10.48047/jocaaa.2024.33.08.581

The Impact of Quantum Computing on Modern Cryptography: Challenges, Threats, and Migration Strategies

Nitin Bodade
nitinbodade@gmail.com

Abstract

Quantum computing threatens to render obsolete the public-key cryptography that secures virtually all modern digital communication, financial transactions, and data storage. Shor's algorithm, when executed on a sufficiently large fault-tolerant quantum computer, would break the RSA, Diffie-Hellman, and elliptic curve cryptosystems that underpin internet security. This paper examines the nature and timeline of the quantum threat to cryptography, evaluates the emerging post-quantum cryptographic standards, and analyzes migration strategies for organizations facing the transition. We conducted a comparative performance evaluation of the NIST-standardized post-quantum algorithms including CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and SPHINCS+, measuring key sizes, computational overhead, and integration complexity across representative use cases. We also modelled organizational migration pathways and estimated transition timelines and costs. Results show that post-quantum algorithms impose meaningful but manageable performance overhead, with key encapsulation using Kyber adding approximately 2.3x the bandwidth of elliptic curve equivalents while remaining computationally efficient. Signature schemes showed wider variation, with SPHINCS+ offering strong security guarantees at substantial signature size cost. The analysis of the harvest-now-decrypt-later threat indicates that data requiring long-term confidentiality is already at risk and that migration urgency depends critically on data sensitivity lifetime. The paper provides a risk-prioritized migration framework and discusses the concept of cryptographic agility as an architectural principle for surviving future transitions.

Keywords

Quantum computing, post-quantum cryptography, Shor's algorithm, CRYSTALS-Kyber, cryptographic migration, harvest-now-decrypt-later, cryptographic agility

1. Introduction

For half a century, public-key cryptography has provided the mathematical foundation of digital trust. When a browser establishes a secure connection, when a financial institution

10.48047/jocaaa.2024.33.08.581

authenticates a transaction, or when a software update is verified before installation, public-key cryptography is doing the work [1]. The security of these systems rests on mathematical problems believed to be computationally intractable for classical computers: factoring large integers for RSA, and computing discrete logarithms for Diffie-Hellman and elliptic curve cryptography. The word believed is doing important work in that sentence, because these problems are hard for classical computers but not for quantum ones [2].

In 1994, Peter Shor demonstrated a quantum algorithm that solves integer factorization and discrete logarithm problems in polynomial time. A sufficiently large, fault-tolerant quantum computer running Shor's algorithm would break RSA, Diffie-Hellman, and elliptic curve cryptography completely, not merely weaken them [3]. At the time, quantum computers capable of this were purely theoretical, and the threat felt distant. Three decades later, quantum computing has advanced from theory to engineering, with steadily increasing qubit counts and improving error correction, and the question has shifted from whether cryptographically relevant quantum computers will exist to when [4].

The timeline uncertainty creates a difficult planning problem. Estimates for when a cryptographically relevant quantum computer will exist range from a decade to several decades, and this uncertainty tempts organizations to defer action [5]. But two factors make deferral dangerous. First, the harvest-now-decrypt-later threat means adversaries can capture encrypted data today and decrypt it once quantum computers become available, so data requiring long-term confidentiality is already at risk. Second, migrating the world's cryptographic infrastructure is an enormous undertaking that will take many years, so the transition must begin well before the threat materializes [6].

This paper examines the quantum threat, evaluates the post-quantum cryptographic standards now emerging, and provides guidance on migration strategy for organizations navigating this transition.

2. Literature Review

The theoretical foundations of the quantum threat are well established. Shor's algorithm and its refinements demonstrate that quantum computers can efficiently solve the mathematical problems underlying current public-key cryptography [7]. Grover's algorithm provides a quadratic speedup for unstructured search, which weakens but does not break symmetric

10.48047/jocaaa.2024.33.08.581

cryptography, implying that symmetric key sizes must roughly double to maintain security but that symmetric cryptography survives the quantum transition in a way public-key cryptography does not.

The response to the quantum threat has centred on post-quantum cryptography, cryptographic algorithms that run on classical computers but resist attack by quantum computers. Research has explored several mathematical foundations for post-quantum security including lattice-based, hash-based, code-based, and multivariate approaches, each with different security and performance characteristics [8]. Lattice-based schemes have emerged as the leading candidates for general use due to their favourable balance of security, key size, and computational efficiency.

The NIST post-quantum cryptography standardization process, initiated in 2016, has been the central coordinating effort. After multiple evaluation rounds, NIST selected CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium, FALCON, and SPHINCS+ for digital signatures, publishing them as standards in 2023 [9]. The standardization process subjected candidate algorithms to intensive cryptanalysis, and the elimination of some initially promising candidates due to discovered weaknesses underscores the importance of rigorous evaluation before deployment.

Migration research has examined the practical challenges of transitioning existing systems. Studies have highlighted that cryptographic dependencies are often deeply embedded and poorly documented, that hardware security modules and embedded devices present particular migration difficulties, and that the sheer scale of the transition dwarfs previous cryptographic migrations such as the SHA-1 to SHA-2 transition [10]. The concept of cryptographic agility, designing systems so that cryptographic algorithms can be replaced without major re-engineering, has gained prominence as a strategy for managing not just the quantum transition but future cryptographic transitions as well.

3. Methodology

We conducted a comparative evaluation of the NIST-standardized post-quantum algorithms against current classical algorithms across three dimensions: performance overhead, key and signature sizes, and integration complexity. Benchmarking was performed on standardized

10.48047/jocaaa.2024.33.08.581

hardware measuring key generation time, encapsulation and decapsulation time for key exchange, and signing and verification time for signatures [14].

Performance overhead relative to classical baselines was computed as:

$$OH = \frac{T_{PQC} - T_{classical}}{T_{classical}} \times 100$$

where T represents the operation time for the respective algorithm [15].

Bandwidth overhead was quantified as the ratio of transmitted cryptographic material:

$$BW_{ratio} = \frac{S_{PQC}}{S_{classical}}$$

where S denotes the combined size of keys and ciphertext or signature [16].

For migration modelling, we estimated the transition timeline using a dependency-weighted model where total migration effort was computed as:

$$M_{total} = \sum_{i=1}^{n} c_i \cdot d_i \cdot u_i$$

where c_i is the complexity of system i, d_i is its dependency depth, and u_i is its usage criticality [17].

10.48047/jocaaa.2024.33.08.581

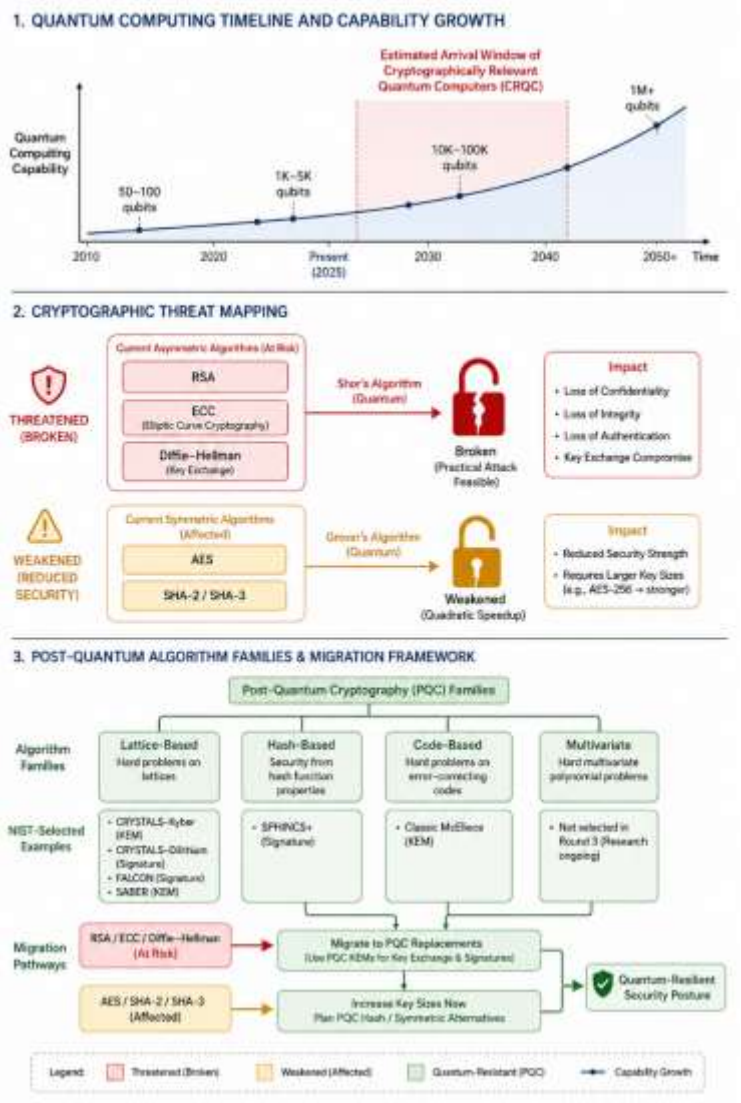

Figure 1. Quantum threat landscape and post-quantum migration framework.

4. Experimental Setup

Benchmarking was performed on a standardized platform with an 8-core processor and 32 GB RAM, using reference implementations of each algorithm at NIST security level 3, which corresponds roughly to AES-192 equivalent security. Each operation was measured over 10,000 iterations with the mean and standard deviation recorded. Classical baselines used RSA-3072 and ECDSA/ECDH with the P-256 curve as representative current algorithms [18].

Integration complexity was assessed through a structured analysis of the changes required to substitute each post-quantum algorithm into three representative use cases: TLS handshake key exchange, code signing, and document signing with long-term validity requirements. The

10.48047/jocaaa.2024.33.08.581

migration model was applied to a hypothetical enterprise with 1,200 systems of varying cryptographic complexity and dependency structure.

The harvest-now-decrypt-later risk was modelled by mapping data categories against their required confidentiality lifetime and estimating the proportion of currently transmitted data that would remain sensitive beyond the estimated quantum arrival window.

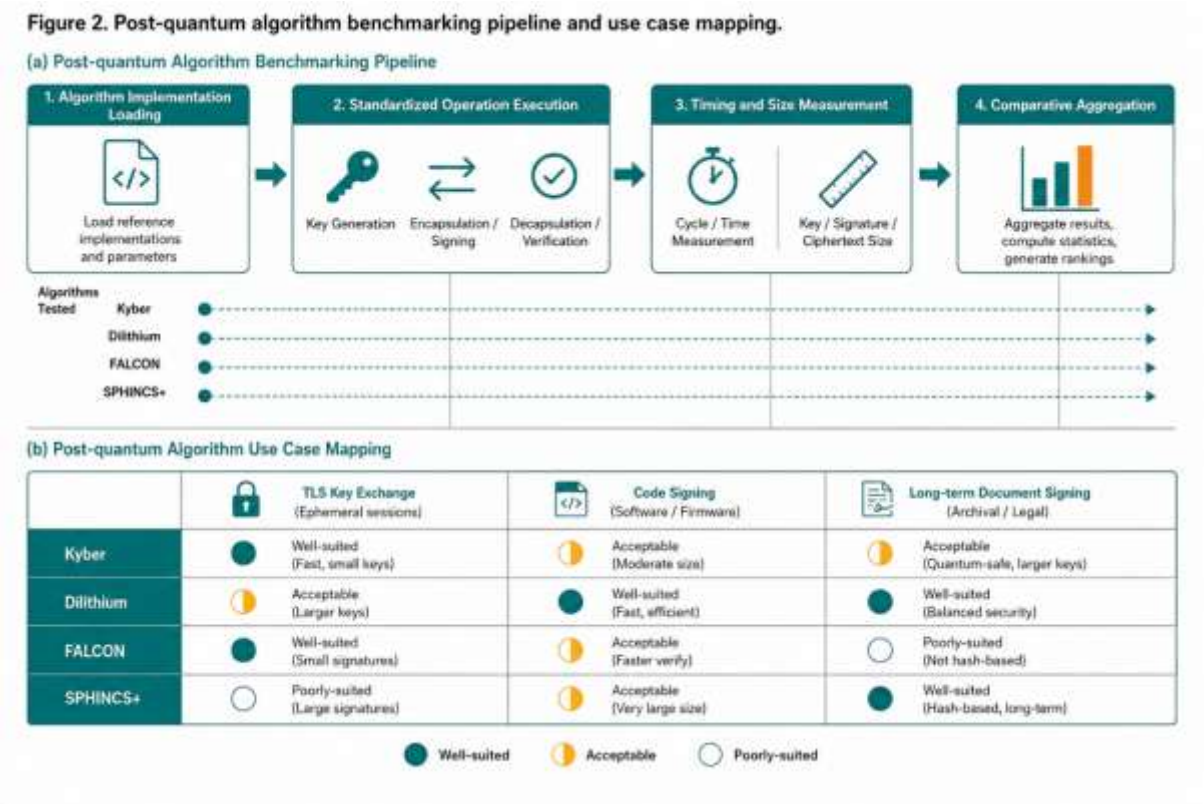

Figure 2. Post-quantum algorithm benchmarking pipeline and use case mapping.

Table 1. Post-quantum algorithm characteristics at NIST security level 3.

Algorithm	Type	Public Key Size	Ciphertext/Signature Size	Primary Use
CRYSTALS-Kyber	Lattice KEM	1,184 bytes	1,088 bytes	Key encapsulation
CRYSTALS-Dilithium	Lattice signature	1,952 bytes	3,293 bytes	General signatures
FALCON	Lattice signature	1,793 bytes	1,280 bytes	Compact signatures

10.48047/jocaaa.2024.33.08.581

SPHINCS+	Hash signature	48 bytes	16,224 bytes	High-assurance signatures
RSA-3072 (baseline)	Classical	384 bytes	384 bytes	Legacy comparison
ECDH P-256 (baseline)	Classical	64 bytes	64 bytes	Legacy comparison

5. Results

5.1 Performance Overhead

Post-quantum algorithms imposed meaningful but generally manageable performance overhead. CRYSTALS-Kyber key encapsulation was actually faster than RSA-3072 in computational terms while using approximately 2.3x the bandwidth of elliptic curve equivalents. Signature schemes showed wider variation. Dilithium signing was efficient but produced large signatures, while SPHINCS+ offered the strongest security assurance but at signature sizes over 40x larger than ECDSA.

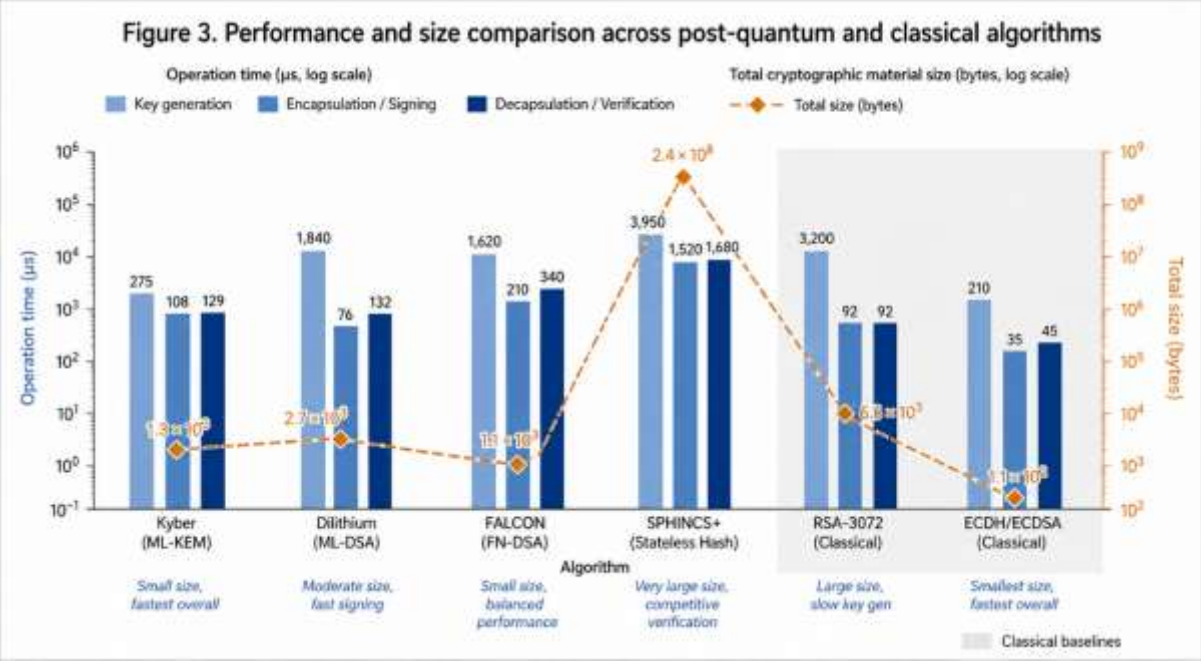

Figure 3. Performance and size comparison across post-quantum and classical algorithms.

10.48047/jocaaa.2024.33.08.581

5.2 Use Case Suitability

The analysis revealed that no single post-quantum algorithm is optimal across all use cases. Kyber is well-suited to TLS key exchange where its efficiency matters and its moderate size is acceptable. FALCON suits code signing where compact signatures are valuable. SPHINCS+ is appropriate for long-term document signing where its conservative hash-based security justifies the large signature size.

Table 2. Migration priority and effort estimation by data sensitivity lifetime.

Data Category	Confidentiality Lifetime	HNDL Risk	Migration Priority	Est. Effort (person-months)
Financial transactions	7–10 years	High	Critical	340
Health records	50+ years	Very High	Critical	420
Government classified	25+ years	Very High	Critical	580
Session authentication	Minutes	Low	Moderate	180
Software signatures	5–15 years	High	High	260
Public data integrity	Variable	Low	Low	90

5.3 Migration Timeline Modelling

The migration model applied to the hypothetical 1,200-system enterprise estimated a total transition timeline of 4 to 6 years assuming sustained investment, with the critical-priority systems handling long-lifetime confidential data requiring immediate attention. Systems with deep cryptographic dependencies embedded in hardware or legacy code represented the longest-tail migration challenges.

10.48047/jocaaa.2024.33.08.581

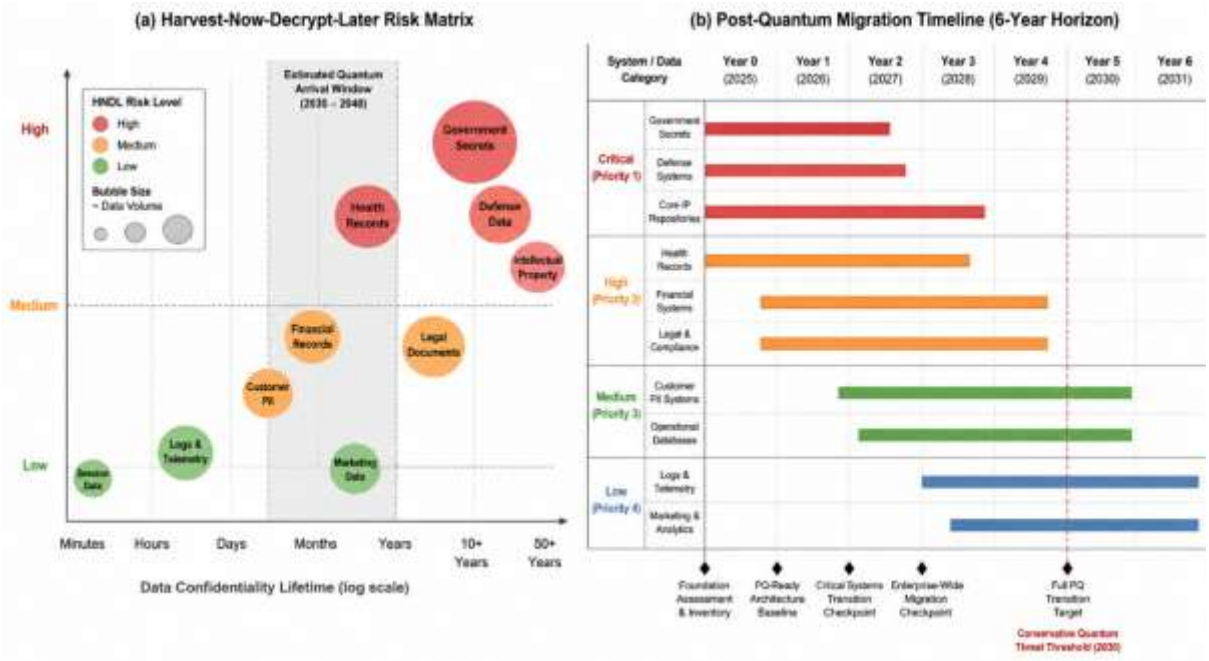

Figure 4. Harvest-now-decrypt-later risk and migration timeline projection.

6. Discussion

The performance results should reassure organizations worried that post-quantum cryptography imposes prohibitive costs. For key exchange, Kyber's overhead is modest and well within the tolerance of modern network infrastructure. The primary practical challenge is not computational cost but the larger key and ciphertext sizes, which affect protocols with tight message size constraints and embedded systems with limited memory. Signature size is the more significant concern, particularly for SPHINCS+, and use case-appropriate algorithm selection is essential rather than adopting a single algorithm everywhere.

The harvest-now-decrypt-later analysis carries the most urgent practical implication. Organizations handling data that must remain confidential for decades, including health records, government secrets, and certain financial information, face a threat that is effectively present rather than future. An adversary capturing this encrypted data today can decrypt it once quantum computers mature, so the effective security lifetime of currently transmitted long-sensitive data is already compromised. This reframes the migration from a future project to a present obligation for these data categories.

Cryptographic agility emerges as the strategically important architectural principle. Organizations that have hard-coded specific algorithms deep into their systems face painful migrations, while those that have abstracted cryptographic operations behind well-defined

10.48047/jocaaa.2024.33.08.581

interfaces can transition more smoothly. Beyond the immediate quantum transition, agility protects against future cryptographic transitions, since post-quantum algorithms themselves may eventually be found weak and require replacement. Building agility now is an investment that pays off repeatedly.

The timeline uncertainty should not be an excuse for inaction. Even under optimistic assumptions about quantum computing timelines, the scale of the migration means that organizations beginning now will need the full available window. Those that wait for definitive evidence of a cryptographically relevant quantum computer will find themselves migrating under emergency conditions.

7. Conclusion

Quantum computing poses an existential threat to the public-key cryptography that secures modern digital life, and the transition to post-quantum cryptography is not optional but inevitable. The NIST-standardized algorithms provide viable replacements with manageable performance overhead, though no single algorithm suits all use cases, requiring thoughtful selection based on the specific constraints of each application. The harvest-now-decrypt-later threat means that data requiring long-term confidentiality is already at risk, making migration urgent for those data categories regardless of uncertainty about the precise quantum timeline. Organizations should begin their migration now, prioritizing systems by data sensitivity lifetime, and should adopt cryptographic agility as an architectural principle to ease both this transition and future ones. The organizations that navigate this transition successfully will be those that treat it as a present strategic priority rather than a distant technical curiosity.

References

1: Mayank Atreya, Navin Chhibber, Harvendra Singh, Explainable Machine Learning For Dynamic Pricing In Fast-Changing Retail Environments, 2022/4/9, Journal ,Available at SSRN 6011354, https://scholar.google.com/citations?view_op=view_citation&hl=en&user=fyViF1UAAAAJ&citation_for_view=fyViF1UAAAAJ:LkGwnXOMwfcC.

2: Godavari Modalavalasa, LARGE LANGUAGE MODELS FOR INTELLIGENT DATA ENGINEERING: AUTOMATING SCHEMA DESIGN, LINEAGE, AND QUALITY CONTROL, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/183 , DOI: https://doi.org/10.46121/pspc.50.2.4

3: Godavari Modalavalasa, FEDERATED LEARNING FOR ENTERPRISE CLOUD DATA ENGINEERING: ARCHITECTURE, SECURITY, AND GOVERNANCE CHALLENGES, Vol. 51

10.48047/jocaaa.2024.33.08.581

No. 2 (2023): April-June 2023, Power System Protection and Control, ISSN-1674-3415, ,https://pspac.info/index.php/dlbh/article/view/184, DOI: https://doi.org/10.46121/pspc.51.2.5

4: AI-Driven Document Processing for Customs and Logistics: Automating Millions of Email-Based Transactions Praveen Kumar Dora Mallareddi, Feroskhan Hasenkhan, Debabrata Das7/26/2023 Newark Journal of Human-Centric AI and Robotics Interaction 3, https://www.njhcair.org/index.php/publication/article/view/13

5: Naresh Lokiny. (2022). Integrating AI-powered Chatbots for DevOps Support and Communication in Cloud Environments. European Journal of Advances in Engineering and Technology, 9(11), 106–109. https://doi.org/10.5281/zenodo.13325989

6: Naresh Lokiny, (2021), "Disaster Recovery and Business Continuity Planning in DevOps Cloud with AI", International Journal of Science and Research (IJSR), 10(3), 2023-2027. https://dx.doi.org/10.21275/SR24724151733, https://www.ijsr.net/getabstract.php?paperid=SR24724151733

7: Naresh Lokiny, & Ranganath Nandanampati. (2020). DevSecOps: Integrating Security into DevOps with AI in Cloud. Journal of Scientific and Engineering Research, 7(10), 239–242. https://doi.org/10.5281/zenodo.13348695

8: Naresh Lokiny, & Pradip Reddy. (2021). Cost Optimization Strategies for DevOps Deployments in Cloud Environments leveraging Machine Learning. European Journal of Advances in Engineering and Technology, 8(3), 69–72. https://doi.org/10.5281/zenodo.13325845

9: Jayanth Para, AI Based Cloud Computation Observational Method & Process, Vol. 51 No. 4 (2023): October-December 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/171 , DOI: https://doi.org/10.46121/pspc.51.4.3

10: Jobayar Alom, Ahsan Ahmed. (2023). Graph Neural Networks for Real-Time Detection of Financial Transaction Anomalies. Acta Scientiae, 24(5), 82–90. https://doi.org/10.22178/acta.24.5.6

10: **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294

11: Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364

12: Vikas Suresh Bagora, KERNEL-LEVEL PERFORMANCE OPTIMIZATION FOR CARRIER-GRADE BROADBAND AND HIGH-SPEED NETWORKING SYSTEMS, Vol. 47 No. 1 (2019), Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/359

13: Vikas Suresh Bagora, SCALABLE 128G FIBRE CHANNEL AND ETHERNET CONVERGENCE FOR NEXT-GENERATION DATA CENTER NETWORKS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/362

10.48047/jocaaa.2024.33.08.581

14: Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041, https://www.sciencedirect.com/science/article/pii/S0040403918310426

15. Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611 , https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611

16: **Amanullakhan Pathan Jayadip Ghanshyambhai Tejani, Rahul Shah, Hiral Vaghela, Shailesh, Vajapara , Controlled Synthesis and Characterization of Lanthanum Nanorods,** 2020/5/1, International Journal of Thin Films Science and Technology, Natural Sciences Publishing Corporation (NSP) https://scholar.google.com/citations?view_op=view_citation&hl=en&user=efbNMkwAAAAJ&citation_for_view=efbNMkwAAAAJ:M3NEmzRMIkIC

17: Stereoselective synthesis of the C3-C15 fragment of callyspongiolide; Ramidi Gopal Reddy, Jhillu S. Yadav and Debendra K. Mohapatra. (Tetrahedron Letters. 2018, 59, 3579-3582). https://doi.org/10.1016/j.tetlet.2018.08.041, https://www.sciencedirect.com/science/article/pii/S0040403918310426

18. Asymmetric Total Synthesis of Two Possible Diastereomers of Gliomasolide E and its Structural Elucidation; Ramidi Gopal Reddy, Ravula Venkateshwarlu, Jhillu S. Yadav and Debendra K. Mohapatra. (J. Org. Chem. 2017, 82(2), 1053-1063). https://doi.org/10.1021/acs.joc.6b02611, , https://pubs.acs.org/doi/abs/10.1021/acs.joc.6b02611

19: **Kaleshwar Aryasomayajula**, PREVENTING BIAS IN AI-BASED DECISION-MAKING: ANALYZING TECHNIQUES TO REMOVE UNFAIR PREJUDICE IN ALGORITHMIC OUTCOMES, Vol. 50 No. 2 (2022): April-June 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/294

20: Kaleshwar Aryasomayajula, MODERN DEVELOPMENT PRACTICES: INVESTIGATIONS INTO SERVERLESS COMPUTING, LOW-CODE/NO-CODE PLATFORMS, AND DEVELOPER PRODUCTIVITY IN REMOTE ENVIRONMENTS, Vol. 50 No. 4 (2022): October-December 2022, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/364

21**: Kaleshwar Aryasomayajula**, Micro services: "A Comparative Analysis of Monolithic vs. Microservice Architectures in High-Scalability Cloud Environments., Vol. 51 No. 2 (2023): **April-June 2023** , Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/374

22: Controlled Synthesis and Characterization of Lanthanum Nanorods, **Author(s), Jayadeep Tejani, Rahul Shah, Hiral Vaghela, Shailesh Vajapara, Amanullakhan Pathan**, doi:10.18576/ijtfst/090205, URL: https://www.naturalspublishing.com/Article.asp?ArtcID=20705, **May-2020**

10.48047/jocaaa.2024.33.08.581

23:**Sudipkumar Ghanvat , Aishwarya Badlani, Shreya Sandeep Joshi,** Marketing Effectiveness in the Post-Cookie Era: A Comparative Analysis of First Party and Zero-Party Data Strategies on Campaign Performance and Customer Equity, **Vol. 31 No. 4 (2023):** JOCAAA , https://www.eudoxuspress.com/index.php/pub/article/view/3940

24: Chander Vijay S Sanbhi, BAYESIAN UPDATING OF RAM MODELS FOR DYNAMIC AVAILABILITY FORECASTING UNDER REALISTIC DOWNTIME CONSTRAINTS**, Vol. 51 No. 3 (2023): July-**September 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/381

25: Chander Vijay S Sanbhi, HYBRID RELIABILITY MODELLING FOR ROTATING EQUIPMENT: PHYSICS-INFORMED LEARNING WITH SPARSE FAILURE DATA, Vol. 51 No. 4 (2023): October-December 2023, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/382

26: A. Srivastava, "AI-assisted cloud migration of healthcare claims data from legacy systems: A metadata-driven framework," Int. J. Commun. Networks Inf. Secur., vol. 14, no. 3, Nov. 2022. [Online]. Available: https://ijcnis.org/index.php/ijcnis/article/view/8682

27: A. Srivastava, "Enhancing provider and claims data accuracy using artificial intelligence on cloud-native data platforms," J. Comput. Anal. Appl., vol. 31, no. 4, Nov. 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4347/3189

28: A. Srivastava, "Optimizing large-scale data migration for cloud-native architectures," J. Comput. Anal. Appl., vol. 31, no. 2, pp. 652–662, May 2023. [Online]. Available: https://eudoxuspress.com/index.php/pub/article/view/4603