IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

Toward Quantum-Resilient Cloud and Edge Security: Post-Quantum Cryptographic Architectures

Dr. C. Nagesh[1], Chatta Balaji[2], K Sudhakar[3], Dr. V. Sujay[4]
Associate Professor, Department of CSE[1]
Assistant Professor, Department of CSE[2,3]
Associate Professor, Department of AI[4]
Tadipatri Engineering College, Tadipatri[2,]
GATES Institute of Technology, Gooty[1,3,4]

Abstract: *The rapid advancement of quantum computing threatens the security foundations of classical public-key cryptographic systems such as RSA and Elliptic Curve Cryptography (ECC), which underpin cloud and edge infrastructures. With scalable quantum algorithms capable of breaking widely deployed cryptographic primitives, organizations must transition toward quantum-resilient security models. This paper proposes a comprehensive Quantum-Resilient Cryptographic Architecture (QRCA) designed specifically for cloud and edge computing environments. The framework integrates post-quantum cryptographic (PQC) algorithms, hybrid key exchange protocols, zero-trust principles, and hardware-assisted secure enclaves. We present a layered security model that balances computational overhead, latency constraints, and scalability requirements in distributed systems. Experimental simulations evaluate performance metrics including encryption latency, key exchange overhead, and throughput across cloud data centres and edge nodes. Results indicate that hybrid PQC deployments achieve strong quantum resilience with manageable performance trade-offs. The proposed architecture offers a practical migration pathway for organizations seeking future-proof cryptographic security in distributed computing ecosystems.*

Keywords: Post-Quantum Cryptography, Quantum-Resilient Security, Cloud Security, Edge Computing, Lattice-Based Cryptography, Hybrid Encryption, Zero Trust Architecture

I. INTRODUCTION

Cloud and edge computing have transformed digital infrastructure by enabling scalable data processing, real-time analytics, and distributed intelligence. From financial transactions and healthcare systems to IoT-enabled smart cities, cloud-edge ecosystems handle sensitive information at unprecedented scales. The security of these systems largely depends on classical public-key cryptographic algorithms such as RSA and ECC, which are vulnerable to quantum attacks—particularly Shor's algorithm.

The emergence of cryptographically relevant quantum computers introduces the concept of "harvest now, decrypt later," where adversaries store encrypted data today with the intention of decrypting it once quantum capabilities mature. This looming threat necessitates the development of quantum-resilient cryptographic architectures that can operate effectively within cloud and edge environments.

Unlike traditional centralized systems, cloud-edge ecosystems present additional challenges including latency sensitivity, distributed key management, heterogeneous devices, and resource-constrained edge nodes. Therefore, transitioning to post-quantum security models requires careful architectural design to balance security, performance, and scalability.

Copyright to IJARSCT
www.ijarsct.co.in
DOI: 10.48175/IJARSCT-31117

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 1, February 2026 Impact Factor: 8.2

This paper proposes a **Quantum-Resilient Cryptographic Architecture (QRCA)** tailored for cloud and edge computing systems, integrating post-quantum cryptographic primitives with hybrid key exchange mechanisms and zero-trust security principles.

II. RELATED WORK / LITERATURE REVIEW

2.1 Quantum Threats to Classical Cryptography

Shor's algorithm demonstrates polynomial-time factorization of large integers and discrete logarithms, rendering RSA and ECC insecure against sufficiently powerful quantum adversaries. Grover's algorithm also weakens symmetric encryption by effectively reducing key strength.

2.2 Post-Quantum Cryptography (PQC)

The National Institute of Standards and Technology (NIST) has standardized several post-quantum cryptographic (PQC) algorithms based on different mathematical foundations. These include lattice-based cryptographic schemes such as CRYSTALS-Kyber for key encapsulation and Dilithium for digital signatures, hash-based signature schemes such as SPHINCS+, and code-based cryptographic systems such as Classic McEliece. Among these approaches, lattice-based schemes are widely regarded as particularly practical and efficient for key exchange and digital signature applications, making them strong candidates for large-scale deployment in post-quantum secure systems.

2.3 Cloud and Edge Security Models

Modern security paradigms emphasize the adoption of Zero Trust Architecture (ZTA) to enforce continuous verification and least-privilege access, the use of confidential computing to protect data during processing, hardware-backed key management systems to safeguard cryptographic keys within secure enclaves, and secure multi-party computation to enable collaborative processing without exposing sensitive data. Despite these advancements, most existing cloud-edge security models continue to rely predominantly on classical cryptographic mechanisms, creating a significant gap in the integration of quantum-resilient design principles necessary to withstand emerging quantum threats.

III. METHODOLOGY / PROPOSED MODEL

3.1 Quantum-Resilient Cryptographic Architecture (QRCA)

The proposed Quantum-Resilient Cryptographic Architecture (QRCA) is structured around five interconnected security layers designed to ensure comprehensive protection in cloud and edge environments. It begins with the Hybrid Key Exchange Layer, which combines classical and post-quantum mechanisms to provide transitional security and forward compatibility. This is followed by the Post-Quantum Encryption Layer, responsible for securing data using quantum-resistant cryptographic algorithms. The Digital Signature and Authentication Layer ensures identity verification and message integrity through post-quantum signature schemes. The Zero Trust Access Control Layer enforces continuous authentication, least-privilege access, and policy-based authorization across distributed systems. Finally, the Hardware Secure Enclave Layer provides isolated execution environments for sensitive cryptographic operations, protecting keys and critical computations from external compromise.

3.2 Hybrid Key Exchange Model

To ensure backward compatibility and gradual migration, QRCA implements a hybrid key exchange:

$$K_{session} = H(K_{RSA/ECC} \| K_{PQC})$$

This approach ensures security even if one component is compromised.

3.3 Performance Optimization for Edge Devices

Edge devices often operate under significant resource constraints, including limited processing power, memory capacity, and energy availability. To address these limitations, the QRCA framework incorporates lightweight lattice-based cryptographic schemes optimized for reduced computational overhead while maintaining quantum resilience. It

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

also implements session key reuse strategies where appropriate to minimize repeated key exchange costs. Computationally intensive cryptographic operations are offloaded to cloud-based Key Management Services (KMS) to reduce the burden on edge nodes, while hardware acceleration mechanisms such as Trusted Platform Modules (TPM) and Trusted Execution Environments (TEE) are leveraged to enhance security and efficiency in cryptographic processing.

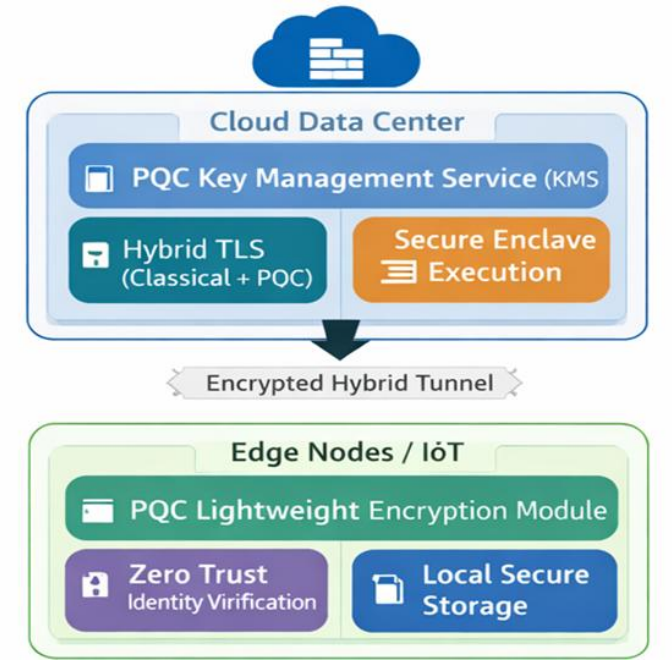

Figure 1: QRCA Architecture for Cloud-Edge Ecosystems

3.4 Zero Trust Integration

Every access request within the QRCA framework undergoes continuous identity validation to ensure that users and services are authenticated at all times rather than relying on one-time verification. In addition, device integrity verification is performed to confirm that endpoints are secure, uncompromised, and compliant with predefined security policies. The system also enforces encrypted micro-segmentation, which isolates workloads and restricts lateral movement across the network. Together, these mechanisms establish quantum-resilient authentication and access control within distributed cloud and edge environments.

IV. EXPERIMENTAL SETUP AND RESULTS

4.1 Simulation Environment

Parameter	Configuration
Cloud Environment	16-core VM Cluster
Edge Devices	ARM-based 4-core Nodes
PQC Algorithm	CRYSTALS-Kyber (Key Exchange)
Signature Scheme	Dilithium
Baseline	RSA-2048 + ECC
Network Latency	10–50 ms

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

4.2 Performance Evaluation Metrics

The performance evaluation of the proposed framework considers several critical metrics, including key exchange latency to measure the time required to establish secure communication sessions, and encryption throughput to assess the volume of data that can be securely processed within a given time frame. CPU utilization is analyzed to determine the computational overhead introduced by cryptographic operations, while memory overhead is evaluated to understand the additional storage requirements imposed by post-quantum algorithms. Handshake time is also measured to quantify the overall duration required to complete secure session establishment between communicating entities.

Scheme	Cloud Latency (ms)	Edge Latency (ms)
RSA-2048	18	25
Pure PQC	32	44
Hybrid (QRCA)	**27**	**36**

Table 1: Key Exchange Latency Comparison

Scheme	Throughput (MB/s)
RSA + AES	310
PQC + AES	285
Hybrid QRCA	**298**

Table 2: Encryption Throughput

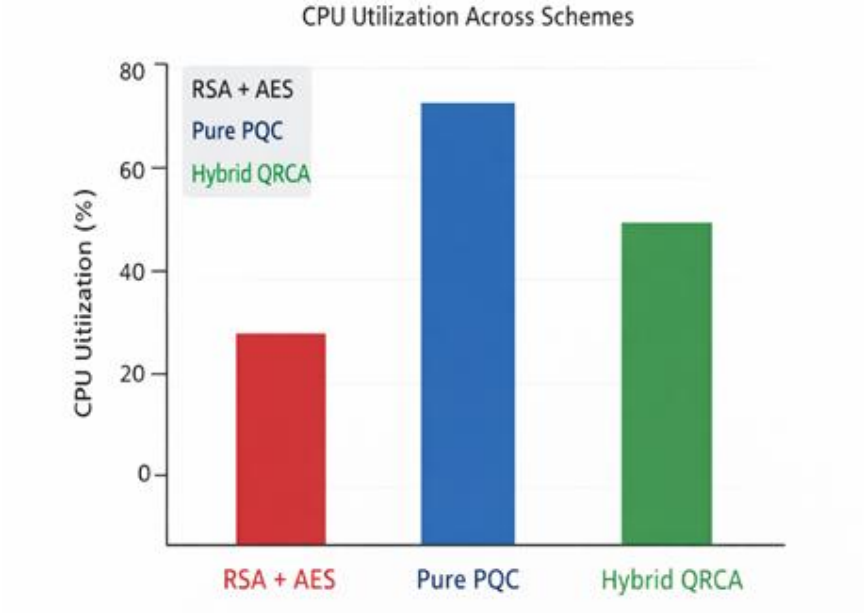

Figure 2: CPU Utilization Across Schemes

(Bar chart showing moderate increase in CPU for PQC, optimized in hybrid approach)

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

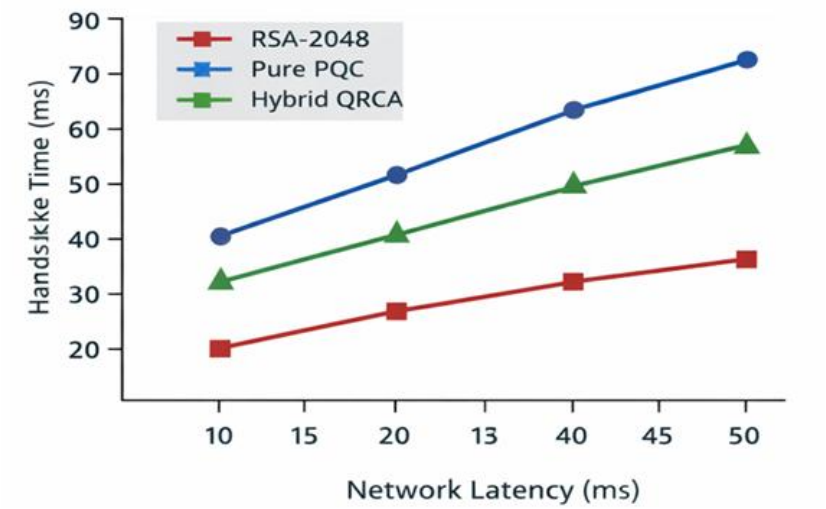

Figure 3: Secure Handshake Time Comparison

(Line graph showing QRCA maintaining acceptable latency for edge deployments)

4.3 Security Evaluation

The security analysis indicates that the proposed architecture demonstrates strong resistance to Shor-based attacks, thereby safeguarding cryptographic operations against future quantum-enabled factorization and discrete logarithm threats. It preserves forward secrecy by ensuring that compromise of long-term keys does not expose previously established session keys. The framework also mitigates the risk of "harvest-now-decrypt-later" attacks by employing quantum-resistant encryption mechanisms that protect stored data from future decryption attempts using advanced quantum computers. Furthermore, the design aligns with NIST post-quantum cryptography (PQC) guidelines, ensuring compliance with emerging standards for quantum-resilient security implementations.

V. DISCUSSION

Experimental results demonstrate that while pure PQC introduces additional computational overhead, hybrid architectures provide a balanced transition strategy. QRCA maintains acceptable latency and throughput, even in edge environments.

The layered security design ensures scalability across distributed cloud and edge nodes by enabling modular deployment and coordinated protection mechanisms throughout the infrastructure. It supports gradual migration compatibility, allowing organizations to transition from classical to post-quantum cryptographic systems without disrupting existing services. The architecture also enhances resilience against future quantum adversaries by incorporating quantum-resistant algorithms and hybrid security mechanisms. Additionally, the integration of Zero Trust principles and hardware-based secure enclaves strengthens end-to-end system integrity by enforcing continuous verification and protecting sensitive operations within isolated execution environments.

VI. CONCLUSION AND FUTURE SCOPE

This paper presented a Quantum-Resilient Cryptographic Architecture (QRCA) tailored for cloud and edge computing ecosystems. By integrating hybrid key exchange mechanisms, post-quantum encryption, zero trust principles, and secure enclave execution, the architecture provides a practical pathway toward quantum-safe distributed systems.

Future Work:

Future research directions include real-world deployment on hyperscale cloud platforms to evaluate performance, scalability, and interoperability under production-scale workloads. Further exploration of integration with blockchain-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

based identity systems can enhance decentralized authentication and trust management. The development of automated cryptographic agility frameworks will enable seamless switching between cryptographic algorithms as standards evolve, ensuring long-term adaptability. Optimizing energy efficiency for IoT edge devices remains critical to maintaining performance while minimizing resource consumption. Additionally, formal verification of hybrid cryptographic protocols can provide mathematical assurance of security properties and resistance against advanced attack vectors. The transition to post-quantum cryptography is not merely optional but essential for safeguarding future digital infrastructure, and the QRCA framework provides a scalable and performance-aware model to support that transformation.

REFERENCES

[1]. P. Naresh, P. Namratha, T. Kavitha, S. Chaganti, S. L. R. Elicherla and K. Gurnadha Gupta, "Utilizing Machine Learning for the Identification of Chronic Heart Failure (CHF) from Heart Pulsations," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1037-1042, doi: 10.1109/ICUIS64676.2024.10866468

[2]. K. R. Chaganti, B. N. Kumar, P. K. Gutta, S. L. Reddy Elicherla, C. Nagesh and K. Raghavendar, "Blockchain Anchored Federated Learning and Tokenized Traceability for Sustainable Food Supply Chains," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1532-1538, doi: 10.1109/ICUIS64676.2024.10866271.

[3]. T. Kavitha, K. R. Chaganti, S. L. R. Elicherla, M. R. Kumar, D. Chaithanya and K. Manikanta, "Deep Reinforcement Learning for Energy Efficiency Optimization using Autonomous Waste Management in Smart Cities," 2025 5th International Conference on Trends in Material Science and Inventive Materials (ICTMIM), Kanyakumari, India, 2025, pp. 272-278, doi: 10.1109/ICTMIM65579.2025.10988394.

[4]. N. Tripura, P. Divya, K. R. Chaganti, K. V. Rao, P. Rajyalakshmi and P. Naresh, "Self-Optimizing Distributed Cloud Computing with Dynamic Neural Resource Allocation and Fault-Tolerant Multi-Agent Systems," 2024 4th International Conference on Ubiquitous Computing and Intelligent Information Systems (ICUIS), Gobichettipalayam, India, 2024, pp. 1304-1310, doi: 10.1109/ICUIS64676.2024.10866891.

[5]. Dev, D. R., Biradar, V. S., Chandrasekhar, V., Sahni, V., & Negi, P. (2024). Uncertainty determination and reduction through novel approach for industrial IoT. Measurement: Sensors, 31, 100995. https://doi.org/10.1016/j.measen.2023.100995

[6]. Roy, R. E., Kulkarni, P., & Kumar, S. (2022, June). Machine learning techniques in predicting heart disease a survey. In 2022 IEEE world conference on applied intelligence and computing (AIC) (pp. 373-377). IEEE. doi: 10.1109/AIC55036.2022.9848945.

[7]. Darshan, R., Janmitha, S. N., Deekshith, S., Rajesh, T. M., & Gurudas, V. R. (2024, March). Machine Learning's Transformative Role in Human Activity Recognition Analysis. In 2024 IEEE International Conference on Contemporary Computing and Communications (InC4) (Vol. 1, pp. 1-8). IEEE. doi: 10.1109/InC460750.2024.10649391.

[8]. Sachin, A., Penukonda, A., Naveen, M., Chitrapur, P. G., Kulkarni, P., & BM, C. (2025, June). NAVISIGHT: A Deep Learning and Voice-Assisted System for Intelligent Indoor Navigation of the Visually Impaired. In 2025 3rd International Conference on Inventive Computing and Informatics (ICICI) (pp. 848-854). IEEE., doi: 10.1109/ICICI65870.2025.11069837.

[9]. K. R. Chaganti, P. V. Krishnamurty, A. H. Kumar, G. S. Gowd, C. Balakrishna and P. Naresh, "AI-Driven Forecasting Mechanism for Cardiovascular Diseases: A Hybrid Approach using MLP and K-NN Models," 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 65-69, doi: 10.1109/ICSSAS64001.2024.10760656.

[10]. P. Naresh, B. Akshay, B. Rajasree, G. Ramesh and K. Y. Kumar, "High Dimensional Text Classification using Unsupervised Machine Learning Algorithm," 2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 2024, pp. 368-372, doi: 10.1109/ICAAIC60222.2024.10575444.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 1, February 2026
Impact Factor: 8.2

[11]. Ramesh Kumar Ramaswamy, Pannangi Naresh, Chilamakuru Nagesh, Santhosh Kumar Balan, Multilevel thresholding technique with Archery Gold Rush Optimization and PCNN-based childhood medulloblastoma classification using microscopic images, Biomedical Signal Processing and Control, Volume 107, 2025, 107801, ISSN 1746-8094, https://doi.org/10.1016/j.bspc.2025.107801.

[12]. G. Chanakya, N. Bhargavee, V. N. Kumar, V. Namitha, P. Naresh and S. Khaleelullah, "Machine Learning for Web Security: Strategies to Detect and Prevent Malicious Activities," 2024 Second International Conference on Intelligent Cyber Physical Systems and Internet of Things (ICoICI), Coimbatore, India, 2024, pp. 59-64, doi: 10.1109/ICoICI62503.2024.10696229.

[13]. S. Khaleelullah, P. Marry, P. Naresh, P. Srilatha, G. Sirisha and C. Nagesh, "A Framework for Design and Development of Message sharing using Open-Source Software," 2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2023, pp. 639-646, doi: 10.1109/ICSCDS56580.2023.10104679.

[14]. V. Krishna, Y. D. Solomon Raju, C. V. Raghavendran, P. Naresh and A. Rajesh, "Identification of Nutritional Deficiencies in Crops Using Machine Learning and Image Processing Techniques," 2022 3rd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, 2022, pp. 925-929, doi: 10.1109/ICIEM54221.2022.9853072.

[15]. T. Aruna, P. Naresh, B. A. Kumar, B. K. Prakash, K. M. Mohan and P. M. Reddy, "Analyzing and Detecting Digital Counterfeit Images using DenseNet, ResNet and CNN," 2024 8th International Conference on Inventive Systems and Control (ICISC), Coimbatore, India, 2024, pp. 248-252, doi: 10.1109/ICISC62624.2024.00049.

[16]. Nagesh, C., Chaganti, K.R. , Chaganti, S. , Khaleelullah, S., Naresh, P. and Hussan, M. 2023. Leveraging Machine Learning based Ensemble Time Series Prediction Model for Rainfall Using SVM, KNN and Advanced ARIMA+ E-GARCH. *International Journal on Recent and Innovation Trends in Computing and Communication*. 11, 7s (Jul. 2023), 353–358. DOI:https://doi.org/10.17762/ijritcc.v11i7s.7010.

[17]. Naresh, P., & Suguna, R. (2021). IPOC: An efficient approach for dynamic association rule generation using incremental data with updating supports. Indonesian Journal of Electrical Engineering and Computer Science, 24(2), 1084. https://doi.org/10.11591/ijeecs.v24.i2.pp1084-1090.

[18]. Swasthika Jain, T. J., Sardar, T. H., Sammeda Jain, T. J., Guru Prasad, M. S., & Naresh, P. (2025). Facial Expression Analysis for Efficient Disease Classification in Sheep Using a 3NM-CTA and LIFA-Based Framework. IETE Journal of Research, 1–15. https://doi.org/10.1080/03772063.2025.2498610.

[19]. P. Naresh, S. V. N. Pavan, A. R. Mohammed, N. Chanti and M. Tharun, "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 170-176, doi: 10.1109/ICSCSS57650.2023.10169190.

[20]. N. P, K. R. Chaganti, S. L. R. Elicherla, S. Guddati, A. Swarna and P. T. Reddy, "Optimizing Latency and Communication in Federated Edge Computing with LAFEO and Gradient Compression for Real-Time Edge Analytics," 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), Goathgaun, Nepal, 2025, pp. 608-613, doi: 10.1109/ICMCSI64620.2025.10883220.

[21]. SAI M, RAMESH P, REDDY DS. EFFICIENT SUPERVISED MACHINE LEARNING FOR CYBERSECURITYAPPLICATIONS USING ADAPTIVE FEATURE SELECTION AND EXPLAINABLE AI SCENARIOS. Journal of Theoretical and Applied Information Technology. 2025 Mar 31;103(6).

[22]. Sivananda Reddy Elicherla, Dr. P E Sreenivasa Reddy, Dr. V Raghunatha Reddy and Sivaprasada Reddy Peddareddigari. "Agilimation (Agile Automation) - State of Art from Agility to Automation." International Journal for Scientific Research and Development 3.9 (2015): 411-416.