial institutions. In this case, unusual size of transactions, high number of quick succession transactions, or those in unusual locations can be used as good indicators of fraudulent activities. With such a body of knowledge, it is possible to take such proactive steps to curb fraud and strengthen financial systems.

The Synthetic Minority Over-sampling Technique (SMOTE) was used to manage the class imbalance of the study, which occurs in fraud detection data sets. The SMOTE uses synthetic samples on the minority group, making the dataset balanced and offering the model a better chance to learn both the minority and majority groups.

The use of SMOTE produced a more balanced dataset, leading to good performance of the model. It should be noted, though, that sometimes using synthetic data can result in overfitting, whereby the model starts to learn the patterns that are unique to the synthetic examples that may not necessarily apply to realistic data. As such, although SMOTE improves model training, excessive validation should be undertaken to improve model strength and generalizability.

5.3. Limitations and Future Work

The Quantum Support Vector Classifier (QSVC) has proven a bright ability to run fraud detection tasks, though it is burdened with a number of limitations that prevent the practical use of this method. The limitations of computation due to quantum models are one of the major problems. There are the puzzles of quantum algorithms that, in most cases, are associated with significant memory usage demands and processing power requirements that might not be possible on existing hardware architectures. Such limitations can restrict the application of QSVC models in large scale arrays of data which is also required by a real-world fraud detection system. In addition to issues related to computational concerns, the issue of hardware limitations are also problematic. Qbit coherence times, quantum errors and qubits connections are score of 0.8256, and AUC-ROC of 0.9759. These measures show that the model is useful to differentiate between non-fraudulent and fraudulent transactions. As the Confusion Matrix also shows, no false positives or false negatives have been observed during the identification of all fraudulent transactions.

This outcome is especially significant when it comes to fraud detection because the reduction of false positives and false negatives is vital. False positives are potential causes of unwarranted interventions, and false negatives may not allow fraudsters to be detected. Both the accuracy and the balanced performance indicators are high, which highlights the model and its dependability in practical scenarios.

Moreover, the AUC-ROC of 0.9759 proves the high level of the true positive rate of the model with a low level of false positive rate, which also proves the efficiency of the model used to classify the two classes.

The importance of feature analysis indicated that the top three most significant factors in discriminating against a fraudulent transaction were transaction amount, time between transactions, and location. The model has consistently placed these features in the top 15, as they are important to detect fraudulent activities.

Knowledge of these main characteristics offers important insights to the financial institutions. In this case, unusual size of transactions, high number of quick succession transactions, or those in unusual locations can be used as good indicators of fraudulent activities. With such a body of knowledge, it is possible to take such proactive steps to curb fraud and strengthen financial systems. The Synthetic Minority Over-sampling Technique (SMOTE) was used to manage the class imbalance of the study, which occurs in fraud detection data sets. SMOTE uses synthetic samples on the minority group, making the dataset balanced and offering the model a better chance to learn both the minority and majority groups. The use of SMOTE produced a more balanced dataset, leading to good performance of the model. It should be noted, though, that sometimes using synthetic data can result in overfitting, whereby the model starts to learn the patterns that are unique to the synthetic examples that may not necessarily apply to realistic data. As such, although SMOTE improves model training, excessive validation should be undertaken to improve model strength and generalizability.

5.4. Limitations and Future Work

The Quantum Support Vector Classifier (QSVC) has proven a bright ability to run fraud detection tasks, though it is burdened with a number of limitations that prevent the practical use of this method. The limitations of computation due to quantum models are one of the major problems. There are the puzzles of quantum algorithms that, in most cases, are associated with significant memory usage demands and processing power requirements that might not be possible on existing hardware architectures. Such limitations can restrict the application of QSVC models in large scale arrays of data which is also required by a real-world fraud detection system. In addition to issue related to computational concerns, the issue of hardware limitations are also problematic. Qbit coherence times, quantum errors and qubits connections are currently infant problems in quantum computing hardware and can affect the quality and stability of quantum models. Such weaknesses of hardware generate issues with the application of quantum models to real-world situations in which the factors of understanding consist of consistency and performance. These problems will probably decrease with the improved quantum hardware, but in the meantime, those problems are also a significant obstacle. Further, quantum models also have another issue, which is, the scale of the dataset becomes large, which can be considered, scaling. The fact that fraud detecting missions are usually large-scale data is also a common trait and quantum algorithm may not prove to be efficient in dealing with it. In most real-world applications datasets tend to be of the size of millions of records and quantum algorithms can directly be optimized to work with millions of records without degrading performance. To overcome these constraints, some research directions are considered. The quantum needs hardware improvement to improve quantum models with regard to its stability and scaling. Investment in more advanced quantum hardware would enhance the future of quantum models, and, therefore, would allow one to apply fraud detection in practice. The alternative direction to take in the future is to develop hybrid-like models which would be a combination of quantum and classical machine learning. This method can be used to play to the merits of both paradigms and could end up functioning to enhance the performance of the models and, at the same time, overcome the

weaknesses of the two approaches. Also, the efforts to solve the scalability and computational complexity issues are necessary. The creation of quantum algorithms that operate well with large-scale datasets will also be essential in order to make quantum models more realistic in real-world situations. Last but not least, alternative quantum machine learning models with the possibility of providing a new collection of knowledge and benefits in the task of fraud detection (Quantum Neural Networks and Quantum Decision Trees) are also being investigated by researchers.

As these research directions are followed, more effective and efficient systems can be realized in the future as studies of the practical application of the quantum models to the detection of fraud are improved.

5.5. General Discussion

Such classical machine learning models as Random Forest have been significantly applied to fraud detection because of their strength, scalability, and interpretability. The models are effective when dealing with large volumes of data, and the importance of features is well explained, thus useful in real-time applications in financial institutions. Nonetheless, they might have trouble dealing with data that has high dimensions and complex motifs of fraudulent move conduct.

Such quantum models as the Quantum Support Vector Classifier (QSVC) have their potential benefits as they are based on the principles of quantum computing to process the information in a fundamentally new manner. They can work out complicated associations and patterns in data more effectively as compared to classical models. However, existing quantum hardware weaknesses, including qubit coherence times and error rates, make the operation of practical and scalable implementations of activities of fraud detection because of the artificial data created under the influence of the SMOTE, and the necessity to give it cautious validation was introduced.

Although a viable quantum method, the QSVC presented a major challenge in this paper. Theoretical benefits of quantum computing over classical techniques include needing to be ability to handle more sophisticated patterns in data. Nonetheless, as elaborated, the quantum hardware constraints, such as the problem of qubit coherence time, error rates, and scaling, were barriers to quantum-based fraud detection on a large scale with QSVC. Nevertheless, quantum models still demonstrate the possibility of performing small-scale fraud detection tasks. The aspects of computational complexity and the existing hardware limitations of quantum computing do not permit efficient processing of large datasets, and currently, it is not possible to use quantum hardware at all scales because it is not available.

Regarding the practical implications, the Random Forest model turned out to be the most appropriate model in the detection of fraud in financial institutions in a real-time environment. The capacity to process large data amounts, the capability to overcome the issue of class imbalance when using the SMOTE method, as well as giving interpretable outputs, is what makes it a solid option in terms of real-world applicability. Conversely, the Quantum models, such as QSVC, when the quantum device becomes better, can completely transform fraud detection since it can now offer greater processing powers to detect more fraudulent patterns with greater accuracy and faster. The potential is, however, limited by the capabilities of quantum hardware and the complexity of quantum algorithms that are presently available. In the future, there is a need to improve quantum hardware to achieve the full potential of quantum models in the detection of fraud. Already improved and scalable quantum systems will enable the implementation of quantum models in larger real fraud detection systems. It is also possible to integrate quantum and classical models into hybrid systems to have the best of both worlds because classical models have demonstrated reliability, and quantum algorithms have demonstrated their capabilities to process information faster. The scalability of quantum models also needs to be investigated in future research, which must keep the models affordable in real-time when dealing with large datasets, without compromising research accuracy and efficiency.

To sum up, this study has provided evidence of the capability of classical and quantum models in fraud detection, showing that although currently Random Forest is a rather useful tool, quantum models hold promising opportunities in the future of fraud detection, assuming that the available errors related to hardware and algorithms will be resolved. Quantum computing in fraud detection systems is a promising future potential to dramatically increase the effectiveness of fraud detection in the financial sector by the application of quantum computing in fraud detection systems.

6. Conclusion

This study examined how classical and the quantum machine learning models can be used to identify fraudulent financial transactions. The fundamental task was to test the effectiveness of the Random Forest in detecting fraud and pit the two options against each other (Quantum Support Vector Classifier (QSVC) as an upcoming model in the sphere of quantum machine learning). We sought to test how well these models could be applied to large-scale financial data

with the following goals: evaluating their ability to deal with large-scale data, paying attention to their scalability, computing needs, and precision. The Random Forest model was outstanding and performed with almost perfect accuracy and an AUC-ROC score of 1.0. This performance stands out especially where the goal is to detect fraud, whereas few false positives as possible should be avoided, and also false negatives should be discouraged as much as possible. The Confusion Matrix and ROC curve showed how this model can effectively distinguish between fraudulent and non-fraudulent deals, which showed strong validity of the model. The importance of the features as analyzed also showed that the number of transactions, the interval between transactions, and the location are essential predictors that make good business information on preventing fraud. Using SMOTE to solve the issue of imbalance in classes is possible; hence, the model was trained on more balanced data, which guaranteed trustworthy output.

To sum up, this study has provided evidence of the capability of classical and quantum models in fraud detection, showing that although currently Random Forest is a rather useful tool, quantum models hold promising opportunities in the future of fraud detection, assuming that the available errors related to hardware and algorithms will be resolved. Quantum computing in fraud detection systems is a promising future potential to dramatically increase the effectiveness of fraud detection in the financial sector by the application of quantum computing in fraud detection systems.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that they have no conflict of interest.

Statement of ethical approval

Ethical approval was not required for this study as it did not involve human or animal participants. The research utilized publicly available and anonymized data.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sector.

Acknowledgments

These authors express gratitude to the developers of credit card fraud detection dataset, who made their dataset publicly available. This is especially owed to the Quantum Computing

References

[1] L. Hernandez Aros, "Financial fraud detection through the application of machine learning techniques," Nature Communications, vol. 15, no. 1, pp. 1-13, 2024. [Online]. Available: https://www.nature.com/articles/s41599-024-03606-0

[2] R. Auer et al., "Quantum algorithms: A new frontier in financial crime prevention," arXiv preprint arXiv:2403.18322, 2024. [Online]. Available: https://arxiv.org/html/2403.18322v1

[3] A. Zafar, "Quantum computing in finance: Regulatory readiness, legal gaps, and the future of secure tech innovation," European Journal of Risk Regulation, vol. 15, no. 3,pp.1-15,2025.[Online].Available: https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/quantum-computing-in-finance-regulatory-readiness-legal-gaps-and-the-future-of-secure-tech-innovation/D6653FF47A68A2CEA51FC1035F186E3B

[4] "Preparing for a post-quantum world: Quantum-safe technology," Mastercard Insights, 2025. [Online]. Available: https://www.mastercard.com/global/en/news-and-trends/Insights/2025/post-quantum-cryptography-white-paper.html

[5] R. Auer et al., "Quantum computing and the financial system," Bank for International Settlements, 2024. [Online].Available: https://www.bis.org/publ/bppdf/bispap149.pdf

[6] "AI fraud detection in banking," IBM Think, 2025. [Online].

[7] Available: https://www.ibm.com/think/topics/ai-fraud-detection-in-banking

[8] "What financial crime compliance regulators are saying about generative AI," Sigma360 Knowledge Center, 2025. [Online]. Available: https://www.sigma360.com/knowledge-center/what-financial-crime-compliance-regulators-are-saying-about-genai

[9] L. Micheal, E. Gehrig, M. Elazar, and Y. H. Lee, "Evaluating the Efficacy of Quantum Support Vector Machines in Detecting Synthetic Identity Fraud in...," ResearchGate,May2024,Available: https://www.researchgate.net/publication/391663917_Evaluating_the_Efficacy_of_Quantum_Support_Vector_Machines_in_Detecting_Synthetic_Identity_Fraud_in_Financial_Datasets

[10] N. Innan et al., "Financial fraud detection using quantum graph neural networks," Quantum Machine Intelligence, vol. 6, no. 1, Feb. 2024, doi: 10.1007/s42484-024-00143-6. Available: https://arxiv.org/abs/2309.01127#

[11] N. Innan, A. Marchisio, M. Bennai, and M. Shafique, "QFNN-FFD: Quantum Federated Neural Network for Financial Fraud Detection," 2025 IEEE International Conference on Quantum Software (QSW), pp. 41–47, Jul. 2025, doi: https://doi.org/10.1109/qsw67625.2025.00015. Available: https://arxiv.org/abs/2404.02595.

[12] N. Innan, M. A.-Z. Khan, and M. Bennai, "Financial fraud detection: A comparative study of quantum machine learning models," International Journal of Quantum Information, vol. 22, no. 02, Nov. 2023, doi: 10.1142/s0219749923500442.Available: https://arxiv.org/abs/2308.05237

[13] Imani, M., Beikmohammadi, A., & Arabnia, H. R. (2025). Comprehensive Analysis of Random Forest and XGBoost Performance with SMOTE, ADASYN, and GNUS Under Varying Imbalance Levels. Technologies, 13(3), 88. https://doi.org/10.3390/technologies13030088

[14] Afriyie, J. K., et al. (2023). A supervised machine learning algorithm for detecting and predicting credit card fraud.ScienceDirect.Available: https://www.sciencedirect.com/science/article/pii/S277266222 3000036

[15] Li, Y., et al. (2025). An improved SMOTE algorithm for enhanced imbalanced classification. Nature. Available: https://www.nature.com/articles/s41598-025-09506-w

[16] T. Suzuki, T. Hasebe, and T. Miyazaki, "Quantum support vector machines for classification and regression on a trapped-ion quantum computer," Quantum Machine Intelligence, vol. 6, no. 1, May 2024, doi: 10.1007/s42484-024-00165-0.Available:https://link.springer.com/article/10.1007/s42484-024-00165-0

[17] R. Nur, "Integrating Quantum Kernel Methods with Deep Learning for Real- Time Fraud Detection in Fintech Platforms," ResearchGate, May 2025, Available: https://www.researchgate.net/publication/392166244_Integrating_Quantum_Kernel_Methods_with_Deep_Learning_for_Rea l-_Time_Fraud_Detection_in_Fintech_Platforms

[18] Y. Gujju, A. Matsuo, and R. Raymond, "Quantum machine learning on near-term quantum devices: Current state of supervised and unsupervised techniques for real-world applications," Physical Review Applied, vol. 21, no. 6, Jun. 2024, doi: 10.1103/physrevapplied.21.067001. Available: https://journals.aps.org/prapplied/abstract/10.1103/PhysRevAp plied.21.067001

[19] P. Sundaravadivel, R. A. Isaac, D. Elangovan, D. KrishnaRaj, V. V. L. Rahul, and R. Raja, "Optimizing credit card fraud detection with random forests and SMOTE," Scientific Reports, vol. 15, no. 1, May 2025, doi: 10.1038/s41598-025-00873-y Available:https://www.nature.com/articles/s41598-025-00873-y

[20] N. Innan, M. A.-Z. Khan, and M. Bennai, "Financial fraud detection: A comparative study of quantum machine learning models," International Journal of Quantum Information, vol. 22, no. 02, Nov. 2023, doi: 10.1142/s0219749923500442. Available: https://arxiv.org/abs/2308.05237

[21] J. Jin and Y. Zhang, "The analysis of fraud detection in financial market under machine learning," Scientific Reports, vol. 15, no. 1, Aug. 2025, doi: 10.1038/s41598-025-15783-2. Available: https://www.nature.com/articles/s41598-025-15783-2

[22] M. Schuld, "Supervised quantum machine learning models are kernel methods," arXiv.org, Jan. 26, 2021.Available: https://arxiv.org/abs/2101.11020

[23] "Quantum Kernel Machine Learning - QiSKIt Machine Learning 0.8.4." Available:https://qiskit-community.github.io/qiskit-machine-learning/tutorials/03_quantum_kernel.html

[24] S. Jerbi, L. J. Fiderer, H. P. Nautrup, J. M. Kübler, H.J. Briegel, and V. Dunjko, "Quantum machine learning beyond kernel methods," Nature Communications, vol. 14, no. 1, Jan. 2023, doi: 10.1038/s41467-023-36159-y. Available: https://pmc.ncbi.nlm.nih.gov/articles/PMC9889392/

[25] T. Suzuki, T. Hasebe, and T. Miyazaki, "Quantum support vector machines for classification and regression on a trapped-ion quantum computer," Quantum Machine Intelligence, vol. 6, no. 1, May 2024, doi: 10.1007/s42484-024-00165-0. Available: https://link.springer.com/article/10.1007/s42484-024-00165-0

[26] "StateVectorSampler (V1.2) | IBM Quantum Documentation,"IBM Quantum Documentation. Available: https://quantum.cloud.ibm.com/docs/en/api/qiskit/1.2/qiskit.primitives.StatevectorSampler

[27] F. Rodríguez-Díaz, D. Gutiérrez-Avilés, A. Troncoso, and F. Martínez-Álvarez, "A survey of Quantum machine learning: foundations, algorithms, frameworks, data and applications," ACM Computing Surveys, Sep. 2025, doi: 10.1145/3764582. Available:https://dl.acm.org/doi/10.1145/3764582

[28] S. Thanasilp, S. Wang, M. Cerezo, and Z. Holmes, "Exponential concentration in quantum kernel methods," arXiv.org, Aug. 23, 2022. Available: https://arxiv.org/abs/2208.11060

[29] "A survey on quantum machine learning: basics, current trends, challenges, opportunities, and the road ahead."Available: https://arxiv.org/html/2310.10315v4

[30] S. Thanasilp, S. Wang, M. Cerezo, and Z. Holmes, "Exponential concentration in quantum kernel methods," Nature Communications, vol. 15, no. 1, Jun. 2024, doi: 10.1038/s41467-024-49287-w.Available:https://www.nature.com/articles/s41467-024-49287-w

[31] L. Slattery, R. Shaydulin, S. Chakrabarti, M. Pistoia,S. Khairy, and S. M. Wild, "Numerical evidence against advantage with quantum fidelity kernels on classical data," Physical Review. A/Physical Review, A, vol. 107, no. 6, Jun. 2023, doi: 10.1103/physreva.107.062417. Available: https://arxiv.org/abs/2211.16551

[32] J. Schnabel and M. Roth, "Quantum kernel methods under scrutiny: a benchmarking study," Quantum Machine Intelligence, vol. 7, no. 1, Apr. 2025, doi: 10.1007/s42484-025-00273-5. Available:https://www.researchgate.net/publication/391113819_Quantum_kernel_methods_under_scrutiny_a_benchmarking_study

[33] T. Albalawi and S. Dardouri, "Enhancing credit card fraud detection using traditional and deep learning models with class imbalance mitigation," Frontiers in Artificial Intelligence, vol.8,Oct.2025,doi: 10.3389/frai.2025.1643292.Available: https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1643292/full

[34] Wikipedia contributors, "Synthetic minority oversampling technique - Wikipedia." Available: https://en.wikipedia.org/wiki/Synthetic_minority_oversamplingtechnique

[35] Y. Kumar, S. Saini, and R. Payal, "Comparative analysis for fraud detection using logistic regression, random forest and support Vector machine," SSRN Electronic Journal, Jan. 2020, doi: 10.2139/ssrn.3751339. Available: https://www.researchgate.net/publication/347446386_COMPARATIVE_ANALYSIS_FOR_FRAUD_DETECTION_USING_LOGISTIC_REGRESSION_RANDOM_FOREST_AND_SUPPORT_VECTOR_MACHINE

[36] V. Saeed and A. M. Abdulazeez, "Credit Card Fraud Detection using KNN, Random Forest and Logistic Regression Algorithms : A Comparative...," ResearchGate, Jan. 2024, Available:https://www.researchgate.net/publication/378288653_Credit_Card_Fraud_Detection_using_KNN_Random_Forest_and_ Logistic_Regression_Algorithms_A_Comparative_Analysis

[37] Nouhaila Innan, M. A.-Z. Khan, and M. Bennai, "Financial Fraud Detection: A Comparative Study of Quantum Machine Learning Models,"arXiv (Cornell University), Jan. 2023, doi: https://doi.org/10.48550/arxiv.2308.05237