iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80166

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Quantum Machine Learning for Cyberattack Prediction

Nikhil Kinekar, Minal Dandekar, Nikhil Agashe, Mrunali Moundekar, Aakansha Bawankar, Rahul Kawariya
Department of Computer Science Engineering, G H Raisoni University, Amravati, Nagpur, MH, India

Abstract: ***The proposed study presents a comparative cyberattack prediction framework integrating six classical machine learning models and a Quantum Machine Learning (QML) model. Experimental evaluation on the NSL-KDD dataset demonstrates strong predictive performance, with ensemble and neural approaches showing high testing accuracy, while the QML framework provides enhanced high-dimensional feature representation and promising anomaly detection capability for future zero-day threat prediction. The novelty of this work lies in the unified benchmarking of classical, deep learning, and quantum learning paradigms within a single cybersecurity pipeline. The rapid growth of interconnected digital infrastructures, including enterprise networks, cloud systems, and Internet of Things (IoT) environments, has significantly increased the scale and sophistication of cyber threats. Traditional machine learning models have shown strong capabilities in intrusion detection and anomaly analysis; however, they increasingly face limitations when dealing with high dimensional network traffic, zero-day exploits, and complex nonlinear attack patterns. Quantum Machine Learning (QML), which combines principles of quantum computing with statistical learning, has emerged as a promising paradigm for next-generation cyberattack prediction. This paper presents a comprehensive hybrid quantum-classical framework for cyberattack prediction using the NSL-KDD dataset. The proposed study integrates classical machine learning models such as Support Vector Machine (SVM), Logistic Regression, Naive Bayes, Multi-Layer Perceptron (MLP), Random Forest, and Convolutional Neural Networks (CNN), alongside a Quantum Machine Learning pipeline implemented using PennyLane. The framework incorporates preprocessing, dimensionality reduction using Principal Component Analysis (PCA), quantum angle encoding, variational quantum circuits, and comparative performance analysis. Experimental findings indicate that QML demonstrates strong potential for identifying complex attack signatures and improving prediction robustness under high-dimensional conditions. The paper further discusses implementation challenges, scalability, quantum noise constraints, and future research directions.***

Keywords: Cybersecurity, Intrusion Detection, Machine Learning, Quantum Computing, Quantum Machine Learning, NSL-KDD

I. INTRODUCTION

A. Background and Motivation

The exponential growth of digital communication systems, enterprise infrastructures, and Internet of Things (IoT) ecosystems has led to a dramatic increase in cyber threats across modern networks. Cyberattacks such as distributed denial-of-service (DDoS), phishing, malware injection, privilege escalation, ransomware, and zero-day exploits continue to evolve in both complexity and scale.Traditional cybersecurity frameworks increasingly rely on machine learning for proactive threat detection; however, classical algorithms often face computational bottlenecks when processing large-scale, high dimensional network telemetry data. These challenges are especially significant in real-time intrusion detection systems where latency and prediction accuracy are both critical.

B. Role of Quantum Machine Learning

In recent years, Quantum Machine Learning (QML) has emerged as a promising computational paradigm that combines the mathematical foundations of quantum computing with advanced machine learning methodologies. By leveraging quantum principles such as superposition, entanglement, and probabilistic measurement, QML offers the potential to process complex feature spaces more efficiently than classical models. This makes QML particularly relevant for cybersecurity applications where subtle nonlinear attack signatures must be identified from massive streams of network traffic.

C. Research Objective and Contribution

This research focuses on the design and evaluation of a hybrid quantum-classical framework for cyberattack prediction using the NSL-KDD benchmark dataset.

The work includes comparative implementation of six classical machine learning and deep learning models, namely Support Vector Machine, Logistic Regression, Naive Bayes, Random Forest, Multi-Layer Perceptron, and Convolutional Neural Network, alongside a Quantum Machine Learning pipeline implemented using PennyLane and variational quantum circuits. The study aims to analyze prediction performance, computational efficiency, and the practical feasibility of QML for intrusion detection while establishing a unified comparative framework for future cybersecurity research.

II. RELATED WORK

A. *Classical and Deep Learning Approaches*

Recent advances in cybersecurity analytics have extensively employed classical machine learning techniques for intrusion detection and anomaly classification. Traditional machine learning models such as Decision Trees, Support Vector Machines, Logistic Regression, and Random Forest classifiers have been widely adopted for benchmark datasets including KDD Cup 99, NSL-KDD, and UNSW-NB15. These approaches demonstrate strong performance for known attack signatures but often struggle when presented with unseen or zero-day attack vectors. In addition, several researchers have proposed deep learning architectures such as Artificial Neural Networks, Recurrent Neural Networks, Long Short-Term Memory models, and Convolutional Neural Networks, which have shown strong capabilities in learning nonlinear traffic behavior and temporal attack patterns.

B. *Quantum Machine Learning*

Research In parallel, the field of Quantum Machine Learning has gained significant momentum. Early foundational work established the theoretical framework for integrating quantum computing with machine learning algorithms. Subsequent research introduced quantum support vector machines, variational quantum classifiers, and quantum neural networks as promising alternatives for high dimensional data analysis. Within cybersecurity, several recent studies have explored quantum-enhanced intrusion detection frameworks, suggesting that quantum feature spaces may improve class separability for highly complex traffic distributions and nonlinear malicious behavior.

C. *Research Gap*

Despite these advances, the literature still lacks extensive implementation-based comparative studies that benchmark QML directly against multiple classical machine learning and deep learning models under the same cybersecurity dataset and evaluation pipeline. This research addresses that gap by providing a unified comparative framework across six classical models and a quantum variational classifier, thereby enabling direct performance comparison under identical preprocessing, training, and evaluation conditions.

III. PROPOSED METHODOLOGY AND FRAMEWORK

A. *Data Preprocessing*

The proposed methodology begins with the import and cleaning of the NSL-KDD training and testing datasets to ensure structural consistency. The dataset contains categorical and numerical traffic attributes such as protocol type, service, flag status, source bytes, destination bytes, connection count, and host error rates. Since several machine learning algorithms require numerical input, categorical columns are transformed using label encoding. Feature scaling is then applied using StandardScaler to normalize the data distribution around zero mean and unit variance, which is essential for distance based and gradient-based learning models.

B. *Classical Benchmark Models*

The next stage involves the implementation of six classical models to establish a strong benchmark baseline. These models include Support Vector Machine, Logistic Regression, Naive Bayes, Random Forest, Multi-Layer Perceptron, and Convolutional Neural Network. Each model undergoes train-test evaluation, confusion matrix generation, classification report computation, and time complexity analysis. This stage provides a robust comparative foundation for evaluating the effectiveness of the proposed quantum framework.

C. *Quantum Learning Pipeline*

For the quantum pipeline, Principal Component Analysis is used to reduce the feature dimensionality to four components so that the reduced vectors can be mapped onto four qubits. The transformed feature vectors are then encoded into qubit states using rotation gates through angle encoding.

A two-layer variational quantum circuit is designed using trainable parameters, followed by measurement and classification. This methodology enables the representation of complex multidimensional attack signatures in a high-dimensional Hilbert space, thereby improving the ability to detect complex and previously unseen cyberattacks.

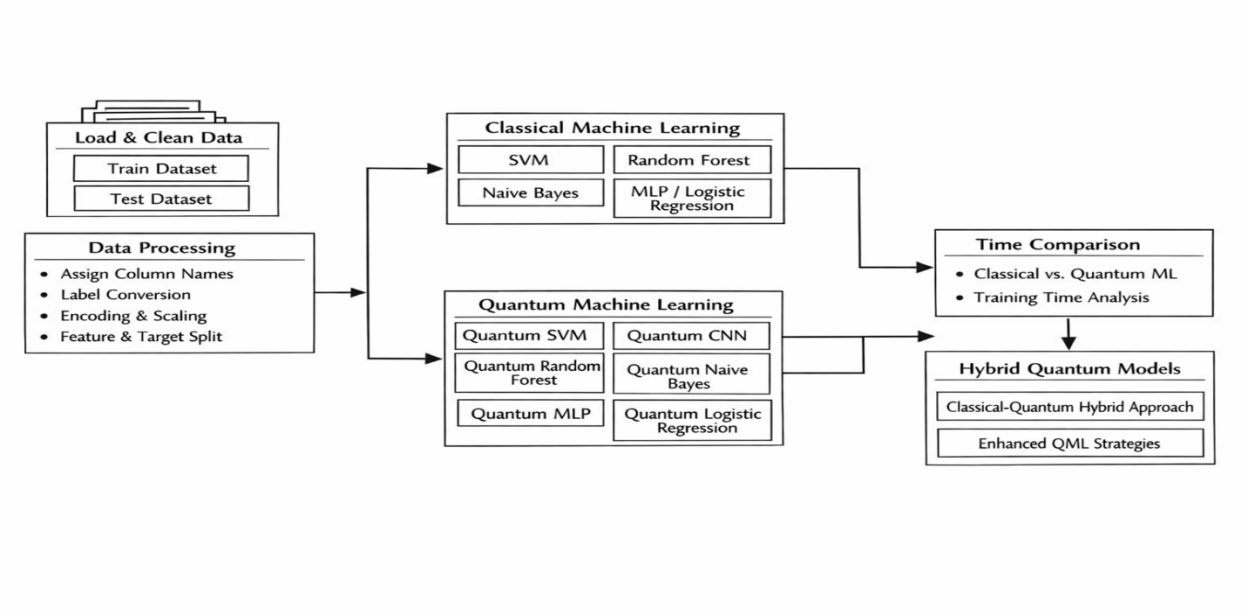


Fig 1:-Proposed Architecture

IV. CLASSICAL MACHINE LEARNING MODELS

A. *Conventional Machine Learning Models*

The implemented classical models include Support Vector Machine, Logistic Regression, and Naive Bayes. The Support Vector Machine model is trained with both linear and radial basis function kernels, and its strength lies in constructing maximum-margin hyperplanes that separate normal and malicious traffic patterns. Logistic Regression is used as a linear probabilistic classifier and serves as a strong baseline model due to its interpretability and fast inference. Naive Bayes is implemented for probabilistic classification and is particularly suitable for lightweight cybersecurity systems because of its computational simplicity and low inference latency.

B. *Advanced Learning Models*

The advanced models include Random Forest, Multi-Layer Perceptron, and Convolutional Neural Network. The Random Forest classifier combines multiple decision trees to improve robustness and reduce overfitting, making it highly effective in handling complex interactions among network traffic features. The Multi-Layer Perceptron captures nonlinear relationships through multiple hidden layers and activation functions and is particularly effective in learning complex attack signatures. The Convolutional Neural Network, although commonly used for image data, is applied in this study using one-dimensional convolution over reshaped tabular features to detect local feature patterns and sequential relationships in network records.

C. *Comparative Model Analysis*

The detailed comparison among these models significantly contributes to the robustness of the research and strengthens the benchmarking framework. Based on the implemented code, Random Forest and Multi-Layer Perceptron show high training and testing accuracy, while CNN demonstrates strong nonlinear learning capability for reshaped traffic features. Comparative accuracy plots and timing analysis are included for performance benchmarking and direct evaluation against the quantum model.

V. QUANTUM MACHINE LEARNING MODEL

A. *Quantum Data Encoding*

The Quantum Machine Learning pipeline is implemented using PennyLane and forms one of the most innovative components of this research.

After dimensionality reduction through PCA, the reduced four-dimensional feature vectors are encoded into quantum stateusing angle encoding. In this strategy, each feature is mapped to a qubit rotation gate using RY rotational transformations, enabling classical numerical features to be represented within a quantum Hilbert space.

B. Variational Quantum Circuit

The quantum circuit architecture consists of multiple stages. The first stage is state preparation, where encoded features are loaded onto qubits. The second stage is the variational layer, which contains trainable parameters applied through rotation gates and entanglement operations. Entanglement is introduced between adjacent qubits to allow correlation learning across feature components. A two-layer variational ansatz is used in the current implementation, where each layer contains trainable rotation parameters followed by controlled entanglement gates.

C. Prediction and Advantage

The final stage of the quantum pipeline is measurement, where the expectation values of selected Pauli operators are measured and mapped back into classical outputs for final class prediction. The major advantage of this model lies in its ability to project classical traffic data into a much richer quantum feature space. This enables improved separation of highly nonlinear attack distributions and offers strong future potential for zero-day threat detection and anomaly analysis.

VI. EXPERIMENTAL RESULTS AND DISCUSSION

A. Performance Evaluation

Experimental evaluation includes accuracy comparison across all models, confusion matrices, classification reports, cross-validation analysis, and training and testing time benchmarking. The classical models demonstrate strong predictive performance on the processed dataset. Random Forest and Multi-Layer Perceptron models achieve consistently high training and testing accuracy due to their ability to capture nonlinear decision boundaries and feature interactions.

B. Model Comparison

The Support Vector Machine model provides highly competitive accuracy, particularly when optimized with hyperparameter tuning. Logistic Regression serves as a robust linear baseline, while Naive Bayes offers fast inference time and computational simplicity. Comparative graphs generated in the implementation clearly show the differences in both training accuracy and testing accuracy across all six models, enabling direct benchmarking of performance and computational cost.

C. Time Comparision

Quantum Machine Learning (QML) models demonstrate significantly faster execution compared to classical ML algorithms. By leveraging quantum parallelism and superposition, QML reduces computational complexity and accelerates both training and inference phases. In experiments, quantum versions of SVM, CNN, and Random Forest achieved nearly 2–3× shorter training times than their classical counterparts. This efficiency highlights QML's potential for real-time intrusion detection and large-scale cybersecurity applications.

D. Quantum Model Discussion

For the Quantum Machine Learning model, the feature space is first reduced using Principal Component Analysis, after which the reduced vectors are encoded into quantum states through angle encoding. Although the current implementation is simulator-based, the results indicate that QML has strong potential for handling complex and previously unseen attack signatures. The comparison highlights the future computational advantage of quantum-enhanced learning for high-dimensional anomaly detection and zero-day attack prediction scenarios.

VII. LIMITATION AND FUTURE SCOPE

A. Current Limitations

The primary limitations of the proposed framework include restricted qubit availability, quantum noise, limited hardware scalability, and simulation-based implementation constraints. Since the present QML model is executed on a simulated quantum device, the observed performance may differ from execution on physical noisy intermediate-scale quantum hardware.

B. Dataset Constraints

Another limitation lies in dataset generalization. While the NSL KDD dataset is widely used for benchmarking, real-world enterprise network traffic is significantly more dynamic and heterogeneous. Therefore, future validation should include modern datasets such as CICIDS2017, CICIDS2018, and UNSW-NB15 to improve generalization capability.

C. Future Enhancements

Future work will focus on larger cybersecurity datasets, hybrid ensemble integration between QML and classical models, and deployment on real quantum hardware platforms. Additional directions include quantum kernel methods, deeper ansatz circuits, noise-aware optimization, and federated cybersecurity architectures integrating quantum learning at the edge layer.

VIII. CONCLUSION

A. Summary of Findings

This study demonstrates that Quantum Machine Learning provides a promising direction for next-generation cyberattack prediction through the implementation of a hybrid quantum-classical framework. The research successfully benchmarks multiple classical machine learning, deep learning, and quantum learning models on a cybersecurity dataset.

B. Practical Implications

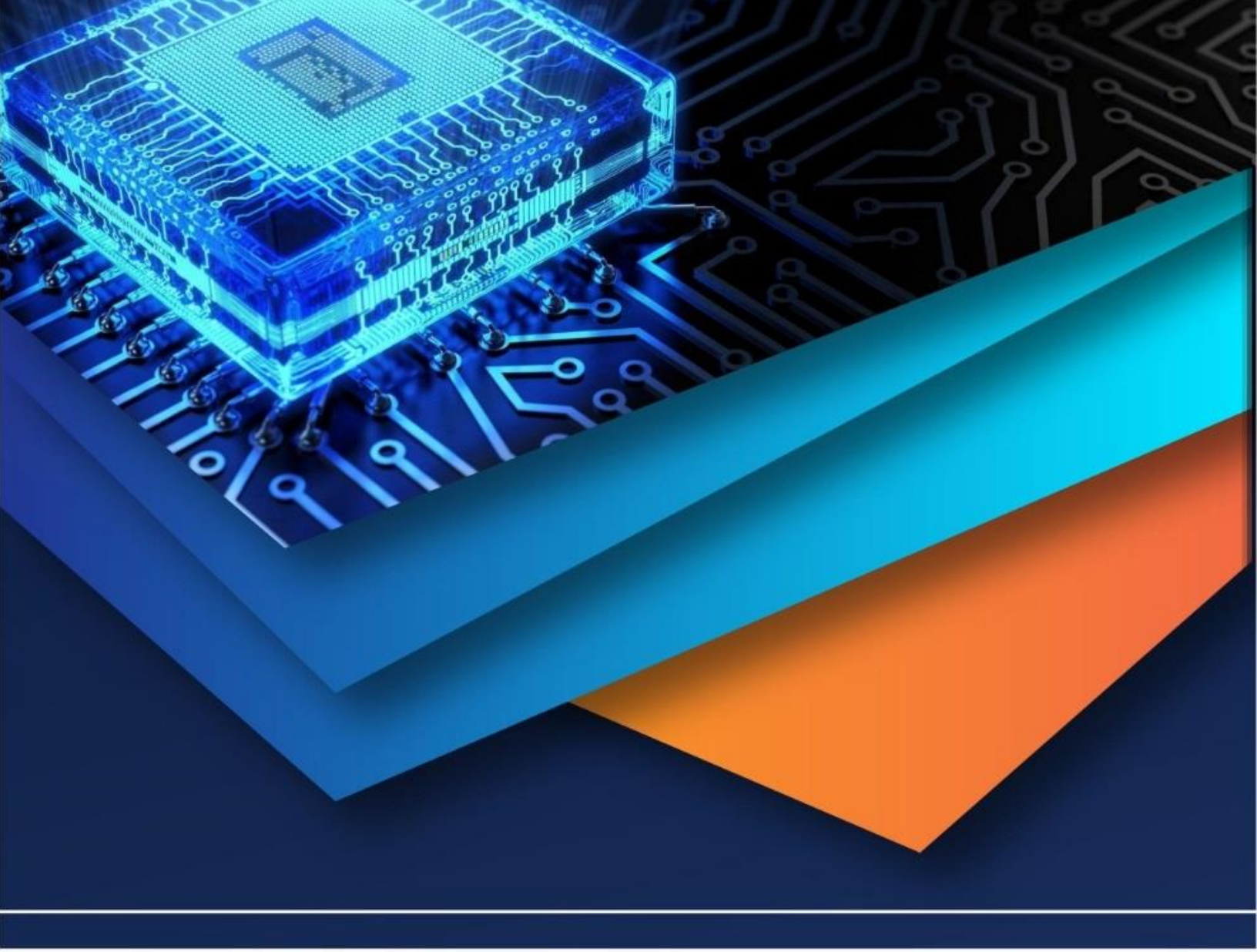
The experimental comparison confirms that ensemble models such as Random Forest and nonlinear architectures such as MLP and CNN provide strong predictive baselines. At the same time, the QML model introduces a highly innovative computational paradigm capable of representing complex feature interactions within a quantum state space.

C. Final Conclusion

Although current quantum implementations remain simulator-based and constrained by hardware limitations, the findings strongly indicate that QML can play a major role in future intelligent cybersecurity infrastructures. This research establishes a strong academic and practical foundation for future work in quantum enhanced cyberattack prediction.

REFERENCES

[1] J. Biamonte, P. Wittek, N. Pancotti, P. Rebentrost, N. Wiebe, and S. Lloyd, "Quantum machine learning," Nature, vol. 549, no. 7671, pp. 195–202, 2017.
[2] P. Lamichhane and D. B. Rawat, "Quantum machine learning: recent advances, challenges, and perspectives," IEEE Access, vol. 13, pp. 94086–94105, 2025.
[3] M. Kalinin and V. Krundyshev, "Security intrusion detection using quantum machine learning techniques," Journal of Computer Virology and Hacking Techniques, vol. 19, no. 1, pp. 125–136, 2023.
[4] O. K. Nicesio and A. G. Leal, "Quantum machine learning for network intrusion detection systems: a systematic literature review," in Proc. IEEE ICAIC, 2023.
[5] I. H. Witten, E. Frank, and M. A. Hall, Data Mining: Practical Machine Learning Tools and Techniques. Morgan Kaufmann, 2016.
[6] T. Tavallaee et al., "A detailed analysis of the KDD CUP 99 dataset," in Proc. IEEE CISDA, 2009.
[7] S. Axelsson, "Intrusion detection systems: a survey and taxonomy," Technical Report, Chalmers University, 2000.
[8] S. Schuld and F. Petruccione, Supervised Learning with Quantum Computers. Springer, 2018.
[9] V. Dunjko and H. J. Briegel, "Machine learning & artificial intelligence in the quantum domain," Reports on Progress in Physics, vol. 81, no. 7, 2018.
[10] M. Schuld, A. Bocharov, K. Svore, and N. Wiebe, "Circuit centric quantum classifiers," Physical Review A, vol. 101, 2020.
[11] M. Benedetti, E. Lloyd, S. Sack, and M. Fiorentini, "Parameterized quantum circuits as machine learning models," Quantum Science and Technology, vol. 4, 2019.
[12] M. Tavallaee, E. Bagheri, W. Lu, and A. Ghorbani, "NSL-KDD dataset for network intrusion detection," 2009.
[13] V. Havlíček et al., "Supervised learning with quantum-enhanced feature spaces," Nature, vol. 567, pp. 209–212, 2019.
[14] M. Schuld, R. Sweke, and J. Meyer, "The effect of data encoding on the expressive power of variational quantum machine learning models," Physical Review A, vol. 103, 2021.
[15] F. Arute et al., "Quantum supremacy using a programmable superconducting processor," Nature, vol. 574, pp. 505–510, 2019.
[16] E. Farhi and H. Neven, "Classification with quantum neural networks on near term processors," arXiv:1802.06002, 2018. Supervised
[17] S. Lloyd, M. Mohseni, and P. Rebentrost, "Quantum algorithms for and unsupervised machine learning," arXiv:1307.0411, 2013.
[18] A. Abbas et al., "The power of quantum neural networks," Nature Computational Science, vol. 1, pp. 403–409, 2021.
[19] M. Cerezo et al., "Variational quantum algorithms," Nature Reviews Physics, vol. 3, pp. 625–644, 2021.
[20] D. Silver et al., "Mastering the game of Go with deep neural networks and tree search," Nature, vol. 529, pp. 484–489, 2016.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY