Securing the Quantum Era: A Comprehensive Review of Post-Quantum Cryptography, Threat Models, Algorithmic Foundations, and Standardization Pathways

Sarthak Sengupta[1], Anindya Bose[2]

[1]ADMIRE Centre for Advancing Digital Health, Institute of Health Management Research, Bangalore, India
[2]Department of Microelectronics and VLSI Technology, Maulana Abul Kalam Azad University of Technology, West Bengal, India.

ABSTRACT: The advent of fault-tolerant quantum computing precipitates a foundational threat to the security of global digital infrastructure by rendering obsolete the mathematical assumptions underlying classical public-key cryptography. Widely deployed algorithms, including RSA, ECDSA, and Diffie-Hellman, which rely on the computational intractability of integer factorization and discrete logarithm problems, are vulnerable to polynomial-time attacks via Shor's algorithm. Concurrently, Grover's algorithm imposes a quadratic reduction in the security strength of symmetric primitives. In response, Post-Quantum Cryptography (PQC) has emerged as a critical field of research, dedicated to developing cryptographic systems secure against both classical and quantum attacks, while remaining deployable on existing classical hardware. This paper presents a comprehensive and in-depth examination of PQC, analyzing the five principal families: lattice-based, code-based, multivariate, hash-based, and isogeny-based cryptography. Each family is scrutinized through rigorous mathematical exposition, conceptual analysis, comparative performance evaluations, and contemporary security assessments. The study situates PQC within the evolving global threat landscape, provides a detailed analysis of the National Institute of Standards and Technology (NIST) PQC standardization process, and addresses critical implementation challenges such as constrained environments, migration strategies, hybrid cryptographic modes, and the imperative for cryptographic agility. The paper concludes by delineating essential future research directions vital for constructing a robust, quantum-resilient global cryptographic infrastructure.

Keywords: post-quantum cryptography, quantum computing, cryptographic standardization, nist, lattice-based cryptography, cryptographic migration, cybersecurity.

I. INTRODUCTION

The integrity and confidentiality of modern digital systems—encompassing secure communications, e-commerce, digital identity, critical national infrastructure, and financial services—are fundamentally dependent on classical public-key cryptography. Algorithms such as RSA, Diffie-Hellman (DH), and the Elliptic Curve Digital Signature Algorithm (ECDSA) derive their security from the presumed computational hardness of problems like integer factorization and the calculation of discrete logarithms[1]. These long-standing cryptographic assumptions, however, are invalidated in the presence of a sufficiently powerful quantum computer capable of executing Shor's algorithm, which solves these problems in polynomial time[2].

This existential threat is exacerbated by the long-term confidentiality requirements inherent in many applications and the viability of "harvest-now, decrypt-later" attacks. In such scenarios, adversaries intercept

and store encrypted data today, with the intention of decrypting it once cryptographically relevant quantum computers (CRQCs) become available[3], [4].

Post-Quantum Cryptography (PQC) addresses this challenge by developing classical algorithms designed to be resistant to attacks from both classical and quantum adversaries. Unlike quantum key distribution (QKD), PQC does not require specialized quantum hardware for communication, enabling global-scale deployment through software and firmware updates. This paper expands upon foundational work to deliver a complete academic treatise, offering[5]:

- A deeper theoretical development of all major PQC families.
- Comprehensive mathematical modeling of underlying hard problems.
- Integrated comparative tables for performance and security.
- A complete elaboration of the NIST PQC standardization pipeline.
- An expanded analysis of performance in constrained and Internet of Things (IoT) devices.
- A detailed forward-looking agenda of research challenges and opportunities.

II. THE QUANTUM THREAT: A NEW CRYPTOGRAPHIC REALITY

1. SHOR'S ALGORITHM AND THE FRAGILITY OF CLASSICAL PUBLIC-KEY CRYPTOSYSTEMS

Shor's algorithm conclusively demonstrated that the integer factorization problem (IFP) and the discrete logarithm problem (DLP) can be solved efficiently on a quantum computer. Consider an RSA modulus $N = pq$. The best-known classical factoring algorithms, such as the General Number Field Sieve (GNFS), require sub-exponential time[6]:

$T_{\text{classical}} \approx \exp\left((1.923 + o(1))(\log N)^{1/3}(\log \log N)^{2/3}\right)$.

In contrast, Shor's algorithm reduces this complexity to:

$T_{\text{Shor}} = O((\log N)^2(\log \log N)(\log \log \log N))$,

effectively breaking RSA for any practical key size.

Similarly, elliptic curve cryptosystems (ECDSA, ECDH) rely on the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP). Given a public key $Q = kP$, where P is a base point and k is a private scalar, Shor's algorithm can efficiently recover k, thereby compromising the security of all standardized elliptic curves.

2. GROVER'S ALGORITHM: QUADRATIC SPEEDUP IN SYMMETRIC CRYPTOGRAPHY

Grover's search algorithm provides a quadratic speedup for unstructured search problems. It reduces the effective security level of a symmetric cipher with a key size of n bits from 2^n to $2^{n/2}$. Consequently, AES-128, which offers 128 bits of classical security, is reduced to a 64-bit quantum security level. For long-term quantum resistance, AES-256 is recommended, as it maintains a 128-bit quantum security level. Similarly, hash functions require output lengths of at least 256 bits to maintain preimage resistance against quantum attacks[7], [8].

3. THE "HARVEST-NOW, DECRYPT-LATER" STRATEGIC THREAT

The quantum threat is not merely a future concern but an immediate strategic risk. Adversaries with foresight can conduct "harvest-now, decrypt-later" attacks, wherein they exfiltrate and archive encrypted data with the expectation of future decryption. Sensitive communications in government, defense, finance, and industrial sectors with long-term confidentiality requirements are particularly vulnerable, making the transition to PQC an urgent priority[9], [10].

III. FAMILIES OF POST-QUANTUM CRYPTOGRAPHY

PQC is categorized into several families, each based on distinct computational problems believed to be intractable for quantum computers[11], [12].

1. LATTICE-BASED CRYPTOGRAPHY

Lattice-based cryptography derives security from the computational hardness of problems in high-dimensional lattices. The principal hardness assumptions include:

- Learning With Errors (LWE): Given $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$, $\mathbf{s} \in \mathbb{Z}_q^n$, and small error vector $\mathbf{e} \in \mathbb{Z}^m$, recovering $\mathbf{s}$ from $\mathbf{b} = \mathbf{As} + \mathbf{e} \bmod q$ is conjectured to be hard.
- Shortest Vector Problem (SVP): Given a lattice $\mathcal{L}$, finding the shortest non-zero vector $\mathbf{v}_{\min} \in \mathcal{L}$ is computationally hard.

Prominent schemes like CRYSTALS-Kyber (KEM), CRYSTALS-Dilithium, and Falcon (signatures) utilize structured variants such as Module-LWE and NTRU lattices, often boasting strong security proofs based on worst-case to average-case reductions.

2. CODE-BASED CRYPTOGRAPHY

This family relies on the NP-hard problem of decoding random linear codes[13]. The McEliece cryptosystem, a cornerstone of this family, constructs a public key by obfuscating a structured code:
$G' = SGP$,

where G is a generator matrix for a binary Goppa code, S is a scrambler matrix, and P is a permutation matrix. Despite large public keys, the McEliece system has withstood cryptanalysis for over four decades.

3. MULTIVARIATE CRYPTOGRAPHY

Multivariate Quadratic (MQ) cryptography is based on the difficulty of solving systems of multivariate quadratic equations over finite fields $\mathbb{F}$:
$P_i(x_1, \ldots, x_n) = \sum \alpha_{jk}^{(i)} x_j x_k + \sum \beta_j^{(i)} x_j + \gamma^{(i)}$,for $i = 1, \ldots, m$.

Finding a solution vector $\mathbf{x}$ is NP-hard. While these schemes can be highly efficient, their security history is checkered, with many proposals broken by exploiting algebraic weaknesses.

4. HASH-BASED SIGNATURES

Hash-based signatures provide security based solely on the properties of cryptographic hash functions, specifically collision resistance and preimage resistance. SPHINCS+, a stateless hash-based signature scheme, offers robust security with minimal assumptions, albeit with relatively large signature sizes[14], [15].

5. ISOGENY-BASED CRYPTOGRAPHY

Isogeny-based schemes rely on the computational hardness of finding an isogeny (a certain kind of morphism) between two supersingular elliptic curves. Given two isogenous curves E and E', finding the isogeny $\phi: E \to E'$ is believed to be difficult. While promising due to small key sizes, this area has faced significant setbacks, notably the total break of the SIKE scheme in 2022, though research into more secure isogeny-based constructs continues[16], [17].

IV. COMPARATIVE ANALYSIS OF PQC SCHEMES

The following tables provide a consolidated comparison of the major PQC families and selected algorithms.

Table 1. Security foundations of major post-quantum cryptography families.

PQC Family	Underlying Hardness Problem	Quantum Resistance	Strengths	Limitations
Lattice-based	SVP, LWE, Ring-LWE	Very strong; worst-case reductions	Efficient; scalable; NIST-standardized	Larger signatures/keys vs. ECC
Code-based	Decoding random linear codes	Exceptionally strong; long track record	Extremely fast decryption; conservative security	Very large public keys (hundreds of KB)
Multivariate	Solving MQ systems	Moderate; structure-dependent	Fast operations; small signatures	Many historical schemes broken
Hash-based	Collision/preimage resistance of hash functions	Extremely strong; minimal assumptions	Simple construction; robust security	Large signature sizes (stateful variants)
Isogeny-based	Computing isogenies between elliptic curves	Emerging; less mature	Very small key sizes	Recent breaks (e.g., SIKE) reduce confidence

Description: This table provides a high-level comparative overview of the five principal families of Post-Quantum Cryptography. It contrasts their underlying hardness assumptions—the mathematical problems that provide their security—and assesses their perceived resistance to quantum cryptanalysis. The analysis of inherent strengths and limitations offers a foundational understanding of the strategic trade-offs involved in selecting a PQC family, highlighting that no single approach is superior in all dimensions. Lattice-based schemes are positioned as a robust general-purpose solution, while code-based and hash-based families offer specialized advantages in conservative security and minimal assumptions, respectively[18], [19].

Table 2. Performance comparison of representative post-quantum algorithms.

Algorithm	Type	Public Key Size	Ciphertext/Signature Size	Computational Performance	Notes / Deployment Suitability
CRYSTALS-Kyber	Lattice (KEM)	~0.8 - 1.5 KB	~0.8 - 1.5 KB	Fast; highly optimized	NIST-selected; ideal for TLS
CRYSTALS-Dilithium	Lattice (Signature)	1 - 2 KB	2 - 3 KB	Fast; robust	Excellent for general-purpose signing

Algorithm	Type	Public Key Size	Ciphertext/Signature Size	Computational Performance	Notes / Deployment Suitability
Falcon	Lattice (Signature)	~0.9 KB	~0.7 KB	Fast verification	Suitable for high-performance systems
Classic McEliece	Code-based (KEM)	250 KB - 1 MB	~0.1 KB	Extremely fast decryption	Preferred where bandwidth is less constrained
SPHINCS+	Hash-based (Signature)	Small	8 - 30 KB	Slower; stateless	Strong fallback option; minimal assumptions

Description: This table presents a concrete performance comparison of specific, prominent PQC algorithms slated for standardization or serious consideration. The data on public key and ciphertext/signature sizes, along with computational performance, are critical for evaluating their practical deployability in real-world protocols and systems. The "Notes" column contextualizes this performance, linking it to specific use cases, such as TLS handshakes (Kyber) or high-performance signing (Falcon). The broken status of SIKE is included as a cautionary note on the risks associated with emerging cryptographic families[20], [21].

Table 3. Resource requirements in constrained environments

PQC Scheme	**Device Platform**	**Key Gen Time**	**Signing/Encryption Time**	**Verification/ Decryption Time**	**Energy Usage**	**Suitability**
Dilithium-II	Raspberry Pi 4	~45-50 ms	~1-4 ms	~1-3 ms	Low	Excellent for IoT
Falcon-512	ARM Cortex-A72	~6-8 ms	<2 ms	<1 ms	Very Low	High-performance verification
Kyber-512	Raspberry Pi 3B	<5 ms	<1 ms	<1 ms	Low	Suitable for TLS handshakes
SPHINCS+-128	Raspberry Pi 4	>100 ms	>40 ms	>30 ms	Medium	Where signature size is not critical

Description: Focusing on the Internet of Things (IoT) and edge computing, this table quantifies the operational costs of PQC algorithms on representative resource-constrained platforms. Metrics such as key

generation, signing/encryption, and verification/decryption times, along with energy usage, are paramount for determining viability in low-power, low-compute environments. The data clearly illustrates the performance superiority of lattice-based schemes like Kyber and Falcon in these settings, while also showing the significant overhead of robust hash-based signatures like SPHINCS+, guiding appropriate algorithm selection based on device capabilities[22], [23], [24].

Table 4. Overview of the nist pqc standardization pipeline.

Round	Number of Candidates	Criteria Applied	Outcome
Initial Call (2016)	82 submissions	Completeness, correctness, basic security	69 accepted for Round 1
Round 1	69 candidates	Initial cryptanalysis, performance	26 advanced to Round 2
Round 2	26 candidates	Deep analysis, implementation benchmarking	15 selected (7 finalists + 8 alternates)
Round 3	15 candidates	Final cryptanalytic evaluation, peer review	**Kyber, Dilithium, Falcon, SPHINCS+** selected for standardization

Description: This table chronologically outlines the multi-round, multi-year NIST PQC standardization process, which began in 2016. It demonstrates the rigorous and iterative nature of the evaluation, showing the progression from a large pool of initial submissions to a final, vetted portfolio of algorithms. The "Criteria Applied" column emphasizes the escalating scrutiny—from basic correctness to deep cryptanalysis and implementation benchmarking—that ensured only the most secure and practical candidates were selected, thereby building global confidence in the final standards.

Table 5. Mathematical structures underpinning pqc schemes.

Algorithm	Mathematical Structure	Formal Definition / Core Equation	Security Impact
Kyber	Module-LWE	$\mathrm{b} = \mathrm{As} + \mathrm{e} \bmod q$	Strong worst-case to average-case reductions
Dilithium	Module-LWE / SIS	$\mathrm{Az} = \mathrm{t} \bmod q$ (with noise)	Lattice hardness ensures strong resistance
Falcon	NTRU Lattices	$f \cdot g \equiv 1 \bmod q$	Efficient, compact signatures
McEliece	Goppa Codes	$\mathrm{c} = \mathrm{m}G' + \mathrm{e}$	Longstanding security track record

Algorithm	Mathematical Structure	Formal Definition / Core Equation	Security Impact
SPHINCS+	Hash Functions	One-way and collision-resistant functions	Minimal assumptions, extremely robust

Description: This table delves into the core mathematical principles that form the security bedrock of the leading PQC algorithms. By presenting the formal definitions or core equations for each scheme, it provides a technical bridge between abstract mathematical problems and their concrete instantiations in cryptographic systems. The "Security Impact" column interprets these mathematical foundations, explaining, for instance, how worst-case to average-case reductions for lattice problems provide strong security guarantees, thereby offering insight into why certain algorithms are considered more theoretically sound than others.

Table 6. Migration and deployment requirements for pqc transition.

Migration Factor	Description	Impact on Deployment
Cryptographic Agility	Ability to switch cryptographic primitives	Essential for long-term adaptability and response to fu breaks
Backward Compatibility	Support for legacy systems and protocols	Critical for incremental, non-disruptive PQC rollout
Hardware Constraints	CPU, RAM, and energy requirements	Determines PQC suitability for IoT and edge devices
Certificate Ecosystem	CA infrastructure and PKI readiness	Major bottleneck for global deployment; requires PQ-F
Hybrid Modes	Combining classical + PQC algorithms	Provides transitional security during migration

Description: Transitioning to PQC extends beyond pure cryptography. This table identifies and defines the critical systemic and operational factors that will determine the success and speed of global PQC adoption. It moves the discussion from algorithmic properties to real-world implementation challenges, emphasizing that issues like cryptographic agility, backward compatibility, and PKI readiness are as crucial as the security of the algorithms themselves. This framework is essential for planners and architects to develop comprehensive migration strategies.

Figure 1. Performance-Security Trade-off of PQC Families.

Description: A conceptual plot illustrating the relative positioning of the major PQC families along the axes of normalized performance (e.g., operations per second) and security level (bits). Lattice-based schemes typically occupy a favorable middle-ground, offering a balanced profile. Code-based schemes show high security but lower performance due to large key sizes, while hash-based schemes show high security but potentially lower performance due to large signatures and slower operations. Multivariate and isogeny-

based schemes are shown as having promising but less certain positions due to maturity and security concerns.

Lattice-based schemes currently offer the most favorable balance of performance and security. Code-based schemes provide a conservative security choice with a long historical track record. Hash-based signatures offer security with minimal assumptions but at the cost of larger outputs. Multivariate and isogeny-based schemes remain active research areas but are currently less mature for immediate widespread standardization.

V. NIST PQC STANDARDIZATION PROCESS

The NIST PQC standardization initiative represents the most extensive public cryptographic evaluation effort since the Advanced Encryption Standard (AES) process in 2001. This multi-year, transparent process engaged the global cryptographic community to vet candidate algorithms thoroughly.

The process progressed through several rigorous stages, commencing with 82 initial submissions. After initial screening for completeness and correctness, 69 candidates advanced to Round 1. Subsequent rounds applied increasingly stringent criteria, including deep cryptanalysis, practical performance benchmarking, and resistance to side-channel attacks. From 26 Round 2 candidates, 15 were selected for the final Round 3. After extensive global review, NIST announced its first selections for standardization:

- CRYSTALS-Kyber for general-purpose Key Encapsulation Mechanisms (KEM).
- CRYSTALS-Dilithium as the primary digital signature algorithm.
- Falcon for applications requiring high-performance digital signatures with compact sizes.
- SPHINCS+ as a robust, hash-based signature fallback option.

This curated portfolio provides a unified and vetted pathway for the global transition to quantum-resistant cryptography.

VI. MIGRATION TO PQC AND FUTURE RESEARCH DIRECTIONS

The transition to a PQC-infused infrastructure necessitates profound architectural changes across software stacks, hardware, network protocols, and public key infrastructure (PKI). Legacy and constrained systems, such as those in the Internet of Things (IoT), medical devices, and industrial control systems, present significant challenges due to hard-coded cryptographic assumptions and severe resource limitations.

Critical migration priorities include:

- The development and deployment of hybrid cryptographic schemes that combine classical and PQC algorithms to maintain security during the transition period.
- The implementation of cryptographic-agility frameworks within protocols and systems, enabling seamless algorithm replacement in response to future cryptographic breaks.
- The creation of hardware accelerators for PQC primitives in CPUs, network interface controllers (NICs), and Hardware Security Modules (HSMs).
- A dedicated focus on developing side-channel resistant implementations of PQC algorithms.
- The redesign of the certificate ecosystem to support PQC, establishing a Post-Quantum Public Key Infrastructure (PQ-PKI).

Future research trajectories must explore new quantum-resistant problem families, construct multi-problem hybrid cryptosystems for enhanced security, optimize PQC for ultra-constrained devices, and develop globally synchronized deployment strategies to ensure a cohesive and secure transition.

Conclusion

Quantum computing represents a paradigm shift with profound implications for cryptographic security. Classical public-key cryptosystems are provably vulnerable to well-defined quantum algorithmic attacks, elevating the development and deployment of Post-Quantum Cryptography from a research topic to an immediate and strategic imperative. Among the current candidates, lattice-based cryptography offers the most practical and mathematically robust foundation for the majority of use cases, complemented by the conservative security of code-based systems and the minimal assumptions of hash-based signatures. The

NIST PQC standardization process provides a critical, stable foundation for this global undertaking. However, significant challenges remain, including implementation complexity, migration logistics, and hardware integration. Ultimately, Post-Quantum Cryptography is not a mere incremental update but a foundational reconstruction of digital trust, essential for securing the information landscape of the quantum century.

REFERENCES

[1] R. B. Marqas, S. M. Almufti, and R. Rebar Ihsan, "Comparing Symmetric and Asymmetric cryptography in message encryption and decryption by using AES and RSA algorithms," *Journal of Xi'an University of Architecture & Technology*, 2020.

[2] T. saad Mohamed, S. mohammed Khalifah, R. Marqas, S. M. Almufti, and R. R. Asaad, "Evaluation of Information Security through Networks traffic traces for machine learning classification," *Babylonian Journal of Networking*, vol. 2025, 2025, doi: 10.58496/bjn/2025/003.

[3] R. Asaad, R. Ismail Ali, and S. Almufti, "Hybrid Big Data Analytics: Integrating Structured and Unstructured Data for Predictive Intelligence," *Qubahan Techno Journal*, vol. 1, no. 2, Apr. 2022, doi: 10.48161/qtj.v1n2a14.

[4] K. Rustamov, "5G-Enabled Internet of Things: Latency Optimization through AI-Assisted Network Slicing," *Qubahan Techno Journal*, vol. 2, no. 1, pp. 1–10, Feb. 2023, doi: 10.48161/qtj.v2n1a18.

[5] D. Ghorbanzadeh, J. F. Espinosa-Cristia, N. S. G. Abdelrasheed, S. S. S. Mostafa, S. Askar, and S. M. Almufti, "Role of innovative behaviour as a missing linchpin in artificial intelligence adoption to enhancing job security and job performance," *Syst Res Behav Sci*, 2024, doi: 10.1002/sres.3076.

[6] S. A. Islam, M. Mohankumar, and U. Khatuna Jannat, "Enhancing Data Security in Mobile Traffic Networks Through Reverse Engineering," in *Proceedings of the 4th International Conference on Ubiquitous Computing and Intelligent Information Systems, ICUIS 2024*, 2024. doi: 10.1109/ICUIS64676.2024.10866267.

[7] K. V. Sheelavathy and V. Udaya Rani, "Detection IoT attacks using Lasso regression algorithm with ensemble classifier," *International Journal of Pervasive Computing and Communications*, vol. 21, no. 1, 2025, doi: 10.1108/IJPCC-09-2022-0316.

[8] T. Muhammad and H. Ghafory, "SQL Injection Attack Detection Using Machine Learning Algorithm," *Mesopotamian Journal of CyberSecurity*, vol. 2022, 2022, doi: 10.58496/MJCS/2022/002.

[9] X. Ye, T. G. Tan, and J. Zhou, "Towards Discovering Quantum-Threats for Applications Using Open-Source Libraries," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2024. doi: 10.1007/978-3-031-61486-6_17.

[10] V. A. Telsang, M. S. Kakkasageri, and A. D. Devangavi, "BLOCKCHAIN-BASED DEVICE AUTHENTICATION IN EDGE COMPUTING USING QUANTUM APPROACH," *Jordanian Journal of Computers and Information Technology*, vol. 11, no. 1, 2025, doi: 10.5455/jjcit.71-1724681080.

[11] P. Shah, P. Prajapati, R. Patel, and D. Patel, "Post Quantum Cryptography: A Gentle Introduction of Lattice-Based Cryptography (Kyber, NTRUCrypto)," in *Lecture Notes in Networks and Systems*, 2025. doi: 10.1007/978-981-97-8602-2_43.

[12] S. Ali and F. Anwer, "A secure framework for IoT-based medical sensors data using homomorphic elliptic curve cryptography," *Cluster Comput*, vol. 28, no. 14, 2025, doi: 10.1007/s10586-025-05537-0.

[13] S. M. Almufti, R. B. Marqas, P. S. Othman, and A. B. Sallow, "Single-based and population-based metaheuristics for solving np-hard problems," *Iraqi Journal of Science*, vol. 62, no. 5, pp. 1710–1720, May 2021, doi: 10.24996/ijs.2021.62.5.34.

[14] P. Shah, P. Prajapati, and D. Patel, "Lattice-Based Post Quantum Cryptography Using Variations of Learning with Error (LWE)," in *Communications in Computer and Information Science*, 2025. doi: 10.1007/978-3-031-88039-1_5.

[15] M. Elhajj and P. Mulder, "A Comparative Analysis of the Computation Cost and Energy Consumption of Relevant Curves of ECC Presented in Literature," *International Journal of Electrical and Computer Engineering Research*, vol. 3, no. 1, 2023, doi: 10.53375/ijecer.2023.318.

[16] E. Zeydan, Y. Turk, B. Aksoy, and S. B. Ozturk, "Recent Advances in Post-Quantum Cryptography for Networks: A Survey," in *Proceedings of the 2022 7th International Conference on Mobile and Secure Services, MobiSecServ 2022*, 2022. doi: 10.1109/MobiSecServ50855.2022.9727214.

[17] B. B. Gupta, D. Kalra, and A. Almomani, *Innovations in modern cryptography*. 2024. doi: 10.4018/979-8-3693-5330-1.

[18] F. Mensah, "Zero Trust Architecture: A Comprehensive Review of Principles, Implementation Strategies, and Future Directions in Enterprise Cybersecurity," *International Journal of Advance Research*, 2024.

[19] Prof. S. Joshi, "Cryptography and Cybersecurity: A Symbiotic Relationship," *Int J Res Appl Sci Eng Technol*, vol. 13, no. 5, 2025, doi: 10.22214/ijraset.2025.70789.

[20] Subhash Bondhala, "Cybersecurity in AI-Driven Data Centers: Reinventing Threat Detection," *International Journal of Advanced Research in Science, Communication and Technology*, 2025, doi: 10.48175/ijarsct-24464.

[21] M. Singirikonda, "Next-Generation Cryptography: Innovations and Challenges in Securing Digital Communication," *J Cybersecur*, vol. 1, no. 6, 2023.

[22] S. M. Almufti and S. R. M. Zeebaree, "Leveraging Distributed Systems for Fault-Tolerant Cloud Computing: A Review of Strategies and Frameworks," *Academic Journal of Nawroz University*, vol. 13, no. 2, pp. 9–29, May 2024, doi: 10.25007/ajnu.v13n2a2012.

[23] G. N. Vivekananda *et al.*, "Retracing-efficient IoT model for identifying the skin-related tags using automatic lumen detection," *Intelligent Data Analysis*, vol. 27, pp. 161–180, 2023, doi: 10.3233/IDA-237442.

[24] T. Thirugnanam *et al.*, "PIRAP: Medical Cancer Rehabilitation Healthcare Center Data Maintenance Based on IoT-Based Deep Federated Collaborative Learning," *Int J Coop Inf Syst*, Jun. 2023, doi: 10.1142/S0218843023500053.