International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 8, Issue 5, pp 319-324, May-2024

https://doi.org/10.47001/IRJIET/2024.805042

Quantum-Assisted Machine Learning for Enhanced Fraud Detection in Cybersecurity

[1]Mohammed Aqeel Abdulrazzaq Altarraji, [2]Ali Mokdad

[1,2]Computer Science Department, American University of Culture & Education, Beirut, Lebanon

***Abstract* - Innovative methods for information security and fraud prevention are required in today's digital environment due to the expanding volume of data and the increasing complexity of cyber threats. The use of quantum computing techniques to improve fraud detection and classification systems is investigated in this study. The study's machine learning framework integrates three distinct quantum algorithms to improve classification techniques. The first technique uses a Pauli feature map and a Quantum Support Vector Classifier (QSVC) that leverages a quantum kernel to transform classical input into quantum states. The second technique use a ZZ feature map with "linear" entanglement and a support vector classifier model, utilizing quantum kernels to enhance quantum systems. The third method utilizes Variational Quantum Circuits (VQC) with actual amplitudes, which integrate quantum and conventional machine learning techniques to provide optimized classification. The best results were obtained by the QSVC using ZZ feature maps and linear entanglement, which had a precision of 1.0 and a notable decrease in false positives. In order to improve fraud detection systems' accuracy and dependability and offer strong solutions to financial institutions, this study shows how quantum computing has the potential to completely transform cybersecurity.**

Keywords: Quantum Computing, Machine Learning, Fraud Detection, Quantum Support Vector Classifier, Variational Quantum Circuits, Pauli Feature Map, ZZ Feature Map.

I. INTRODUCTION

Ensuring information security and combating fraud has become an enormous task in today's linked digital landscape due to the growth of data and the sophistication of cyber threats [1]. Cyber threats, such as identity theft and massive financial fraud, are ever-present and constitute a threat to individuals, companies, and financial institutions [2]. Although sturdy, traditional computer methods can no longer adequately handle these growing dangers. Therefore, novel approaches are required immediately to detect and prevent fraudulent actions with greater accuracy, efficiency, and dependability. Integrating quantum computing into cybersecurity frameworks is one such way.

Quantum computing signifies a fundamental change in computational capacity. Quantum computers differ from conventional computers in that they utilize quantum bits, or qubits, which can concurrently exist in various states due to the laws of superposition and entanglement, as opposed to binary bits (0s and 1s) used by classical computers to process information [3]. Quantum computers have the ability to carry out intricate computations at unparalleled velocities, which has the potential to bring about significant changes in many domains such as cybersecurity and machine learning.

The use of machine learning (ML) has been crucial in the battle against cybercrime, since it has provided robust resources for identifying patterns and detecting anomalies. Unfortunately, traditional ML models frequently fail to adequately address important domains like fraud detection due to the sheer volume and complexity of modern data. One promising approach to improving these capabilities is quantum machine learning (QML) [4], which combines quantum computing with machine learning. QML makes use of quantum algorithms to analyze massive datasets more effectively and efficiently.

Classical machine learning models have scalability problems and slower processing speeds since they require ever-increasingly massive computational resources, which is becoming more problematic as data quantities keep growing exponentially. In addition to using a lot of resources and requiring substantial feature engineering and parameter optimization, these methods might not work as well in real-time situations. A revolutionary strategy merging the benefits of quantum computing with state-of-the-art machine learning methods is necessary to tackle these challenges. The goal of this integration is to improve cybersecurity measures across several domains and deliver a more reliable, scalable, and accurate solution for detecting fraud. The aim of the study is to evaluate the use of quantum computing in cybersecurity, with a particular focus on how quantum algorithms can be improved for fraud detection and to provide useful insights into the potential benefits of quantum computing in this field.

II. RELATED WORK

The capacity of machine learning models to sift through massive datasets in search of patterns suggestive of fraudulent activity has made them an indispensable tool in the fight against fraud. These models incorporate a number of algorithms that have been fine-tuned through time to reduce false positives and maximize detection accuracy. Fraudulent transactions are the basis of credit card fraud detection in [5]. Random Forest algorithm was used to classify the dataset as the approach is based on supervised learning and the confusion matrix was used to evaluate the performance of the algorithm and obtain an accuracy of up to 90%. The authors in [6] addressed the issue of class imbalance in financial fraud transaction data by utilizing Generative Adversarial Network (GAN) to generate samples of the minority class. This was done to improve the accuracy of the classifiers used for training. In [7], a new anomaly detection framework is proposed that uses attention-grabbing autoencoders and GANs to effectively decouple large transaction data. Credit card fraud detection systems have been developed using Random Forest and Adaboost algorithms in [8] to identify suspicious transactions.

Quantum computing brings about a fundamental change by utilizing qubits to process information, making use of principles from quantum mechanics such as superposition and entanglement. Quantum computers have the capability to carry out specific computations at a significantly higher speed compared to traditional computers. In [9], a novel approach to this significant subject was suggested, employing the concept of quantum-assisted quantum machine learning. An assessment was conducted utilising IBM QX in simulation mode and demonstrated that quantum-assisted algorithms can attain remarkable precision, rivalling the top outcomes of conventional SVM, contingent upon the characteristics of the dataset. A comparative analysis was conducted in [10] to compare quantum neural networks (QNN) with classical neural networks (NN) using a dataset called ClaMP, which consists of software supply chain attack data. The objective is to distinguish the performance disparity between QNN and NN and carry out the experiment.

Hybrid models integrate quantum and conventional computing components to exploit the benefits of both. These approaches seek to maximize computational resources and improve the performance of machine learning tasks. Hybrid approaches strive to achieve a harmonious equilibrium between the processing capabilities of quantum computing and the well-established techniques in classical computing. It offers a pragmatic way forward, as complete quantum solutions are still being developed. Nevertheless, the process of combining the two models might be intricate, necessitating meticulous evaluation of their compatibility and optimization. The integration of quantum and classical neural networks enables the compression of intricate high-dimensional features into a more compact yet more useful feature space, which can subsequently be analyzed by currently available quantum computers. In [11], a quantum-classical hybrid neural network was developed and utilized to detect amplitude shift cyberattacks on an automotive Controller Area Network (CAN) dataset. The results showed that the hybrid NN achieved a detection success rate of up to 94%, surpassing the success rates of long-term memory (LSTM) (87%) and quantitative NN (62%). Botnet DGA classification was the focus of the study that compared traditional deep learning models with hybrid quantum-classical ones [12]. With a sample size of 1,000, the hybrid quantum deep learning model achieves an accuracy of 93.9%, which is marginally better than the classical model. Due to the impact of the initially utilized random seed values, it was found that Hybrid deep learning models were not as accurate as anticipated.

Quantum machine learning research is now in its early phases but exhibits potential in addressing intricate challenges that classical algorithms find challenging. The main emphasis is on the development of quantum algorithms that can surpass their classical equivalents in terms of both speed and accuracy.

III. METHODOLOGY

The objective of the research is to better the identification of fraudulent activities and improve cybersecurity by employing three quantum procedures. These methodologies are utilized to augment existing detection techniques, as illustrated in Figure 1. The study examines various feature maps, entanglement patterns, and variable quantum circuits to provide useful insights into the possible advantages of quantum computing in solving the complexity of information security challenges. This approach presents a systematic method for investigating the value of combining quantum computing and machine learning in the field of cybersecurity. It involves gathering and analyzing data, using quantum programming frameworks to implement the algorithm, and assessing its performance by comparing it to traditional machine learning models. The qiskit Machine Learning module has been used to enable access to quantum machine learning algorithms. Additionally, the qiskit library has been installed to facilitate the transfer of supplementary quantum algorithms and functions. The ZZ Feature Map and Pauli Feature Map will be utilized to convert credit card transaction records into quantitative representations. These maps enhance the capacity of quantum kernels to grasp intricate connections among data items.

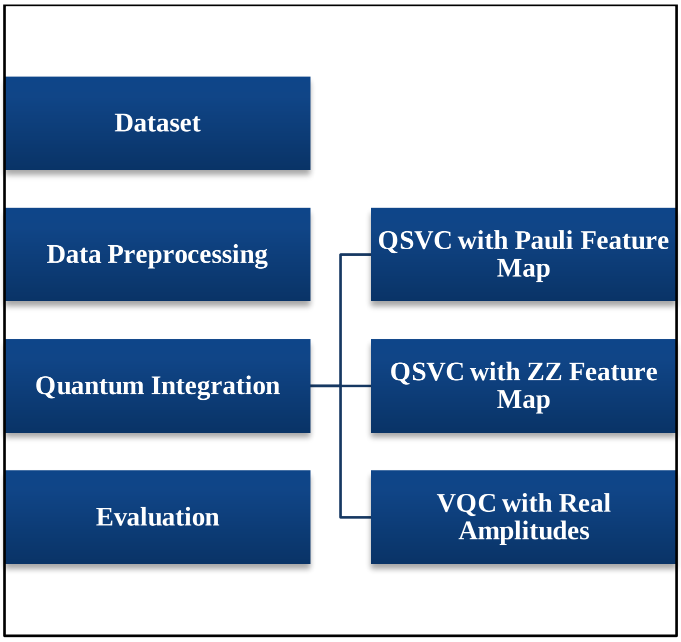

Figure 1: Proposed methodology for applying quantum-assisted machine learning for fraud detection

3.1 Dataset

The dataset utilized comprises credit card transactions conducted by European cardholders in September 2013. It comprises 32 attributes, including "Time" and "Amount". The "Class" attribute represents the dependent variable, which is a binary value. A value of 1 indicates a fraudulent transaction, whereas a value of 0 indicates otherwise. The dataset consists of 492 instances of fraudulent transactions out of a total of 284,807 transactions, resulting in a substantial class imbalance. The positive class instances, which correspond to fraud, account for just 0.172% of all transactions.

3.2 Data Preprocessing

Correlation coefficients were computed for each feature to ascertain the relationship between the features and the "class" variable. The magnitudes of these coefficients were arranged in a decreasing order to rank the features based on their correlation with the target variable. Figure 2 displays the outcome of computing pairwise correlation coefficients. Missing data were eliminated and a sampling strategy was employed to ensure a balanced data set. A sample of 300 transactions that were not fraudulent was randomly chosen to match the quantity of fraudulent transactions. Subsequently, these two sections were merged to form a well-balanced training dataset. Testing is allocated 25% of the data, whereas training is allocated 75%. Subsequently, the data was normalized to achieve a mean of 0 and a standard deviation of 1. Principal component analysis (PCA) was then employed to decrease the number of features (or dimensions) in the dataset while retaining the most significant information.

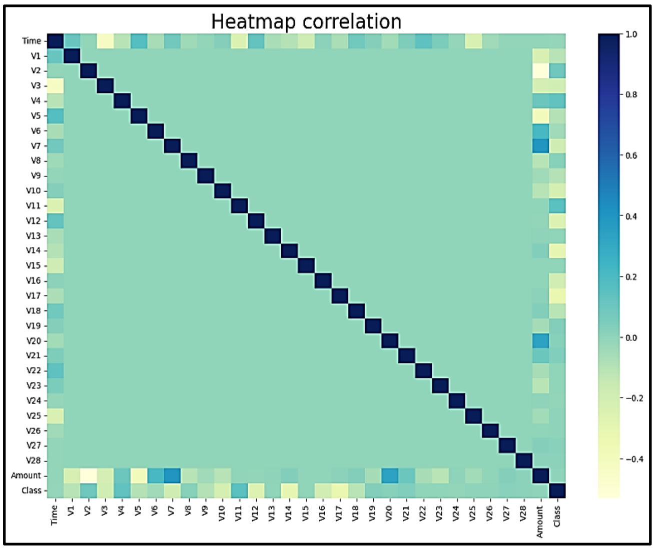

Figure 2: Correlation between dataset columns

The Min-Max scaling technique was employed to make features falling within a specific range ([0, 4]). Scaling is a crucial step for certain machine learning algorithms in order to guarantee that all features have an equal impact on the model training process. Figure 3 illustrates the sampling distribution of a dataset following the process of reduction and scaling.

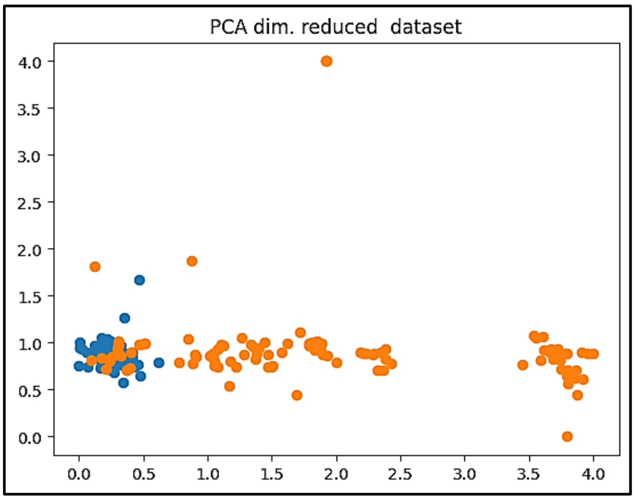

Figure 3: Distribution of samples in the dataset after processing

3.3 QSVC with Pauli Feature Map

This approach employs Pauli feature maps to convert classical data into quantum states. The Quantum Support Vector Classifier (QSVC) utilizes the inherent characteristics of Pauli matrices to process quantum states and carry out classification tasks. Quantum kernels are used to quantify the similarity between quantum states. This allows the QSVC to classify data points more efficiently by taking advantage of quantum parallelism. Pauli feature maps have the capability to capture intricate data linkages, hence enhancing the model's capacity to differentiate between fraudulent and legitimate transactions.

3.4 QSVC with ZZ Feature Map

ZZ feature map utilizes ZZ interaction to entangle qubits, so generating a high-dimensional representation of the data. This meshing effectively depicts the intricate interconnections present within the data. This approach utilizes a "linear" interlacing pattern to organize the data representation, hence improving the classification capability of QSVC. The accuracy metric assesses the resemblance of quantum states produced by ZZ feature maps, offering an efficient method to evaluate data correlations.

3.5 VQC with Real Amplitudes

Variable Quantum Circuits (VQCs) are quantum circuits that may be trained using real-valued amplitudes to determine the parameters. These circuits are enhanced utilizing traditional techniques to carry out classification jobs. VQCs employ a methodology that combines both quantum and classical components. The quantum portion is responsible for executing the calculations, while the classical portion focuses on optimizing the parameters. VQCs offer versatility and adjustability by leveraging the advantages of both quantum and conventional computing to improve classification accuracy.

IV. EVALUATION AND RESULTS

Through the investigation of these cutting-edge quantum and hybrid algorithms, the purpose of this research is to make major advancements in the identification of fraudulent activity, hence providing solutions that are more robust and scalable to address cybersecurity concerns. Table 1 provides a complete comparison of the performance of the three quantum models that are utilized for the detection of fraudulent credit card transactions.

- QSVC model with Pauli Feature Maps exhibited impressive performance, achieving an accuracy of 0.9189, precision of 0.96, and recall of 0.83. It successfully reduced the number of incorrect identifications and precisely categorized incidents of fraud.
- QSVC model with ZZ feature maps, which exhibit linear entanglement, demonstrated exceptional performance, achieving an accuracy of 0.9459, precision of 1.00, and recall of 0.87. The model effectively minimized instances of false positives while preserving a robust equilibrium between precision and recall.
- VQC using real amplitudes demonstrated an accuracy of 0.8514, indicating the potential of these models in fraud detection. However, their performance was inferior to the other two models.

Table 1: Comparing performance of the three quantum models

Metrics	QSVC with Pauli Feature Maps	QSVC with ZZ Feature Maps (entanglement="linear")	VQC with Real Amplitudes
Accuracy	0.9189	0.9459	0.8514
Precision	0.96	1.00	….
Recall	0.83	0.87	…

Quantum models effectively strike a robust equilibrium between precision and recall, which is crucial for the successful detection of fraud. Comparative investigation shows that ZZ feature maps with QSVC exhibit the highest test scores and achieve 100% precision. The results show significant progress in addressing cybersecurity challenges, as shown in Table 2 when compared to previous studies that used the same credit card fraud data set.

Table 2: Comparing the results with previous studies that used the same dataset

Ref	ML Algorithm	Resalts
[5]	Random Forest	Accuracy 90%
[6]	Generative Adversarial Network	Recall 0.70
[7]	Autoencoders and Generative Adversarial Network	Precision 0.9795 Recall 0.7553
[8]	Random Forest AdaBoost	Accuracy 93%
Proposed Approach	QSVC with Pauli Feature Maps QSVC with ZZ Feature Maps VQC with Real Amplitudes	Accuracy 0.9459 Precision 1.00 Recall 0.87

With an accuracy of 94.59%, the suggested model outperformed previous machine learning techniques used in earlier studies on the same dataset. A remarkable ability to detect cases of credit card fraud with an exceptionally low proportion of false positives is indicated by a precision of 1.00. The results demonstrate that by combining quantitative machine learning with QSVC and VQC models, better cybersecurity solutions can be provided. Credit card fraud detection tasks including discrimination and classification appear to be improved by quantum variable circuits and quantum feature maps. Table 3 shows comparing against other studies that used different quantum machine learning algorithms. Our model outperformed those studies by a wide margin.

Table 1: Comparing the results with studies that used QML algorithms in cybersecurity

Ref	Quantum ML Algorithm	Dataset	Best Accuracy
[9]	Quantum SVM	NSL KDD NB15	75%
[10]	Quantum Neural Network	ClaMP	53%
[11]	Hybrid quantum classical Neural Network	HCRL Dataset	94%
[12]	VQC algorithm-based model Hybrid quantum-classical deep learning model	Botnet DGA Dataset	93.5%
Proposed Approach	QSVC with Pauli Feature Maps QSVC with ZZ Feature Maps VQC with Real Amplitudes	Credit Card Fraud Detection	94.59%

V. CONCLUSION

In today's digital world, the continuous growth of data and the increasing complexity of cyber threats require new approaches to guarantee information security and prevent fraud. Conventional computing, albeit strong, faces difficulties in dealing with the complex challenges presented by contemporary cybersecurity problems. Quantum computing possesses remarkable processing capabilities that have the potential to revolutionize machine learning and cybersecurity. This study utilizes quantum computing methods to improve classification and fraud detection processes. The study's machine learning framework incorporates three separate quantum algorithms. The initial technique utilizes a Pauli feature map and a QSVC that leverages a quantum kernel to transform classical input into quantum states. The second technique use a ZZ feature map with "linear" entanglement and a support vector classifier model, utilizing quantum kernels to enhance quantum systems. The third method utilizes VQC that incorporate real amplitudes. This strategy combines quantum and classical machine learning approaches to achieve optimized classification. The QSVC with ZZ feature maps and linear entanglement demonstrated exceptional performance, achieving a precision of 1.0. This indicates a near-perfect capacity to detect fraudulent transactions while effectively minimizing false positives. The high level of precision in this context has significant ramifications for financial institutions, since any incorrect categorizations might result in severe repercussions for both clients and enterprises. In order to advance in the field of quantum studies, it is imperative to transition from simulated quantum environments to real quantum devices. Quantum computing, if correctly utilized, has the potential to revolutionize the approach to difficult problems and decision-making due to its computational benefits.

REFERENCES

[1] Y. Li, and Q. Liu, “A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments,” *Energy Reports*, vol. 7, pp. 8176-8186, 2021.

[2] A. Q. Stanikzai, and M. A. Shah, “Evaluation of cyber security threats in banking systems,” *In 2021 IEEE Symposium Series on Computational Intelligence (SSCI)*,pp. 1-4, 2021.

[3] M. Lee, “Quantum Computing and Cybersecurity,” *Belfer Center for Science and International Affairs Harvard Kennedy School, Cambridge*, 2021.

[4] J. Shara, “Quantum Machine Learning and Cybersecurity,” *Quantum*, vol. 12, no. 6, pp. 47-56, 2023.

[5] M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini, “Credit card fraud detection using random forest algorithm,” *in 2019 3rd International Conference on Computing and Communications Technologies (ICCCT)*, pp. 149-153, Feb. 2019.

[6] U. Fiore, A. De Santis, F. Perla, P. Zanetti, and F. Palmieri, “Using generative adversarial networks for improving classification effectiveness in credit card fraud detection,” *Information Sciences*, vol. 479, pp. 448-455, 2019.

[7] S. Jiang, R. Dong, J. Wang, and M. Xia, “Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network,” *Systems*, vol. 11, no. 6, p. 305, 2023.

[8] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, “Credit card fraud detection using machine learning techniques: A comparative analysis,” *in 2017 International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1-9, Oct. 2017.

[9] A. Gouveia and M. Correia, “Towards quantum-enhanced machine learning for network intrusion detection,” *in 2020 IEEE 19th International Symposium on Network Computing and Applications (NCA)*, pp. 1-8, Nov. 2020.

[10] M. S. Akter, M. J. H. Faruk, N. Anjum, M. Masum, H. Shahriar, N. Sakib, A. Rahman, F. Wu, and A. Cuzzocrea, “Software supply chain vulnerabilities detection in source code: Performance comparison between traditional and quantum machine learning algorithms,” *In 2022 IEEE International Conference on Big Data (Big Data)*,pp. 5639-5645, 2022.

[11] M. Islam, M. Chowdhury, Z. Khan, and S. M. Khan, “Hybrid Quantum-Classical Neural Network for Cloud-supported In-Vehicle Cyberattack Detection,” *IEEE Sensors Letters, vol*. 6, no. 4, pp. 1-4, 2022.

[12] H. Suryotrisongko and Y. Musashi, “Evaluating hybrid quantum-classical deep learning for cybersecurity botnet DGA detection,” *Procedia Computer Science*, vol. 197, pp. 223-229, 2022.

Citation of this Article:

Mohammed Aqeel Abdulrazzaq Altarraji, Ali Mokdad, “Quantum-Assisted Machine Learning for Enhanced Fraud Detection in Cybersecurity”, Published in *International Research Journal of Innovations in Engineering and Technology* - *IRJIET*, Volume 8, Issue 5, pp 319-324, May 2024. Article DOI https://doi.org/10.47001/IRJIET/2024.805042

****