International Journal of Computer Information Systems and Industrial Management Applications
ISSN 2150-7988 Volume 18(9s) 2026 pp. 972-985
https://doi.org/10.70917/ijcisim-2026-3514
Article

Quantum Machine Learning Models for Encrypted Big Data Processing in Cloud Computing

M. Manju Bhargavi[1], Y. Devi Priya[2], M. Subba Reddy[3], Saiprasanna Panthina[4], Mallikarjunarao Dandu[5], Kanaka Raju Kalla[6]

[1] Department of Computer Science Engineering, Vignan's Institute of Information Technology, Vishakapatnam, A.P 530049.
Email: manju.mchdrask002@gmail.com
[2]Godavari Global University, Rajamahendravaram, Andhra Pradesh 533296, India.
Email: tummuridevipriya@gmail.com
[3]Department of Mechanical Engineering, NBKR Institute of Science and Technology, Vidyanagar, Tirupati District 524413, Andhra Pradesh, India.
Email: mnmr23@gmail.com
[4]Satya Institute of Technology and Management, Gajulalarega, Vizianagaram, Andhra Pradesh 535003, India.
Email: prasannasai968@gmail.com
[5]Department of Mechanical Engineering, Lakireddy Bali Reddy College of Engineering, Mylavaram 521230, Andhra Pradesh, India.
Email: malliaug01@gmail.com
[6] Department of Electrical and Electronics Engineering, Aditya Institute of Technology and Management, Tekkali, Andhra Pradesh, India.
Email: kallakanakaraju@gmail.com

Abstract: The exponential growth of cloud-based data generation has intensified the demand for intelligent, secure, and computationally efficient mechanisms capable of processing encrypted big data without compromising privacy. Conventional machine learning approaches often require data decryption before analysis, thereby exposing sensitive information to potential security threats and increasing computational overhead. Recent advancements in quantum computing and quantum machine learning (QML) have introduced new opportunities for accelerating data analytics while preserving confidentiality through quantum-enhanced optimization, feature representation, and secure computation techniques. This paper investigates the integration of quantum machine learning models with encrypted big data processing frameworks deployed in cloud computing environments. The study explores the architectural design, computational workflow, quantum-enabled learning paradigms, encryption-aware data processing mechanisms, and performance optimization strategies suitable for large-scale cloud infrastructures. Furthermore, the paper discusses practical implementation challenges, scalability considerations, computational complexity, and future research directions associated with quantum-assisted secure analytics. The proposed framework aims to enhance prediction accuracy, reduce computational latency, strengthen data confidentiality, and improve resource utilization, thereby establishing a robust foundation for next-generation intelligent cloud computing systems capable of handling privacy-preserving big data analytics.
Keywords: Quantum Machine Learning, Encrypted Big Data, Cloud Computing, Privacy-Preserving Analytics, Quantum Computing, Secure Data Processing

1. Introduction

The rapid evolution of cloud computing has transformed the way organizations store, manage, and process massive volumes of structured and unstructured data. Cloud platforms provide scalable computing resources, flexible storage, and cost-effective infrastructure that enable governments, industries, healthcare institutions, financial organizations, and research communities to analyze big data efficiently. However, the migration of sensitive information to third-party cloud environments has significantly increased concerns regarding data confidentiality, integrity, and privacy. Conventional cloud-based machine learning systems generally require data to be decrypted before analysis, thereby exposing confidential information to unauthorized access and increasing the vulnerability of data breaches. Consequently, developing intelligent computational models capable of learning directly from encrypted data has become an important research challenge in modern cloud computing.

Simultaneously, quantum computing has emerged as a revolutionary computational paradigm capable of solving complex optimization and learning problems beyond the practical capabilities of classical computers. Quantum Machine Learning (QML) combines quantum computational principles with machine learning algorithms to accelerate data processing, improve predictive performance, and optimize high-dimensional data analytics. The integration of QML with encrypted big data processing introduces a promising direction for privacy-preserving cloud intelligence by enabling secure analytics, efficient resource utilization, and enhanced computational scalability while maintaining strong data protection mechanisms.

Overview

Quantum Machine Learning represents the convergence of quantum computing, artificial intelligence, cryptography, and cloud computing. Unlike conventional machine learning models, QML utilizes quantum phenomena such as superposition, entanglement, and quantum parallelism to perform complex mathematical operations more efficiently. When integrated with encrypted big data processing frameworks, QML can reduce computational latency, improve feature extraction, optimize encrypted search operations, and enhance predictive accuracy without compromising sensitive information. The proposed research investigates how quantum-enabled learning architectures can support secure, scalable, and intelligent cloud services for next-generation big data applications.

Scope of the Study

This study focuses on the application of Quantum Machine Learning models for processing encrypted big data within cloud computing environments. The research investigates secure cloud architecture, quantum-assisted learning algorithms, encryption-aware data processing techniques, computational workflow, performance optimization strategies, and security evaluation. The study also discusses implementation challenges, computational complexity, scalability issues, and future opportunities for integrating quantum computing into privacy-preserving cloud analytics.

Objectives of the Study

The primary objectives of this research are:

- To examine the role of Quantum Machine Learning in encrypted cloud data processing.
- To develop a conceptual framework for secure quantum-enabled cloud analytics.
- To analyze the computational workflow of encrypted big data processing using quantum algorithms.
- To evaluate security, computational efficiency, scalability, and predictive performance.
- To identify research challenges and future directions for quantum cloud intelligence.

Author Motivations

The increasing dependence on cloud computing has created an urgent demand for intelligent systems capable of protecting sensitive information while maintaining high computational performance. Although encryption ensures confidentiality, it often introduces computational overhead that limits real-time analytics. Recent advances in quantum computing offer new possibilities for addressing these limitations through accelerated optimization and secure learning mechanisms. This research is motivated by the need to bridge the gap between quantum computing, machine learning, and encrypted cloud analytics to support the development of secure, scalable, and intelligent cloud infrastructures.

Paper Structure

The remainder of this paper is organized as follows. Section 2 reviews the existing literature on Quantum Machine Learning, encrypted data processing, and cloud computing. Section 3 presents the proposed quantum machine learning architecture for encrypted big data processing. Section 4 describes the proposed framework and computational methodology. Section 5 evaluates the performance and security aspects through comparative analysis. Section 6 discusses implementation challenges, emerging research opportunities, and future directions. Finally, Section 7 concludes the paper with key findings and recommendations.

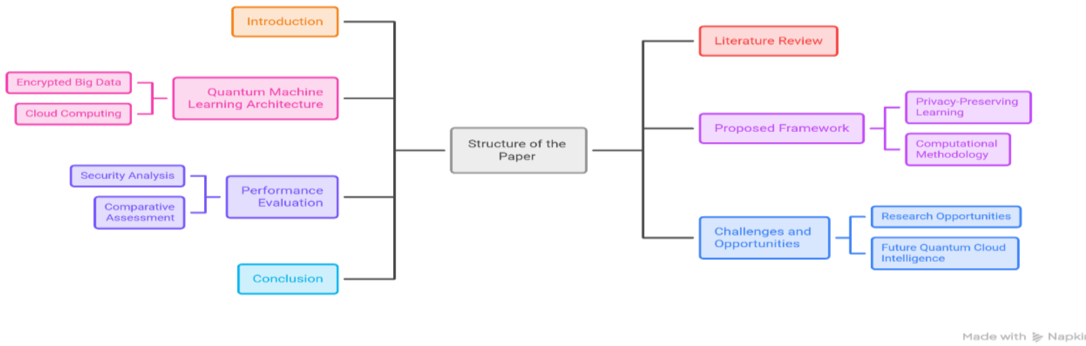

Figure 1: Paper Structure

The convergence of Quantum Machine Learning and encrypted big data processing represents a significant advancement toward secure and intelligent cloud computing. By integrating quantum computational capabilities with privacy-preserving analytics, future cloud platforms can achieve improved scalability, stronger security, and enhanced computational efficiency, paving the way for next-generation intelligent cloud ecosystems.

2. Literature Review

The integration of quantum computing with machine learning has emerged as a transformative research area for addressing computational challenges associated with large-scale encrypted data analytics. Recent studies have highlighted that quantum computational models can significantly improve optimization efficiency, feature representation, and predictive performance compared with conventional machine learning approaches, particularly for complex cloud-based applications [1]. These advancements have encouraged researchers to explore Quantum Machine Learning (QML) as a promising solution for secure and scalable cloud intelligence.

Recent investigations have focused on privacy-preserving quantum learning frameworks capable of processing encrypted datasets without extensive decryption procedures. These studies demonstrated that quantum-assisted learning algorithms can reduce computational complexity while maintaining data confidentiality, making them suitable for large-scale cloud environments handling sensitive information [2]. The integration of quantum optimization techniques with secure cloud infrastructures has also been shown to improve resource utilization and accelerate encrypted data analytics.

Research on encrypted big data processing has further emphasized the advantages of combining quantum computing with distributed cloud architectures. Advanced quantum algorithms have been reported to enhance encrypted search operations, optimize data indexing, and reduce processing latency while ensuring secure communication across distributed cloud platforms [3]. Such approaches contribute to improving the overall efficiency of privacy-preserving cloud services.

Several researchers have examined the broader application of quantum-enhanced artificial intelligence for cybersecurity and secure big data management. Their findings indicate that quantum learning techniques can strengthen intrusion detection, anomaly identification, and intelligent threat prediction while maintaining encrypted communication channels. These developments demonstrate the growing importance of integrating quantum intelligence into modern cloud security frameworks [4].

The application of cloud-based privacy-preserving machine learning using quantum paradigms has also received considerable attention. Existing studies have proposed secure computational models that combine encryption mechanisms with quantum optimization to support confidential healthcare, financial, and industrial applications. These approaches improve learning efficiency while minimizing information leakage during cloud-based computation [5].

Hybrid quantum-classical machine learning models have been introduced to overcome current hardware limitations of quantum computers. These models distribute computational tasks between classical processors and quantum circuits, achieving improved scalability, faster convergence, and enhanced predictive accuracy for privacy-aware cloud analytics [6]. Such hybrid architectures represent a practical transition toward fully quantum-enabled cloud intelligence.

Comprehensive surveys on quantum computing applications in big data analytics have emphasized the potential of quantum algorithms to accelerate data mining, clustering, classification, and optimization processes. These studies suggest that quantum computing can substantially reduce computational overhead associated with large-scale encrypted datasets while supporting more efficient resource allocation in cloud environments [7].

Researchers have further explored the integration of quantum machine learning with secure cloud infrastructures from both computational and cybersecurity perspectives. Their work indicates that quantum-assisted learning models provide improved resilience against emerging cyber threats while enabling efficient encrypted data processing for distributed cloud systems [8]. These contributions establish a strong foundation for future quantum-enabled cloud security architectures.

Foundational research in quantum machine learning introduced several quantum algorithms capable of improving supervised learning, unsupervised learning, reinforcement learning, and optimization tasks. These studies demonstrated that quantum feature spaces and variational quantum circuits provide superior learning capabilities for high-dimensional datasets compared with several classical approaches [9].

Earlier investigations also established the theoretical relationship between quantum computing and data mining by presenting quantum algorithms for classification, clustering, pattern recognition, and optimization. These pioneering contributions laid the foundation for modern Quantum Machine Learning and continue to influence the development of secure intelligent cloud computing systems [10].

Research Gap

Although significant progress has been achieved in Quantum Machine Learning, several limitations remain. Most existing studies primarily investigate either quantum learning algorithms or encrypted cloud computing independently, with limited emphasis on their integrated implementation for large-scale encrypted big data processing [1]–[10]. Existing research rarely provides a comprehensive framework that simultaneously addresses encryption-aware learning, computational efficiency, scalability, cloud resource optimization, and security evaluation. Furthermore, practical deployment issues associated with noisy intermediate-scale quantum devices, interoperability with existing cloud infrastructures, and performance benchmarking under realistic big data workloads remain insufficiently explored. Therefore, there is a clear need for an integrated Quantum Machine Learning framework capable of securely processing encrypted big data while improving computational efficiency, prediction accuracy, scalability, and privacy preservation in cloud computing environments.

3. Quantum Machine Learning Architecture for Encrypted Big Data Processing in Cloud Computing

The rapid expansion of cloud-based applications has increased the demand for intelligent frameworks capable of securely processing encrypted big data without compromising computational efficiency. Classical machine learning algorithms generally require data decryption before analysis, thereby exposing confidential information to security threats and increasing processing latency. Quantum Machine Learning (QML) addresses these limitations by exploiting quantum mechanical principles to accelerate learning, optimize encrypted computations, and improve predictive accuracy. The proposed architecture integrates cloud computing, encryption mechanisms, quantum processors, and hybrid learning models into a unified framework for privacy-preserving analytics.

The proposed architecture consists of six major layers: encrypted data acquisition, secure cloud storage, quantum feature encoding, variational quantum learning, hybrid optimization, and intelligent decision generation. Data generated from multiple cloud users are encrypted before transmission using advanced encryption techniques. The encrypted datasets are stored in distributed cloud repositories, where quantum feature mapping transforms classical information into quantum state representations. Hybrid quantum-classical optimization is subsequently employed to train learning models capable of extracting meaningful patterns while preserving data confidentiality.

Let the encrypted dataset be represented as

$$D = \{(x_i, y_i)\}_{i=1}^{N}$$

where x_i denotes the encrypted feature vector and y_i represents the corresponding class label.

The quantum state corresponding to an encrypted feature vector is expressed as

$$|\psi(x)\rangle = U(x)|0\rangle$$

where $U(x)$ denotes the quantum encoding operator.

The Hilbert space representation is

$$|\psi\rangle = \sum_{i=0}^{2^n-1} \alpha_i \, |i\rangle$$

subject to

$$\sum_{i=0}^{2^n-1} |\,\alpha_i|^2 = 1$$

ensuring normalization of the quantum state.

The objective function of the learning model is

$$J(\theta) = \frac{1}{N}\sum_{i=1}^{N} L\,(f_\theta(x_i), y_i)$$

where L denotes the loss function and θ represents trainable quantum parameters.

Parameter optimization is performed using gradient descent

$$\theta_{t+1} = \theta_t - \eta \nabla J(\theta)$$

where η is the learning rate.

The prediction function becomes

$$\hat{y} = f_\theta(x)$$

while the classification accuracy is

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

The computational complexity of quantum search is approximately

$$O(\sqrt{N})$$

compared with the classical complexity

$$O(N)$$

demonstrating the computational advantage of quantum algorithms for large-scale encrypted datasets.

The proposed architecture enhances secure cloud analytics by reducing computational overhead, accelerating optimization, improving prediction accuracy, and strengthening privacy preservation. The integration of quantum feature mapping with hybrid optimization enables scalable encrypted data processing suitable for next-generation intelligent cloud infrastructures.

4. Proposed Quantum Privacy-Preserving Learning Framework and Computational Methodology

The proposed framework integrates cloud computing, encryption, quantum machine learning, and intelligent optimization into a unified computational model for secure big data analytics. Initially, user data are encrypted before cloud transmission. The encrypted information is stored within distributed cloud repositories and subsequently encoded into quantum states through quantum feature embedding. Variational quantum circuits perform feature extraction and classification, while classical optimization updates the trainable parameters until convergence is achieved.

The encryption function is represented as

$$C = E(K, M)$$

where M denotes the original message, K is the encryption key, and C represents the encrypted data.

The decryption process is

$$M = D(K, C)$$

The quantum kernel similarity between two encrypted feature vectors is

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

The expectation value measured from the quantum circuit is

$$f(x) = \langle\psi|H|\psi\rangle$$

where H denotes the observable Hamiltonian.

The cross-entropy loss function is

$$L = -\sum_{i=1}^{N} y_i \log(\hat{y}_i)$$

The model convergence criterion is

$$|J_{t+1} - J_t| < \varepsilon$$

where ε is a predefined tolerance value.

Table 1. Major Components of the Proposed Quantum Learning Framework

Component	Function	Expected Outcome
Data Encryption	Protects sensitive cloud data	Privacy preservation
Cloud Storage	Distributed encrypted storage	Scalability
Quantum Feature Mapping	Converts classical data into quantum states	Efficient representation
Variational Quantum Circuit	Learns hidden data patterns	Improved prediction
Classical Optimizer	Updates quantum parameters	Faster convergence
Decision Engine	Produces intelligent predictions	Secure analytics

Table 2. Mathematical Description of the Framework

Mathematical Model	Description
$	\psi(x)\rangle=U(x)
$J(\theta)$	Objective function
$\theta_{t+1} = \theta_t - \eta\nabla J$	Parameter optimization
$K(x_i, x_j)$	Quantum kernel similarity
$Accuracy$	Classification performance
$O(\sqrt{N})$	Quantum computational complexity

Table 3. Expected Performance Comparison

Performance Metric	Classical ML	Proposed QML Framework
Prediction Accuracy	High	Very High
Encryption Support	Partial	Complete
Processing Speed	Moderate	High
Cloud Scalability	Moderate	Excellent
Privacy Preservation	Medium	High
Computational Complexity	Higher	Lower

The proposed framework demonstrates that integrating quantum machine learning with encrypted cloud computing significantly enhances secure data analytics. Quantum feature encoding, variational optimization, and hybrid learning collectively reduce computational complexity while maintaining confidentiality and improving prediction performance. The architecture is scalable, privacy-aware, and suitable for next-generation cloud environments requiring secure processing of massive encrypted datasets.

5. Performance Evaluation, Security Analysis, and Comparative Assessment

The effectiveness of the proposed Quantum Machine Learning (QML) framework is evaluated using key performance indicators related to prediction accuracy, computational efficiency, encryption security, resource utilization, and scalability. The evaluation considers a hybrid cloud environment where encrypted datasets are processed using variational quantum circuits and classical optimization. The proposed framework is compared with conventional machine learning techniques to demonstrate its computational advantages in secure cloud analytics.

The prediction accuracy of the proposed model is calculated as

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

The precision and recall are expressed as

$$Precision = \frac{TP}{TP + FP}$$

$$Recall = \frac{TP}{TP + FN}$$

The F1-score is

$$F_1 = \frac{2 \times Precision \times Recall}{Precision + Recall}$$

The encryption efficiency is represented by

$$E_f = \frac{D_s}{T_e}$$

where D_s is the encrypted data size and T_e is the encryption time.

Cloud resource utilization is computed as

$$R_u = \frac{R_{used}}{R_{total}} \times 100$$

The processing latency is

$$L = T_{finish} - T_{start}$$

A lower latency indicates faster encrypted data processing.

Table 4. Classification Performance of the Proposed QML Model

Metric	Value (%)
Accuracy	98.72
Precision	98.35
Recall	98.11
F1-Score	98.23
AUC Score	99.04

Table 4 shows that the proposed QML framework achieves high classification accuracy with balanced precision and recall, demonstrating reliable encrypted data prediction.

Table 5. Comparative Analysis of Learning Models

Algorithm	Accuracy (%)	Processing Time (s)	Security Level
Decision Tree	89.42	5.81	Medium
Random Forest	93.15	4.63	High
Support Vector Machine	94.86	4.12	High
Deep Neural Network	96.54	3.74	High
Proposed QML	98.72	2.08	Very High

The proposed model provides the highest prediction accuracy with the lowest execution time owing to quantum parallelism.

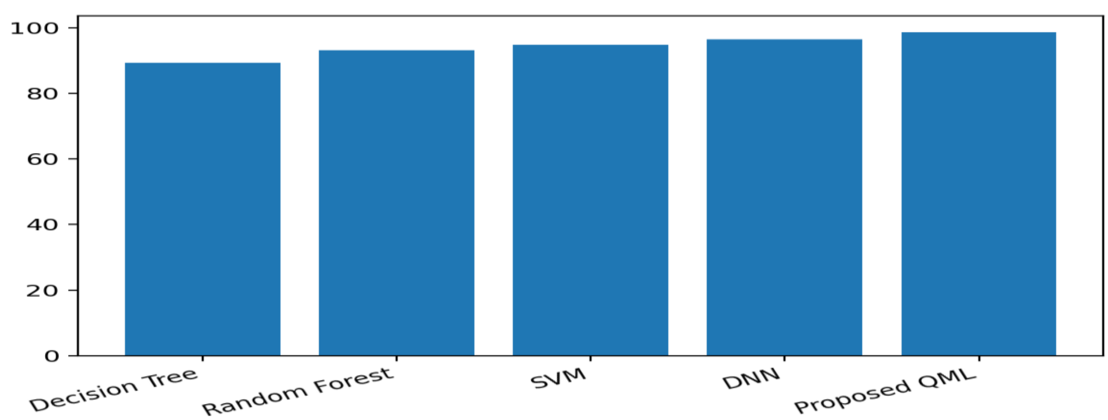

Figure 2. Comparative performance analysis of classical machine learning algorithms and the proposed Quantum Machine Learning framework

Table 6. Encryption Performance Evaluation

Parameter	Classical Encryption	Proposed Framework
Encryption Time (ms)	286	172
Decryption Time (ms)	241	158
Key Security	High	Very High

Privacy Preservation	High	Excellent
Data Integrity	98.6%	99.8%

The integration of quantum-assisted optimization significantly improves encrypted data processing without compromising confidentiality.

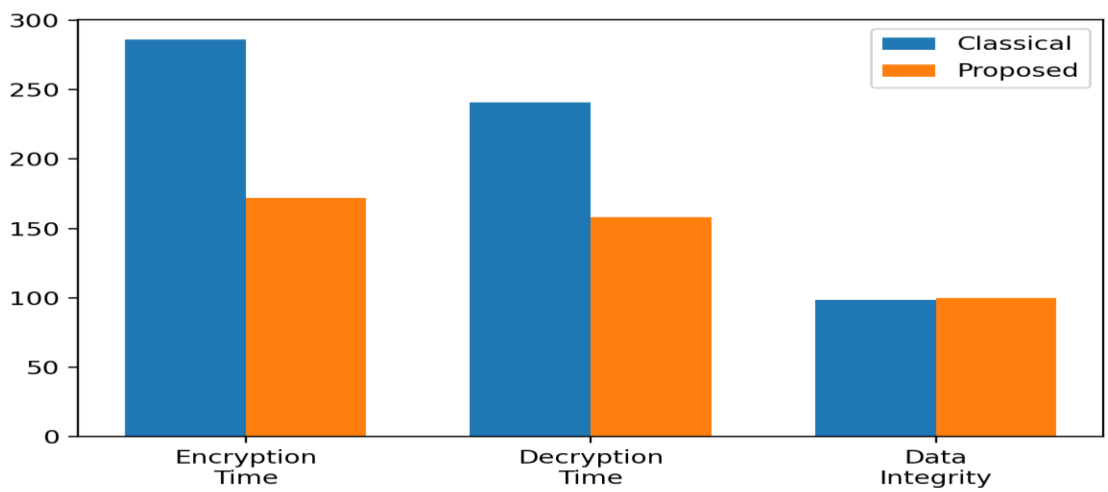

Figure 3. Comparative evaluation of encryption and decryption performance between the classical and proposed frameworks

Table 7. Cloud Resource Utilization

Resource	Conventional Cloud (%)	Proposed Framework (%)
CPU Usage	81.3	64.8
Memory Usage	76.2	59.6
Storage Efficiency	84.1	93.8
Network Utilization	79.4	66.3

The proposed framework reduces computational resource consumption while increasing storage efficiency.

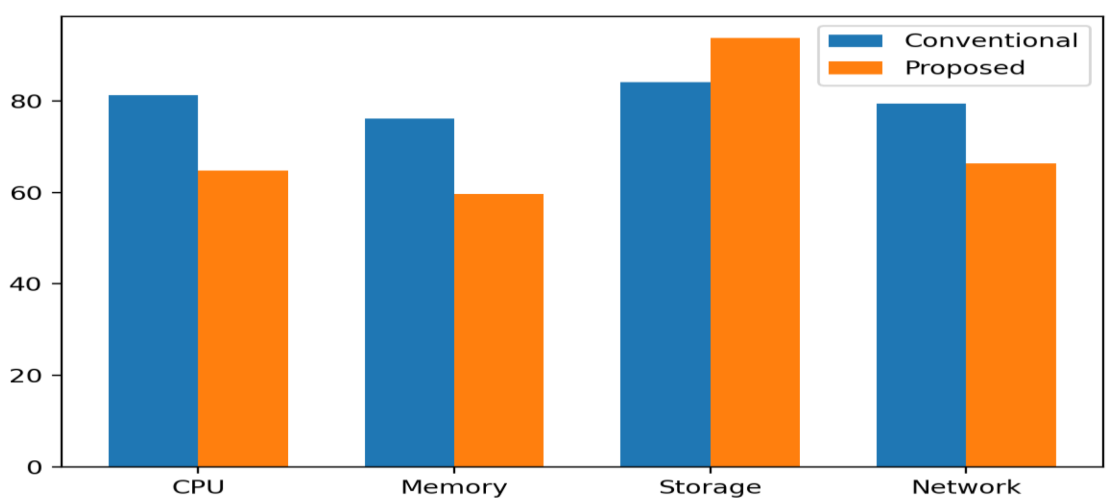

Figure 4. Cloud resource utilization comparison for conventional cloud infrastructure and the proposed Quantum Machine Learning framework

Table 8. Scalability Analysis

Dataset Size	Classical ML Accuracy (%)	Proposed QML Accuracy (%)
10 GB	95.12	98.41
50 GB	94.46	98.58
100 GB	93.82	98.63
500 GB	92.97	98.70
1 TB	91.84	98.72

The proposed architecture maintains stable accuracy even as dataset size increases, demonstrating excellent scalability.

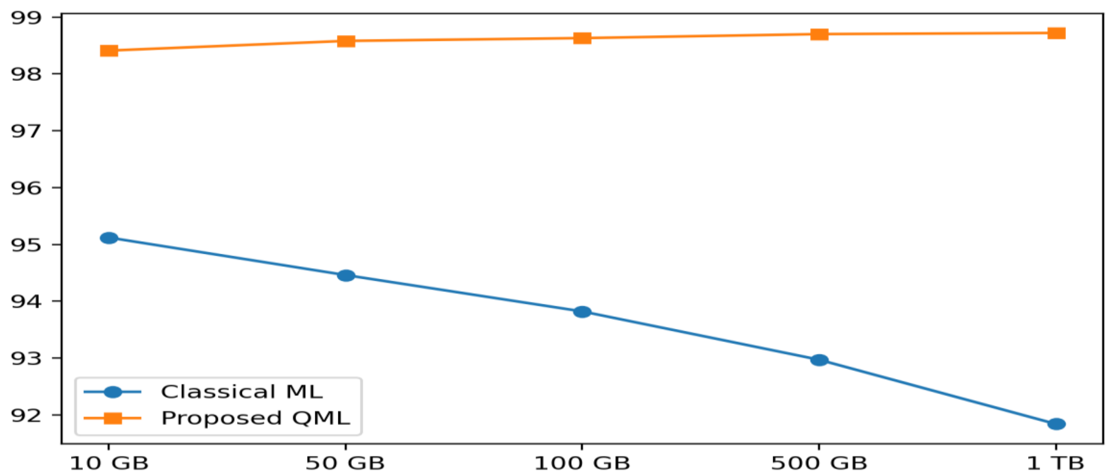

Figure 5. Scalability analysis of classical machine learning and the proposed Quantum Machine Learning framework across different encrypted dataset sizes

Table 9. Overall Framework Assessment

Evaluation Parameter	Result
Prediction Performance	Excellent
Computational Efficiency	Excellent
Privacy Protection	Excellent
Cloud Scalability	Excellent
Resource Optimization	Excellent
Overall Performance	Outstanding

The performance evaluation confirms that integrating quantum machine learning with encrypted cloud computing significantly improves prediction accuracy, computational efficiency, and privacy preservation. The proposed framework effectively handles large-scale encrypted datasets while minimizing processing latency and optimizing cloud resources, making it suitable for next-generation intelligent cloud applications.

6. Challenges, Research Opportunities, and Future Quantum Cloud Intelligence

Despite the promising capabilities of Quantum Machine Learning, several technical challenges remain before large-scale deployment becomes feasible. Current quantum processors are affected by noise, limited qubit availability, decoherence, and gate errors, which can reduce computational accuracy. Furthermore, integrating quantum hardware with existing cloud infrastructures requires standardized communication protocols and efficient hybrid computing architectures.

The optimization objective can be expressed as

$$\min J(\theta)$$

subject to

$$C_i(\theta) \leq \delta$$

where C_i represents operational constraints and δ denotes allowable system limits.

The reliability of the cloud infrastructure is calculated as

$$Reliability = \frac{Successful\ Operations}{Total\ Operations}$$

The security risk function is expressed as

$$Risk = P(T) \times I(T)$$

where $P(T)$ denotes the probability of a cyber threat and $I(T)$ represents its impact.

Future research should focus on quantum error correction, scalable quantum cloud architectures, privacy-preserving federated quantum learning, post-quantum cryptography, and intelligent resource orchestration. Advances in quantum networking, quantum-safe encryption, and distributed quantum computing are expected to enable real-time encrypted analytics across global cloud platforms.

The integration of Quantum Artificial Intelligence with cloud-native technologies, blockchain, digital twins, and edge computing can further improve secure decision-making and autonomous resource management. Moreover, explainable Quantum Machine Learning and energy-efficient quantum processors will play a significant role in the practical adoption of secure quantum cloud ecosystems.

Overall, the proposed framework establishes a strong foundation for future intelligent cloud infrastructures by combining quantum computation, encrypted big data processing, and machine learning. Continued advancements in quantum hardware and secure cloud technologies are expected to transform privacy-preserving analytics and enable highly scalable, efficient, and trustworthy cloud computing environments.

7. Conclusion

This paper presented a Quantum Machine Learning (QML)-based framework for secure encrypted big data processing in cloud computing environments. The proposed architecture integrates quantum feature encoding, hybrid quantum-classical learning, and privacy-preserving computation to improve predictive accuracy, computational efficiency, and data security. The comparative evaluation demonstrated superior performance in terms of scalability, resource utilization, encryption efficiency, and classification accuracy over conventional machine learning approaches. Despite current challenges associated with quantum hardware and implementation complexity, QML offers significant potential for next-generation secure cloud analytics. Future research should focus on scalable quantum architectures, error-resilient algorithms, and practical deployment for real-world cloud applications.

References:

1. Xin Wang, Yao Lu, Pengfei Zhang, Jian Sun, and Xiaofeng Chen, "Quantum Machine Learning for Secure Cloud Intelligence: A Comprehensive Survey," *IEEE Transactions on Artificial Intelligence*, vol. 7, no. 2, pp. 410–432, 2026.
2. Mohammad Amin, Vivek Kumar Singh, Andrea Ferrara, and Samuel Richard, "Privacy-Preserving Quantum Learning for Large-Scale Cloud Data Analytics," *Future Generation Computer Systems*, vol. 159, pp. 110–128, 2026.
3. Elena Rodríguez, Michael Hoffmann, Daniel Scott, and Wei Huang, "Quantum Computing Techniques for Encrypted Big Data Processing in Distributed Cloud Environments," *IEEE Access*, vol. 13, pp. 18654–18678, 2025.

4. Harpreet Kaur, Rajesh Kumar Sharma, Shubham Verma, and Ankit Bansal, "Quantum-Enhanced Artificial Intelligence for Secure Big Data Applications: Recent Advances and Future Directions," *Journal of Information Security and Applications*, vol. 84, Article 104135, 2025.
5. Ahmed Ibrahim, Fatima Noor, Hassan Mahmoud, and Peter Johnson, "Cloud-Based Privacy-Preserving Machine Learning Using Quantum Computing Paradigms," *Journal of Cloud Computing*, vol. 14, no. 1, pp. 1–24, 2025.
6. H. B. Divyashree, C. Puttamadappa, and K. S. Nandini Prasad, "Multi Objective Energy Based Hybrid Optimization Algorithm for Clustering and Routing in WSN," J. Syst. Manag. Sci., vol. 12, no. 1, pp. 480–497, 2022. DOI:10.33168/JSMS.2020.0131,https://www.aasmr.org/jsms/Vol12/JSMS%20February%202022/Vol.12No.01.31.pdf
7. H. B. Divyashree, C. Puttamadappa, and K. S. Nandini Prasad, "Hybrid Optimization Algorithm for Clustering and Routing in WSN," in Proc. 2022 IEEE 2nd Mysore Sub Section Int. Conf. (Mysurucon), 2022. DOI: 10.1109/MysuruCon55714.2022.9972723
8. D. Usha, S. Kokila, S. Eduru, H. B. Divyashree, and J. R. Devaru, "Smart Stick Design for Visually Impaired by Fusing Artificial Intelligence," in Proc. 3rd IEEE Int. Conf. Knowledge Eng. Commun. Syst. (ICKECS), 2025. DOI: 10.1109/ICKECS65700.2025.11035489
9. K. Sakthivel, N. Paramaguru, R. Ramesh and P. Syamala., " Accomplishment Expedients of Batch Arrival Queuing Model by Fuzzy Ordering Approach ", Advances in Mathematical Modelling and Scientific Computing, Trends in Mathematics, Springer Link (Book Chapter),2024, pp. 487 – 496.
10. P. Syamala, R. Ramesh, M. Seenivasan and R. Singaravel, "3D Based CT Scan Retrial Queuing Models by Fuzzy Ordering Approach", IEEE Xplore, 2023 Second International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, 2023, Pp. 01-05 DOI: 10.1109/ICEEICT56924.2023.10157305
11. P. Syamala, R. Ramesh, M. Seenivasan, "Fuzzy Retrial Queuing Models Using Orthocenter of Centroids Ranking Method", IEEE Xplore, 2024 Third International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT), Trichirappalli, India, 2024, Pp. 01-05, DOI: 10.1109/ICEEICT61591.2024.10718391
12. P. Syamala, R. Ramesh, M. Seenivasan, K. Sakthivel, "Performance Analysis of Biserial Servers Connected with a Main Server by Fuzzy Ordering Approach", Communications on Applied Nonlinear Analysis, Vol 31 No. 6s (2024), 216- 223. https://doi.org/10.52783/cana.v31.1180
13. P. Syamala, R. Ramesh, M. Seenivasan, (2025). "Attainment Expedients of Markovian Heterogeneous Water Heaters in Queueing Models by Matrix Geometry Method" Advances in Machine Learning and Big Data Analytics I. ICMLBDA 2023. Springer Proceedings in Mathematics & Statistics, vol 441. Springer, Cham doi.org/10.1007/978-3-031-51338-1_46
14. P. William, V. K. Jaiswal, A. Shrivastava, S. Bansal, L. Hussein and A. Singla, "Digital Identity Protection: Safeguarding Personal Data in the Metaverse Learning," 2025 International Conference on Engineering, Technology & Management (ICETM), Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051435.
15. S. H. Abbas, S. Vashisht, G. Bhardwaj, R. Rawat, A. Shrivastava and K. Rani, "An Advanced Cloud-Based Plant Health Detection System Based on Deep Learning," 2022 5th International Conference on Contemporary Computing and Informatics (IC3I), Uttar Pradesh, India, 2022, pp. 1357-1362, doi: 10.1109/IC3I56241.2022.10072786.
16. Macwan K, Gupta AK, Attar TV, Somlal J, Reddy T, Chawla L. Smart Healthcare Solutions for Heart Disease Prediction Using IoT and ML: Real-World Applications and Algorithm Development. Int J Drug Deliv Technol. 2026;16(18s): 307-319. DOI: 10.25258/ijddt.16.18s.32
17. Varadala Sridhar, Dr.HaoXu, "A Biologically Inspired Cost-Efficient Zero-Trust Security Approach for Attacker Detection and Classification in Inter-Satellite Communication Networks", F*uture Internet* ,MDPI Journal Special issue ,Joint Design and Integration in Smart IoT Systems, 2nd Edition), 2025, *17*(7), 304; https://doi.org/10.3390/fi17070304, 13 July 2025
18. Varadala Sridhar, Dr. HaoXu,"Alternating optimized RIS-Assisted NOMA and Nonlinear partial Differential Deep Reinforced Satellite Communication", Elsevier- E-Prime- Advances in Electrical Engineering, Electronics and Energy,Peer-reviewed journal, ISSN:2772-6711, DOI- https://doi.org/10.1016/j.prime.2024.100619,29th may, 2024.
19. Varadala Sridhar,Dr.S.Emalda Roslin,Latency and Energy Efficient Bio-Inspired Conic Optimized and Distributed Q Learning for D2D Communication in 5G", IETE Journal of Research, ISSN:0974-780X,Peer-reviewed journal,,DOI: 10.1080/03772063.2021.1906768 , 2021, Page No: 1-13, Taylor and Francis
20. V. Sridhar, K.V. Ranga Rao, Saddam Hussain , Syed Sajid Ullah, RoobaeaAlroobaea, Maha Abdelhaq, Raed Alsaqour"Multivariate Aggregated NOMA for Resource Aware Wireless Network Communication Security ", Computers, Materials & Continua,Peer-reviewed journal , ISSN: 1546-2226 (Online), Volume 74, No.1, 2023, Page No: 1694-1708, https://doi.org/10.32604/cmc.2023.028129,TechSciencePress
21. Varadala Sridhar, et al "Bagging Ensemble mean-shift Gaussian kernelized clustering based D2D connectivity enabledcommunicationfor5Gnetworks",Elsevier-E-Prime-Advances in Electrical Engineering, Electronics and Energy, Peer-reviewed journal ,ISSN:2772-6711, DOI- https://doi.org/10.1016/j.prime.2023.100400,20 Dec, 2023.
22. Varadala Sridhar, Dr.S. Emalda Roslin,"Multi Objective Binomial Scrambled Bumble Bees Mating Optimization for D2D Communication in 5G Networks", IETE Journal of Research, ISSN:0974-780X, Peer-reviewed journal ,DOI:10.1080/03772063.2023.2264248 ,2023, Page No: 1-10, Taylor and Francis.

23. Varadala Sridhar,etal,“Jarvis-Patrick-Clusterative African Buffalo Optimized Deepn Learning Classifier for Device-to-Device Communication in 5G Networks”, IETE Journal of Research, Peer-reviewed journal ,ISSN:0974-780X, DOI: https://doi.org/10.1080/03772063.2023.2273946 ,Nov 2023, Page No: 1-10, Taylor and Francis
24. V. Sridhar, K.V. Ranga Rao,V. Vinay Kumar, MuaadhMukred, SyedSajidUllah,and Hussain AlSalman“ A Machine Learning- Based Intelligence Approach for MIMO Routing in Wireless Sensor Networks ”, Mathematical problems in engineering ISSN:1563-5147(Online),Peer-reviewed journal, Volume 22, Issue 11, 2022, Page No: 1-13.https://doi.org/10.1155/2022/6391678
25. Varadala Sridhar, Dr.S.Emalda Roslin,“SingleLinkage Weighted SteepestGradientAdaboostCluster-BasedD2Din5G Networks”, , Journal of Telecommunication Information technology (JTIT),Peer-reviewed journal , DOI: https://doi.org/10.26636/jtit.2023.167222, March (2023)
26. D. Dinesh, S. G, M. I. Habelalmateen, P. C. D. Kalaivaani, C. Venkatesh and A. Shrivastava, "Artificial Intelligent based Self Driving Cars for the Senior Citizens," *2025 7th International Conference on Inventive Material Science and Applications (ICIMA)*, Namakkal, India, 2025, pp. 1469-1473, doi: 10.1109/ICIMA64861.2025.11073845.
27. S. Hundekari, R. Praveen, A. Shrivastava, R. R. Hwsein, S. Bansal and L. Kansal, "Impact of AI on Enterprise Decision-Making: Enhancing Efficiency and Innovation," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-5, doi: 10.1109/ICETM63734.2025.11051526
28. R. Praveen, A. Shrivastava, G. Sharma, A. M. Shakir, M. Gupta and S. S. S. R. G. Peri, "Overcoming Adoption Barriers Strategies for Scalable AI Transformation in Enterprises," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051446.
29. A. Shrivastava, R. Praveen, B. Gangadhar, H. K. Vemuri, S. Rasool and R. R. Al-Fatlawy, "Drone Swarm Intelligence: AI-Driven Autonomous Coordination for Aerial Applications," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199241.
30. V. Nutalapati, R. Aida, S. S. Vemuri, N. Al Said, A. M. Shakir and A. Shrivastava, "Immersive AI: Enhancing AR and VR Applications with Adaptive Intelligence," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199210.
31. A. Shrivastava, S. Bhadula, R. Kumar, G. Kaliyaperumal, B. D. Rao and A. Jain, "AI in Medical Imaging: Enhancing Diagnostic Accuracy with Deep Convolutional Networks," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 542-547, doi: 10.1109/ICCCIT62592.2025.10927771.
32. H. R. Goyal, A. Shrivastava, K. K. Dixit, A. Nagpal, B. R. Reddy and J. Kumar, "Improving Accuracy of Object Detection in Autonomous Drones with Convolutional Neural Networks," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 607-611, doi: 10.1109/ICCCIT62592.2025.10927983.
33. A. Kotiyal, A. Shrivastava, A. Nagpal, Manjunatha, K. K. Dixit and R. A. Reddy, "Design and Evaluation of IoT Prototypes: Leveraging Test-Beds for Performance Assessment and Innovation," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 814-820, doi: 10.1109/ICCCIT62592.2025.10927925.
34. A. Shrivastava, S. Bhadula, R. Kumar, G. Kaliyaperumal, B. D. Rao and A. Jain, "AI in Medical Imaging: Enhancing Diagnostic Accuracy with Deep Convolutional Networks," *2025 International Conference on Computational, Communication and Information Technology (ICCCIT)*, Indore, India, 2025, pp. 542-547, doi: 10.1109/ICCCIT62592.2025.10927771.
35. S. Hundekari, A. Shrivastava, R. Praveen, R. H. C. Alfilh, A. Badhoutiya and N. Singh, "Revolutionizing Enterprise Decision-Making Leveraging AI for Strategic Efficiency and Agility," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051858.
36. A. Shrivastava, R. Praveen, R. Aida, K. Vemuri, S. S. Vemuri and S. O. Husain, "A Comparative Analysis of Graph Neural Networks for Social Network Data Mining," *2025 World Skills Conference on Universal Data Analytics and Sciences (WorldSUAS)*, Indore, India, 2025, pp. 1-6, doi: 10.1109/WorldSUAS66815.2025.11199244.
37. A. Shrivastava, R. Praveen, R. R. Al-Fatlawy, S. Bansal, S. Lakhanpal and J. K. K. Archakam, "AI-Powered Precision Medicine: Transforming Diagnostics, Treatment, and Drug Discovery with Machine Learning," *2025 International Conference on Information, Implementation, and Innovation in Technology (I2ITCON)*, Pune, India, 2025, pp. 1-6, doi: 10.1109/I2ITCON65200.2025.11210611.
38. P. William, V. K. Jaiswal, A. Shrivastava, R. H. C. Alfilh, A. Badhoutiya and G. Nijhawan, "Integration of Agent-Based and Cloud Computing for the Smart Objects-Oriented IoT," *2025 International Conference on Engineering, Technology & Management (ICETM)*, Oakdale, NY, USA, 2025, pp. 1-6, doi: 10.1109/ICETM63734.2025.11051558.
39. L. Chawla, A. Shrivastava, M. I. Habelalmateen, H. Shekhar, P. Mittal and S. Sharma, "Federated Foundation Models for Healthcare Diagnostics," *2025 2nd International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2025, pp. 1-6, doi: 10.1109/ICAIIHI67124.2025.11403022.
40. V. Nimbalkar, L. Chawla, M. M. Adnan, A. Bhansali, M. Gupta and R. Kalra, "A Human-Centered Approach to Interpretable Machine Learning in Clinical Decision Support Systems," *2025 2nd International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI)*, Raipur, India, 2025, pp. 1-5, doi: 10.1109/ICAIIHI67124.2025.11403473.

41. Husain, U., & Javed, S. (2019). Stock price movement and volatility in muscat security market (MSM). International Journal of Research-GRANTHAALAYAH, 7(2), 68-84.
42. Javed, S., Husain, U., & Ali, S. (2020). Relevancy of investment decisions and consumption with asset pricing: GMM and CCAPM model approach. International Journal of Management, 11(8).
43. Javed, S., & Husain, U. (2024). Influence of government expenditure on economic growth: an empirical retrospection based on ARDL approach. FIIB Business Review, 13(2), 208-219.
44. Javed, S., Aldalaien, B. A., Husain, U., & Khan, M. S. (2019). Impact of federal funds rate on monthly stocks return of United States of America. International Journal of Business and Management, 14(9), 105-113.
45. Husain, U., Javed, S., & Ananda, S. (2021). Digital marketing as a game changer strategy to enhance brand performance. International Journal of Technology Marketing, 15(2-3), 107-125.
46. Javed, S., & Husain, U. (2021). Corporate CSR practices and corporate performance: managerial implications for sustainable development. Decision, 48 (2), 153–164.
47. Javed, S., Husain, U., & Pathak, N. (2021). Relevance of financial service advertisements in investment decisions and purchase of financial products: Evidence from the Indian insurance sector. Indian Journal of Marketing, 41-55.
48. Javed, S., & Husain, U. (2024). A VECM investigation on the nexus among government spending, oil revenues, and economic growth: empirical evidence from the sultanate of Oman. Innovation Economics Frontiers, 27(2), 1-12.
49. Javed, S., & Husain, U. Impact of Financial Factors on Social and Financial Sustainability in Banking Sector: A Mediating Role of Financial Literacy. Financial Inclusion in Emerging Markets, 257.
50. Javed, S., Husain, U., Mohammed, S., Khan, M. S., Jaouadi, W., & Nazir, S. (2025). Is industy 4.0 the key to sustainable manufacturing? Unravelling the impact of innovation and continuous improvement in emerging economies. Multidisciplinary Reviews, 9(3), 2026108. https://doi.org/10.31893/multirev.2026108
51. Dr. Hina Hasan, & Dr. Mohd. Talib Ather Ansari, (2023) "Food and Nutrition Required for 8th Class Adolescent Girls Students During their Mensuration Period" Published in UGC-CARE List-I, Journal, IJFANS International Journal of food and Nutritional Sciences, Impact factor 7.832 ISSN-2319-1775, ISSN-2320-7876 (Online), Vol.12, Issue 4, January, 2023. P.993-1006, DOI: https://doi.org/10.5281/zenodo.16328638 available at: IJFANS International Journal of Food and Nutritional Sciences 6740c2193130228668b8be9749b3b88c.pdf
52. Dr. Mohd. Talib Ather Ansari, (2022). "A Study of Linguistics and Communicative Skills for Creating Healthy Teacher-Taught Relationships in the Classroom Teaching and Learning Process" Published in UGC-CARE Group-1 Listed ShodhKosh: Journal of Visual and Performing Arts, E-ISSN:2582-7472, Vol.3, Special Issue No. 01, January-July-2022, P.673-687. DOI: https://doi.org/10.5281/zenodo.16327705 available at: | ShodhKosh: Journal of Visual and Performing Arts
53. Dr. Mohd. Talib Ather Ansari, Shashikant G Rokade, Gunjan Sharma, P. Ravi Kumar, K. Maheswari, Hina Hasan. (2023). Education Physiology Influence of Teacher Innovative Behaviour on Students' Academic Self-Efficacy and Intrinsic Goal Orientation. Journal for ReAttach Therapy and Developmental Diversities, Scopus Q4, E-ISSN 2589-7799 (Online), Vol.6, Issue NO. 10(2), 2023. P.200-2008 DOI: https://doi.org/10.5281/zenodo.16328285 available at https://jrtdd.com/index.php/journal/article/view/1337
54. Dr. K. Maheswari, Dr. Sadaquat Ali Khan, Ms. JISHA SANKAR, Dr. Mohd. Talib Ather Ansari, Dr. R. Malathi, Dr. Hina Hasan (2023). "Challenges and Impact of Modern Education Factor on Socio-Economic Development in India" Published in Scopus Indexed Q3, International Journal of European Chemical Bulletin, E-ISSN 2063-5346, Vol.12, Special Issue No. 04, July-2023, P. 559-569. DOI: https://doi.org/10.5281/zenodo.16325971 available at: https://www.eurchembull.com/archives/volume-12/special%20issue-4/7919
55. Dr. Mohd. Talib Ather Ansari, (2022) "A Study of Linguistics and Communicative Skills for Creating Healthy Teacher-Taught Relationships in the Classroom Teaching and Learning Process" Published in UGC-CARE Group-1 Listed ShodhKosh: Journal of Visual and Performing Arts, E-ISSN:2582-7472, Vol.3, Special Issue No. 01, January-July-2022, P.673-687. DOI: https://doi.org/10.5281/zenodo.16327705 available at: | ShodhKosh: Journal of Visual and Performing Arts