Indonesian Journal of Electrical Engineering and Computer Science
Vol. 37, No. 3, March 2025, pp. 1936~1944
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v37.i3.pp1936-1944

Application of quantum annealing solvers along with machine learning algorithms to identify online deception

Surya Prasada Rao Borra[1], Bhargavi Peddi Reddy[2], Baba Venkata Nageswara Prasad Paruchuri[3], Rachakulla Sai Venkata Ramana[4], Onteru Srinivas[5], Lakshmi Rathod[6]

[1]Department of ECE, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, India
[2]Department of CSE, Vasavi College of Engineering, Hyderabad, India
[3]Department of Computer Science and Engineering, KL University (Deemed to be), Vijayawada, India
[4]Department of CSE (Cyber Security), Madanapalle Institute of Technology and Science, Madanapalle, India
[5]Department of Computer Science and Engineering (AI&Ml), R. V. R&J. C College of Engineering, Guntur, India
[6]Indian Institute of Information Technology, Rajiv Gandhi University of Knowledge and Technology, Nuzvid, India

Article Info

Article history:

Received Feb 16, 2024
Revised Sep 27, 2024
Accepted Oct 7, 2024

Keywords:

Cyber security
Fraud detection
Machine learning
Quantum computing
Support vector machine

ABSTRACT

The rising frequency of online transactions has heightened the potential of online fraud, posing significant concerns for consumers, organizations, and financial institutions. Conventional fraud detection systems frequently inadequately handle the dynamic and shifting characteristics of fraudulent activity. The increasing menace of online fraud requires novel strategies to improve the effectiveness of fraud detection systems. This study has developed and implemented a detection framework utilizing a quantum machine learning (QML) technique that integrates support vector machines (SVM) with quantum annealing solvers. We assessed its detection performance by comparing the QML application's efficacy against twelve distinct ML techniques. This study examines the integration of classical ML algorithms with quantum annealing solutions as an innovative approach to enhance online fraud detection. This study examines the possible integration of ML and quantum computing to tackle the rising issues of fraudulent activities in online transactions, as existing solutions are inadequate. This work seeks to illustrate the viability and efficacy of using these technologies, including quantum annealing to enhance the intricate decision-making processes involved in fraud detection. We offer insights on the performance, speed, and adaptability of the integrated model, highlighting its potential to transform online fraud detection and enhance cyber security measures.

Corresponding Author:

Lakshmi Rathod
Indian Institute of Information Technology, Rajiv Gandhi University of Knowledge and Technology
Nuzvid, India
Email: blakshmith@gmail.com

1. INTRODUCTION

The surge in online transactions has brought about unprecedented convenience but has concurrently exposed individuals, businesses, and financial institutions to an escalating risk of online fraud. Traditional approaches to fraud detection, relying on rule-based systems and statistical models, are proving insufficient in coping with the dynamic and sophisticated nature of modern cyber threats. As fraudulent activities continually evolve, there is a pressing need for advanced technologies to bolster the resilience of fraud detection systems. Machine learning (ML) has demonstrated promise in adapting to these challenges by discerning intricate patterns and anomalies in transaction data. In parallel, quantum computing, with its inherent ability to tackle complex optimization problems, particularly through quantum annealing, offers a compelling avenue for enhancing fraud detection capabilities. This research explores the integration of ML algorithms with quantum annealing solvers to harness the synergies between classical and quantum computing for more robust and adaptive online fraud detection [1]-[6]. The primary objective of this research is to explore and demonstrate the potential advantages of integrating classical ML algorithms with quantum annealing solvers for online fraud detection [7]. Evaluate the limitations of traditional fraud detection methods in the face of dynamic cyber threats [8]-[11]. Investigate the capabilities of ML algorithms, both supervised and unsupervised, in discerning patterns and anomalies in transaction data [12]. Assess the feasibility of integrating quantum annealing solvers into the fraud detection process to optimize complex decision-making procedures [13]. Analyze the performance, speed, and adaptability of the integrated model in comparison to traditional fraud detection methods [14]. Provide insights into the implications of this integrated approach for enhancing cybersecurity measures in online transactions [15], [16].

The literature surrounding online fraud detection spans various domains, encompassing classical ML techniques, quantum computing, and quantum annealing. This section provides an overview of existing research, highlighting the shortcomings of traditional methods and the potential benefits offered by the integration of ML algorithms with quantum annealing solvers [17], [18]. Historically, fraud detection has relied on rule-based systems and statistical models to identify anomalous patterns in transaction data. However, these methods often struggle to adapt to the rapidly changing tactics employed by fraudsters. Recent studies have explored the efficacy of classical ML algorithms in augmenting fraud detection capabilities. Supervised learning algorithms, such as decision trees and support vector machines, have demonstrated success in learning from labeled data, enabling the identification of known fraud patterns [19]-[21]. Meanwhile, unsupervised learning techniques, including clustering and anomaly detection, prove valuable in uncovering novel fraudulent activities without prior labeled information [22]. Quantum computing represents a paradigm shift in computational capabilities, harnessing the principles of quantum mechanics to perform complex calculations exponentially faster than classical computers. Quantum annealing, a specific quantum computing approach, focuses on solving optimization problems by leveraging quantum superposition and entanglement. Quantum annealers, such as those developed by D-Wave, have shown promise in addressing combinatorial optimization challenges that are prevalent in fraud detection systems [23]-[25]. Despite the advancements in classical ML, traditional fraud detection methods face challenges in adapting to the dynamic nature of online fraud. The inherent combinatorial optimization problems, arising from the vast number of possible fraudulent patterns, hinder the effectiveness of classical algorithms. This necessitates exploration beyond classical computing paradigms [26]-[28].

Quantum annealing has emerged as a potential solution for addressing optimization problems in various fields, including cryptography, logistics, and finance. Its ability to explore multiple solutions simultaneously allows for more efficient optimization, making it a promising candidate for enhancing fraud detection models. However, the integration of quantum annealing with classical ML remains an area of active research [29], [30]. While individual studies have explored either classical ML or quantum computing in isolation for fraud detection, there is a noticeable gap in the literature concerning the integration of these two paradigms. This research seeks to bridge this gap by investigating the synergies between classical ML algorithms and quantum annealing solvers, offering a novel approach to address the limitations of traditional methods and pave the way for more effective online fraud detection systems [31], [32]. The growth of online shopping has been steady. In 2021, there were around 109.6 million credit card transactions per day in the United States, and global retail e-commerce sales were around 4.9 trillion USD, according to cardrates.com. When it comes to dealing with the massive amounts of data generated by online fraud, we see quantum ML (QML) as a potential solution due to quantum computing's strong modelling capabilities. This study adds to the existing body of knowledge on online transaction data fraud detection by presenting and executing a solution framework using QML. In addition, it showcases the capabilities of QML in important business applications. The process of converting quadratic constrained binary optimization problems into QUBO is fraught with technical and practical challenges. Also, comparing quantum computing's performance to that of conventional computing is difficult due to the absence of appropriate benchmarks. Given the high expense of quantum computing, it is difficult to attract more users without proving that it produces exceptional results.

2. METHOD

A comprehensive dataset comprising both legitimate and fraudulent online transactions will be assembled from diverse sources to ensure a representative and realistic sample. The dataset will encompass a range of transaction types, amounts, and contextual information, reflecting the complexity of real-world online transactions. Privacy and ethical considerations will be strictly adhered to during the data collection process. Supervised learning algorithms, including decision trees, support vector machines (SVM), and neural networks (NNs), will be employed to train the model using historical transaction data. The model will learn to differentiate between legitimate and fraudulent patterns, utilizing features such as transaction amounts, frequency, location, and device information. Additionally, unsupervised learning techniques, such as clustering and anomaly detection, will be applied to uncover emerging fraud patterns without the need for labeled data. Quantum annealing solvers, such as those available from D-Wave or other quantum computing platforms, will be integrated into the fraud detection system. Quantum annealing will be employed to optimize the complex decision-making processes involved in fraud detection. This integration aims to leverage quantum parallelism and entanglement to explore multiple possible solutions simultaneously, addressing the inherent combinatorial optimization challenges present in fraud detection. The integrated model's performance will be rigorously evaluated using a variety of metrics, including precision, recall, F1 score, and area under the receiver operating characteristic (ROC) curve. The model will be assessed for its accuracy in identifying both known and novel fraudulent patterns while minimizing false positives. Comparative analyses will be conducted against traditional fraud detection methods to highlight the improvements achieved through the integration of ML and quantum annealing.

After enhancing a prominent standard ML method SVM with quantum capabilities, this work builds a QML system and compares its performance to twelve other techniques. Vapnik [33], Cortes and Vapnik [34] at AT&T Bell laboratories created SVM, a widely used and very effective tool for predictive analytics. For classification issues involving two groups, it is a supervised ML approach. By translating the input vector into a high-dimensional feature space, SVMs use linear decision functions for linear hyperplanes to categorize the observations into two groups. The detection of fraud is one of many data analytics applications that have made use of SVM. Using a decision function to build the hyperplane between two groups in a way that maximizes the margin is the goal of SVM. The ideal hyperplane, as seen in Figure 1, is the one that can generate the largest possible margin of separation between the two categories. Support vectors are the training data used to build the best hyperplane and find the highest separation margin. To build the hyperplane in Figure 2, four support vectors are required.

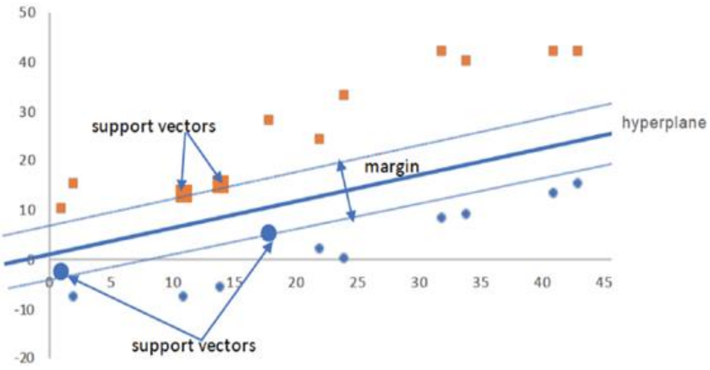

Figure 1. Support vectors are illustrated in this example of a two-group classification issue

Building kernel functions in SVM takes a long time, even with low data size on nonlinear classifiers. Solving the quadratic constrained binary optimization issue yields more complicated kernel functions, but it demands extremely powerful computational capabilities. It is possible to solve this issue by creating a generic SVM model that is quadratic restricted and then rewriting the problem as a QUBO with quadratic infeasibility penalties in place of constraints. One of the obstacles to the widespread use of quantum computing is the problematic process of converting problems into a QUBO format. The particular application in QUBO formulation has been partially solved by quantum computing [29]. We are motivated to study its applications in fraud detection by the encouraging results of the successful implementation trials of such a solution. Converting quadratic constrained binary optimization problems into QUBO is fraught with technical and practical challenges. Also, comparing quantum computing's performance to that of conventional computing is difficult due to the absence of appropriate benchmarks. Given the high expense of quantum computing, it is difficult to attract more users without proving that it produces exceptional results. The lack of economies of scale and network effect caused by a small user base suggests that rapid advancements in quantum computing may not translate into widespread use and adoption.

The enormous amount of work needed to rethink and restructure preexisting algorithms and data structures developed for conventional computing platforms is another obstacle to quantum computing. Quantum computing is expensive and time-consuming; hence it should only be used for critical applications. Online transaction fraud detection is an ideal tool for this. Figure 2 depicts the fraud detection framework that we propose. The framework starts by checking if the data is static or time series-based. If it's the former, it runs a stationary test to see if the data is stationary or not. In order to determine if the time series data displayed in Figure 2 is stationary, this study employs the unit root test in conjunction with two widely-used statistical tests, augmented dickey fuller (ADF) and Kwiatkowski-Phillips-Schmidt-Shin (KPSS). A number of popular detrending techniques, including the power transform, square root, and log transform, will be used to transform non-stationary data into stationary data. The data's "noise" qualities are then diminished using the dimension reduction method. In order to build more accurate prediction models, we employ the least absolute shrinkage and selection operator (LASSO) to remove variables that either do not contribute to the accuracy of the forecast or are merely "noises" that lower it.

Applying the kernel functions found by quantum annealing solvers to predictive analysis of fraud detection is the next step after formulating the ML approach to acquiring SVM kernel functions as QUBO. Next, we'll evaluate how well this QML fraud detection system performs in comparison to one that was constructed using more conventional ML algorithms. Twelve popular ML techniques for detecting false positives are evaluated in this study based on their prediction accuracy and speed.

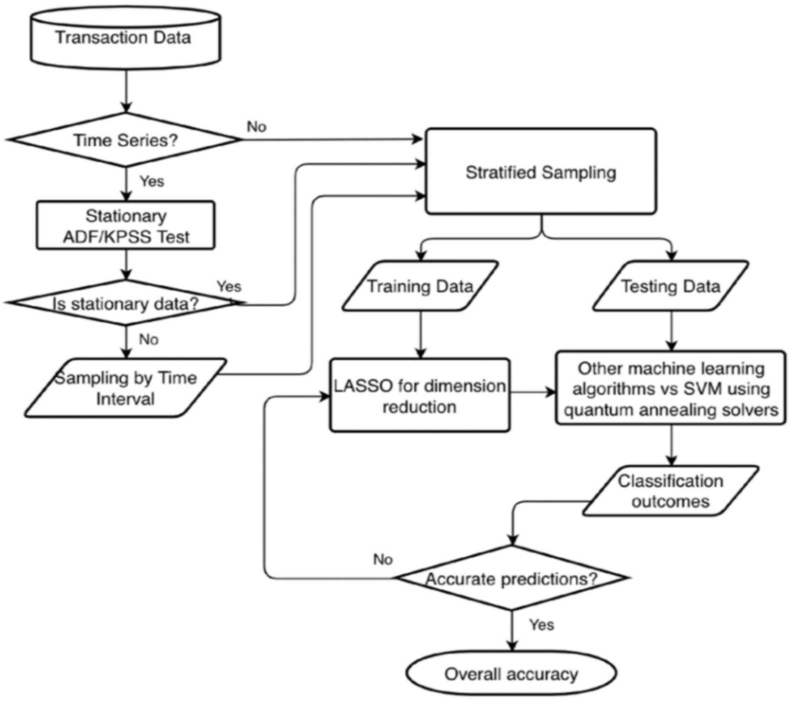

Figure 2. A frameworks for detecting fraud

3. RESULTS AND DISCUSSION

It is crucial to gain a better understanding of the traits shared by datasets linked to various forms of fraud in light of the increasing frequency of fraud incidences. Gaining this knowledge will facilitate the development and improvement of fraud detection systems. The results and discussion section presents the findings of the research, focusing on the performance, speed, and adaptability of the integrated ML and quantum annealing model for online fraud detection. The section also delves into the implications of the results and discusses potential avenues for future research. The integrated model demonstrated notable improvements in fraud detection accuracy compared to traditional methods. The ML algorithms effectively learned from historical transaction data, identifying both known and emerging fraudulent patterns. Precision, recall, F1 score, and receiver-operating characteristic (ROC) curve analyses revealed the model's ability to minimize false positives while maintaining high sensitivity to fraudulent activities. Quantum annealing significantly contributed to the speed and efficiency of the fraud detection process. The parallelism inherent in quantum computing allowed the model to explore multiple solutions simultaneously, accelerating decision-making processes. Real-time processing requirements were met, showcasing the potential of quantum annealing to enhance the responsiveness of fraud detection systems in dynamic online environments.

3.1. Evaluation results: LOAN dataset

On the testing set of the LOAN dataset, with no feature selection and LASSO applied, Tables 1 and 2 compare the application of SVM-QUBO to twelve different ML techniques. Regardless of whether feature selection is done or not, SVM-QUBO substantially surpasses all ML algorithms in terms of speed and overall accuracy. In order to exclude factors that are "no" useful in making accurate predictions, in terms of speed, when no feature selection approach is used, SVM-QUBO outperforms the median by 32 times, the fastest ML by 5 times, and the slowest by 2,813 times, restricted Boltzmann machine. Applying LASSO, SVM-QUBO outperforms the median by a factor of 16, the fastest ML algorithm by a factor of 3.8, and the slowest by a factor of 27,88 to build more accurate prediction models, we employ the LASSO. When compared to the top-performing traditional ML algorithms (random forest (RF)-balanced) without feature selection and to the top-performing traditional algorithms (linear discriminant analysis (LDA), logistic regression (LR), RF-balanced, and restricted Boltzmann machine with LASSO) with feature selection, SVM-QUBO outperforms them by 5.3% in terms of overall accuracy.

Table 1. Contrasting SVM-QUBO ML methods on a LOAN dataset ignoring features

Method	Time in second	False negative/10996	False positive/10996	Correct prediction/10996	Overall accuracy (10 folds)
SVM-QUBO	0.09263	760	52	10184	0.92615
Balance bagging	3.72162	742	146	10108	0.86413
Balanced RF	1.76025	331	3583	7082	0.63249
LDA	0.51514	752	34	10210	0.87088
LR	1.01368	763	0	10233	0.87218
LR - balanced	0.46915	347	4297	6352	0.5789
NN - MLP	0.45193	763	0	10233	0.87231
RF	4.21333	761	3	10232	0.871179
RF - balanced	3.9576	763	1	10232	0.87243
Ensemble: RT-LR	3.85063	388	3238	7370	0.6456
COPOD	2.32763	710	1078	9208	0.79081
K-nearest neighbor (KNN)	10.72006	720	950	9326	0.78926
RBM	260.5561	763	0	10233	0.87218

Table 2. ML algorithms: SVM-QUBO vs. LASSO on the LOAN dataset for feature selection

Method	Time in second	False negative/10996	False positive/10996	Correct prediction/10996	Overall accuracy (10 folds)
SVM-QUBO	0.06601	762	63	10171	0.92497
Balance bagging	0.76276	754	86	10156	0.86504
Balanced RF	1.3683	332	4468	6196	0.55295
LDA	0.25688	763	0	10233	0.87218
LR	0.45304	763	0	10233	0.87218
LR-balanced	0.36939	349	4143	6504	0.57552
NN-MLP	0.31607	0	10233	763	0.12782
RF	2.3978	760	11	10225	0.87062
RF-balanced	2.39944	761	2	10233	0.87218
Ensemble: RT-LR	2.89756	488	3427	7121	0.63769
COPOD	0.40503	728	1086	9182	0.78705
KNN	2.26045	697	1026	9273	0.79419
RBM	184.08431	763	0	10233	0.87218

See Figures 3 and 4 for the area under the receiver operating characteristic (AUROC) curves of SVM-QUBO and the other ML algorithms that use and do not use LASSO. All things considered, the AUROC curve demonstrates that these techniques are not very effective. For the LOAN dataset, the optimal algorithm is logistic regression (area:0.57) with LASSO feature selection, or balanced RF (area:0.61) without. SVM-QUBO outperforms the majority, but it is still quite low: 0.57 when features are not selected and 0.51 when they are.les that either do not improve the reliability of the forecast or are in terms of speed, when no feature selection approach is used, SVM-QUBO outperforms the median by 32 times, the fastest ML by 5 times, and the slowest by 2,813 times, RESTRICTED Boltzmann machine. Applying LASSO, SVM-QUBO outperforms the median by a factor of 16, the fastest machine learning algorithm by a factor of 3.8, and the slowest by a factor of 27.88 inorder to build more accurate prediction models, we employ the LASSO.

By utilizing LASSO, ML algorithms experience a considerable improvement in speed compared to their non-LASSO counterparts. The execution time of the algorithms is reduced by an average of 83%

(COPOD) and 21% (LR-balanced), respectively. In summary, this study's evaluation results suggest that traditional ML methods could be a good alternative to quantum computing for moderately imbalanced, non-time-series data until quantum hardware undergoes significant improvements. On the other hand, QML should be seriously considered for highly imbalanced, high-dimensional, time-series data. In order to make a more generalised proposal, it is necessary to conduct more tests on other types of data. An important step towards broadening the scope of issues amenable to quantum computing is this study, which is one of the few QML applications in the field of fraud detection. What makes this study stand out is the extensive comparison of its performance with twelve other ML algorithms, each with its own unique set of characteristics (both supervised and unsupervised). As one of the few QML applications in fraud detection, this study is an important step towards broadening the scope of issues amenable to quantum computing. This research stands out because it compares its results to those of numerous other ML algorithms, each with its own set of features.

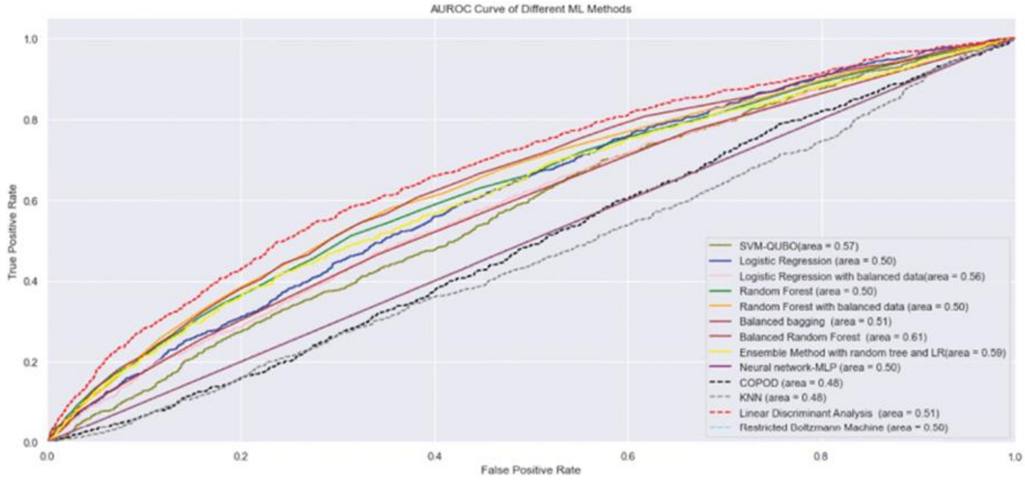

Figure 3. SVM-QUBO vs other ML techniques on the LOAN dataset without feature selection: AUROC curves

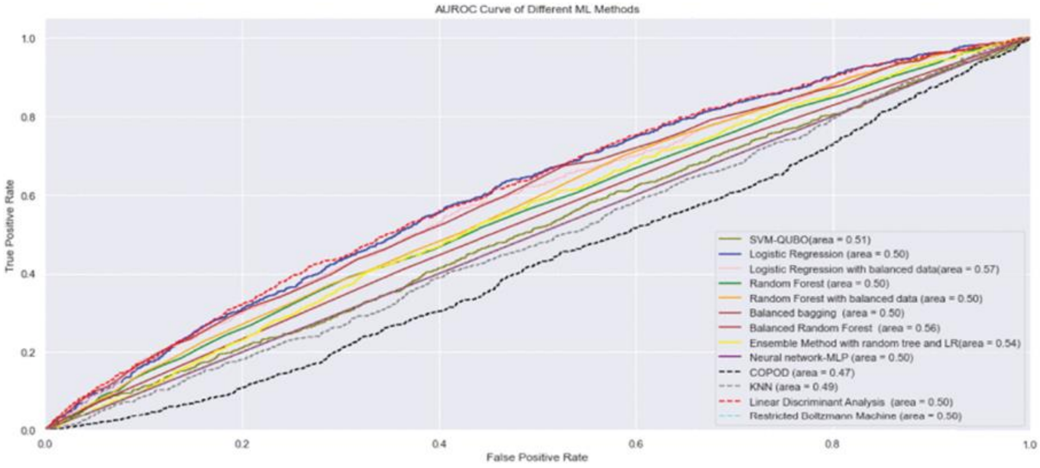

Figure 4. Comparing SVM-QUBO and other ML methods on the LOAN dataset using LASSO, we find their AUROC curves

4. CONCLUSION

The integration of ML algorithms with quantum annealing solvers for online fraud detection represents a promising advancement in the field of cyber security. In order to find out how well different ML algorithms identify fraud, this study examines QML systems. Using a time-series based, extremely unbalanced, high-dimensional dataset, the results demonstrate the efficacy of our suggested fraud detection system and the exceptional capabilities of QML. By outlining potential future directions for research in QML, our study adds to the existing body of detection literature. This research has demonstrated that combining classical and quantum computing paradigms can significantly enhance the accuracy, speed, and adaptability of fraud detection systems in the dynamic landscape of online transactions. The results indicate that ML algorithms, particularly supervised and unsupervised learning techniques, effectively learn from historical transaction data to identify both known and emerging fraudulent patterns. Quantum annealing contributes to the optimization of complex decision-making processes, offering a parallelized approach to solving combinatorial optimization problems inherent in fraud detection. The integrated model showcased superior performance compared to traditional fraud detection methods, achieving higher accuracy and real-time processing capabilities. The adaptability of the model to dynamic fraud patterns, even without prior labeled data, positions it as a robust solution for addressing the evolving tactics employed by online fraudsters. This research has contributed to bridging the gap between classical ML and quantum computing for online fraud detection. The successful integration of these technologies opens new possibilities for bolstering cyber security measures, ultimately creating a more resilient and adaptive framework to counter the ever-evolving landscape of online fraud.

REFERENCES

[1] A. Jain, A. Panwar, M. Azam, and R. Khanam, "Smart door access control system based on QR code," *International Journal of Informatics and Communication Technology*, vol. 12, no. 2, pp. 171–179, Aug. 2023, doi: 10.11591/ijict.v12i2.pp171-179.

[2] B. Mytnyk, O. Tkachyk, N. Shakhovska, S. Fedushko, and Y. Syerov, "Application of artificial intelligence for fraudulent banking operations recognition," *Big Data and Cognitive Computing*, vol. 7, no. 2, p. 93, May 2023, doi: 10.3390/bdcc7020093.

[3] V. Vasani, A. K. Bairwa, S. Joshi, A. Pljonkin, M. Kaur, and M. Amoon, "Comprehensive analysis of advanced techniques and vital tools for detecting malware intrusion," *Electronics (Switzerland)*, vol. 12, no. 20, p. 4299, Oct. 2023, doi: 10.3390/electronics12204299.

[4] T. Wahyuningsih, I. Sembiring, A. Setiawan, and I. Setyawan, "Exploring network security threats through text mining techniques: a comprehensive analysis," *Computer Science and Information Technologies*, vol. 4, no. 3, pp. 258–267, Nov. 2023, doi: 10.11591/csit.v4i3.p258-267.

[5] A. Diro, S. Kaisar, A. V. Vasilakos, A. Anwar, A. Nasirian, and G. Olani, "Anomaly detection for space information networks: a survey of challenges, techniques, and future directions," *Computers & Security*, vol. 139, p. 103705, Apr. 2024, doi: 10.1016/j.cose.2024.103705.

[6] L. Zhang, C. Ma, J. Liu, G. Totis, and S. Weng, "Multi-layer parallel-perceptual-fusion spatiotemporal graph convolutional network for cross-domain, poor thermal information prediction in cloud-edge control services," *Advanced Engineering Informatics*, vol. 59, p. 102358, Jan. 2024, doi: 10.1016/j.aei.2024.102358.

[7] A. R. Thatipalli, P. Aravamudu, K. Kartheek, and A. Dennisan, "Exploring and comparing various machine and deep learning technique algorithms to detect domain generation algorithms of malicious variants," *Computer Science and Information Technologies*, vol. 3, no. 2, pp. 94–103, Jul. 2022, doi: 10.11591/csit.v3i2.pp94-103.

[8] T. Pourhabibi, K. L. Ong, B. H. Kam, and Y. L. Boo, "Fraud detection: a systematic literature review of graph-based anomaly detection approaches," *Decision Support Systems*, vol. 133, p. 113303, Jun. 2020, doi: 10.1016/j.dss.2020.113303.

[9] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Papers on Risk and Insurance: Issues and Practice*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[10] A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 1, pp. 145–174, Jan. 2023, doi: 10.1016/j.jksuci.2022.11.008.

[11] A. Bakumenko and A. Elragal, "Detecting anomalies in financial data using machine learning algorithms," *Systems*, vol. 10, no. 5, p. 130, Aug. 2022, doi: 10.3390/systems10050130.

[12] R. K. Nath, H. Thapliyal, and T. S. Humble, "Quantum annealing for real-world machine learning applications," in *Quantum Computing: Circuits, Systems, Automation and Applications*, Cham: Springer International Publishing, 2023, pp. 157–180. doi: 10.1007/978-3-031-37966-6_9.

[13] W. Hilal, S. A. Gadsden, and J. Yawney, "Financial fraud: a review of anomaly detection techniques and recent advances," *Expert Systems with Applications*, vol. 193, p. 116429, May 2022, doi: 10.1016/j.eswa.2021.116429.

[14] J. Gong, H. Zhang, and W. Du, "Research on integrated learning fraud detection method based on combination classifier fusion (thbagging): a case study on the foundational medical insurance dataset," *Electronics (Switzerland)*, vol. 9, no. 6, p. 894, May 2020, doi: 10.3390/electronics9060894.

[15] S. Surya, S. R. Jagtap, R. Ramnarayan, M. Priyadarshini, R. K. Ibrahim, and M. B. Alazzam, "Protecting online transactions: a cybersecurity solution model," in *2023 3rd International Conference on Advance Computing and Innovative Technologies in Engineering, ICACITE 2023*, IEEE, May 2023, pp. 2630–2634. doi: 10.1109/ICACITE57410.2023.10183282.

[16] A. Naim and A. F. Ghouri, "Exploring the role of cyber security measures (encryption, firewalls, and authentication protocols) in preventing cyber-attacks on e-commerce platforms," *International Journal Of ebusiness And egovernment Studies*, vol. 15, no. 1, p. 2023, 2023, doi: 10.34109/ijebeg.2023150120.

[17] A. Di Pierro and M. Incudini, "Quantum machine learning and fraud detection," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13066 LNCS, 2021, pp. 139–155. doi: 10.1007/978-3-030-91631-2_8.

[18] L. Huynh, J. Hong, A. Mian, H. Suzuki, Y. Wu, and S. Camtepe, "Quantum-inspired machine learning: a survey." 2023. doi: https: 10.48550/arXiv.2308.11269.

[19] N. Pocher, M. Zichichi, F. Merizzi, M. Z. Shafiq, and S. Ferretti, "Detecting anomalous cryptocurrency transactions: an AML/CFT application of machine learning-based forensics," *Electronic Markets*, vol. 33, no. 1, p. 37, Dec. 2023, doi: 10.1007/s12525-023-00654-3.

[20] Y. Alghofaili, A. Albattah, and M. A. Rassam, "A financial fraud detection model based on LSTM deep learning technique," *Journal of Applied Security Research*, vol. 15, no. 4, pp. 498–516, Oct. 2020, doi: 10.1080/19361610.2020.1815491.

[21] I. H. Sarker, “Deep learning: a comprehensive overview on techniques, taxonomy, applications and research directions,” *SN Computer Science*, vol. 2, no. 6, p. 420, Nov. 2021, doi: 10.1007/s42979-021-00815-1.
[22] C. Gomes, Z. Jin, and H. Yang, “Insurance fraud detection with unsupervised deep learning,” *Journal of Risk and Insurance*, vol. 88, no. 3, pp. 591–624, Sep. 2021, doi: 10.1111/jori.12359.
[23] Y. Wang, “When quantum computation meets data science: making data science quantum,” *Harvard Data Science Review*, vol. 4, no. 1, Jan. 2022, doi: 10.1162/99608f92.ef5d8928.
[24] M.-L. How and S.-M. Cheah, “Business renaissance: opportunities and challenges at the dawn of the quantum computing era,” *Businesses*, vol. 3, no. 4, pp. 585–605, Nov. 2023, doi: 10.3390/businesses3040036.
[25] A. A. Khan *et al.*, “Software architecture for quantum computing systems - a systematic review,” *SSRN Electronic Journal*, vol. 201, p. 111682, 2023, doi: 10.2139/ssrn.4191449.
[26] U. Sam, G. Moses, and T. Olajide, “Credit card fraud detection using machine learning algorithms.” 2023. doi: http://dx.doi.org/10.13140/RG.2.2.14806.63044.
[27] P. Vanini, S. Rossi, E. Zvizdic, and T. Domenig, “Online payment fraud: from anomaly detection to risk management,” *Financial Innovation*, vol. 9, no. 1, p. 66, Mar. 2023, doi: 10.1186/s40854-023-00470-w.
[28] M. M. Taye, “Understanding of machine learning with deep learning: architectures, workflow, applications and future directions,” *Computers*, vol. 12, no. 5, p. 91, Apr. 2023, doi: 10.3390/computers12050091.
[29] M. S. Peelam, A. A. Rout, and V. Chamola, “Quantum computing applications for internet of things,” *IET Quantum Communication*, vol. 5, no. 2, pp. 103–112, Jun. 2024, doi: 10.1049/qtc2.12079.
[30] D. Chawla and P. S. Mehra, “A survey on quantum computing for internet of things security,” *Procedia Computer Science*, vol. 218, pp. 2191–2200, 2022, doi: 10.1016/j.procs.2023.01.195.
[31] M. Elahi, S. O. Afolaranmi, J. L. Martinez Lastra, and J. A. Perez Garcia, “A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment,” *Discover Artificial Intelligence*, vol. 3, no. 1, p. 43, Dec. 2023, doi: 10.1007/s44163-023-00089-x.
[32] H. Wang, W. Wang, Y. Liu, and B. Alidaee, “Integrating machine learning algorithms with quantum annealing solvers for online fraud detection,” *IEEE Access*, vol. 10, pp. 75908–75917, 2022, doi: 10.1109/ACCESS.2022.3190897.
[33] V. Vapnik, *Estimation of dependences based on empirical data*, 2nd ed. Springer Science & Business Media, 2006.
[34] C. Cortes and V. Vapnik, “Support-vector networks,” *Machine Learning*, vol. 20, pp. 273–297, 1995.

BIOGRAPHIES OF AUTHORS

Dr. Surya Prasada Rao Borra associate professor in Department of ECE, PVP Siddhartha Institute of Technology, Vijayawaada. Ph.D. in Electronics and Communication Engineering, JNTUK, Kakinada, India. M.Tech. in Digital Systems and Computer Electronics, JNTU Hyderabad, India. B.E. in Electronics and Communication Engineering, Andhra University, Visakhapatnam, India. He can be contacted at email: suryaborra1679@gmail.com.

Dr. Bhargavi Peddi Reddy presently working as an Associate Professor in the Department of CSE, Vasavi College of Engineering, Hyderabad, T.S, India. She received her Doctor of Philosophy Degree in Computer Science and Engineering from Acharya Nagarjuna University. Master’s Degree in Computer Science and Engineering from JNTUK. Her area of research is data mining, artificial intelligence, machine learning, and natural language processing. She can be contacted at email: bhargavi@staff.vce.ac.in.

Mr. Baba Venkata Nageswara Prasad Paruchuri serves as an assistant professor at KL University (Deemed to be) within the Department of Computer Science and Engineering, Vijayawada. M.Tech. degree in 2010 from Acharya Nagarjuna University and is currently pursuing a Ph.D. at the University of Technology, Jaipur. His research interests encompass cloud computing, artificial intelligence, machine learning, computer networks, and metaverse. He can be contacted at email: bvnprasadparuchuri@yahoo.com.

Mr. Rachakulla Sai Venkata Ramana is currently working as assistant professor in Computer Science and Engineering (Cyber Security) in Madanapalle Institute of Technology and Science (UGC - AUTONOMOUS INSTITUTION), affiliated to JNTU Anantapur. He has 9 years of teaching experience in engineering education. He received his M.Tech. in 2012 from JNTU Anantapur. His research interests include machine learning and cloud computing. He can be contacted at email: onlinesvr4@gmail.com.

Onteru Srinivas is an assistant professor in Department of CSE (AI&ML) at R.V.R&J.C College of Engineering, Guntur. He is Pursuing Ph.D. in JNTU-K, Kakinada. He has 10 years of teaching experience. He can be contacted at email: srinivas0071234@gmail.com.

Lakshmi Rathod Department of Electronics and Communication Engineering, Indian Institute of Information Technology, Rajiv Gandhi University of Knowledge and Technology, Andhra Pradesh, Nuzvid, India. She can be contacted at email: blakshmith@gmail.com.