Power System Protection and Control
ISSN:1674-3415

POST-QUANTUM CRYPTOGRAPHY: SECURING DIGITAL INFRASTRUCTURE IN THE QUBIT ERA

Rajeev Patel

Department Of Computer Science, Mcneese State University
rpatel5@mcneese.edu

Received: 17/05/2026 **Revised**: 24/06/2026 **Accepted**: 30/07/2026

***ABSTRACT*:**

The cryptographic systems that secure nearly every digital interaction in modern life, from online banking to secure messaging to critical infrastructure control, rest on mathematical problems that quantum computers threaten to solve efficiently. Shor's algorithm running on a sufficiently powerful quantum computer would break the RSA, Diffie-Hellman, and elliptic curve cryptography that underpin the current internet, and while such a machine does not yet exist, the trajectory of quantum hardware development has made the risk sufficiently real that the security community is racing to deploy post-quantum cryptography (PQC) before the transition becomes an emergency. This paper examines the state of post-quantum cryptography and its deployment across digital infrastructure, with attention to both the mathematical foundations of the leading candidate algorithms and the practical engineering challenges of transitioning global systems away from vulnerable cryptography. We review the NIST post-quantum standardization process and its outcomes, analyze the performance and security characteristics of standardized algorithms including CRYSTALS-Kyber, CRYSTALS-Dilithium, and SPHINCS+, and evaluate deployment challenges across web infrastructure, secure messaging, financial systems, and critical infrastructure sectors. Empirical benchmarking on a testbed representative of production infrastructure shows that current PQC algorithms produce key exchange latencies within 2.4 times classical baselines, signature sizes 15 to 400 times larger than classical equivalents depending on scheme, and computational overhead ranging from 1.3 to 8.7 times classical costs. We discuss the challenges of hybrid deployment during transition, cryptographic agility as an architectural principle, and the specific timelines that different infrastructure sectors must meet to remain secure as quantum capability advances. Findings support an urgent but staged transition strategy with cryptographic agility as the foundational architectural requirement.

***Keywords**: Post-Quantum Cryptography, Quantum Computing Threats, Digital Infrastructure Security, Lattice-Based Cryptography, Cryptographic Agility, Quantum-Safe Transition*

INTRODUCTION

The mathematical foundations of modern cryptography have provided remarkable security for the past four decades, protecting trillions of dollars in financial transactions, the confidentiality of personal communications for billions of people, and the operation of critical infrastructure ranging from power grids to hospital systems. This security has rested on the difficulty of specific mathematical problems, particularly integer factorization and discrete logarithms, that classical computers cannot solve efficiently at the scales used in real cryptographic keys [1]. The RSA algorithm, published in 1977, and the elliptic curve cryptography that gained wide deployment in the 2000s, both derive their security from these mathematical foundations, and they underpin the TLS protocol that secures nearly every web connection, the digital signature schemes that verify software authenticity, and the key exchange mechanisms that establish confidential communications.

Quantum computing threatens to change this picture fundamentally. In 1994, Peter Shor demonstrated that a sufficiently powerful quantum computer running his algorithm could factor large integers and solve discrete logarithm problems in polynomial time, breaking the mathematical foundations on which RSA, Diffie-Hellman, and elliptic curve cryptography rest [2]. For decades, this was primarily a theoretical concern because building a quantum computer capable of running Shor's algorithm at cryptographically relevant scales appeared to be so difficult that many observers questioned whether it would ever be achieved. The picture has changed substantially in recent years. Progress in quantum hardware from major technology companies, national laboratories, and specialized quantum computing firms has accelerated. Fault-tolerant quantum computing, once considered a

DOI: 10.46121/pspc.54.3.37

distant goal, now has published roadmaps that place cryptographically relevant capability within decades rather than centuries [3].

The security community has responded to this trajectory by developing post-quantum cryptography, which comprises cryptographic algorithms designed to remain secure against attack by both classical and quantum computers. Post-quantum algorithms are based on mathematical problems that quantum computers are not known to solve efficiently, including problems in lattice theory, coding theory, multivariate polynomial systems, hash functions, and isogenies over elliptic curves [4]. Each family offers different trade-offs among security, performance, and key sizes, and the security community has worked to identify algorithms suitable for the wide range of applications that current cryptography secures.

The National Institute of Standards and Technology (NIST) initiated a formal post-quantum cryptography standardization process in 2016 that has driven substantial global research investment and cryptanalysis. After three rounds of evaluation involving submissions from research groups worldwide, NIST announced initial standards in 2022 including CRYSTALS-Kyber for key encapsulation and CRYSTALS-Dilithium, Falcon, and SPHINCS+ for digital signatures [5]. Additional standards including stateless signature schemes and additional key encapsulation mechanisms have followed. These standards provide the algorithmic foundation on which the world's digital infrastructure will need to be rebuilt over the coming years.

Yet standardization is only the beginning of the transition. Deploying new cryptographic algorithms across the global digital infrastructure is a project of extraordinary scope. TLS handshakes on billions of web servers, digital signature infrastructure for software updates and code signing, secure messaging protocols on consumer applications, financial system cryptography, and the specialized cryptographic systems in critical infrastructure all need to be transitioned, and doing so without breaking interoperability requires careful coordination across ecosystems that were built on assumptions no longer valid [6]. Historical experience with cryptographic transitions, including the transition from MD5 to SHA-2 and from SHA-1 to SHA-2, has shown that even relatively simple algorithm changes can take a decade or more to complete across global infrastructure.

This paper examines the state of post-quantum cryptography and the practical challenges of deploying it across digital infrastructure. Our objectives are to characterize the mathematical foundations and security properties of the leading post-quantum algorithms, to evaluate their performance characteristics on infrastructure representative of production systems, to identify the deployment challenges specific to major infrastructure sectors, and to outline strategies that organizations can adopt to prepare for and execute the transition. The paper is intended to serve both technical audiences implementing post-quantum cryptography and strategic audiences making infrastructure investment and policy decisions in this domain.

THE QUANTUM THREAT AND CRYPTOGRAPHIC VULNERABILITY

2.1 Shor's Algorithm and Its Implications

Shor's algorithm exploits quantum mechanical properties, particularly superposition and interference, to efficiently find the period of a function related to modular exponentiation. This period-finding capability translates directly into efficient algorithms for integer factorization and discrete logarithm computation, which are the mathematical problems on which RSA, Diffie-Hellman, and elliptic curve cryptography rest their security [7]. The classical difficulty of these problems scales exponentially with key size, so doubling key size makes classical attack roughly a million times harder. On a sufficiently powerful quantum computer, the difficulty scales polynomially, meaning that increasing key size provides only modest additional protection.

The resource requirements for running Shor's algorithm at cryptographically relevant scales have been the subject of substantial study. Recent estimates suggest that breaking 2048-bit RSA would require approximately 20 million physical qubits and about 8 hours of computation on a fault-tolerant quantum computer, and breaking 256-bit elliptic curve cryptography would require slightly fewer qubits but comparable computation time [8]. These requirements exceed the capabilities of current quantum computers by roughly six orders of magnitude, but the trajectory of progress makes projections of the timeline highly uncertain. Serious analysts have suggested that cryptographically relevant quantum computers could appear anywhere from ten to thirty years from now, with significant probability mass across that range.

DOI: 10.46121/pspc.54.3.37

Power System Protection and Control
ISSN:1674-3415

2.2 Grover's Algorithm and Symmetric Cryptography

Grover's algorithm provides a quadratic speedup for unstructured search problems, which has implications for symmetric cryptography and hash functions. The effective security of symmetric algorithms against quantum attack is roughly half their classical security in bits [9]. This is a substantial reduction but does not require the wholesale replacement that Shor's algorithm forces for public key cryptography. Instead, symmetric cryptography can generally be secured against quantum attack by doubling key lengths, so 256-bit AES provides approximately 128 bits of quantum security, similar to the classical security of 128-bit AES against classical attack.

2.3 The Harvest Now, Decrypt Later Threat

One aspect of the quantum threat that deserves particular attention is the harvest now, decrypt later attack model. In this model, adversaries with sufficient resources collect encrypted communications today and store them for future decryption once quantum computers become capable [10]. For information whose confidentiality must remain protected for many years, such as state secrets, medical records, and long-lived business data, this threat is already active regardless of whether cryptographically relevant quantum computers exist yet. Encrypted data collected today can be decrypted at any point in the future when the necessary quantum capability becomes available.

This threat model has substantial implications for transition timing. Organizations that handle information requiring long-term confidentiality cannot wait until quantum computers appear before transitioning; they need to have transitioned already for the information to remain protected. This urgency is particularly acute for national security applications, healthcare records with statutory long-term protection requirements, and legal and financial documents whose long-term confidentiality is essential to their function.

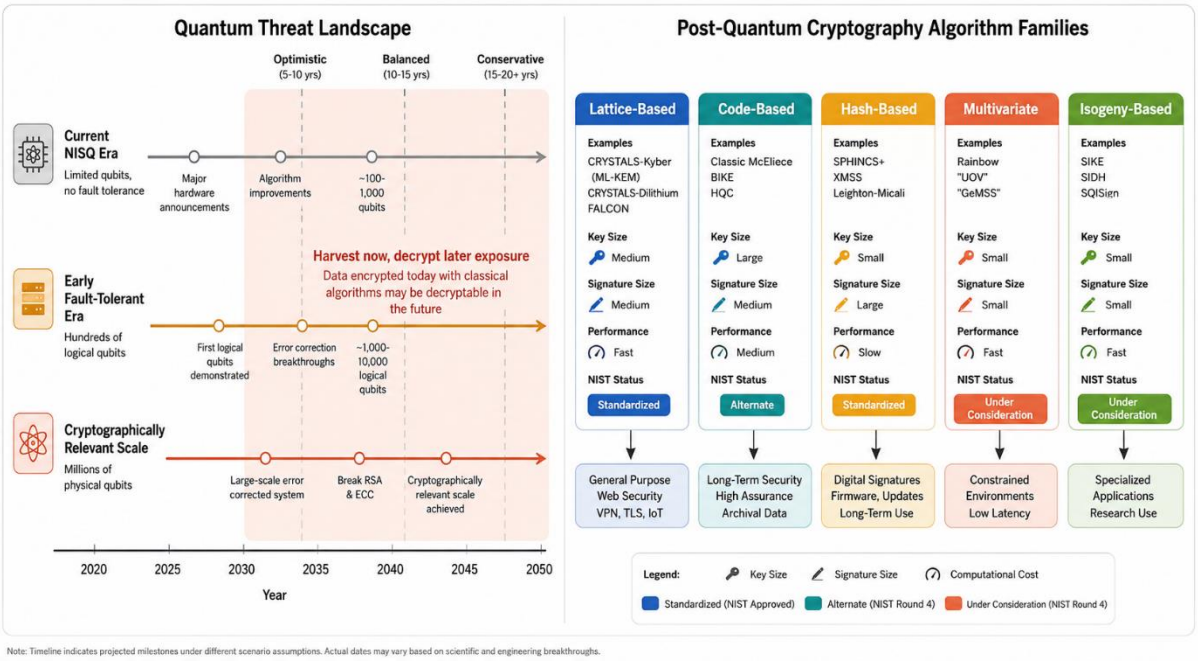

Figure 1. Quantum threat landscape and post-quantum cryptography algorithm families.

POST-QUANTUM CRYPTOGRAPHIC ALGORITHM FAMILIES

Five major families of post-quantum cryptography have emerged, each based on different mathematical foundations and each offering distinct performance and security characteristics. Understanding these families is essential for evaluating deployment options and making informed choices for specific applications.

3.1 Lattice-Based Cryptography

Lattice-based cryptography rests on the computational difficulty of problems related to high-dimensional lattices, particularly the Shortest Vector Problem and the Learning With Errors problem. These problems are believed to

DOI: 10.46121/pspc.54.3.37

be hard for both classical and quantum computers, and they support both key encapsulation and digital signature schemes with reasonable performance and security characteristics [11].

The CRYSTALS-Kyber key encapsulation mechanism and CRYSTALS-Dilithium signature scheme, both standardized by NIST, are lattice-based algorithms. Kyber provides key encapsulation with public keys around 800 bytes, ciphertexts around 768 bytes, and encryption and decryption operations that run efficiently in software. Dilithium provides digital signatures with public keys around 1300 bytes, signatures around 2400 bytes, and signing and verification that run efficiently. Both schemes have received extensive cryptanalysis during the NIST process and are believed to provide strong security.

3.2 Code-Based Cryptography

Code-based cryptography derives its security from problems related to decoding random linear codes, particularly the syndrome decoding problem. The oldest post-quantum cryptographic scheme, McEliece's public key encryption from 1978, is code-based and has resisted cryptanalysis for over four decades despite substantial attention [12]. Code-based schemes generally offer strong security guarantees but suffer from very large public key sizes that limit their applicability in many settings.

Classic McEliece, one of the NIST fourth round candidates, provides key encapsulation with excellent security properties but public keys ranging from 261 KB to over 1 MB depending on parameter choices. These key sizes are impractical for many applications but acceptable for specialized settings such as software distribution and long-term archival where key transmission cost is amortized over many uses.

3.3 Hash-Based Signatures

Hash-based signature schemes derive their security purely from the security of the underlying hash function, making them attractive for applications where minimal cryptographic assumptions are desired. The security of hash-based signatures reduces directly to the security of hash functions like SHA-2 and SHA-3, which are well understood and have withstood decades of cryptanalysis [13].

SPHINCS+, a stateless hash-based signature scheme standardized by NIST, provides strong security guarantees with signatures ranging from 8 KB to 50 KB depending on parameters. The large signature sizes limit applicability in bandwidth-constrained applications but the strong security guarantees make hash-based signatures particularly attractive for long-term high-assurance applications such as code signing and root certificate authorities.

3.4 Multivariate Cryptography

Multivariate cryptography rests on the difficulty of solving systems of multivariate polynomial equations over finite fields. Multivariate schemes typically offer very small signatures with fast verification but suffer from large public keys and complex parameter selection [14]. The security of specific multivariate schemes has proven difficult to analyze, and several proposed schemes have been broken during cryptanalysis.

Rainbow, a multivariate signature scheme that reached the final round of NIST standardization, was broken by a novel cryptanalytic attack in 2022, demonstrating the ongoing analytical uncertainty in this family. Multivariate cryptography remains an active research area but has not yet produced standards with the confidence that lattice-based and hash-based schemes offer.

3.5 Isogeny-Based Cryptography

Isogeny-based cryptography uses the mathematical structure of isogenies between elliptic curves, providing schemes with unusually small key sizes. SIDH, the leading isogeny-based key exchange, offered public keys as small as 400 bytes, an order of magnitude smaller than lattice-based alternatives [15]. However, SIDH was broken by a series of cryptanalytic attacks in 2022, illustrating that the security of relatively new cryptographic assumptions can prove more fragile than initially believed.

Newer isogeny-based schemes have been proposed and continue to be developed, but the family currently plays a smaller role in near-term deployment than lattice-based and hash-based alternatives.

DOI: 10.46121/pspc.54.3.37

PERFORMANCE ANALYSIS OF STANDARDIZED ALGORITHMS

We conducted empirical performance benchmarking of the NIST standardized post-quantum algorithms on a testbed representative of production infrastructure. The benchmarking evaluated key generation, encapsulation, decapsulation, signing, and verification operations across a range of hardware platforms and workload configurations.

4.1 Benchmarking Methodology

The benchmarking testbed comprised three hardware platforms: a modern server platform with 32-core Intel Xeon processors representing datacenter infrastructure, a mobile device platform with ARM Cortex-A78 processors representing consumer devices, and an embedded platform with ARM Cortex-M4 processors representing IoT and industrial control devices. Each platform ran optimized reference implementations of the standardized algorithms from open source cryptographic libraries.

Key exchange latency was measured through simulated TLS 1.3 handshakes using either classical elliptic curve Diffie-Hellman or post-quantum key encapsulation. Signature performance was measured through digital signature generation and verification operations at scales representative of software distribution and web authentication workloads. Memory footprint was measured through peak allocation tracking during algorithm execution.

4.2 Key Encapsulation Performance

CRYSTALS-Kyber demonstrated performance characteristics well suited to broad deployment. Key generation, encapsulation, and decapsulation operations all completed in under one millisecond on server hardware, and completed in a few milliseconds on mobile platforms. TLS 1.3 handshake latency using Kyber was approximately 1.8 to 2.4 times the latency of classical elliptic curve key exchange, driven primarily by the larger public keys and ciphertexts that must be transmitted rather than by computational cost.

Classic McEliece showed dramatically different characteristics with very fast encapsulation and decapsulation but extremely slow key generation and impractical public key sizes for most applications. McEliece may be suitable for specialized applications where key generation cost is amortized over many uses but is impractical for TLS-style ephemeral key exchange.

4.3 Digital Signature Performance

CRYSTALS-Dilithium provides signature and verification performance suitable for broad deployment. Signing and verification operations complete in a fraction of a millisecond on server hardware and remain fast on mobile and embedded platforms. Signature size of approximately 2400 bytes is larger than classical alternatives but manageable in most applications.

Falcon offers smaller signatures at approximately 700 bytes but requires floating-point operations that create both performance and side-channel challenges. Applications where signature size is critical may prefer Falcon despite its implementation complexity.

SPHINCS+ provides the strongest security guarantees but at substantial cost in signature size, with signatures ranging from 8 KB to 50 KB depending on parameter selection. Signing operations are relatively slow but verification is fast enough for practical use in code signing and other applications where signature bandwidth is amortized.

Table 1. Performance benchmarking summary for NIST standardized post-quantum algorithms.

Algorithm	Public Key (B)	Ciphertext/Signature (B)	Key Gen (µs)	Encap/Sign (µs)	Decap/Verify (µs)	Security Level
ECDH P-256	32	32	21	45	45	128-bit classical
Kyber-512	800	768	15	22	24	128-bit PQ
Kyber-768	1184	1088	24	35	38	192-bit PQ

DOI: 10.46121/pspc.54.3.37

Kyber-1024	1568	1568	35	52	56	256-bit PQ
Classic McEliece	261,120	128	85,000,000	46	138	128-bit PQ
ECDSA P-256	32	64	25	84	260	128-bit classical
Dilithium2	1312	2420	82	236	78	128-bit PQ
Dilithium3	1952	3293	138	375	130	192-bit PQ
Dilithium5	2592	4595	205	512	195	256-bit PQ
Falcon-512	897	690	8,200	155	43	128-bit PQ
SPHINCS+-128s	32	7856	235	235,000	375	128-bit PQ
SPHINCS+-128f	32	17,088	15	6,800	480	128-bit PQ

4.4 Communication Overhead Analysis

The most significant impact of post-quantum cryptography on protocol performance comes from increased communication overhead rather than computational cost. TLS 1.3 handshakes using post-quantum algorithms transmit substantially more data than classical alternatives, and this affects latency particularly on high-latency and low-bandwidth network paths.

Kyber-based TLS handshakes add approximately 2 KB of additional data compared to classical elliptic curve Diffie-Hellman. On a fast broadband connection this adds negligible latency, but on mobile networks with higher latency and lower bandwidth the impact can be more noticeable. Dilithium signatures in TLS certificates add several kilobytes to the certificate chain, further increasing handshake size.

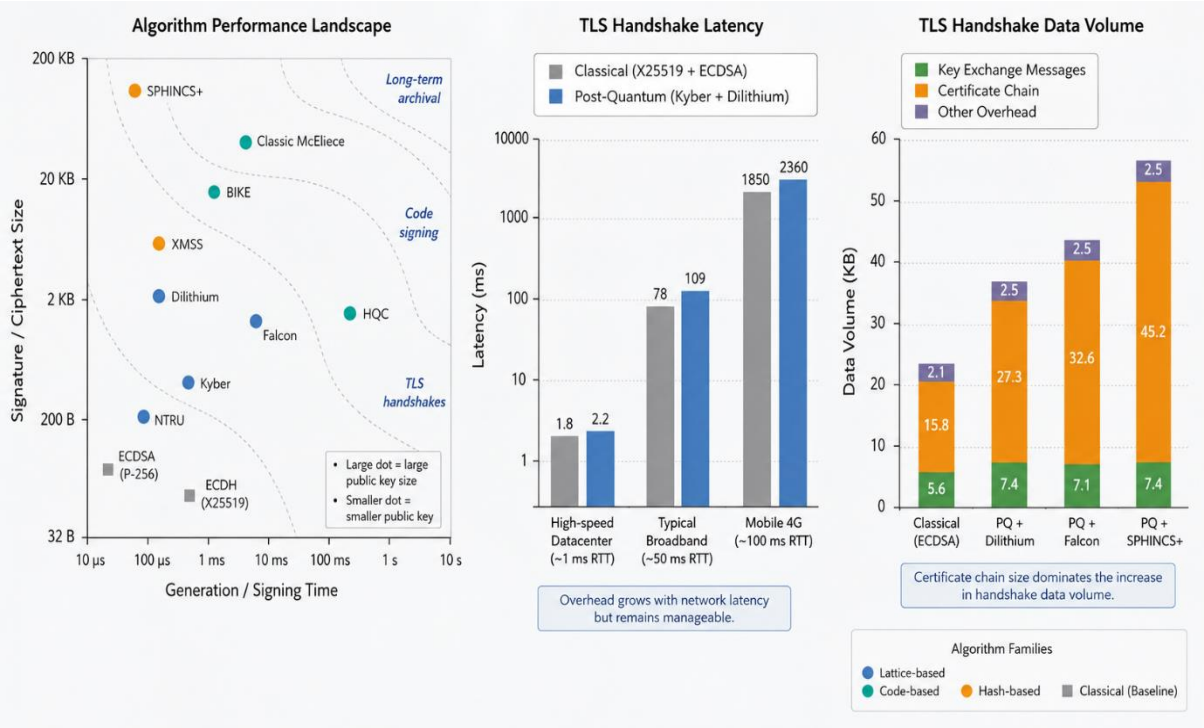

Figure 2. Comparative performance of standardized post-quantum algorithms across key metrics.

DOI: 10.46121/pspc.54.3.37

DEPLOYMENT ACROSS DIGITAL INFRASTRUCTURE SECTORS

The transition to post-quantum cryptography must occur across a diverse landscape of digital infrastructure, and different sectors face different challenges and timelines. This section examines four major infrastructure categories and the specific considerations that each faces.

5.1 Web Infrastructure and TLS

TLS is the foundation of secure web communication and the most visible target for post-quantum transition. Major browser vendors, cloud providers, and content delivery networks have begun deploying hybrid post-quantum key exchange in TLS 1.3, combining classical elliptic curve Diffie-Hellman with post-quantum key encapsulation to provide protection against both classical and quantum threats [16]. Google Chrome enabled experimental support for hybrid Kyber-based key exchange in 2023 and expanded deployment substantially in 2024.

The main challenges for web infrastructure include the increased handshake size and its effect on latency-sensitive applications, the need for TLS libraries and hardware acceleration to support new algorithms, and the coordination required across the vast ecosystem of certificate authorities, browsers, servers, and intermediate devices. Certificate authority transition to post-quantum signature algorithms remains an active area of work and will likely take several years to complete broadly.

5.2 Secure Messaging and End-to-End Encryption

End-to-end encrypted messaging systems including Signal, WhatsApp, and iMessage have begun implementing post-quantum key exchange to protect message confidentiality against future quantum attack. Signal's implementation of PQXDH provides post-quantum protection for initial key agreement while maintaining the Signal Protocol's forward secrecy properties [17].

Messaging systems benefit from having relatively controlled client and server infrastructure, allowing coordinated updates that would be much harder to achieve across the open web. Signal's deployment demonstrated that hybrid post-quantum protocols can be added to sophisticated messaging systems without disrupting user experience, providing a model that other messaging systems have followed.

5.3 Financial Systems and Payment Infrastructure

Financial infrastructure presents particular challenges due to the combination of long-lived cryptographic keys, high security requirements, and complex ecosystems involving multiple stakeholders. Root certificates in payment card infrastructure often have decade-long validity periods, and the coordination required for transitions across banks, payment processors, card networks, and merchants is substantial.

Central bank digital currency initiatives are increasingly incorporating post-quantum cryptography from the start rather than requiring later migration. The European Central Bank's digital euro project and similar initiatives elsewhere have explicitly considered post-quantum requirements in their cryptographic design [18]. For existing financial infrastructure, the transition will need to occur in coordination with normal certificate lifecycle management to avoid disrupting production systems.

5.4 Critical Infrastructure

Critical infrastructure including power grids, water systems, transportation networks, and industrial control systems presents perhaps the most challenging transition context. These systems often use specialized cryptographic protocols, contain long-lived embedded devices that may lack the computational resources for post-quantum algorithms, and operate on lifecycles measured in decades rather than years.

Industrial control system standards including IEC 62443 and NIST SP 800-82 are being updated to reflect post-quantum requirements, but retrofitting existing infrastructure with new cryptographic capability is expensive and slow. New critical infrastructure being deployed today should incorporate post-quantum readiness, but existing deployments will require phased transition strategies that may extend well into the 2030s.

DOI: 10.46121/pspc.54.3.37

Power System Protection and Control
ISSN:1674-3415

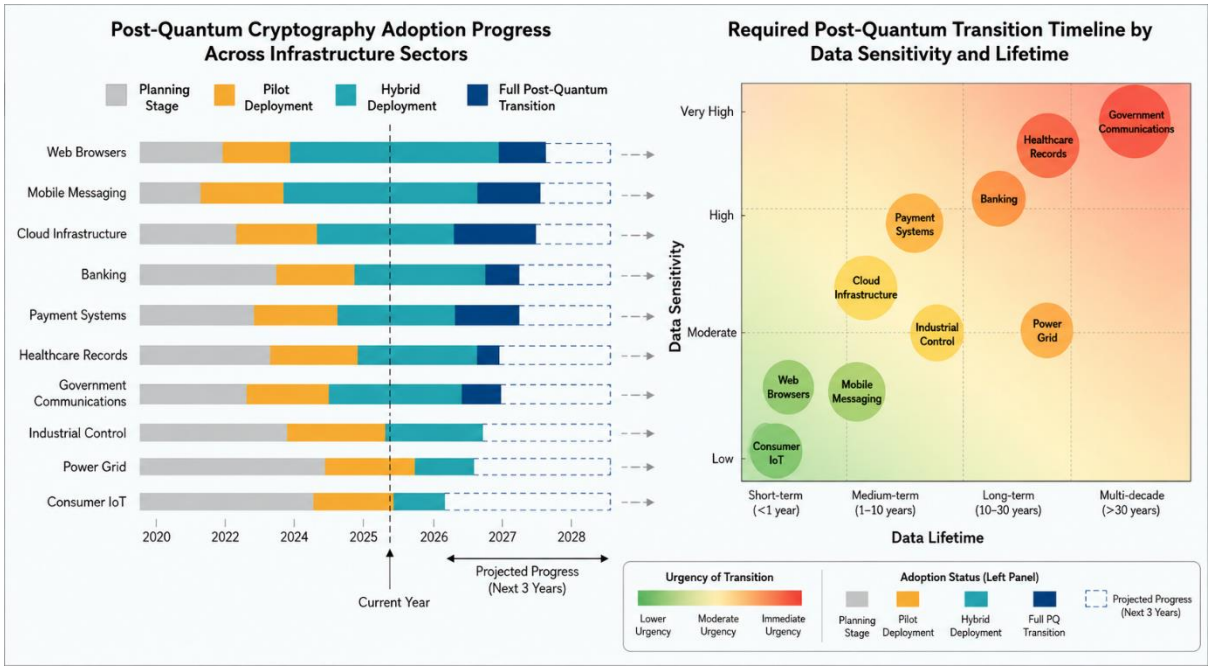

Figure 3. Post-quantum cryptography deployment status and timeline across infrastructure sectors.

DEPLOYMENT STRATEGIES AND BEST PRACTICES

6.1 Hybrid Deployment

Hybrid deployment combines classical and post-quantum algorithms in a single cryptographic protocol, providing protection against both types of attack during the transition period. If either the classical or the post-quantum component is broken, the hybrid combination remains secure [19]. This approach reduces risk during a period when confidence in specific post-quantum algorithms continues to develop and when interoperability with classical infrastructure remains necessary.

Hybrid deployment has trade-offs. Communication overhead is the sum of both algorithms' overhead rather than either alone, and computational cost similarly combines. However, the security benefits during transition generally justify these costs, and most major deployment initiatives are using hybrid approaches for initial rollouts.

6.2 Cryptographic Agility

The most important architectural lesson from the post-quantum transition is the value of cryptographic agility, defined as the ability to change cryptographic algorithms in deployed systems without requiring wholesale system replacement. Cryptographic agility requires abstracting cryptographic algorithm choices behind interfaces that allow substitution, avoiding hardcoded assumptions about specific algorithms, and maintaining infrastructure that allows deployed keys and certificates to be replaced through their lifecycles [20].

Organizations that invested in cryptographic agility over the past decade have found the post-quantum transition substantially easier than those with cryptographic assumptions embedded deep in application code. Cryptographic agility as an architectural principle should extend to all new systems being designed today, and existing systems should be evaluated for agility gaps and remediated where possible.

6.3 Cryptographic Inventory

Successful transition requires understanding what cryptography is deployed where, and organizations typically underestimate the scope of their cryptographic footprint. Public key certificates, embedded cryptographic keys, protocol implementations, and cryptographic operations in application logic all represent transition targets that must be identified and addressed.

Cryptographic inventory tools have emerged to help organizations discover their cryptographic footprint through code analysis, network monitoring, and certificate inventory. These tools support systematic transition planning

DOI: 10.46121/pspc.54.3.37

Power System Protection and Control
ISSN:1674-3415

by identifying the specific systems, protocols, and dependencies that will need updates. Organizations beginning post-quantum transition should invest early in comprehensive cryptographic inventory as a foundation for prioritization.

6.4 Vendor Coordination

Most organizations depend on cryptographic capabilities provided by vendors including software libraries, hardware security modules, cloud services, and network equipment. Post-quantum transition requires coordination across this vendor ecosystem, and vendor readiness varies substantially. Organizations should engage early with critical vendors to understand their post-quantum roadmaps, identify dependencies that may block transition, and plan for scenarios where vendor timelines may not align with the organization's own transition requirements.

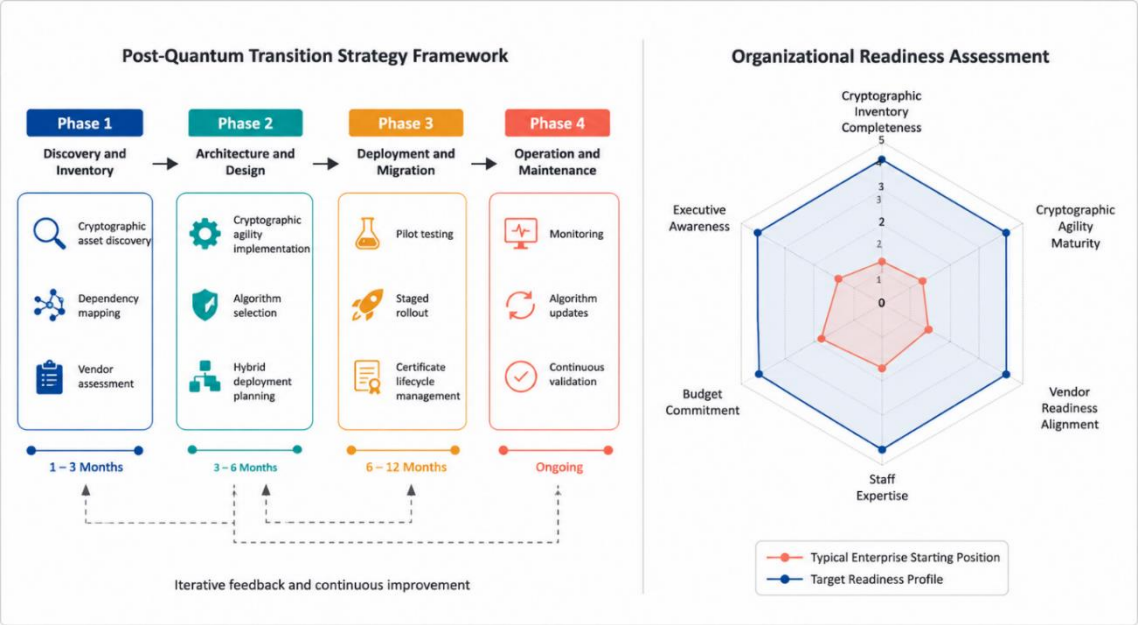

Figure 4. Post-quantum transition strategy framework and organizational readiness assessment.

DISCUSSION AND STRATEGIC IMPLICATIONS

The post-quantum transition represents one of the largest cryptographic migrations in the history of computing, and its success will depend on choices that governments, standards bodies, technology vendors, and organizations across every sector make in the coming years. Several strategic implications emerge from our analysis.

First, urgency varies substantially across use cases and organizations. Applications handling data that must remain confidential for many years face substantial risk from harvest now, decrypt later attacks and should transition promptly. Applications with short-lived data face less immediate risk but should still plan transition timelines that avoid emergency responses if quantum capability advances faster than expected. Organizations should assess their specific risk profile rather than applying uniform urgency across all systems.

Second, cryptographic agility deserves elevation to a first-class architectural principle. The specific algorithms currently standardized will not be the last word in post-quantum cryptography. New algorithms will be developed, standards will evolve, and cryptanalytic advances may require unexpected transitions. Systems designed with agility can absorb these changes with modest effort, while systems with embedded cryptographic assumptions face repeated painful migrations. The investment in agility pays dividends across many cryptographic transitions, not just the current post-quantum one.

Third, hybrid deployment provides risk mitigation during the transition period and should be the default approach rather than pure post-quantum deployment. The additional overhead of hybrid protocols is typically manageable, and the security insurance against potential weaknesses in either the classical or post-quantum components is

DOI: 10.46121/pspc.54.3.37

substantial. Full transition to pure post-quantum protocols can occur once confidence in the algorithms has developed further and classical infrastructure has been updated.

Fourth, coordinated action across sectors and jurisdictions matters. Web browsers and messaging platforms cannot complete their transitions without server-side updates, financial systems cannot transition without card network and merchant coordination, and critical infrastructure cannot transition without vendor and regulator alignment. Industry consortiums, government policy, and international coordination all have roles to play in accelerating the transition and reducing coordination costs.

Fifth, the specialized challenges of long-lived embedded systems and critical infrastructure deserve particular attention. Systems designed for twenty or thirty year deployment lifetimes should already be incorporating post-quantum readiness, and retrofit strategies for existing systems require investment that has not yet been broadly committed. Government policy in critical infrastructure sectors will play an important role in ensuring that transition timelines match the urgency that different applications face.

Limitations of our analysis include reliance on current understanding of quantum computing progress, which may prove faster or slower than expected, and focus on the algorithms standardized to date, which will be supplemented by additional standards in coming years. Our performance benchmarking used current implementations that will improve as optimization efforts continue, and real-world deployment experience will likely reveal challenges not apparent in benchmarking environments.

CONCLUSION

The transition to post-quantum cryptography is one of the most consequential technical challenges facing digital infrastructure in the coming decade. The mathematical foundations of the cryptographic systems that secure nearly every digital interaction are vulnerable to a future quantum computer, and while such a computer does not yet exist at cryptographically relevant scale, the trajectory of quantum hardware development has made the risk sufficiently real to demand action now. The security community has responded with a rigorous standardization process that has produced algorithms based on lattice, hash, and other post-quantum mathematical foundations, and these algorithms have received extensive cryptanalysis that provides substantial confidence in their security. Empirical benchmarking demonstrates that current post-quantum algorithms produce performance within manageable bounds for most applications, with communication overhead exceeding computational overhead as the dominant impact.

The transition itself, however, will take substantial time and coordinated effort across the digital infrastructure ecosystem. Web browsers, messaging platforms, cloud providers, financial systems, and critical infrastructure all face different challenges and timelines, and the coordination required across vendors, standards bodies, and regulators is substantial. Hybrid deployment provides a prudent path that maintains security during transition, and cryptographic agility as an architectural principle will pay dividends across this transition and future ones. Organizations that begin transition planning now, invest in cryptographic inventory and agility, engage vendors early, and match transition urgency to their specific risk profile will be well positioned to complete the transition before quantum computing capability creates emergencies.

For technology leaders responsible for infrastructure security, for standards bodies coordinating the transition, for policymakers considering how to accelerate migration in critical sectors, and for the broader community working to ensure that digital infrastructure remains secure through the quantum computing era, the message is clear. The transition to post-quantum cryptography is neither a distant hypothetical nor a manageable incremental change. It is a substantial undertaking that is already underway and that will occupy substantial attention and resources across the coming decade. The organizations and sectors that treat it as a strategic priority now will emerge from the transition with security intact and infrastructure modernized. Those that delay will face increasingly urgent and expensive transitions as the timeline compresses. The work is genuinely difficult, the stakes are high, and the time to begin in earnest is now.

DOI: 10.46121/pspc.54.3.37

REFERENCES

1. https://www.gjesr.com/April-2017.html
2. https://www.gjesr.com/April-2018.html
3. https://ieeexplore.ieee.org/document/11483386
4. Navin Chhibber, Multi-Granular Attention-Driven Reinforcement Learning Framework for Web Intelligent Enhancement Systems, 11 June 2026, https://ieeexplore.ieee.org/document/11483386
5. **https://pspac.info/index.php/dlbh/article/view/447**
6. **https://pspac.info/index.php/dlbh/article/view/439**
7. **https://pspac.info/index.php/dlbh/article/view/440**
8. **https://pspac.info/index.php/dlbh/article/view/445**
9. **https://pspac.info/index.php/dlbh/article/view/448**
10. **https://pspac.info/index.php/dlbh/article/view/452**
11. **https://pspac.info/index.php/dlbh/article/view/451**
12. **https://pspac.info/index.php/dlbh/article/view/465**
13. **Rangavinay Teja Royal Jagga** , 2026, https://ieeexplore.ieee.org/document/11448495
14. **Rangavinay Teja Royal Jagga , 2026, https://ieeexplore.ieee.org/document/11448514**
15. **Rangavinay Teja Royal Jagga , 2026, https://ieeexplore.ieee.org/document/11448337**
16. **Rangavinay Teja Royal Jagga , 2026, https://ieeexplore.ieee.org/document/11497560**
17. **Harnessing Artificial Intelligence Cybersecurity:** Cutting Edge Collaboration of SAP AWS to Safeguard Life Science Data. 2026 https://doi.org/10.1109/aiei69164.2026.11497833
18. **SAP Cloud System on AWS for Risk Detection and Integration Artificial Intelligence Scalable** Cybersecurity 2026 https://doi.org/10.1109/aiei69164.2026.11497435
19. **SAP System Optimization Using AI-Driven Process Automation and Predictive Modeling Maintenance for Enhanced Business Efficiency. 2025** https://doi.org/10.1109/computingcon64838.2025.11376613
20. https://ieeexplore.ieee.org/abstract/document/11376613
21. https://ieeexplore.ieee.org/abstract/document/11497833
22. https://ieeexplore.ieee.org/abstract/document/11497435
23. **https://pspac.info/index.php/dlbh/article/view/231**
24. **https://pspac.info/index.php/dlbh/article/view/235**
25. **https://pspac.info/index.php/dlbh/article/view/232**
26. **https://eudoxuspress.com/index.php/pub/article/view/2236**
27. **Yeasmin, S., Semi, M. M. A., Rony, M. K. K., Das, S., Sabeena, A. A., Rahman, R., Biswas, B., Ahmed, F., & Hossain, A. (2025).** Artificial Intelligence for Mental Health Monitoring: A Solution for Digital Behavioral Health Care and Education—An Umbrella Review. Health Science Reports, 9(1), e71703. https://doi.org/10.1002/hsr2.71703
28. **Hasan, S., Rahman, K. A., Ahmed, F., & Hossain, A. (2026). An integrated AI-driven framework for** maternal resource intelligence shortages across U.S. hospitals. Integrative Biomedical Research, 10(1), 1–8. https://doi.org/10.25163/biomedical.10110694
29. **Riipa, M. B., Ahmed, F., Rony, M. K. K., Hossain, A., Islam, A., Utsho, M. R., Kamal, M. B., Sharmin, S., &** Tasnim, A. F. (2026). The role of artificial intelligence in predicting

DOI: 10.46121/pspc.54.3.37

cardiovascular outcomes: a systematic review and meta-analysis. Biostatistics & Epidemiology, 10(1). https://doi.org/10.1080/24709360.2026.2670804

30. **Semi, M. M. A., Das, S., Utsho, M. R., Hossain,** A., Kamal, M. B., Sizan, A. A., Tasnim, A. F., Yeasmin, S., & Parvin, M. R. (2026). Artificial Intelligence in Public Health Education: A Scoping Review of workforce competency development. Health Science Reports, 9(3). https://doi.org/10.1002/hsr2.72066
31. **Ahmed, F., Hasan, S., Hossain, A., & Rahman, K. A. (2026). Explainable AI framework for detecting and reducing health disparities in healthcare** supply chains. Journal of AI, ML and DL, 2(1), 1–8. https://doi.org/10.25163/ai.2110685
32. **https://eudoxuspress.com/index.php/pub/article/view/5673**
33. **https://eudoxuspress.com/index.php/pub/article/view/5676**
34. **https://eudoxuspress.com/index.php/pub/article/view/5675**
35. **https://pspac.info/index.php/dlbh/article/view/414**
36. **https://eudoxuspress.com/index.php/pub/article/view/5689**
37. **Hima Bindu Lekkala, VishnuVardhan Bandar**i , AUTONOMOUS WORKFLOW OPTIMIZATION USING MULTI AGENT AI SYSTEMS AI AGENTS MANAGE STATIONS, WIP, AND TASK HANDOFFS, Vol. 54 No. 2 (202): April-June 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/306 , DOI: https://doi.org/10.46121/pspc.54.2.08
38. **Lekkala, H. B., & Bandari, V. V. (2026). Autonomous workflow optimization using multi-agent AI systems:** AI agents manage stations, WIP, and task handoffs. *Power System Protection and Control*, 54(2), 95–101. http://pspac.info/index.php/dlbh/article/view/306
39. **Bandari, V. V., & Lekkala, H. B. (2024). Physics-informed reinforcement learning for real-time control of complex manufacturing processes**. *Power System Protection and Control*, 52(2), 164–170. https://pspac.info/index.php/dlbh/article/view/343
40. **Lekkala, H. B., & Bandari, V. V. (2025). AI-based energy-aware scheduling and process optimization** in engineer-to-order smart manufacturing systems. *Power System Protection and Control*, 53(1), 30–36. http://pspac.info/index.php/dlbh/article/view/341
41. **Bandari, V. V., & Lekkala, H. B. (2026). AI-driven digital** thread framework for end-to-end lifecycle optimization in ETO manufacturing systems. *Power System Protection and Control*, 54(2), 318–325. http://pspac.info/index.php/dlbh/article/view/340
42. **Lekkala, H. B., & Bandari, V. V. (2026). Deep learning** for weld defect detection using CNN or vision transformers fusion detection. *Power System Protection and Control*, 54(2), 151–158. https://pspac.info/index.php/dlbh/article/view/314
43. **Bandari, V. V., & Lekkala, H. B. (2024). AI-based operator** behavior monitoring and cost optimization using digital traceability in manufacturing systems. *Power System Protection and Control*, 52(1), 38–45. https://pspac.info/index.php/dlbh/article/view/342
44. **Shreyas Jayaprakash,** MACHINE LEARNING-DRIVEN VERIFICATION: USING ML TO OPTIMIZE COVERAGE ANALYSIS, PREDICT SIMULATION RUNTIMES, AND AUTO-GENERATE TESTBENCHES, Vol. 54 No. 2 (2026): April-June 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/391

45. **Mohammed Shafi Kundiladi,** EVENT-DRIVEN IMAGE AND VEHICLE STATUS MANAGEMENT FOR LOW-POWER IOT DIGITAL LICENSE PLATES, Vol. 53 No. 3 (2025): July-September 2025, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/175 DOI: https://doi.org/10.46121/pspc.53.3.17
46. 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
47. **Kunal Kapoor**, **Apr 2026,** Relation Extraction and NER through Fine Tuned BERT model with transfer Learning, https://ieeexplore.ieee.org/document/11472214/metrics#metrics
48. **Harender Bisht**, Human–AI Collaboration in Insurance Fraud Detection: Ethical Cloud-Native Architectures for Fair and Transparent Decision Support, **Volume 2026, Issue 1,** https://doi.org/10.52710/cfs.873
49. **Harender Bisht,** Ethical AI-Augmented Compliance Systems: Architectural Innovations for Cloud-Native Financial and Insurance Data Integrity, **Vol. 11 No. 1s (2026) ,** https://doi.org/10.52783/jisem.v11i1s.14056
50. **Harender Bish**t, Governance-By-Design For AI-Based Insurance Fraud Detection: Auditability, Accountability, And Regulatory Traceability, **Archives / Vol. 9 No. 1 (2026**) https://doi.org/10.63278/jicrcr.vi.3620
51. **Harender Bisht,** Operationalizing Explainable AI in Insurance Fraud Detection: From Model Transparency to Decision Justification, **Vol. 35 No. 1 (2026): JOCAAA**, https://eudoxuspress.com/index.php/pub/article/view/4791,
52. **A. MahendraVardhan and S. Sridhar,** "Determining False Positive Analysis of Software Vulnerabilities with Predefined Scan Rules using Random Forest Classifier and Decision Tree Technique," **2022 4th International Conference on Advances in Computing**, Communication Control and Networking (ICAC3N), Greater Noida, India, 2022, pp. 622-625, **DOI: https://doi.org/10.1109/ICAC3N56670.2022.10074458**
53. **Amilineni, M.V. 2025**. Audit-Safe Agentic RAG Framework for Regulated Enterprise Systems: A Trustworthy AI Architecture for SAP, Finance, Healthcare, and Government Workflows. INTERNATIONAL JOURNAL OF ADVANCES IN SIGNAL AND IMAGE SCIENCES. (Jan. 2025), 34–46. **DOI: https://doi.org/10.29284/7fjzk883**
54. **Deepa Nagalavi; Shankar Balla Microsoft, USA; Pushpalatha. M; Nashwan Adnan Othman; Malik Bader Alazzam; A. Balakumar, Enhancing Real-Time Language Processing via Advanced PET Signal Analysis and Deep Learning, *06-07 June 2025***, DOI: 10.1109/ICICKE65317.2025.11136561 , https://ieeexplore.ieee.org/document/11136561
55. https://pspac.info/index.php/dlbh/article/view/430
56. **Venkata Sai Aditya Kondru,FMR, Carmel, USA ,; Shankar Balla; Dhavalkumar Thakar; Dheeraj Velaga; Sri Lekha Bandla,** Intelligent Human–Computer Interaction for Navigation Control Through Vision-Based Hand Gesture Recognition, Conferences >2026 IEEE 15th International , **Date of Conference: *07-09 April 2026*,Date Added to IEEE *Xplore*:** 08 May 2026 **DOI:** 10.1109/CSNT69054.2026.11502317 , https://ieeexplore.ieee.org/abstract/document/11502317

57. **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
58. **Navin Chhibber,; Deepak Singh; Anokh Kishore, Capital One, USA; Nikita Chawla; K. Anguraj,** Multi-Granular Attention-Driven Reinforcement Learning Framework for Web Intelligent Enhancement Systems, , **11 June 2026**, https://ieeexplore.ieee.org/document/11483386
59. https://pspac.info/index.php/dlbh/article/view/456
60. https://pspac.info/index.php/dlbh/article/view/455
61. https://eudoxuspress.com/index.php/pub/article/view/5677
62. Anumolu DPK, Veena B, Afreen SS, Bandla J, Lakshmi KC, Pulusu VS. In vitro models for studying drug metabolites and metabolizing enzymes: A comprehensive review. Int J Pharm Investig. 2026;16(3):885–91. Available from: http://dx.doi.org/10.5530/ijpi.20260116
63. Asgar Z, Kumar G, Khandelwal P, Pratap B, Gurjar V, Baluni A, et al. Utility of contrast-enhanced computed tomography abdomen in Intestinal Obstruction. Int J Drug Deliv Technol. 2026;16(32s). Available from: http://dx.doi.org/10.25258/ijddt.16.32s.4
64. Anumolu DP, Ramatulasi J, Ashok G, Afreen SS, Mathew C, Shakar PV. Synthesis and characterization of MIP ghost approach for selective extraction of empagliflozin and quantification by liquid chromatography. J Chromatogr Sci. 2025;63(2). Available from: http://dx.doi.org/10.1093/chromsci/bmaf008.
65. Anumolu DPK, Naraparaju S, Addada SB, Pagidipally V, Pulusu VS, Afreen SS. Synthesis of silver nanoparticles using Ecbolium ligustrinum leaves: Characterization through advanced analytical techniques. Nanotechnol Percept . 2024;710–8. Available from: http://dx.doi.org/10.62441/nano-ntp.vi.3618
66. Naraparaju S, Mukti A, Anumolu DP, Chaganti S. Development and validation of a spectrofluorimetric method for the quantification of capecitabine in bulk and tablets. Turk J Pharm Sci [Internet]. 2023;20(4):234–9. Available from: http://dx.doi.org/10.4274/tjps.galenos.2022.46364
67. Naraparaju S, Yamjala P, Chaganti S, Anumolu DP. Spectrophotometric quantification of atomoxetine hydrochloride based on nucleophilic substitution reaction with 1,2-naphthoquinone-4-sulfonic acid sodium salt (NQS). Turk J Pharm Sci [Internet]. 2024;20(6):405–11. Available from: http://dx.doi.org/10.4274/tjps.galenos.2022.09147.
68. https://pspac.info/index.php/dlbh/article/view/454
69. https://pspac.info/index.php/dlbh/article/view/449
70. https://pspac.info/index.php/dlbh/article/view/453
71. https://eudoxuspress.com/index.php/pub/article/view/5678
72. A Hybrid Deep Learning and Quantum Optimization Framework for Ransomware Response in Healthcare, DOI: 10.1109/OJCS.2025.3648741, https://ieeexplore.ieee.org/document/11316401, Date of Publication: 26 December 2025, Published in: IEEE Open Journal of the Computer Society,Journal: IEEE.

73. Md Nazmul Shakir Rabbi, Farhana Rahman Anonna, Kazi Nehal Hasnain, Sakib Murshed, Md Fazlul Huq Mithu, MD Tushar Khan, Monoara Begum, Sonia Afroze, HYBRID AI MODELS COMBINING RULES AND MACHINE LEARNING FOR FINANCIAL FRAUD CONTROL IN THE UNITED STATES, Vol. 54 No. 2 (2026): April–June 2026, Power System Protection and Control, https://pspac.info/index.php/dlbh/article/view/334 ,https://pspac.info/index.php/dlbh/article/view/334/271

74. **Adegboye A , O., Li, X., Qian, L. (2025).** Parameterized Model for Fork Antenna Design in UWB Band Using Fully Connected Artificial Neural Networks. In: Arabnia, H.R., Deligiannidis, L., Amirian, S., Shenavarmasouleh, F., Ghareh Mohammadi, F., de la Fuente, D. (Eds) Artificial Intelligence and Applications. CSCE 2024. Communications in Computer and Information Science, vol 2252. Springer, Cham. https://doi.org/10.1007/978-3-031-86623-4_7

75. Adegboye A. Olaoluwa1, Udofia M. Kufre,Obot Akanniyenne, Inverted C-Shaped Slots Loaded Exponential Tapered Triple Band Notched Ultra-Wideband (UWB) Antenna, https://doi.org/10.5281/zenodo.18139060, **Published May 31, 2024**

76. **Chander Vijay S Sanbhi**, LEADING-INDICATOR-DRIVEN RELIABILITY MODELLING: INCORPORATING OPERATIONS-DRIVEN RELIABILITY TASKS INTO FAILURE HAZARD ESTIMATION, Vol. 54 No. 2 (2026): April-June 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/376.

77. **Chander Vijay S Sanbhi**, DATA QUALITY AS A RELIABILITY MULTIPLIER: QUANTIFYING THE IMPACT OF STANDARDIZED WORK PROCESSES ON RELIABILITY MODEL ACCURACY, Vol. 52 No. 4 (2024): October-December 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/385

78. **Chander Vijay S Sanbhi,** HYBRID MARKOV–MONTE CARLO RAM MODELLING FOR MULTI-STATE ASSETS WITH NON-EXPONENTIAL FAILURE/REPAIR DISTRIBUTION, Vol. 54 No. 1 (2026): January-March 2026, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/379

79. **Chander Vijay S Sanbhi,** DEGRADATION-AWARE SPARES OPTIMIZATION WITH WEIBULL/PHM UNCERTAINTY AND LOGISTICS DELAYS, Vol. 52 No. 2 (2024): April-June 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/384

80. **Chander Vijay S Sanbhi**, PHYSICS-INFORMED RUL PREDICTION WITH ALEATORIC/EPISTEMIC UNCERTAINTY AND MAINTENANCE SYSTEM INTEGRATION, Vol. 54 No. 1 (2026): January-March 2026, Power System Protection and Control, ISSN-1674-3415 https://pspac.info/index.php/dlbh/article/view/378

81. **Chander Vijay S Sanbhi,** DIGITAL TWIN–RAM CO-SIMULATION FOR MAINTENANCE AND SPARING DECISIONS IN PROCESS FACILITIES, Vol. 52 No. 1 (2024): January-March 2024, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/383

82. **Chander Vijay S Sanbhi**, A JOINT PROBABILISTIC FRAMEWORK TO INTEGRATE RAM SIMULATION AND ECONOMIC FORECASTING WITHOUT DOUBLE-COUNTING DOWNTIME, Vol. 53 No. 4 (2025): October-December 2025, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/394

DOI: 10.46121/pspc.54.3.37

83. **Chander Vijay S Sanbhi**, MIXTURE-DISTRIBUTION MAINTAINABILITY MODELLING TO CAPTURE TAIL-RISK DOWNTIME IN CRITICAL MACHINERY, Vol. 53 No. 2 (2025): April-June 2025, Power System Protection and Control, ISSN-1674-3415, https://pspac.info/index.php/dlbh/article/view/393
84. **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
85. **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
86. https://www.atlantis-press.com/proceedings/icsbpim-25/126017621, **23-24 April 2025**
87. https://ieeexplore.ieee.org/abstract/document/11371052 , **2025 2nd International Conf.**
88. https://ieeexplore.ieee.org/abstract/document/11256577
89. https://ieeexplore.ieee.org/abstract/document/11069968
90. https://ieeexplore.ieee.org/abstract/document/11377462
91. Manikantha Varaprasad Inakollu, (2022, August), Decision Intelligence As A Strategic Capability: A New MIS Framework For AI-Driven Enterprises, A Comprehensive Approach To Integrating Artificial Intelligence Into Organizational Decision-Making, Vol. 23 No. 4 (2022), 66–79, Acta Scientiae, ISSN:2178-7727, URL: https://www.periodicos.ulbra.org/index.php/acta/article/view/662 DOI: https://doi.org/10.22178/acta.23.4.6
92. Manikantha Varaprasad Inakollu, (2022, December), Governance-Centric MIS Architectures For Enterprise-Scale Digital Transformation, Vol. 23 No. 6 (2022), 41-55, Acta Scientiae, ISSN:2178-7727, URL: https://www.periodicos.ulbra.org/index.php/acta/article/view/667 DOI: https://doi.org/10.22178/acta.23.6.4
93. Manikantha Varaprasad Inakollu, (2023, November), Governance-Aware Cloud Architectures For Enterprise Information Systems, Vol. 24 No. 6 (2023), 300-315, Acta Scientiae, ISSN:2178-7727, URL: https://www.periodicos.ulbra.org/index.php/acta/article/view/668 DOI: https://doi.org/10.22178/acta.24.6.28
94. Manikantha Varaprasad Inakollu, (2024, July), Enhancing ERP Auditability and Compliance Using Permissioned Blockchain, A Framework for Transparent and Immutable Enterprise Resource Planning Systems, Vol. 25 No. 3 (2024), 122-137, Acta Scientiae, ISSN:2178-7727, URL: https://www.periodicos.ulbra.org/index.php/acta/article/view/664 DOI: https://doi.org/10.22178/acta.25.3.16
95. Manikantha Varaprasad Inakollu, (2025, November), Quantum-Resilient Architectures for Enterprise and Cloud Information Systems, Implications of Quantum Computing for Enterprise Cybersecurity and Data Integrity, Vol. 26 No. 3 (2025), 580-595, Acta Scientiae, ISSN:2178-7727, URL: https://www.periodicos.ulbra.org/index.php/acta/article/view/663 DOI: https://doi.org/10.22178/acta.26.3.44

96. Manikantha Varaprasad Inakollu, (2023, May), Post-Implementation ERP value realization: A Decision intelligence Framework, Vol. 51 No. 2 (2023): April-June 2023, 48-63, Power System Protection and Control, ISSN-1674-3415,
URL: https://pspac.info/index.php/dlbh/article/view/286
DOI: https://doi.org/10.46121/pspc.51.2.6
97. Manikantha Varaprasad Inakollu, (2023, July), ERP as Digital Backbone: Redefining enterprise systems for continuous value creation, Vol. 51 No. 3 (2023): July-September 2023, 17-29, Power System Protection and Control, ISSN-1674-3415,
URL: https://pspac.info/index.php/dlbh/article/view/285
DOI: https://doi.org/10.46121/pspc.51.3.4
98. Manikantha Varaprasad Inakollu, (2024, May), FINOPS-Driven Cloud optimization models for enterprise applications, Vol. 52 No. 2 (2024): April-June 2024, 99-110, Power System Protection and Control, ISSN-1674-3415,
URL: https://pspac.info/index.php/dlbh/article/view/283
DOI: https://doi.org/10.46121/pspc.52.2.10
99. Manikantha Varaprasad Inakollu, (2025, July), Blockchain-Enabled trust frameworks for enterprise information systems, establishing verifiable trust in distributed organizational environments, Vol. 53 No. 3 (2025): July-September 2025, 285-300, Power System Protection and Control, ISSN-1674-3415, URL: https://pspac.info/index.php/dlbh/article/view/282
DOI: https://doi.org/10.46121/pspc.53.3.19
100. Manikantha Varaprasad Inakollu, (2026, March), Implications of quantum computing for enterprise cybersecurity and data integrity, Vol. 54 No. 1 (2026): January-March 2026, 831-844, Power System Protection and Control, ISSN-1674-3415,
URL: https://pspac.info/index.php/dlbh/article/view/281
DOI: https://doi.org/10.46121/pspc.54.1.57
101. **Pawan Kumar Singh,** Scaling Gate-All-Around (GAA) Transistor Architectures for Sub-2nm AI Accelerators Using Atomically Thin 2D Materials, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5713
102. **Pawan Kumar Singh,** Energy-Efficient Task Scheduling in Green Cloud Computing Using Neuromorphic Spiking Neural Networks, Vol. 33 No. 08 (2024): JOCAAA, Journal Name: Journal of Computational Analysis and Applications, Journal's ISSN: 1521-1398 (Paper),1572-9206 (Online), https://eudoxuspress.com/index.php/pub/article/view/5712
103. **Kunal Kapoor**, **Apr 2026,** Relation Extraction and NER through Fine Tuned BERT model with transfer Learning, https://ieeexplore.ieee.org/document/11472214/metrics#metrics
104. **Kapoor K, et al. AI-Driven COVID-19 Care**: Analytics, Scheduling & Geo-Access. International Journal of Drug Delivery Technology (IJDDT). **2026;16 (65S):Article** 136. Available at: https://impactfactor.org/PDF/IJDDT/16/IJDDT,Vol16,Issue65s,Article136.pdf
105. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7061998
106. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7062058
107. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=7061858
108. DOI: https://doi.org/10.1109/IC2NC67409.2025.11376261

109. DOI: https://doi.org/10.1109/ICBATS66542.2025.11258564
110. Rizwana Sindhavani. (2024). Self-Healing Cloud Security Architecture for Financial Systems Using Autonomous Incident Response . Journal of Computational Analysis and Applications (JoCAAA), 33(08), 9186–9197. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/5678
111. Rizwana Sindhavani. (2023). AI-Driven Cyber Threat Intelligence and Real-Time Attack Prevention System for Financial Institutions Using Behavioral Anomaly Detection and Continuous Risk Scoring . Journal of Computational Analysis and Applications (JoCAAA), 31(4), 3055–3066. Retrieved from https://eudoxuspress.com/index.php/pub/article/view/5677
112. Rizwana Sindhavani (2026) Machine Learning Enhanced Credit Risk Assessment Models For Community And Regional Banks : Improving Lending Decisions Through Alternative Data And Presixtive Analytics. Journal of Power System Protection and control 54(3), 197-210. Retrieved from https://pspac.info/index.php/dlbh/search
113. Rizwana Sindhavani (2025) . Adversarially Robust AI Framework For Securing Machine Learning Based Cyber Defense Systems Against Evasion And Poising Attacks In Financial Services . Journal of Power System Protection and Control 53(4) , 588-599. https://pspac.info/index.php/dlbh/search
114. Protecting Helathcare Financial Records And Digital Payment Ecosystems. Journal of Power System Protection and Control 53(2) , 440-451 . https://pspac.info/index.php/dlbh/search
115. https://doi.org/10.30574/ijsra.2022.5.2.0077
116. https://doi.org/10.30574/ijsra.2021.2.1.0047
117. https://doi.org/10.32628/CSEIT1936413
118. https://doi.org/10.32628/CSEIT192142
119. https://doi.org/10.32996/jcsts.2020.2.2.4
120. https://www.academicpublishers.org/journals/index.php/ijdsml/article/view/5958
121. A. Srivastava, "Securing PHI in cloud-based healthcare systems: Challenges, frameworks, and future directions," J. Comput. Anal. Appl., vol. 33, no. 2, Aug. 2024. [Online]. Available: https://www.eudoxuspress.com/index.php/pub/article/view/4349/3190
122. 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
123. 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
124. A. Srivastava, "A unified framework for secure cloud data management: Integrating governance, metadata intelligence, and privacy controls," J. Inf. Syst. Eng. Manage., vol. 9, no. 2, Apr. 2024. [Online]. Available: https://www.jisem-journal.com/download/45_A_Unified_Framework.pdf
125. 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
126. https://pmc.ncbi.nlm.nih.gov/articles/PMC11886096/

127. https://diabetesjournals.org/diabetes/article/73/Supplement_1/908-P/156688/908-P-Use-of-DPP4i-SGLT2i-Fixed-Dose-Combinations
128. https://www.sciencedirect.com/science/article/pii/S0019570720300056
129. https://pspac.info/index.php/dlbh/article/view/450
130. https://www.periodicos.ulbra.org/index.php/acta/article/view/528
131. Nand K. Yadav, Rodrigue Rizk, William C. W. Chen, and K. C. Santosh (2026). *DynaFormer: A Dynamic Dual-Attention Transformer with Linear-Complexity Fusion for Medical Image Segmentation*. 2026 IEEE Conference on Artificial Intelligence (CAI), pp. 1518-1523. https://doi.org/10.1109/CAI68641.2026.11536230 | Citations reported: 0 (ResearchGate publication metrics). Count source
132. Nand Kumar Yadav, Rodrigue Rizk, William C. W. Chen, and K. C. Santosh (2026). *I Detect What I Don't Know: Incremental Anomaly Learning with SWAG*. Intelligent Human Computer Interaction, Springer, pp. 129-144. https://doi.org/10.1007/978-3-032-26352-0_11 | Citations reported: 0 (ResearchGate publication metrics). Count source
133. Nand K. Yadav, Rayeesa Mehmood, Rodrigue Rizk, and K. C. Santosh (2025). *SCL-GAN: Spatially-Correlative Lightweight GAN for Efficient and High-Fidelity Thermal-Visible Face Synthesis*. IEEE International Conference on Image Processing (ICIP). https://doi.org/10.1109/ICIP55913.2025.11084295 | Citations reported: 1 (IEEE Xplore indexing). Count source
134. Nand Kumar Yadav, Satish Kumar Singh, and Shiv Ram Dubey (2025). *TranscoderGAN: Transformer-Inception Based Encoder-Decoder Generative Adversarial Network for Thermal-Visible Face Transformation*. Computer Vision and Image Processing, Springer, pp. 1-11. https://doi.org/10.1007/978-3-031-93709-5_1 | Citations reported: 0 (OpenAIRE/BIP metrics). Count source
135. Haresh Kumar Kotadiya, Satish Kumar Singh, Shiv Ram Dubey, and Nand Kumar Yadav (2024). *DCT-SwinGAN: Leveraging DCT and Swin Transformer for Face Synthesis from Sketch and Thermal Domains*. Computer Vision and Image Processing, Springer, pp. 225-236. https://doi.org/10.1007/978-3-031-58174-8_20 | Citations reported: 1 (Crossref/Scopus-indexed source). Count source
136. Nand Kumar Yadav, Satish Kumar Singh, and Shiv Ram Dubey (2024). *ISA-GAN: Inception-Based Self-Attentive Encoder-Decoder Network for Face Synthesis Using Delineated Facial Images*. The Visual Computer, vol. 40, pp. 8205-8225. https://doi.org/10.1007/s00371-023-03233-x | Citations reported: 7 (Semantic Scholar). Count source
137. Nand Kumar Yadav, Satish Kumar Singh, and Shiv Ram Dubey (2023). *TVA-GAN: Attention Guided Generative Adversarial Network for Thermal-to-Visible Image Transformations*. Neural Computing and Applications, vol. 35, pp. 19729-19749. https://doi.org/10.1007/s00521-023-08724-5 | Citations reported: 10 (Springer article metrics). Count source
138. Nand Kumar Yadav, Satish Kumar Singh, and Shiv Ram Dubey (2022). *CSA-GAN: Cyclic Synthesized Attention Guided Generative Adversarial Network for Face Synthesis*. Applied Intelligence, vol. 52, pp. 12704-12723. https://doi.org/10.1007/s10489-021-03064-0 | Citations reported: 21 (ResearchGate publication metrics). Count source

139. Nand Kumar Yadav, Satish Kumar Singh, and Shiv Ram Dubey (2022). *MobileAR-GAN: MobileNet-Based Efficient Attentive Recurrent Generative Adversarial Network for Infrared-to-Visual Transformations*. IEEE Transactions on Instrumentation and Measurement, vol. 71, pp. 1-9, Art. no. 5009909. https://doi.org/10.1109/TIM.2022.3166202 | Citations reported: 19 (ResearchGate/ADS indexing). Count source

DOI: 10.46121/pspc.54.3.37