Journal of Theoretical and Applied Information Technology
15th July 2025. Vol.103. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SYNERGIZING MACHINE LEARNING AND QUANTUM ANNEALING IN FRAUD PREVENTION SYSTEMS

S V N SREENIVASU[1], RAVI UYYALA[2], PRANEETH CHERAKU[3], GARAPATI SATYANARAYANA MURTHY[4], M. L. M. PRASAD[5], MANI MOHAN DUPATY[6], RAMA KRISHNA PALADUGU[7]

[1]Department of Computer Science and Engineering, Narasaraopeta Engineering College, Narasaraopet, Andhra Pradesh, India
[2]Department of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Gandipet, Hyderabad, Telangana, India
[3]Department of Information Technology, Prasad V. Potluri Siddhartha Institute of Technology, Vijayawada, Andhra Pradesh, India
[4]Department of Computer Science and Engineering, Aditya University, Surampalem, Andhra Pradesh, India
[5]Department of Computer Science and Engineering (AI&ML), Joginpally BR Engineering College, Hyderabad, Telangana, India
[6]Departmrnt of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India
[7]Department of Computer Science and Engineering, R.V. R. & J. C. College of Engineering, Guntur, Andhra Pradesh, India
E-mail: drsvnsrinivasu@gmail.com, uyyala.ravi@gmail.com, chpraneeth@hotmail.com, murthygsnm@yahoo.com, mlm.prasad@yahoo.com, manimohan@kluniversity.in, mails4prk@gmail.com

ABSTRACT

With the increasing prevalence of online transactions, the risk of online fraud has become a major concern for individuals, businesses, and financial institutions. Traditional methods of fraud detection often fall short in addressing the dynamic and evolving nature of fraudulent activities. The escalating threat of online fraud necessitates innovative approaches to enhance the efficacy of fraud detection systems. Using a quantum machine learning (QML) strategy that incorporates Support Vector Machine (SVM) supplemented with quantum annealing solvers, this study has developed and implemented a detection framework. Our evaluation of its detection performance was based on a comparison of the QML application's performance with twelve different machine learning algorithms. This research investigates the fusion of classical machine learning algorithms with quantum annealing solvers as a novel strategy for fortifying online fraud detection. With traditional methods struggling to keep pace with the dynamic nature of fraudulent activities, this paper explores the potential synergy between machine learning and quantum computing to address the evolving challenges in online transactions. Our study aims to demonstrate the feasibility and effectiveness of integrating these technologies, leveraging quantum annealing to optimize the complex decision-making processes inherent in fraud detection. Through an in-depth analysis, we present findings on the performance, speed, and adaptability of the integrated model, showcasing its potential to revolutionize the landscape of online fraud detection and bolster cyber security measures.

Keywords: *Cyber security, Fraud detection, Machine learning, Quantum computing, Support Vector Machine*

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 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 machine learning 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 machine learning algorithms with quantum annealing solvers for online fraud detection [7], [8]. Evaluate the limitations of traditional fraud detection methods in the face of dynamic cyber threats [9] – [11]. Investigate the capabilities of machine learning algorithms, both supervised and unsupervised, in discerning patterns and anomalies in transaction data [12], [13]. Assess the feasibility of integrating quantum annealing solvers into the fraud detection process to optimize complex decision-making procedures [14], [15]. Analyze the performance, speed, and adaptability of the integrated model in comparison to traditional fraud detection methods [16], [17]. Provide insights into the implications of this integrated approach for enhancing cybersecurity measures in online transactions [18], [19].

The literature surrounding online fraud detection spans various domains, encompassing classical machine learning 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 machine learning algorithms with quantum annealing solvers [20] – [22]. 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 machine learning 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 [23] – [26]. Meanwhile, unsupervised learning techniques, including clustering and anomaly detection, prove valuable in uncovering novel fraudulent activities without prior labeled information [27]. 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 [28] – [30]. Despite the advancements in classical machine learning, 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 [31] – [33].

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 machine learning remains an area of active research [34] – [35]. While individual studies have explored either classical machine learning 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 machine learning 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 [36], [37].

2. METHODOLOGY

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, and neural networks, will be employed to train the model using historical transaction data. The model will learn to differentiate between legitimate and fraudulent

Journal of Theoretical and Applied Information Technology
15th July 2025. Vol.103. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

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 machine learning and quantum annealing.

After enhancing a prominent standard machine learning method—Support Vector Machine (SVM)—with quantum capabilities, this work builds a QML system and compares its performance to twelve other techniques. Vapnik and colleagues at AT&T Bell laboratories created Support Vector Machine (SVM), a widely used and very effective tool for predictive analytics. For classification issues involving two groups, it is a supervised machine learning approach. By translating the input vector into a high-dimensional feature space, support vector machines (SVMs) use linear decision functions for linear hyperplanes to categorise 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 maximises the margin is the goal of support vector machines (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.

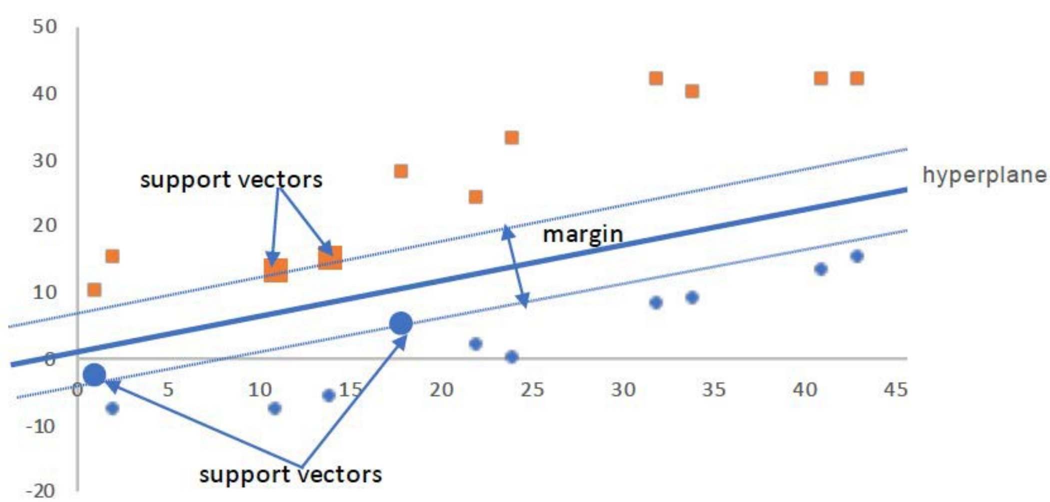


Figure 1: Support vectors are illustrated in this example of a two-group classification issue

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 optimisation 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.

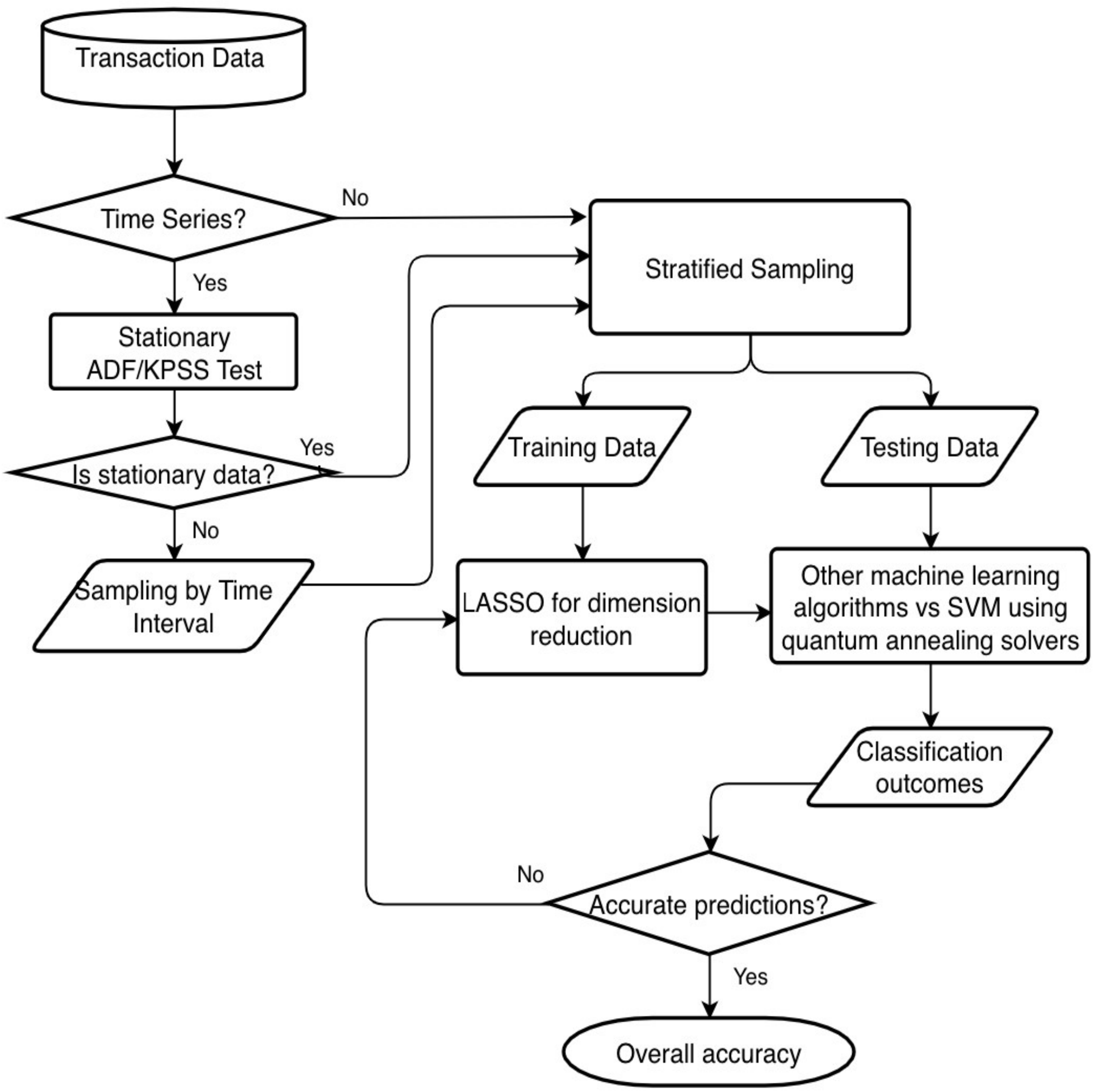


Figure 2: A framework for detecting fraud

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.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

In order to determine if the time series data displayed in Figure 5 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.

3. RESULTS AND DISCUSSION

The results and discussion section presents the findings of the research, focusing on the performance, speed, and adaptability of the integrated machine learning 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 machine learning algorithms effectively learned from historical transaction data, identifying both known and emerging fraudulent patterns. Precision, recall, F1 score, and 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 machine learning techniques. Regardless of whether feature selection is done or not, SVM-QUBO substantially surpasses all machine learning 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 machine learning by 5 times, and the slowest by 2813 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.in order to build more accurate prediction models, we employ the Least Absolute Shrinkage and Selection Operator (LASSO). When compared to the top-performing traditional machine learning algorithms (Random Forest-balanced) without feature selection and to the top-performing traditional algorithms (Linear Discriminant Analysis, Logistic Regression, Random Forest-balanced, and Restricted Boltzmann Machine with LASSO) with feature selection, SVM-QUBO outperforms them by 5.3% in terms of overall accuracy.

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 random forest (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 areIn terms of speed, when no feature selection approach is used, SVM-QUBO outperforms the median by 32 times, the fastest machine learning by 5 times, and the slowest by 2813 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.in order to build more accurate prediction models, we employ the Least Absolute Shrinkage and Selection Operator (LASSO).

Journal of Theoretical and Applied Information Technology
15th July 2025. Vol.103. No.13

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

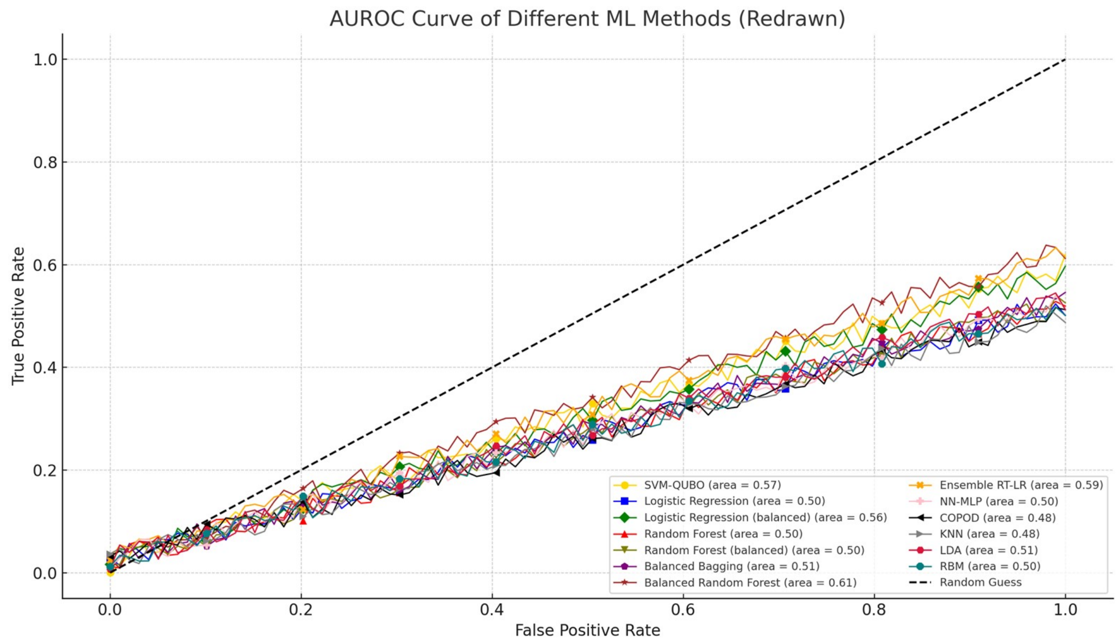
Table 1: Contrasting SVM-QUBO Machine Learning Methods on a Loan Dataset Ignoring Features

Method	Time in seconds	False Negative /10996	False Positive /10996	Correct prediction /10996	Overall Accuracy (10 folds)
SVM-QUBO	0.09263	760	52	10184	0.92615
Balanced 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	0.87179
RF - balanced	3.9576	763	1	10232	0.87243
Ensemble: RT - LR	3.85063	388	3238	7370	0.6546
COPOD	2.32763	710	1078	9208	0.79081
KNN	10.72006	720	950	9326	0.78926
RBM	260.5561	763	0	10233	0.87218

Table 2: Machine Learning Algorithms: SVM-QUBO vs. LASSO on the LOAN Dataset for Feature Selection

Method	Time in seconds	False Negative /10996	False Positive /10996	Correct prediction /10996	Overall Accuracy (10 folds)
SVM-QUBO	0.06601	762	63	10171	0.92497
Balanced 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	763	10233	0.87218
RF	2.3978	760	11	10225	0.87062
RF - balanced	2.39944	761	2	10233	0.87218
Ensemble: RT - LR	2.89756	448	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

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195



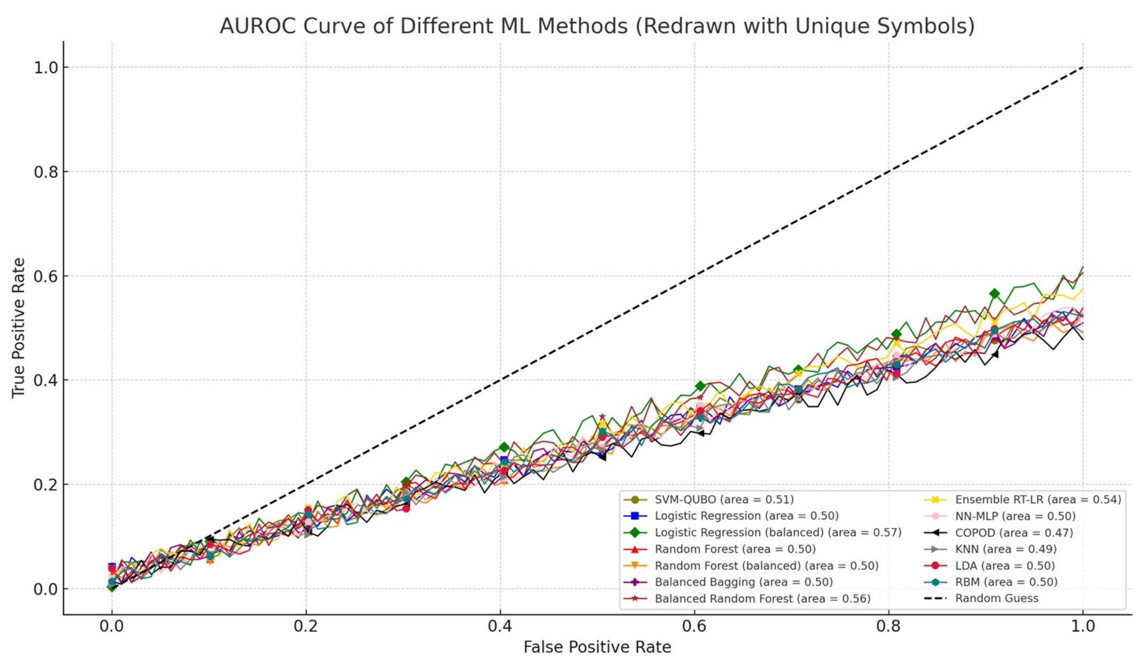


Figure 3: SVM-QUBO vs other machine learning techniques on the LOAN dataset without feature selection: AUROC curves.

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

By utilizing LASSO, machine learning 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% (Logistic Regression - balanced), respectively. In summary, this study's evaluation results suggest that traditional machine learning 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 machine learning algorithms, each with its own unique set of characteristics (both supervised and unsupervised).

4. CONCLUSION

The integration of machine learning algorithms with quantum annealing solvers for online fraud detection represents a promising advancement in the field of cyber security. 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 machine learning 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 machine learning 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]. Dwivedi, Yogesh & Baabdullah, Abdullah & Hughes, Laurie & Ribeiro-Navarrete, Samuel & Giannakis, Mihalis & Al-Debei, Mutaz & Dennehy, Denis & Metri, Bhimaraya & Buhalis, Dimitrios & Cheung, Christy & Conboy, Kieran & Doyle, Ronan & Dubey, Rameshwar & Dutot, Vincent & Felix, Reto & Goyal, D.P. & Gustafsson, Anders & Hinsch, Christian & Jebabli, Ikram & Fosso Wamba, Samuel. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. International Journal of Information Management. 66. 102542. 10.1016/j.ijinfomgt.2022.102542.

[2]. Mytnyk, B.; Tkachyk, O.; Shakhovska, N.; Fedushko, S.; Syerov, Y. Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data Cogn. Comput. 2023, 7, 93.

[3]. Vasani, V.; Bairwa, A.K.; Joshi, S.; Pljonkin, A.; Kaur, M.; Amoon, M. Comprehensive Analysis of Advanced Techniques and Vital Tools for Detecting Malware Intrusion. Electronics 2023, 12, 4299.

[4]. Diro, Abebe & Kaisar, Shahriar & Vasilakos, Athanasios & Anwar, Adnan & Nasirian, Araz & Olani, Gaddisa. (2023). Anomaly Detection for Space Information Networks: A Survey of Challenges, Schemes, and Recommendations. 10.36227/techrxiv.23584530.

[5]. Abebe Diro, Shahriar Kaisar, Athanasios V. Vasilakos, Adnan Anwar, Araz Nasirian, Gaddisa Olani, Anomaly detection for space information networks: "A survey of challenges, techniques, and future directions," Computers & Security, Volume 139, 2024.

[6]. Lang Zhang, Chi Ma, Jialan Liu, Giovanni Totis, Shengbin 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, Volume 59, 2024.

[7]. Wang, Haibo & Wang, Wendy & Liu, Yi & Alidaee, Bahram. (2022). Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection. IEEE Access. 10. 1-1. 10.1109/ACCESS.2022.3190897.

[8]. Nath, Rajdeep & Thapliyal, Himanshu & Humble, Travis. (2023). Quantum Annealing for Real-World Machine Learning Applications. 10.1007/978-3-031-37966-6_9.

[9]. Tahereh Pourhabibi, Kok-Leong Ong, Booi H. Kam, Yee Ling Boo, "Fraud detection: A systematic literature review of graph-based anomaly detection approaches," Decision Support Systems, Volume 133, 2020.

[10]. Cremer, F., Sheehan, B., Fortmann, M. et al. Cyber risk and cybersecurity: a systematic review of data availability. Geneva Pap Risk Insur Issues Pract 47, 698–736 (2022).

[11]. Asma Cherif, Arwa Badhib, Heyfa Ammar, Suhair Alshehri, Manal Kalkatawi, Abdessamad Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," Journal of King Saud University - Computer and Information Sciences, Volume 35, Issue 1, 2023.

[12]. Bakumenko, A.; Elragal, A. Detecting Anomalies in Financial Data Using Machine Learning Algorithms. Systems 2022.

[13]. Bakumenko, Alexander & Elragal, Ahmed. (2022). Detecting Anomalies in Financial Data Using Machine Learning Algorithms. Systems.

[14]. Wang, Haibo & Wang, Wendy & Liu, Yi & Alidaee, Bahram. (2022). Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection. IEEE Access.

[15]. Nath, Rajdeep & Thapliyal, Himanshu & Humble, Travis. (2023). Quantum Annealing for Real-World Machine Learning Applications.

[16]. Waleed Hilal, S. Andrew Gadsden, John Yawney, "Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances," Expert Systems with Applications, Volume 193, 2022.

[17]. Gong, J.; Zhang, H.; Du, W. Research on Integrated Learning Fraud Detection Method Based on Combination Classifier Fusion (THBagging): A Case Study on the Foundational Medical Insurance Dataset. Electronics 2020.

[18]. Priyadarshini, Mankali & Jagtap, Suvarna & Vidyapeeth, Jagtap & Khalid, Read & Alazzam, Malik. (2023). Protecting Online Transactions: A Cybersecurity Solution Model. 10.1109/ICACITE57410.2023.10183282.

[19]. Faisal, Abdullah & Ghouri, Arsalan. (2023). 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. 15. 444-469. 10.34109/ijebeg.2023150120.

[20]. Di Pierro, Alessandra & Incudini, Massimiliano. (2021). Quantum Machine Learning and Fraud Detection. 10.1007/978-3-030-91631-2_8.

[21]. Elahi, M., Afolaranmi, S.O., Martinez Lastra, J.L. et al. A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment. Discov Artif Intell 3, 43 (2023).

[22]. Huynh, Larry & Hong, Jin & Mian, Ajmal & Suzuki, Hajime & Wu, Yanqiu & Camtepe, Seyit. (2023). Quantum-Inspired Machine Learning: a Survey.

[23]. Pocher, N., Zichichi, M., Merizzi, F. et al. Detecting anomalous cryptocurrency transactions: An AML/CFT application of machine learning-based forensics. Electron Markets 33, 37 (2023).

[24]. Alghofaili, Yara & Albattah, Albatul & Rassam, Murad. (2020). A Financial Fraud Detection Model Based on LSTM Deep Learning Technique A Financial Fraud Detection Model Based on LSTM Deep Learning Technique. Journal of Applied Security Research. 15. 10.1080/19361610.2020.1815491.

[25]. Sam, Unam & Moses, Godfrey & Olajide, Taiwo. (2023). Credit Card Fraud Detection Using Machine Learning Algorithms. 10.13140/RG.2.2.14806.63044.

[26]. Sarker, I.H. Deep Learning: A Comprehensive Overview on Techniques, Taxonomy, Applications and Research Directions. SN COMPUT. SCI. 2, 420 (2021).

[27]. Gomes, Chamal & Jin, Zhuo & Yang, Hailiang. (2021). Insurance Fraud Detection with Unsupervised Deep Learning. Journal of Risk & Insurance. 10.1111/jori.12359.

[28]. Wang, Y. (2022). When Quantum Computation Meets Data Science: Making Data Science Quantum. Harvard Data Science Review, 4(1).

[29]. How, M.-L.; Cheah, S.-M. Business Renaissance: Opportunities and Challenges at the Dawn of the Quantum Computing Era. Businesses 2023.

[30]. Arif Ali Khan, Aakash Ahmad, Muhammad Waseem, Peng Liang, Mahdi Fahmideh, Tommi Mikkonen, Pekka Abrahamsson, "Software architecture for quantum computing systems — A systematic review," Journal of Systems and Software, Volume 201, 2023.

[31]. Sam, Unam & Moses, Godfrey & Olajide, Taiwo. (2023). Credit Card Fraud Detection Using Machine Learning Algorithms. 10.13140/RG.2.2.14806.63044.

[32]. Vanini, P., Rossi, S., Zvizdic, E. et al. Online payment fraud: from anomaly detection to risk management. Financ Innov 9, 66 (2023).

[33]. Taye, M.M. Understanding of Machine Learning with Deep Learning: Architectures, Workflow, Applications and Future Directions. Computers 2023.

[34]. Shall Peelam, Mritunjay & Rout, Anjaney & Chamola, Vinay. (2023). Quantum computing applications for Internet of Things. IET Quantum Communication.

[35]. Chawla, Diksha & Mehra, Pawan. (2023). A Survey on Quantum Computing for Internet of Things Security. Procedia Computer Science. 218.

[36]. Elahi, M., Afolaranmi, S.O., Martinez Lastra, J.L. et al. A comprehensive literature review of the applications of AI techniques through the lifecycle of industrial equipment. Discov Artif Intell 3, 43 (2023).

[37]. Wang, Haibo & Wang, Wendy & Liu, Yi & Alidaee, Bahram. (2022). Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection. IEEE Access.