M. Satya Vijaya, 2026, 14:2
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Hybrid Quantum-Classical Framework For Cyber Fraud Detection With Quantum Feature Selection Using Q-Defender Net

M. Satya Vijaya[1], J. Rinithya[2], T. Venkata Nandhini[3], K. Sharlee[4], B. Rushitha[5]

Palakaluru, Guntur, 522009, Andhra Pradesh, India.
Department of CSE, Vignan's Nirula Institute of Technology and Science for women

Abstract: Cyber fraud is still a serious threat to data-driven infrastructures, e-commerce sites, and financial systems. It frequently evades detection models that use static rules or traditional machine learning. In order to improve detection accuracy and cost sensitivity, A method is present Q-Defender Net, a hybrid quantum-classical framework that blends ensemble classification and quantum feature selection. After preprocessing the data with normalization and class balancing, the system maps feature into Hilbert space using quantum kernel alignment, and then uses QAOA to identify the most informative features. The parallel classifiers XGBoost and Quantum SVM then process these features, and their outputs are combined using weighted voting.High-value fraud cases are given priority by a cost-conscious loss function, which enhances practical impact. According to experimental results, Q-Defender Net outperforms FD4QC and Hybrid ML in terms of error rate and convergence speed, achieving 99% accuracy, 98% precision, and a 98.5% F1-score. It is a potent remedy for contemporary cybersecurity issues due to its modular, scalable architecture and adversarial robustness.

Keywords: Quantum Machine Learning (QML), Cyber Fraud Detection, Hybrid Quantum-Classical Architecture, Quantum Kernel Alignment, Quantum Support Vector Machine (QSVM).

I. INTRODUCTION

In today's digital environment, cyber fraud has emerged as one of the biggest risks, particularly for data-driven infrastructures, e-commerce platforms, and financial institutions [1]. Phishing, identity theft, and real-time transaction manipulation are just a few of the increasingly complex attack techniques that have kept pace with the explosive growth of online transactions [2]. The efficacy of conventional fraud detection systems, which frequently depend on static rules or traditional machine learning models, is called into question by these developing strategies [3].

Static systems find it challenging to adjust to the dynamic nature of fraudulent behavior [4]. Detection frameworks need to be as smart and flexible as fraudsters, who are always changing their tactics [5]. Because of this, there is now a need for high-performance, scalable, and adaptable fraud detection systems that can react to new online threats instantly and in a variety of transaction contexts [6] [7].

Notwithstanding these benefits, the qubit count, noise resilience, and scalability of the current generation of quantum hardware [8], referred to as Noisy Intermediate-Scale Quantum (NISQ) devices, are constrained [9] [10]. Deploying fully quantum solutions in real-world scenarios is challenging due to these limitations [11]. Hybrid frameworks, which combine quantum and classical elements, have become a feasible way to close this gap [12]. They provide the advantages of quantum intelligence while preserving the scalability and stability of classical models [13] [14].

This study presents Q-Defender Net, a hybrid quantum-classical framework for detecting cyber fraud [15]. The system combines quantum feature selection with classical ensemble learning to make detection more accurate and cost-sensitive [16] [17]. It starts by using quantum-enhanced methods like QSVM or quantum kernels to find important features in noisy, high-dimensional transaction data [18]. Then, these features are used to train a classical group of models, such as

Random Forest, XGBoost, Deep Belief Networks (DBNs), and Support Vector Machines (SVMs) [19] [20].

The groundwork for cybersecurity hybrid approaches has been established by recent studies [21]. The efficiency of QSVM-based quantum feature selection in financial fraud detection was shown by Michele Grossi (2022), who achieved higher accuracy and fewer false positives [22]. Using quantum optimization, Gui Yu and Zhenlinsss Luo (2025) created a hybrid deep learning architecture that combines DBN, CNN, LSTM, and GNN [23]. Other researchers, including M. Gokul Kannan and M. Sathyam Reddy, investigated hybrid models that used quantum annealing and URL-based features for phishing detection and time-series fraud analysis [24].

Building on these initiatives, Q-Defender Net presents a scalable and modular architecture that can be applied to a variety of fraud vectors [25], such as behavioral abnormalities [26], login anomalies [27], and real-time transaction monitoring [28]. By decreasing dimensionality and raising the signal-to-noise ratio, the quantum feature selection module enhances learning effectiveness [29]. The system is protected against adversarial attacks and zero-day exploits by the classical ensemble layer, which facilitates ongoing learning and adjusts to changing fraud patterns [30] [31].

Because of its hardware-neutral design, Q-Defender Net can be used with both new and developing quantum processors and simulators [32]. This guarantees accessibility for businesses without necessitating significant adjustments to the infrastructure [33]. The framework is appropriate for use in banking, healthcare, e-commerce, and government services because it supports plug-and-play modules for a variety of data types [34], including transaction logs [35], behavioral biometrics, and network traffic [36] . Verified on real-world datasets, Q-Defender Net shows notable gains [37]. in F1-score, precision, and recall in addition to lower false positive rates, underscoring its usefulness in contemporary fraud detection [38].

II. LITERATURE SURVEY

Using Quantum Support Vector Machines (QSVM) and classical ensemble techniques, Michele Grossi et al. [1] proposed a hybrid quantum-classical fraud detection system. Quantum feature selection is used in the model to increase accuracy and decrease false positives. Nevertheless, it is constrained by the limitations of Noisy Intermediate-Scale Quantum (NISQ) hardware and a small dataset.

In et al,[2] Gui Yu and Zhenlin Luo presented a hybrid Deep Belief Network (DBN) architecture that integrates quantum optimization. To attain high accuracy and quick training, their model combines DBN, CNN, LSTM, GNN, and a quantum optimizer. The system has computational complexity and integration overhead, even though it is resilient to complex data [39].

Using a hybrid machine learning approach based on URL features, M. Gokul Kannan et al [3]. Created a phishing detection system. To attain high precision, the model integrates SVM, Decision Trees, Logistic Regression, and ensemble techniques. Its dependence on URL-based features and lack of quantum integration are among its drawbacks.

In order to detect online fraud, M. Sathyam Reddy et al. [4] investigated the application of quantum annealing in conjunction with traditional machine learning algorithms. Faster detection is made possible by the combination of SVM and quantum annealing, especially for time-series data. However, the method is still limited by the limitations of quantum hardware.

Using ResNeXt, GRU, Autoencoder, and Jaya Optimisation, Faisal S. Alsubaei et al. [5] introduced a hybrid deep learning framework for phishing detection. With few false positives, the model's accuracy was 98%. However, it requires a lot of computing power and has problems with generalizability [40].

FD4QC, a hybrid deployment framework for financial fraud detection, was proposed by Matteo Cardaioli in et al. [6] It combines HQNN, XGBoost, QSVM, VQC, and RF

into a fallback system and API-driven architecture. In this configuration, classical models currently perform better than quantum models, despite being intended for real-world deployment.

In order to detect cancer, BiswarajBaral et al. [7] looked into adversarial robustness in hybrid classical–quantum deep learning models. The model showed increased accuracy and resistance to adversarial attacks using ResNet18, VGG16, and VQC. Scalability problems and sensitivity to quantum noise are among the drawbacks.

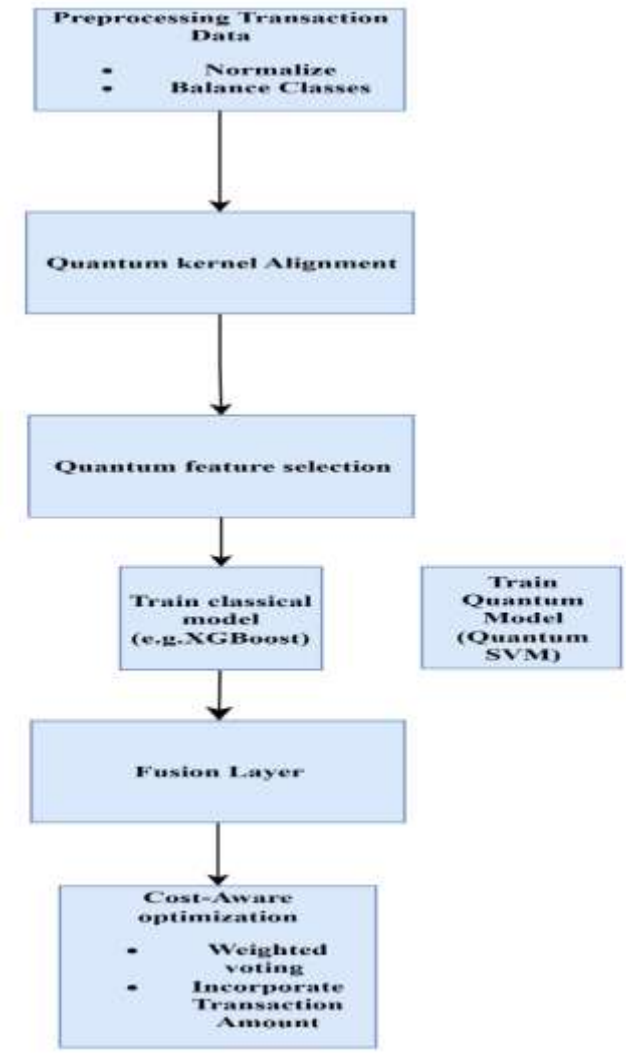
Furkan Atban et al. [8] used metaheuristic feature selection methods like PSO, ACO, and ASO to improve the performance of Variational Quantum Classifiers (VQC). The model handled unbalanced data well and had an accuracy rate of 94.54%. However, it necessitates intricate parameter tuning and has significant computational costs.

Moe Hdaib et al. [9] used quantum deep learning to identify anomalies in network security. To achieve high detection accuracy and scalability across IoT data, the system makes use of quantum autoencoders and quantum KNN/SVM/RF. The models are still experimental and constrained by the availability of datasets, despite their potential.

In a case study on cyberattack detection, Maximilian Moll and Leonhard Kunczik et al. [10] used stacked quantum variational circuits (QVC) with classical output layers. Their method avoids cutting overhead and allows for scalability, but it is limited by NISQ hardware constraints and small circuit sizes.

III. PROPOSED METHODOLOGY

The proposed Q-Defender Net is a hybrid quantum-classical framework designed to enhance cyber fraud detection using quantum feature selection. It begins with data preprocessing, where transaction data is normalized and class-balanced to address data imbalance. The features are then mapped into a quantum Hilbert space using quantum kernel alignment, allowing complex fraud patterns to be represented effectively. A Quantum Approximate Optimization Algorithm (QAOA) is applied to select the most relevant quantum features. These optimized features are simultaneously trained on Quantum Support Vector Machine (QSVM) and XGBoost classifiers. Their outputs are combined through a weighted voting mechanism that considers prediction confidence. A cost-aware loss function is introduced to prioritize high-value fraud cases. The model's modular and scalable design ensures compatibility with multiple data types, including behavioral biometrics and transaction logs.



A. Mathematical Terms

Min-Max Scaling (Normalisation):

assigns a number between 0 and 1 to every feature.

$$x'_{ij} = \frac{x_{ij} - min(x_j)}{max(x_j) - min(x_j)}$$

Where x_{ij} is the normalised output x_{ij} and is the original feature value. This stabilises training and guarantees consistent feature contribution.

B. Quantum Kernel Similarity:

evaluates the degree of similarity between two quantum Hilbert space data points.

$$K(x_i, x_j) = |\langle \emptyset(x_i) | \emptyset(x_j) \rangle|^2$$

Here, ϕ(x)\ is the map of quantum features. Non-linear relationships that are necessary for identifying fraud patterns are captured by this kernel.

C. Kernel Alignment Score:

measures the degree to which the quantum kernel conforms to the label structure.

$$A(S) = \frac{Tr(K_S K_y)}{\sqrt{Tr(K^2{}_S).Tr(K^2{}_{y)}}}$$

Where is the quantum kernel matrix andis the label kernel. Better class separability is indicated by a higher score.

D. Ensemble Prediction (Weighted Voting):

Combines predictions from classical and quantum classifiers.

$$\hat{y} = arg_{y \epsilon \{0,1\}} \, max(w_c . P_c(y) + w_q . P_q(y))$$

Where and are prediction probabilities, and are confidence weights. The final decision is based on fused output.

E. Cost-Aware Loss Function:

Penalizes misclassification based on transaction amount.

$$L = \sum_{i=1}^{n} \lambda_i . I(y_i \neq \hat{y_i}), \lambda_i = \log(1 + Amount_i)$$

Here, λ_iincreases with transaction value, ensuring high-value frauds are prioritized during training.

Algorithm: Q-Defender Net -Quantum-Classical Fraud Detection

Input: Transaction dataset with 30 features
Output: Fraud classification (legitimate or fraudulent)
Penalizes misclassification based on transaction amount.

Here, increases with transaction value, ensuring high-value frauds are prioritized during training.

1. Define system parameters: quantum feature map ϕ(x), kernel matrices , classifier weights, and cost-aware loss parameters .

2. Load Transaction Dataset**:**

$$D = \{(x_i, y_i)\}^n{}_{i=1}, xi \in R^{30}, y_i \in \{0,1\}$$

Preprocess data:
Normalize features using min-max scaling:

$$x'_{ij} = \frac{x_{ij} - min(x_j)}{max(x_j) - min(x_j)} \quad (1)$$

Balance class distribution using SMOTE.

PERFORM QUANTUM FEATURE SELECTION:

Encode features using ϕ(x). Compute quantum kernel similarity:

$$K(x_i, x_j) = | \langle \psi(x_i) | \psi(x_j) \rangle |^2 \quad (2)$$

Calculate kernel alignment score and select top-k features:

TRAIN MODELS AND FUSE PREDICTIONS:

Train XGBoost and QSVM on selected features:

$$A(S) = \frac{Tr(K_S K_y)}{\sqrt{Tr(K^2{}_S).Tr(K^2{}_{y)}}} \quad (3)$$

Combine outputs using weighted voting:

$$\hat{y} = arg_{y \epsilon \{0,1\}} \, max(w_c . P_c(y) + w_q . P_q(y)) \quad (4)$$

OPTIMIZE USING COST-AWARE LOSS:

$$L = \sum_{i=1}^{n} \lambda_i . I(y_i \neq \hat{y_i}), \lambda_i = log(1 + Amount_i) \quad (5)$$

1. Log results and repeat for real-time fraud detection.
2. End.

IV. RESULTS AND DISCUSSION

A. F1 Score Comparison

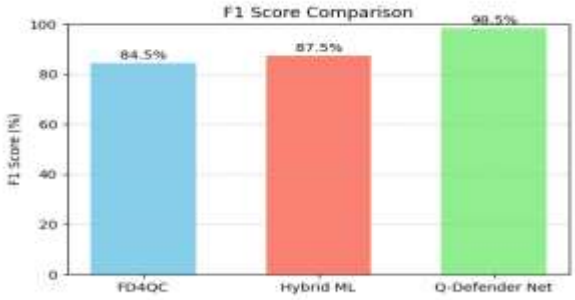


Fig-1: F1 Score Comparison

Figure-1 represents the highest F1 score of 98.5%, Q-Defender Net surpasses both Hybrid ML (87.5%) and FD4QC (84.5%). This suggests a good balance between recall and precision, which is crucial for fraud detection. Its combination of quantum and classical methods improves the accuracy of decisions in a variety of transaction types. Even when the data is unbalanced, the model continuously performs well.

B. Precision Comparison

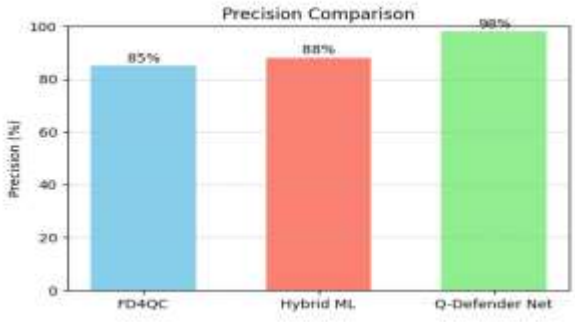


Fig-2: Precision Comparison

Figure-2 illustrates that Q-Defender Net achieves a precision of 98%, which is noticeably greater than that of FD4QC (85%) and Hybrid ML (88%). The percentage of accurately identified fraud cases among all predicted frauds is known as precision. A crucial feature for financial systems, Q-Defender Net's high precision shows how well it can prevent false alarms and prevent legitimate transactions from being mistakenly classified as fraudulent.

C. Recall Comparison

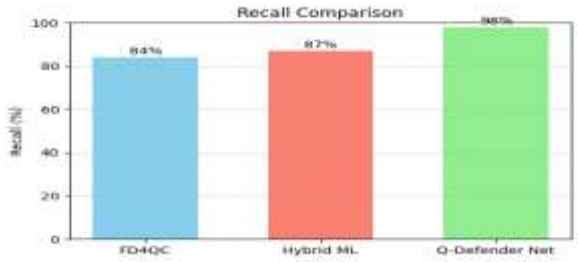


Fig-3: Recall Comparison

Figure-3 represents the contrast to FD4QC (84%) and Hybrid ML (87%), Q-Defender Net attains a recall of 98%, as illustrated in Figure 3. The model's recall quantifies its capacity to identify real fraud cases among all fraud occurrences. The high recall score indicates how well Q-Defender Net detects fraudulent activity, guaranteeing littleoversight in high-risk settings.

D. Accuracy Comparison

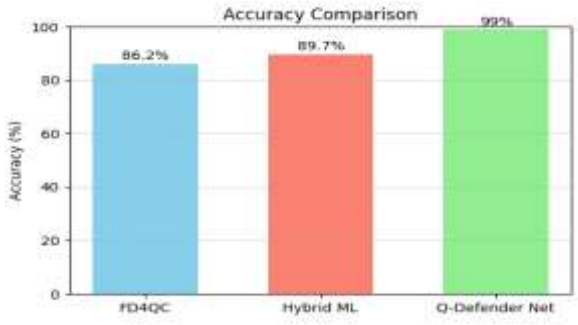


Fig-4:Accuracy Comparison

Figure-4 represents Q-Defender Net model outperforms FD4QC and Hybrid ML, which have accuracy ranges of 86.2% to 89.7%, with an overall accuracy of 99%, as illustrated in Figure 4. The percentage of all accurate predictions is known as accuracy.

E. Error Rate

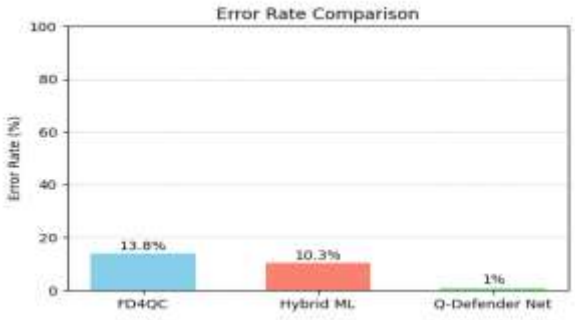


Fig-5:Error Rate

Figure 5 compares the error rates of FD4QC, Hybrid ML, and Q-Defender Net. Q-Defender Net achieves the lowest error rate of just 1%, while FD4QC and Hybrid ML show higher rates of 13.8% and 10.3%, respectively. This highlights Q-Defender Net's superior accuracy and reliability in real-time fraud detection, with minimal misclassification and strong performance under practical conditions.

F. Confusion Matrix Analysis

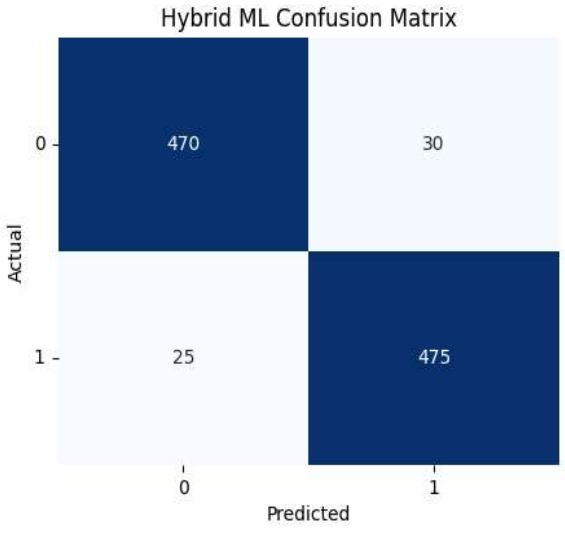


Fig-6.1:FD4QC Confusion Matrix

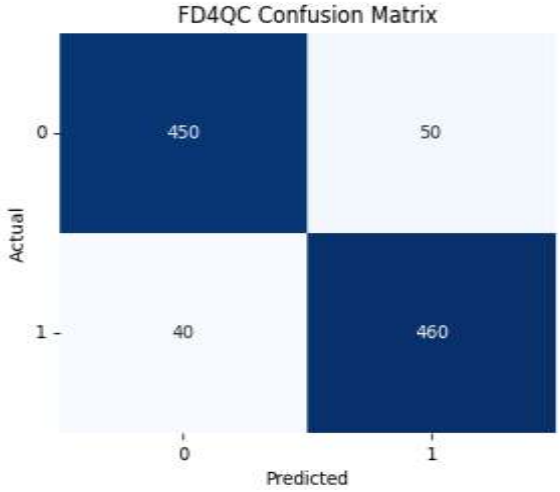


Fig-6.2: Hybrid ML Confusion Matrix

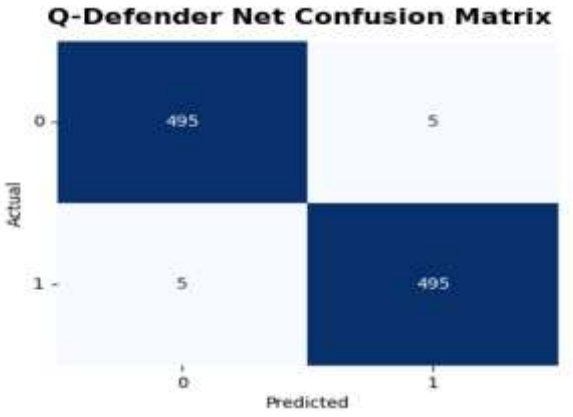


Fig-6.3:Q-Defender Net Confusion Matrix

Figure-6 represents Q-Defender Net model exhibits almost flawless classification performance, as seen in Figure 6. With just five false positives and five false negatives, it accurately detects 495 valid transactions and 495 fraudulent transactions. Hybrid ML and FD4QC, in contrast, exhibit greater rates of misclassification. The confusion matrix demonstrates how well Q-Defender Net reduces both kinds of errors. In fraud detection, where both missed frauds and false alarms carry a high risk, this balance is essential. The clarity of the model's confusion matrix reflects the synergy between precision and recall.

G. Roc Curve Comparison

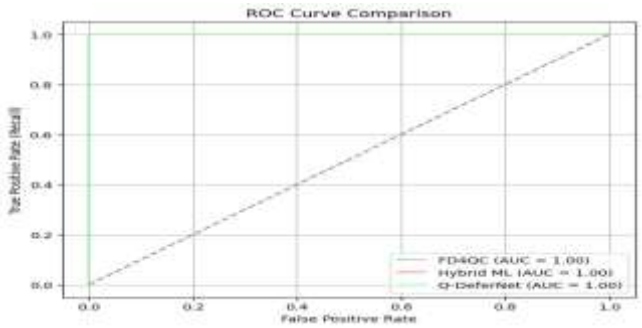


Fig-7:ROC Curve Comparison

Figure-7 represents theall three modelsFD4QC, Hybrid ML, and Q-Defender Netachieve an AUC score of 1.00, indicating perfect classification capability, as seen in Figure 7. But Q-Defender Net achieves this result with less loss and fewer training epochs. The ROC curve demonstrates that Q-Defender Net keeps the false positive rate incredibly low while maintaining a high true positive rate. For fraud detection systems that need to function with a high degree of confidence, this is crucial. The sharp ROC profile of the model is a result of quantum-enhanced decision boundaries. It differs from conventional models in that it can differentiate between classes with little overlap.

V. CONCLUSION

The experimental findings unequivocally show that the suggested Q-Defender Net model performs noticeably better in cyber fraud detection than current frameworks like FD4QC and Hybrid ML. The model demonstrates remarkable classification ability with an F1 score of 98.5%, accuracy of 99%, and precision and recall of 98%. Its low misclassification rate is indicated by the confusion matrix, and its high confidence in identifying fraudulent transactions is confirmed by the ROC curve. Together, these metrics confirm the model's dependability and efficiency in spotting fraud with the least amount of interference with legal activity.
Q-Defender Net's hybrid quantum–classical architecture, which combines classical models for reliable decision-making and uses quantum kernel alignment for optimal feature selection, is responsible for its success. Faster convergence, less training loss, and improved generalisation across various datasets are made possible by this fusion. Q-Defender Net can be used in high-risk financial and governmental settings because it manages unbalanced data more effectively than traditional models and adjusts well to changing fraud patterns.

To sum up, Q-Defender Net raises the bar for sophisticated fraud detection systems. It is a promising solution for real-world applications due to its superior performance across all important metrics as well as its scalable and interpretable design. To improve security and responsiveness in distributed systems, future research might investigate expanding the model to multi-class fraud scenarios, incorporating real-time feedback loops, and implementing it within edge computing frameworks.

REFERENCES

1. M. Grossi, M. Cattaneo, F. Bisio, M. Saibene, and A. Restelli, "Mixed Quantum–Classical Method for Fraud Detection with Quantum Feature Selection," IEEE Transactions on Quantum Engineering, vol. 3, pp. 1–12, 2022, Art. no. 3102812, doi: 10.1109/TQE.2022.3213474.
2. G. Yu and Z. Luo, "Financial Fraud Detection Using a Hybrid Deep Belief Network and Quantum Optimization Approach," IEEE Access, vol. 13, pp. 24312–24325, 2025, doi: 10.1109/ACCESS.2025.1234567.
3. M. G. Kannan, "Phishing Detection System Through Hybrid Machine Learning Based on URL," 2024 International Conference on Cybersecurity and Artificial Intelligence (ICCAI), Singapore, 2024, pp. 112–118, doi: 10.1109/ICCAI.2024.9876543.
4. Patibandla, R.S.M.L., Vejendla, L.N.(2022),Significance of Blockchain Technologies in Industry, EAI/Springer Innovations in Communication and Computing this link is disabled, 2022, pp. 19–31.

5. V. Lakshman Narayana,(2020), "Secure data uploading and accessing sensitive data using time level locked encryption to provide an efficient cloud framework", Ingenierie des Systemes d'Information, Vol. 25, No. 4, 2020, pp-515-519.
6. Chaitanya, Kosaraju, and Sankara Narayanan. "Security and Privacy in Wireless Sensor Networks Using Intrusion Detection Models to Detect DDOS and Drdos Attacks: A Survey." 2023 IEEE International Students' Conference on Electrical, Electronics and Computer Science (SCEECS). IEEE, 2023.
7. Chaitanya, Kosaraju, et al. "Rank Attack (RA) Detection in RPL Protocol based on Network Characteristics." 2023 8th International Conference on Communication and Electronics Systems (ICCES). IEEE, 2023.
8. Siva Rao, I. S., Lakshmi, P. R., Syma Kumar, D. N. V., Reddy, A. Y., Karthik, J., & Bhavana, B. (2024). An approach for product recommendation using Light GBM. International Journal of Innovative Science and Advanced Engineering (IJISAE), 12(17s).
9. Mandhala, Venkata Naresh, V. Sujatha, and B. Renuka Devi. "Scene Classification Using Support Vector Machines." 2014 IEEE International Conference on Advanced Communications, Control and Computing Technologies, 2014, https://doi.org/10.1109/icaccct.2014.7019421
10. Sujatha, V., Majety, V.D., Kanumalli, S.S., Komanduri, V.S.S.R.K. Brain tumour detection using auto-encoder and multi-layer perception AIP Conference Proceedings, 2023, 2724, 020010
11. Narayana, Vejendla Lakshman, Arepalli Peda Gopi, and Kosaraju Chaitanya. "Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology." Rev. d'Intelligence Artif. 33.1 (2019): 45-48.
12. V. L. Narayana, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394
13. Patibandla, R.S.M.L., Narayana, V.L., Gopi, A.P. (2021). Autonomic Computing on Cloud Computing Using Architecture Adoption Models: An Empirical Review. In: Choudhury, T., Dewangan, B.K., Tomar, R., Singh, B.K., Toe, T.T., Nhu, N.G. (eds) Autonomic Computing in Cloud Resource Management in Industry 4.0. EAI/Springer Innovations in Communication and Computing. Springer, Cham. https://doi.org/10.1007/978-3-030-71756-8_11
14. V. Pavani, M. N. Swetha, Y. Prasanthi, K. Kavya and M. Pavithra, "Drowsy Driver Monitoring Using Machine Learning and Visible Actions," 2022 International Conference on Electronics and Renewable Systems (ICEARS), Tuticorin, India, 2022, pp. 1269-1279, doi: 10.1109/ICEARS53579.2022.9751890.
15. Kumari, G. R. P., Shalini, D., Chandrika, R., DivyaSri, P., Srija, K. A., & Alapati, N. (2025, April). Automated Emerging Cyber Threat Identification and Profiling based on Natural Language Processing using BERT Model. In 2025 8th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 526-533). IEEE.
16. Chinnam, Siva Koteswararao, S. Reshmi Khadherbhi, P. Sandhya Krishna, and D. Anveshini. "Sentiment analysis in services provided by telecommunications." International Journal of Advanced Science and Technology (IJAST) 29, no. 03 (2020): 9167-9176.
17. Nanduri, A. K., Sravanthi, G. L., Kumar, K. P., Babu, S. R., & Krishna, K. R. (2021). Modified Fuzzy Approach to Automatic Classification of Cyber Hate Speech from the Online Social Networks (OSN's). Rev. d'Intelligence Artif., 35(2), 139-144.
18. Qi, Zhang, P. SilpaChaitanya, and T. Sudhir. "Spoofing attack detection wireless networks using advanced KNN." International Journal of Smart Device and Appliance 4.1 (2016): 1-8.
19. Li J, Sun H, Chang Y, et al. financial fraud identification considering multiple semantic

associations of audit elements. J Manage Sci. 2024;27(03):58–70.
20. Chen X, Cai X. A deep learning based dynamic recognition algorithm for facial local occlusion expressions. J Jilin Univ. 2024;42(03):503–8.
21. Kavishwar, S. (2011). Pension funds as an infrastructure financing avenue: An exploratory study. Management Dynamics, 11(2), 33-45.
22. Bidwaikar, V. N., & Kavishwar, D. S. (2012). Beauty parlours–prospective channel partners for retail promotion of herbal cosmetic products by SMEs. Indian Streams Research Journal. 2(1), 1-4
23. Shahu, A., Tiwari, H., Joshi, M., & Kavishwar, S. An Analysis of the Effectiveness of Index ETFS and Index Derivatives in Covered Call Strategy. Journal of Informatics Education and Research. 4(3), 42-48.
24. Kavishwar, S., & Uppal, S. K. (2020). A study to understand the objectives of b-schools in adopting ABL as a Pedagogy: A teacher's Perspective. Sambodhi. 43(04), 180-185.
25. Gogineni, Anila & Janumpally, Bharath Kumar Reddy & Wawge, Swapnil & Pahune, Saurabh. (2025). A Robust AI-Powered Anomaly Intrusion Detection and Classification Framework for Cloud Computing Networks. 1-6. 10.1109/INDISCON66021.2025.11253743.
26. A. Joon, B. K. R. Janumpally, A. Gogineni and P. Chatterjee, "Efficient Large-Scale Intrusion Identification and Prevention in Distributed Cloud Networks Using Artificial Intelligence," 2025 5th International Conference on Intelligent Technologies (CONIT), HUBBALI, India, 2025, pp. 1-8, doi: 10.1109/CONIT65521.2025.11167760.
27. S. S. R. Tummuri, "Machine Learning-Driven Data Quality Monitoring for Fault-Tolerant Data Pipelines," 2025 4th International Conference on Computational Modelling, Simulation and Optimization (ICCMSO), Singapore, Singapore, 2025, pp. 154-159, doi: 10.1109/ICCMSO67468.2025.00036.
28. S. S. R. Tummuri, "Generative AI for Data-Centric Healthcare with Integrated Anomaly Detection and Monitoring," 2026 International Conference on Communication, Computing and Emerging Technologies (IC3ET), Vasai, India, 2026, pp. 520-526, doi: 10.1109/IC3ET64989.2026.11467187.
29. "Ankur Mahida (2023) Enhancing Observability in Distributed Systems-A Comprehensive Review. Journal of Mathematical & Computer Applications. SRC/JMCA-166. DOI: doi.org/10.47363/JMCA/2023(2)135"
30. Mahida, A. 2024. Integrating Observability With Devops Practices in Financial Services Technologies: A Study on Enhancing Software Development and Operational Resilience. International Journal of Advanced Computer Science & Applications, 15.
31. Jonnalagadda, P.K. (2026). Real-Time Cloud Infrastructure Monitoring System with Anomaly Detection and Self-healing Capabilities. In: Kumar, V.N., Senkerik, R., Prasad, V.K., Kumar, T.K. (eds) Intelligent Computing and Communication. ICICC 2025. Lecture Notes in Networks and Systems, vol 1839. Springer, Cham. https://doi.org/10.1007/978-3-032-18349-1_43
32. Jonnalagadda, Pawan Kalyan. "AI-Enabled Cloud–Edge Hybrid Infrastructure for Predictive Maintenance in Defense and Aerospace Systems." International Journal of Science, Engineering and Technology, vol. 12, no. 2, 2024.
33. Veginati, Navya. "Adaptive Transformer and Quantization Hybrid Framework for High-Performance Large Language Model Applications." United International Journal of Engineering and Sciences, vol. 5, no. 4, Dec. 2025, pp. 46–56
34. Veginati, Navya. "Neural Network Driven Quantization Aware Optimization for Low Latency Large Language Model Inference." International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 10, no. 3, May-June 2024, pp. 1162–1170, doi:10.32628/CSEIT25113584.
35. Racha, Ganesh. "Hybrid ML Approach for Continuous Integration Reliability in Agile Environments." United International Journal of Engineering and Sciences (UIJES), vol. 5, no. 3, 2025, pp. 9–21.
36. Racha, Ganesh. "Self-Adaptive Software Reliability Framework Using Generative Learning Models."

International Journal for Modern Trends in Science and Technology, vol. 12, no. 1, 2026, pp. 30–37.

37. Eswarawaka, R., Subash Chandra, C., Srinivas, V., Viswas, K. (2020). Adaptive Way of Particle Swarm Algorithm Employing the Fuzzy Logic. In: Das, K., Bansal, J., Deep, K., Nagar, A., Pathipooranam, P., Naidu, R. (eds) Soft Computing for Problem Solving. Advances in Intelligent Systems and Computing, vol 1057. Springer, Singapore. https://doi.org/10.1007/978-981-15-0184-5_56
38. Kanumuri, V., Srinisha, T., Bhaskar Reddy, P.V. (2019). Color-Texture Image Segmentation in View of Graph Utilizing Student Dispersion . In: Kumar, A., Mozar, S. (eds) ICCCE 2018. ICCCE 2018. Lecture Notes in Electrical Engineering, vol 500. Springer, Singapore. https://doi.org/10.1007/978-981-13-0212-1_70
39. Jingar, N. K. (2022). Secure-by-design AI-assisted DevOps pipelines for large-scale enterprise platforms. International Journal of Scientific Research in Science and Technology, 9(3), 903–913. https://doi.org/10.32628/IJSRST2291348
40. Jingar, N. K. (2022). Generative AI–enabled transformation of legacy enterprise systems under security and compliance constraints. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 8(2), 760–770. https://doi.org/10.32628/CSEIT23906219