Grenze International Journal of Engineering and Technology, June Issue

Exploring the Role of Quantum Machine Learning for Credit Card Fraud Detection: A Hybrid Approach

Kashish Solanki[1], Tushar Saini[2], Sandeep Raj[3] and Ritu Pahwa[4]
[1-4]CSE (AIML), Dronacharya College of Engineering Gurugram, India
Email: solankikashish41@gmail.com, tusharsainii829@gmail.com, sandeepbainy01@gmail.com, ritu.pahwa@ggnindia.dronacharya.info

***Abstract*— Detecting fake credit card payments is a demanding problem. It occurs because valid transactions are very frequent then once false and signals of fraud are difficult to recognize.**
QML presents a strong approach to possibly enhance together the correctness and quickness of identification by attaching unique features of quantum machines. In this research we examine three QML simulations— the Variational Quantum Classifier (VQC), Sampler Quantum Neural Network (SQNN), Estimator Quantum Neural Network (EQNN)—with two specific data sets. We also experiments with multiple converters and model architecture.
Our conclusions show that VQC steadily produces highly solid output, obtaining F!-score of 0.88. SQNN also exhibits solid execution, while the EQNN has complication in understanding the data. Moreover we implement QUBO-based classification model on a neural-atom quantum processor, exploring several system configurations in hybrid model approaches.
Examine a real quantum device, using setups of upto 24 atoms, display a significant strength against system noise. Notably, in some cases, a low level of sound even linked to a little better outcomes. These novelties highlight the significance of well- planned QML model development and aim to significant potential of atom-based quantum system or improving fake transaction detection in digital security.

***Keywords*— Quantum Machine Learning, Credit Card Fraud Detection, Variational Quantum Classifier, Quantum Neural Networks, Quadratic Unconstrained Binary Optimization, Neutral Atom Quantum Processing Unit, Ensemble Learning, Noise Resilience, Cybersecurity.**

I. INTRODUCTION

Credit Cards can has turned out to be a universal concern i.e. beside being high-priced but also steadily more complex. Each year, lots of people and uncountable business suffer loses to false transactions, with financial damage growing quickly. For instance UK finance stated that in 2022, UK lost more than £1.2 billion to scam, about 80% of cases linked to web-frauds. In the United States, the Federal Trade Commission approximated that buyers suffered from loses were about $8.8 billion in the same year, however information from European banking authority and the European Central Bank reported credit card fraud resulted in
€633 million merely in initial six months of 2023([7][8]). These figures are beyond huge data—they point to a growing problem that damages reliance in online transaction and weakens reliability of banking system.
Through the times, fraud detection as improved expressively, machine learning(ML)models are widely used to marked doubtful payments[8].

Grenze ID: 01.GIJET.12.2.36_20

However, regardless of these progresses, persistent problems continue. Fraudulent activity signifies a small fraction of all transactions, causing imbalance data sets that are challenging for computer programs to understand. Additionally, the tactics of fraudsters frequently shifts, needing monitoring system to proceed quickly. The arising level and complications pf financial data also stress standard machine learning approaches, mainly in real-time monitoring where precision and immediate actions are important.[3]

These remaining space forcing the exploration for unique computing technologies proficient of handling complex, many- layered data fields effectively[9].

Quantum Machine Learning (QML) merges the natural, multi-tasking ability of quantum systems with pattern-recognition power of ML. By using essential quantum effects—superposition and strong links between the particles[11]—QML procedures can determine information in more refined. This lets them to find complex connection and usual techniques possibly will fully avoid([1][2]).

This capability formerly understood in the domains varying from making different treatments and modeling atmosphere to designing new substances and mounting online protections[7]. Given these initial growths, a finance field is now relying on QML as a favorable supporter to prevent scams([4][6][10]).

Yet, a model's success is not automated. It relies on several fundamental design options: However data is described into quantum space (feature encoding) the layout of the quantum network itself and how quantum and regular computing components function together in integrated workflow. This correct mix is main factor for accessing QML's real-world strength([1][5][10][11]).

On this stage, we analyze how these plan selections consequence three QML—the Variational Quantum Classifier (VQC), the Sampler Quantum Neural Network (SQNN), and Estimator Quantum Neural Network (EQNN)— in recognizing illegal([3][4][9]).

With two actual, varying collection of fake data-sets, we check how different data-mapping and model setup impact precision, sensitivity, combined performance score.

We extend this research to QUBO-based category i.e. Support Vector Machine (SVM), executed on neutral atom QPU ([5][6]). Neutral atom QPUs are well-known for high scalability, quantum state life-time and stability for optimization issues. By implementing simulations and actual- physical components experiments—grading up to 24 atoms we examine model's implementation under different noise stages, average noise level in fact recover classification accuracy([5]).

In this analysis objective is to link gap advanced quantum computing advancements([6]). Our discoveries reveal how structure of QML model outline effects detection accuracy it also focuses on capability of neutral atom QPUs.

II. Literature Review

A. Credit Card Fraud Detection

Credit Card Fraud (CCF)become threat in today's financial security system([7]). Commonly Deceptive transactions pretend to be legal, but at beginning its not easy to detect. Common types of fraud contains card-not-present (CNP) fraud, where illegally obtained account information used for E-commerce purchase; identify burglary, where offenders pretend to be original account holder; fake card fraud, contain copying magnetic stripe cards; application fraud, where fake individuality used to obtain illegal card.

The main issue in detecting fraud is class imbalance problem—fraud cases usually show less than 1% of entire data([8]). Conventional Machine Learning (ML) techniques widely implemented to tackle this problem. Logistic Regression value for its simplicity and interpretability, yet efforts to model non-linear relations. Decision Trees and Random Forests capture complicated conclusion boundaries more effectively, however they can simply overfit imbalanced datasets.

Alternatively, Neural Networks (NNs) and Deep Learning (DL) designs prove robust analytical power, specifically in removing unseen designs from transactions, but require huge expanses of categorized data and great computational resources ([7][8]).

Formally, given a dataset:

$$D = \{(xi, yi) \mid xi \in R^d,\ yi \in \{0,1\}\}^N \qquad i=1$$

where xi stand for the transaction feature vector and yi is the binary class label (fraud = 1, legitimate = 0), the purpose is to study a decision function

$$f(x): R^d \rightarrow \{0,1\}$$

that reduces both false positives and false negatives. Despite constant progresses, old-style ML methodologies face complications when impostors adapt and develop their techniques. These restrictions have promote researchers to research quantum-enhanced techniques as a probable outcomes.

B. Fundamentals of Quantum Computing

Quantum computing used “superposition” and “Entanglement”, two essential principles of quantum mechanics, to implement computations that would unrealistic for standard machines([6][11]). Different traditional bits, which exist in a certain state (0 or 1), a quantum bit (qubit) can exist in a superposition of both:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad where\ |\alpha|^2 + |\beta|^2 = 1$$

A typical quantum circuit distributed into three main steps:

- State preparation – Transforming classical data into quantum level.
- Unitary evolution – Implementing HADAMARD, PAULI, CNOT to manipulate qubits.
- Measurement – Transforming the quantum state into standard outcomes using measurement([11]).

Primary benefits of quantum systems their ability to explore multi-dimensional Hilbert spaces simultaneously, where traditional techniques process one by one. The ability to create quantum computing specific for assuring anomaly detection challenges, where identifying infrequent fraud indications is dangerous.

C. Quantum Machine Learning (QML)

Quantum Machine Learning (QML) integrates quantum calculation with ML concepts to create models that implements better classical techniques in certain situations([11]).

- Quantum Support Vector Machines (QSVMs): This reframe the SVM enhancing project as a Quadratic Unconstrained Binary Optimization (QUBO) problem, with the cost function([6]):

$$E(a) = a^T Q a, \qquad a \in \{0,1\}^n$$

where QQQ is the QUBO matrix. Process for cases “Quantum Approximate Optimization Algorithm (QAOA)” and “adiabatic quantum computing” are generally implemented to solve this issue([5]).

- Quantum Neural Networks (QNNs): Built from parameterized quantum circuits, QNNs consist adjustable limitations θ transformed using normal optimizers to minimize a loss function $J(\theta)$. Such as include Variational Quantum Classifiers (VQC) and Estimator QNNs (EQNN) ([4][9]).
- Quantum Kernels: These mapping standard data into multi-dimensional quantum feature areas, developing data divisibility and refining execution of kernel-based methods ([4][9]).

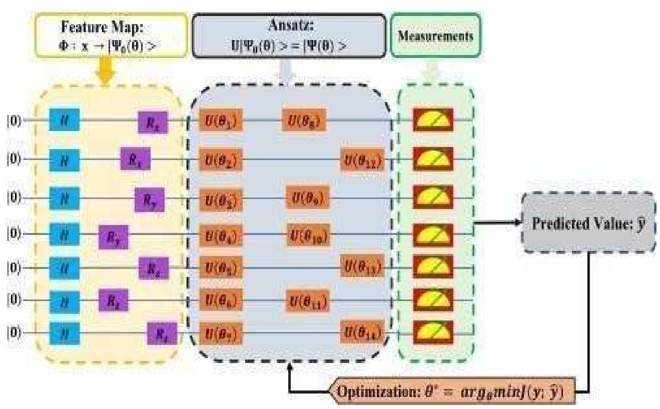


Fig 1

D. Related Work

Current literature has marked the ability of QML in fraud detection and anomaly detection([1][2][3][6][7][9][10]). For example, Huot et al. implement Quantum Amplitude Estimation (QAE) to imbalanced fraud datasets and experimental changed accuracy compared with traditional models. Further research examined VQCs for financial fraud detection, achieving F1-scores as high as 0.88, superior conventional neural networks on non- standardized data. In addition, experiments with neutral atom QPUs proven the scalability of QUBO-based QSVMs to 24 atoms, with remarkable flexibility contrary to noise ([5][6]).

Nevertheless, important confronts persevere. Noisy Intermediate-Scale Quantum (NISQ) devices are unassisted by decoherence and gate faults [11]. Preparing QNNs is also modified by the barren plateau problem, wherever gradients disappear in huge constraint areas, restricting optimization. In addition, most QML research remain stay at the simulation stage, and one or two have been verified in real financial circumstances ([4][6][8]).

In general, recent discoveries directed while QML deals thrilling opportunities for credit card fraud detection, development in quantum hardware reliability, error correction, and scalable hybrid algorithms is still crucial for realistic, production-level deployment.

III. Proposed Methodology

A. Data Preprocessing

The dataset used in this research consist a extremely tilted dispensation, with fraudulent transactions displaying not more than 1% of overall record. To plan it for modeling, various preprocessing steps were execute:

- Data Cleaning: Elimination of unnecessary and varying records ([3][7]).
- Feature Normalization: Constant characteristics such as transaction amount and time be normalized to a standard scale. This confirmed that no individual feature ruled the discovering practice, classical and quantum optimizers become stable.([3][7]).
- Categorical Encoding: Transaction types and merchant identifiers transformed to format it in same way with quantum circuits ([3][7)].
- Imbalance Handling: Fraud cases were simplified through oversampling (SMOTE) and undersampling techniques to balance the dataset for developed model training([3][7]).

B. Classical Baselines

To found context functioning, several standard ML models implemented:

- Logistic Regression: Simple and explained but not for non-linear patterns.
- Decision Trees & Random Forests: Exact in capturing tough linkage of features, but horizontal to overfitting on imbalanced data.
- Neural Networks (NNs): Able to research detailed transaction pattern, yet required huge data and calculation sources ([7][8]).

These standard beginning point pretend as target for quantum- increased techniques.

C. Hybrid Classical–Quantum Models

The primary support for this procedure for analysis of fusion models that joins traditional data preprocessing and optimizers with quantum circuits for developed feature mapping.

- Quantum Classifier (VQC): Implements means of restricted quantum circles where conventional optimizers developed circuit restrictions. This classifier highlighted as standardized features into a multi-dimensional Hilbert space, filtering contribution of fraud and authentic transactions ([3][4][9]).
- Quantum Neural Networks (QNNs): Variations such as Analyst QNNs and Estimator QNNs were examined for fraud detection. These linkages used variational routes and gradient-based bring up to date to optimize implementation ([4][9]).
- Quantum Support Vector Machines (QSVM): Redeveloped as a QUBO problem, resolved thru Quantum Approximate Optimization Algorithm (QAOA). QSVM was specifically in effect when merged with quantum kernels ([5][6]).
- Qiskit-learn(Q-sklearn): This implement arranges a connection for operating the potential of quantum computing to machine learning projects by Qiskit's exclusive collection ([3][7]). It approaches a straightforward method to examine quantum- boosted models together with their founded, standard counterparts from scikit-learn.
- Support Vector Machines (SVM) and Quantum SVM (QSVM): On its foundation, binary classification is an essential machine learning task. The purpose of straightforward : to mechanically allot every section of input data into one of two probable clusters.

In this project, Support Vector Machine (SVMs) is broadly faithful and actual tool, identified for their reliable execution amongst a lot of unique practical problems[5]. The main indication behind a SVM is to obviously plot data into a higher- dimensional space. This conversion permits to effectively split.

Although this process is robust, it can request important computing sources, becoming a block along vast datasets. To streamline this method, SVMs employ "kernel functions". This executed as cunning shortcuts, allow the needed multi- dimensional calculation without heavy computational lift.([5][6]).

Advantages of SVMs is their expertise with minor datasets, where data-hungry approaches as deep learning frequently disappoint. Nevertheless, as a data develops equally in quantity and complexity, kernel functions can face scalability restrictions.
This is where Quantum Support Vector Machines (QSVM's) enter the illustration. QSVMs consumes the exclusive assets of quantum computing[6].

IV. RESULT AND CONCLUSION

A. Dataset and Matrices

In this research, various datasets were consumed to estimate the presentation of traditional and quantum-based prototypes for fraud detection and anomaly detection challenges. Every dataset has its individual features, level of imbalance, preprocessing necessities. The datasets are classified into two main groups: Credit Card Fraud Detection datasets([1][3][6][8][10]) and Multivariate/Univariate Time Series datasets[2].

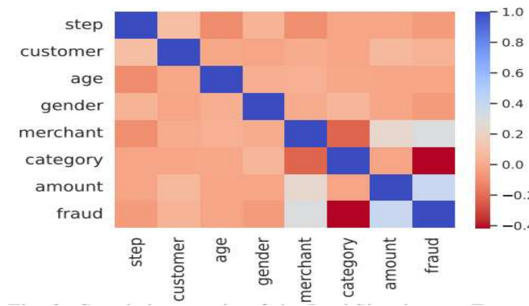


Fig. 1: Correlation matrix of the BankSim dataset.

Features such as "Category" represent a robust negative correlation with the label "Fraud", while "Merchant" and "Amount" have positive correlations, directing their significance in fraud detection.([3])

B. European Credit Card Fraud Dataset (Kaggle)

This dataset, commonly used in fraud detection examination, holds European credit cardholder transactions. Due to secrecy, the characteristics were converted using Principal Component Analysis (PCA), parting only anonymized numerical variables. Out of 284,807 transactions, only 492 are fraudulent, which accounts for 0.172% of the dataset, making creating it highly imbalanced ([3][7]). Preprocessing Steps:

- PCA applied to generate 28 anonymized features (V1– V28).
- Features "Time" and "Amount" retained.
- Random under-sampling performed to balance fraud vs. non-fraud transactions (492 each).
- Final dataset prepared with balanced ratio for training/validation, while the test set remained imbalanced to simulate real-world conditions. ([3][7]).

TABLE I: PERFORMANCE METRICS OF THE VQC MODEL ([3])

Model	Feature Map	Ansatz	Accuracy	Precision	Recall	F1_score
	Z	Real Amplitudes	0.7	1	0.34	0.51
		Two Local	0.88	1	0.73	0.84
		Efficient SU2	0.86	1	0.68	0.81
		Pauli Two Design	**0.9**	**1**	**0.78**	**0.88**
VQC	ZZ	Real Amplitudes	0.74	1	0.43	0.6
		Two Local	**0.87**	**1**	**0.71**	**0.83**
		Efficient SU2	0.78	0.94	0.55	0.69
		Pauli Two Design	0.73	0.77	0.56	0.65
	Pauli	Real Amplitudes	0.74	1	0.43	0.6
		Two Local	**0.87**	**1**	**0.71**	**0.83**
		Efficient SU2	0.78	0.94	0.55	0.69
		Pauli Two Design	0.81	0.96	0.6	0.73

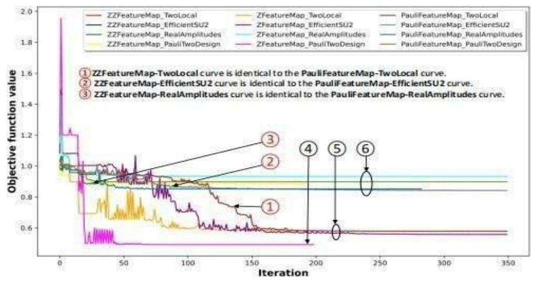


Fig. 2: VQC loss function on the European dataset.

The configuration in 4 demonstrates fast convergence with minimal loss, showing some oscillations during the first 50 iterations before stabilizing. The configurations in 5 exhibit similar behaviour, converging steadily over 200 iterations to achieve relatively low loss values. In contrast, the configurations in indicating suboptimal performance. 6 converge more rapidly but stabilize at a higher loss value. ([3])

C. BankSim Dataset

The BankSim dataset is a synthetic banking transaction dataset generated using an agent-based simulator. It is based on real aggregated transaction data provided by a Spanish bank. Fraudulent activities were simulated by modeling theft events and fraudulent purchases ([6][8]).

Key Characteristics:

- Contains 594,643 transactions over 180 days (~6 months).
- Includes 7,200 fraud cases (≈1.2% fraud rate).
- Nine feature columns + one target column.
- Features include customer ID, merchant ID, age, gender, category, amount, and fraud label.
- Preprocessing Steps:
- Resolved inconsistencies in categorical variables (e.g., age groups).
- Encoded categorical features numerically.
- Dropped low-variance features such as zip codes.
- Balanced using random under-sampling (fraud vs. non-fraud = 1:1).

TABLE II: PERFORMANCE METRICS OF THE VQC MODEL ON THE BANKSIM DATASET.([3])

Model	Feature Map	Ansatz	Accuracy	Precision	Recall	F1_score
	Z	Real Amplitudes	0.52	0.48	0.8	0.6
		Two Local	**0.54**	**0.5**	**0.84**	**0.62**
		Efficient SU2	0.65	0.68	0.44	0.54
		Pauli Two Design	0.55	0.51	0.51	0.51
VQC	ZZ	Real Amplitudes	0.74	0.75	0.62	0.68
		Two Local	**0.65**	**0.62**	**0.6**	**0.61**
		Efficient SU2	0.76	0.85	0.56	0.68
		Pauli Two Design	0.51	0.46	0.42	0.44
	Pauli	Real Amplitudes	0.73	0.69	0.72	0.7
		Two Local	**0.73**	**0.69**	**0.72**	**0.71**
		Efficient SU2	0.76	0.85	0.56	0.68
		Pauli Two Design	0.5	0.45	0.46	0.46

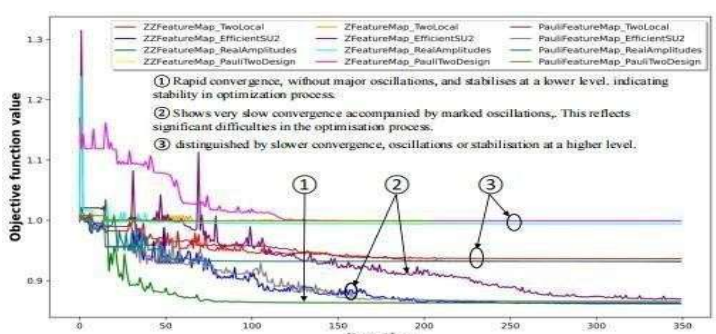


Fig 3: VQC loss function on the BankSim dataset

Most configuration demonstrate stabilization over time, indicating consistent optimization behaviour. However, some configurations exhibit a zigzag pattern during convergence, reflecting oscillatory dynamics before eventual stabilization.

TABLE III: IMPLEMENTATION METRICS OF THE EQNN MODEL ON THE BANKSIM DATASET.

Model	Feature Map	Ansatz	Accuracy	Precision	Recall	F1_score
	Z	Real Amplitudes	0.45	0.22	0.49	0.31
		Two Local	0.46	0.22	0.50	0.31
		Efficient SU2	0.46	0.22	0.50	0.31
		Pauli Two Design	0.32	0.28	0.34	0.28
EQNN	ZZ	Real Amplitudes	0.45	0.46	0.48	0.37
		Two Local	0.50	0.57	0.53	0.42
		Efficient SU2	0.53	0.60	0.56	0.49
		Pauli Two Design	**0.51**	**0.52**	**0.52**	**0.50**
	Pauli	Real Amplitudes	0.47	0.49	0.49	0.41
		Two Local	0.55	0.63	0.58	0.51
		Efficient SU2	0.52	0.53	0.52	0.51
		Pauli Two Design	**0.60**	**0.61**	**0.61**	**0.59**

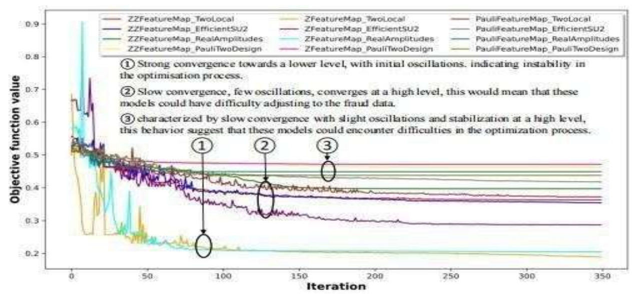


Fig. 4: EQNN loss function on the BankSim dataset

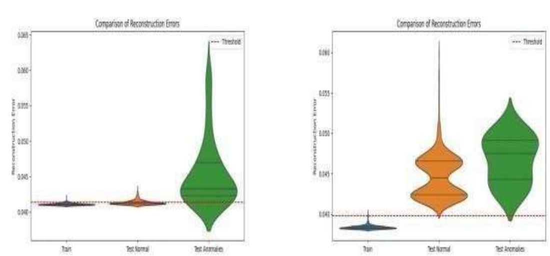
Most arrangements prove stable convergence, stabilizing after a phase of oscillations and reaching varying levels of loss. While some achieve minimal loss, others stabilize at higher values, reflecting differences in optimization effectiveness. ([3])

D. Server Machine Dataset (SMD)

The SMD dataset contains system observing data composed from 28 servers in a large data center above five weeks. It consists telemetry signals such as CPU load, disk usage, and I/O performance, making it suitable for anomaly detection research ([2]).

TABLE IV: SERVER MACHINE DATASET (SMD) ([2])

Property	Value
Machines Monitored	28 (grouped into 3 categories)
Duration	5 weeks
Features Used	load_1, disk_r, disk_svc, disk_w, disk_wb
Window Size	100 time steps (dimensionality = 500)
Labels	Provided per timestamp (normal/anomaly)
Preprocessing Applied	Split into train/test, anomalies in test set



(a) machine-1-1 (b) machine-1-5

Fig.5: Violin plots exemplifying the distribution of rebuilding errors of QAE on two different machines of the SMD dataset ([2]).

E. Microsoft Cloud Monitoring Dataset (MSCM)

The MSCM dataset is derivative from telemetry signals across Microsoft services, used for estimating anomaly detection in practical production systems. It contains 67 univariate time series with anomalies labeled by experts ([2]).

TABLE V: MICROSOFT CLOUD MONITORING DATASET (MSCM) ([2])

Property	Value
Time Series Count	67
Domains Covered	API query rates, DB latencies, crash rates
Features	Univariate telemetry signals
Labeling	Manual expert annotation
Preprocessing Applied	Removed subsets with no anomalies

V. CONCLUSION

In this research proves that the efficiency of quantum machine learning for fraud detection depends powerfully on the arrangement of feature maps, ansatz configurations, and dataset properties. While VQC and SQNN presents strong adaptability with communicative feature map–ansatz pairs ([9]), EQNN efforts with the complexity of data patterns ([4]). The proposed QAE-FD framework further improve detecting fraud by converting multi-dimensional data into quantum states, developing anomaly recognition and calculation effectiveness ([1][2]). Researchable results prove authentication of traditional models, reinforcing the potential of quantum techniques in practical financial safety. In future project will aimed the QAE-FD model in inconsistency of recognized machine learning techniques and assess its calculation effect, creating it appropriate for scalable applications in detecting fraud and expands cybersecurity domains ([1][2][6])

REFERENCES

[1] C. HUOT, S. HENG, T. K. KIM, AND Y. HAN, "QUANTUM AUTOENCODER FOR ENHANCED FRAUD DETECTION IN IMBALANCED CREDIT CARD DATASET," IEEE ACCESS, 2024.
[2] K. Tscharke, M. Wendlinger, A. Ahouzi, P. Bhardwaj, K. Amoi-Taleghani, M. Schrödl-Baumann, and P. Debus, "Quantum autoencoder for multivariate time series anomaly detection," arXiv preprint arXiv:2504.17548, 2025.
[3] U. Jabeen and K. Singh, "Implementing quantum machine learning in credit card fraud detection," in Proc.
[4] 2025 Int. Conf. Networks and Cryptology (NETCRYPT), pp. 1891– 1896, IEEE, May 2025.
[5] A. N. Basa, "The role of quantum neural networks in fraud detection: Opportunities and challenges," [Online]. Available: (publisher/source not specified).
[6] E. Canonici and F. Caruso, "QUBO-based SVM for credit card fraud detection on a real QPU," arXiv preprint arXiv:2409.11876, 2024.
[7] M. Cardaioli, L. Marangoni, G. Martini, F. Mazzolin, L. Pajola, A. F. Parodi, … and M. C. Vernillo, "FD4QC: Application of classical and quantum-hybrid machine learning for financial fraud detection – A technical report," arXiv preprint arXiv:2507.19402, 2025.
[8] T. K. Behera and S. Panigrahi, "Credit card fraud detection: A hybrid approach using fuzzy clustering and neural network," in Proc. 2015 2nd Int. Conf. Advances in Computing and Communication Engineering (ICACCE), pp. 494–499, IEEE, May 2015.
[9] C. Pati, "Fraud detection using hybrid classical- quantum machine learning," 2023. [Online]. Available: (publisher/source not specified).
[10] F. Atban, M. Y. Küçükkara, and C. Bayılmış, "Enhancing variational quantum classifier performance with meta-heuristic feature selection for credit card fraud detection," Eur. Phys. J. Special Topics, pp. 1–14, 2025.
[11] M. A. Nielsen and I. L. Chuang, Quantum Computation and Quantum Information, 10th Anniversary ed. Cambridge, U.K.: Cambridge Univ. Press, 2010.