JIRBDAI

Journal of Institutional Research, Big Data Analytics and Innovation

ASSESSING THE SIGNIFICANCE OF CRYPTOGRAPHIC TECHNIQUES IN ENHANCING PERSONAL DATA SECURITY IN MODERN INFORMATION SYSTEMS

Tajudeen Olanrewaju Toyyib, Sikirullah Abdussomad Olose, Saka K. Kamil
Department of Computer Science, Al-Hikmah University Ilorin, Nigeria
toyyibolanrewajutajudeen@gmail.com, abdussomadolose@gmail.com,
kamilsaka67@gmail.com

ABSTRACT: Personal data breaches have emerged as a defining challenge of contemporary digital infrastructure, driven by the proliferation of cloud-connected systems and accelerating adversarial capabilities. Cryptographic techniques remain the foundational mechanism through which organisations protect confidentiality, integrity, and authenticity once perimeter controls have been circumvented. This paper presents a critical, evidence-based assessment of cryptography's role in securing personal data across modern information systems. The scope encompasses symmetric encryption (AES-256-GCM), asymmetric cryptography (RSA and ECC), authenticated key exchange (TLS 1.3), and the post-quantum standardisation landscape under NIST FIPS 203/204/205, finalised in August 2024. Cryptographic capabilities are systematically mapped against major data protection frameworks, including GDPR, HIPAA Security Rule, PCI DSS v4.0, ISO/IEC 27001:2022, and NIST CSF 2.0, and evaluated using a structured Cryptographic Strength-Vulnerability (CSV) framework applied across eight security dimensions. Drawing on breach cost data from IBM Security (2023, 2024) and adoption figures from the 2023 Thales Data Threat Report, the paper demonstrates that organisations with fully deployed encryption consistently sustained breach costs averaging USD 1.25 million lower than those without. A persistent implementation gap, driven by key management failures, protocol misconfiguration, and side-channel vulnerabilities, is identified as the primary obstacle between theoretical cryptographic guarantees and operational security outcomes. Six evidence-based recommendations are provided for practitioners and policymakers, centred on cryptographic agility, HSM adoption, TLS 1.3 migration, post-quantum transition planning, privacy-by-design integration, and workforce development.

KEYWORDS: Cryptography, AES-256, Post-quantum Cryptography, ML-KEM, TLS 1.3, data breach, GDPR, key management, information security, IoT encryption

I. INTRODUCTION

Data is the defining strategic resource of the twenty-first century. As organisations migrate core operations to cloud environments and globally distributed networks, the attack surface expands correspondingly. According to Verizon (2024), confirmed data breaches in the 2024 Data Breach Investigations Report reached record levels, with ransomware and extortion-related incidents accounting for the majority of financially motivated attacks. IBM Security (2024) reported an average global breach cost of USD 4.88 million in 2024, a 10% increase over 2023 and the largest single-year rise since the COVID-19 pandemic. Healthcare sustained the highest average costs at USD 9.77 million, a figure it has held for the fourteenth consecutive year, reflecting both the

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

sensitivity of protected health information and the relative immaturity of cybersecurity investment in clinical settings. The empirical case for structural data protection, over perimeter-based approaches, is now compelling. Cryptographic controls operate differently from firewalls and intrusion detection systems: they protect the data itself. Even when an adversary successfully exfiltrates ciphertext, what they obtain is computationally intractable to exploit without the corresponding key material. Rescorla (2018), in the specification of TLS 1.3 (RFC 8446), formalised this protective principle, mandating authenticated encryption with associated data (AEAD) and eliminating all cipher suites that do not provide forward secrecy. Article 34 of the GDPR further reinforces this by providing a notification exemption for breaches where affected data was rendered unintelligible through encryption, creating a direct financial incentive for cryptographic deployment (European Parliament and Council, 2016; European Data Protection Board, 2023).

Despite these incentives, a gap between theoretical cryptographic security and operational practice persists. The exploitation of incorrectly configured cryptographic systems, including hardcoded keys, reused nonces, and absent key rotation, accounts for a disproportionate share of breach severity (IBM Security, 2024). This gap motivates the paper's central focus: not whether cryptography is theoretically adequate, but whether its potential is actually realised in deployed systems. The 2021-2024 period produced a step-change in breach frequency, driven by accelerated cloud adoption, remote-work infrastructure vulnerabilities, and the professionalisation of ransomware-as-a-service operations (Verizon, 2024). This structural context underpins the paper’s central argument: that correctly deployed cryptography represents the most reliable mechanism for limiting the exploitability of exfiltrated data. The paper is structured as follows. Section II presents the literature review, covering conceptual, theoretical, and empirical foundations, and identifies the research gap. Section III describes the methodology. Section IV presents the results and discussion. Section V presents conclusions and recommendations. Detailed comparison tables are provided in the Appendices.

II. RELATED WORKS

This section reviews the existing body of knowledge on cryptographic techniques in personal data security across three lenses: conceptual foundations, theoretical frameworks, and empirical evidence. A research gap is identified from this synthesis.

A. Conceptual Review

Cryptography provides the mathematical architecture ensuring that digital information can be stored and transmitted accessibly only to authorised parties. Confidentiality, integrity, and authenticity, the three pillars of information security, correspond directly to properties that cryptographic primitives are designed to provide (Barker, 2020). Symmetric encryption addresses confidentiality by transforming plaintext into ciphertext indistinguishable from random data without the key. Authenticated encryption, as deployed in AES-256-GCM and the TLS 1.3 record layer, provides both confidentiality and integrity in a single primitive, a significant practical improvement over separate encryption-and-MAC schemes, which historically generated authentication bypass vulnerabilities through implementation complexity (Rescorla, 2018).

The Advanced Encryption Standard (FIPS 197) remains the dominant symmetric encryption algorithm in deployed information systems worldwide. AES-256-GCM, combining AES in Galois/Counter Mode with an authentication tag, simultaneously guarantees confidentiality and integrity in a single cryptographic operation (Barker, 2020). Under quantum computation, Grover's

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

algorithm halves the effective key length, reducing AES-256 to approximately 128 bits of post-quantum security, a level that remains adequate and has driven NIST's recommendation of AES-256 over AES-128 for long-term data protection. Hardware AES-NI acceleration, available across all major processor families, eliminates performance as a barrier to adoption.

Public-key cryptography resolves the key distribution problem inherent in symmetric systems. RSA remains widely deployed but is increasingly disfavoured for new deployments, owing to its computational expense and vulnerability to Shor's quantum algorithm (Ullah et al., 2023). Elliptic curve cryptography (ECC) achieves equivalent security to RSA with significantly shorter key sizes and lower computational overhead. A 256-bit ECC key on NIST P-256 provides approximately 128 bits of classical security, equivalent to RSA-3072 (Adeniyi et al., 2024). Curve25519/X25519 provides the same security level with superior resistance to implementation side-channels due to its constant-time design, and is central to TLS 1.3's ECDHE key exchange and FIDO2/WebAuthn authentication. For IoT environments, Kumar and Kumar (2024) demonstrated that hybrid AES-ECC schemes deliver strong confidentiality with computational overhead manageable on microcontroller-class hardware.

The principle of privacy by design, codified in GDPR Article 25, requires cryptographic controls to be embedded as architectural components from system inception rather than retrofitted as compliance measures (European Parliament and Council, 2016). This shift from reactive to proactive cryptographic deployment has practical implications for procurement, software development lifecycles, and vendor assessment.

The regulatory landscape governing personal data security has undergone significant development in the 2020-2025 period. All major frameworks converge on encryption as either a mandated or strongly recommended technical control. The GDPR's Article 34 notification exemption for encrypted breaches creates a positive incentive structure: organisations that deploy encryption reduce both breach impact and regulatory liability exposure (European Data Protection Board, 2023). PCI DSS v4.0, which became fully mandatory in 2025, represents the most prescriptive cryptographic specification in the commercial sector, mandating TLS 1.2+ with explicit forward secrecy requirements (Payment Card Industry Security Standards Council, 2022). A critical gap across most commercial frameworks is the absence of mandatory post-quantum transition timelines, a structural risk that practitioners must address through internal policy in advance of regulatory compulsion (Kinyua, 2025). Detailed regulatory requirements and penalty structures are provided in Appendix A (Table A1).

B. Theoretical Review

The formal security notion of indistinguishability under chosen-ciphertext attack (IND-CCA2) captures a precise requirement: that an adversary with access to a decryption oracle cannot distinguish between encryptions of two chosen plaintexts. AES-256-GCM satisfies this standard under the random oracle model (Jager & Schwenk, 2021). Crucially, IND-CCA2 security belongs to a correctly instantiated scheme; nonce reuse in GCM mode, for example, catastrophically breaks confidentiality even though the underlying cipher remains secure. This insight is central to the implementation gap literature. TLS 1.3 (RFC 8446) represents the current gold standard for authenticated key exchange and secure channel establishment. Cremers et al. (2021) provided a comprehensive cryptographic analysis demonstrating that TLS 1.3 achieves multi-stage key secrecy and authentication under standard hardness assumptions. The elimination of all non-AEAD cipher suites, deprecation of static RSA key exchange, and mandatory use of ECDHE

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

ensure that compromise of the server's long-term private key does not retroactively decrypt previously captured sessions. Jager and Schwenk (2021) further provided tight security proofs enabling theoretically sound parameter selection at practical scales, underpinning TLS 1.3 as the recommended universal transport security standard.

The NIST post-quantum cryptography standardisation process, concluded with the publication of FIPS 203, 204, and 205 in August 2024, is the most consequential development in applied cryptography of the 2020-2025 period. An eight-year evaluation of 82 algorithms from 25 countries preceded the outcome. NIST selected CRYSTALS-Kyber (ML-KEM, FIPS 203) for key encapsulation, CRYSTALS-Dilithium (ML-DSA, FIPS 204) as the primary digital signature algorithm, and SPHINCS+ (SLH-DSA, FIPS 205) as a hash-based signature backup (National Institute of Standards and Technology, 2024a, 2024b, 2024c). ML-KEM's security derives from the Module Learning With Errors (MLWE) problem, for which no efficient quantum algorithm is known. SLH-DSA's hash-based construction provides security under the minimal assumption that the underlying hash function is second-preimage resistant, providing algorithmic diversity against the possibility that lattice-based assumptions are eventually weakened (Alagic et al., 2022). A critical asymmetry is evident: AES-256 retains adequate post-quantum security at 128 effective bits after Grover's attack, while all currently deployed public-key algorithms face existential threat from Shor's algorithm. This asymmetry demands a hybrid transition strategy combining classical ECC with post-quantum ML-KEM during the migration period (Bernstein & Lange, 2020; Cremers et al., 2022). A comparative algorithm analysis is provided in Appendix B (Table B1).

Fully homomorphic encryption (FHE) permits arbitrary computation on ciphertext such that decryption of the result is identical to computing on the plaintext, enabling cloud providers to process sensitive data without decrypting it. Vanin et al. (2023) demonstrated a blockchain-based FHE architecture for personal health records satisfying HIPAA requirements while enabling collaborative research analytics. The primary limitation of FHE in production environments remains computational overhead: Kiesel et al. (2023) found overhead approximately two to three orders of magnitude greater than plaintext computation for complex workloads. Wibawa et al. (2022) demonstrated that combining FHE with federated learning for privacy-preserving COVID-19 detection maintained model accuracy while providing formal privacy guarantees, demonstrating a practical hybrid approach for scenarios where regulatory compliance prevents data centralisation.

Side-channel attacks exploit physical information leakage from cryptographic implementations, including power consumption, electromagnetic emissions, cache access patterns, and timing variations, to recover key material without engaging the mathematical hardness of the cipher. Lipp et al. (2020) demonstrated in the Meltdown disclosure that speculative execution in modern processors creates cache-timing side channels capable of recovering kernel memory, including cryptographic key material, from user-space processes on shared cloud infrastructure. Well-engineered libraries including OpenSSL 3.x, BoringSSL, and libsodium provide constant-time implementations that mitigate timing side channels. Amrita et al. (2024) documented that many resource-constrained IoT implementations trade constant-time properties for performance optimisations, creating practical side-channel exposure in physically accessible devices.

Encryption workflow in modern information systems integrates key generation, lifecycle management, authenticated encryption, integrity verification, secure transport, and controlled decryption. Figure 1 presents this composite process, reflecting best-practice implementation aligned with NIST SP 800-57 Rev. 5 and RFC 8446 TLS 1.3.

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

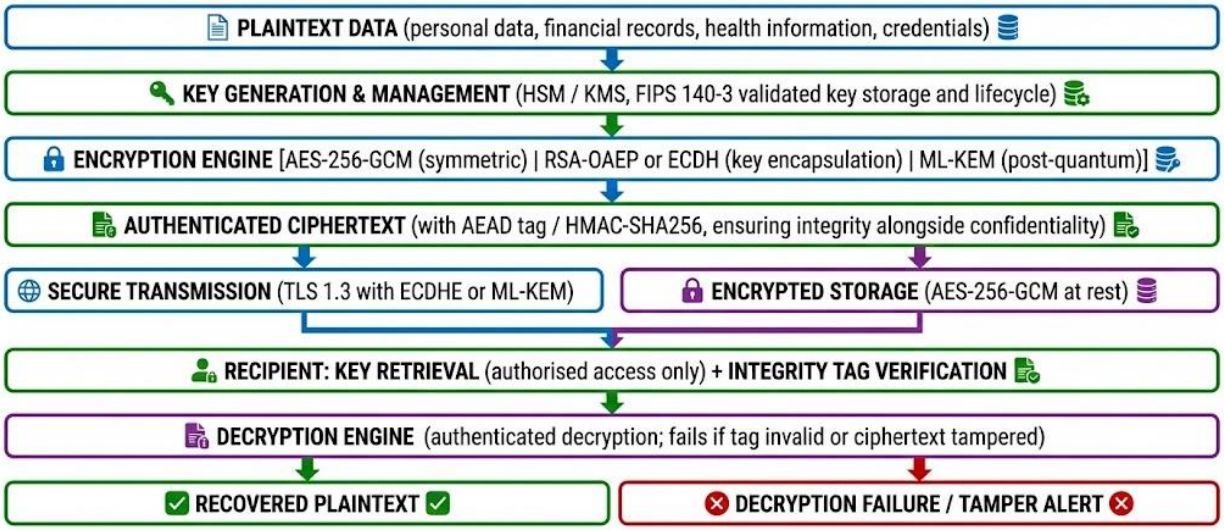

Figure 1: Encryption Workflow in Modern Information Systems. Note. Adapted from NIST SP 800-57 Part 1 Rev. 5 (Barker, 2020) and The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446) (Rescorla, 2018).

C. Empirical Review

The empirical literature establishes a consistent and measurable financial case for cryptographic deployment. IBM Security (2024) found that organisations with fully deployed encryption sustained average breach costs USD 1.25 million lower than those without encryption, with healthcare and government demonstrating the largest differentials. Thales Group (2023) reported that 37% of organisations suffering a breach in 2023 confirmed that affected data had been rendered unreadable to attackers through encryption, effectively neutralising the confidentiality impact of the event. Sector-specific analyses further illuminate the stakes. IBM Security (2024) reported that healthcare breaches cost an average of USD 9.77 million in 2024, a level sustained since 2011, reflecting both the value of protected health information to adversaries and the sector's historically slow adoption of security controls. Mahadik et al. (2024) found that encryption adoption in clinical settings lags other regulated industries primarily because of legacy electronic health record systems not designed with encryption-at-rest capabilities. PCI DSS v4.0 represents the most prescriptive cryptographic standard in the financial sector, with Thales Group (2023) finding that 87% of financial services organisations reported full encryption deployment for sensitive workloads.

Thales Group (2023) further reported that 87% of organisations identified key management as the most challenging aspect of their encryption deployments, spanning insufficient key rotation intervals, insecure key storage mechanisms, inadequate key access controls, and the absence of automated revocation procedures. This finding is consistent across industry surveys and motivates the key management analysis in the results section. On the IoT frontier, El-Hajj et al. (2023) found that while AES-128 with hardware acceleration remains achievable on ARM Cortex-M class processors, public-key operations impose prohibitive overhead for many constrained devices, making ECC essential as the minimum viable asymmetric primitive. NIST's Lightweight Cryptography standardisation programme resulted in the selection of ASCON, providing a validated path for resource-constrained environments (Rana et al., 2022). Thabit et al. (2023) documented that the transition from RSA to ECC in IoT authentication protocols reduces key

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

generation time by over 90% on microcontroller hardware while maintaining equivalent security levels; Alshudukhi et al. (2021) further demonstrated lightweight privacy-preserving ECC-based authentication for vehicular ad hoc networks, confirming ECC's practical viability for secure communication in resource-constrained mobile environments. Blockchain architectures additionally rely on cryptographic primitives including SHA-256 hash chaining and ECDSA/Ed25519 digital signatures, with Vanin et al. (2023) demonstrating that FHE and blockchain can be composed to address complex regulatory requirements such as GDPR's right to erasure through crypto-shredding.

Customer-managed encryption key (CMEK) schemes, offered by AWS KMS, Azure Key Vault, and Google Cloud KMS, provide tenant-controlled key hierarchies that prevent cloud providers from accessing customer data without explicit key sharing. Rafiq et al. (2022) conducted a systematic review of privacy preservation techniques in big data cloud environments, finding that encryption combined with access control represents the most effective defence combination, but noting that key management complexity significantly limits deployment in practice. Zhang et al. (2022) implemented a multi-key homomorphic encryption scheme for privacy-preserving cloud computing that allows multiple data owners to jointly compute over their encrypted data without sharing keys, offering a production-scale pathway toward data sovereignty in cloud environments. Figure 2 presents the layered cryptographic security architecture employed in enterprise-grade information systems, illustrating how cryptographic controls should be integrated across every layer of the technology stack.

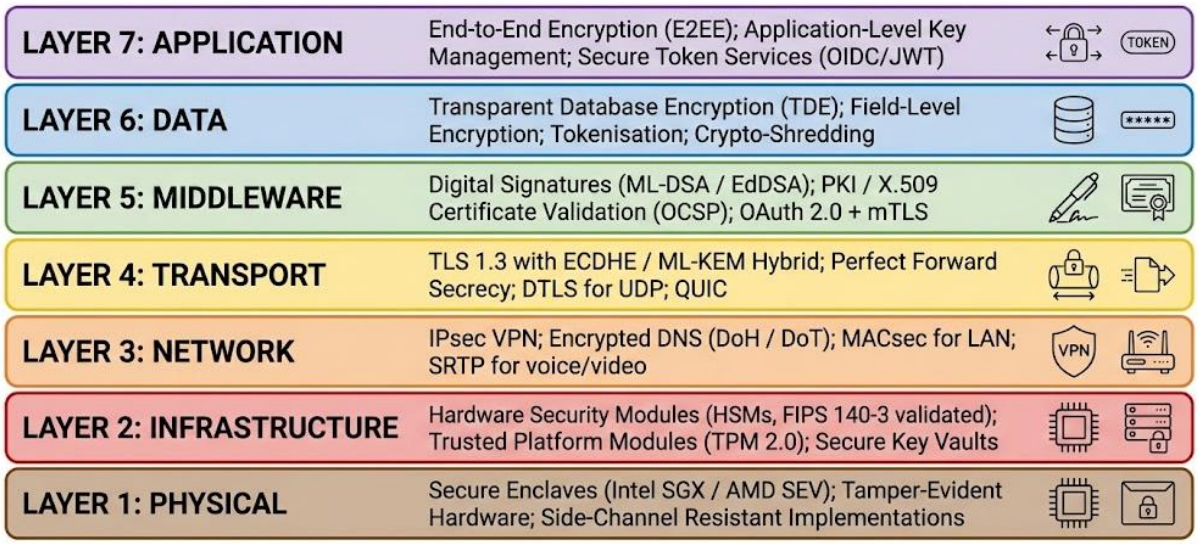

Figure 2: *Layered Cryptographic Security Architecture in Enterprise Information Systems.* Note. Adapted from NIST Cybersecurity Framework (CSF) 2.0 (National Institute of Standards and Technology, 2024d) and NIST SP 800-57 Part 1 Rev. 5 (Barker, 2020).

Figure 3 presents sector-level encryption adoption data synthesised from Thales Group (2023) and IBM Security (2024), illustrating the pronounced heterogeneity in deployment across industries.

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

Industry Sector	Adoption %	Relative Adoption Rate
Cloud / SaaS Providers	91%	(Highest)
Financial Services	87%	
Telecommunications	79%	
Healthcare	73%	
Government / Defence	70%	
Retail / E-commerce	62%	
Manufacturing / OT	45%	(Below Median)
Higher Education	38%	(Lowest)

Figure 3: Industry Adoption of Encryption as Primary Data Protection Control (2023-2024)
Note. Adoption figures reflect deployment of encryption as a primary control for sensitive data workloads, not total use of encryption in any form. Data synthesised from Thales Group (2023) and IBM Security (2024). OT = Operational Technology.

Cloud and SaaS providers (91%) lead adoption, driven by contractual obligations and competitive market dynamics. Financial services (87%) and telecommunications (79%) follow, propelled by regulatory mandates. Manufacturing and operational technology (45%) and higher education (38%) both fall well below the median, with legacy control system hardware and constrained security budgets being the predominant factors respectively (Rafiq et al., 2022). Manufacturing's low adoption is of particular concern given escalating targeting of operational technology environments by state-sponsored threat actors documented in recent Verizon DBIR reports.

D. Research Gap

Prior surveys address cryptographic techniques from primarily domain-specific or algorithm-level perspectives. Ullah et al. (2023) provided a comprehensive survey of ECC applications and challenges but did not integrate breach cost economics or regulatory mapping. Rana et al. (2022) surveyed lightweight cryptography in IoT networks without cross-sector comparative analysis. Adeniyi et al. (2024) categorised ECC applications for IoT security without addressing the post-quantum transition imperative or empirical breach impact data. Mahadik et al. (2024) examined digital privacy in healthcare from a policy perspective without a technical cryptographic framework. Rafiq et al. (2022) focused on big data cloud environments without extending to IoT, financial, or government domains. No existing study simultaneously integrates: (a) a structured multi-dimensional cryptographic strength-vulnerability assessment across eight security dimensions; (b) cross-sector empirical breach cost differentials attributable to encryption deployment; (c) systematic mapping of cryptographic controls to five major regulatory frameworks; and (d) a unified analysis of the post-quantum transition imperative alongside current operational deployment challenges. This paper addresses that gap by applying an original Cryptographic Strength-Vulnerability (CSV) framework across all four analytical dimensions, providing a cross-cutting assessment relevant to practitioners, regulators, and researchers

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

simultaneously. Empirical data cited were critically appraised against stated methodologies; figures from IBM Security and Thales Group are interpreted as indicative sector estimates rather than precise measurements, and are presented accordingly throughout.

III. Methodology

This paper employs a structured critical review methodology, integrating three complementary analytical approaches to address the research gap identified in Section II.

A. Research Design

The study adopts a qualitative-quantitative synthesis design, combining systematic literature review with secondary empirical data analysis. The research questions guiding the study are: (1) What is the demonstrated financial and operational significance of cryptographic protection across modern information system domains? (2) Where do the primary implementation failures occur between theoretical cryptographic guarantees and operational outcomes? (3) What does the post-quantum standardisation landscape require of organisations immediately?

B. Literature Search and Selection

A systematic search of peer-reviewed literature published between 2020 and 2025 was conducted across IEEE Xplore, ACM Digital Library, ScienceDirect, and Google Scholar, supplemented by NIST standards documentation and grey literature from IBM Security, Thales Group, and Verizon. Search terms included combinations of: cryptography, AES, ECC, RSA, TLS, post-quantum, key management, data breach, GDPR, HIPAA, IoT security, homomorphic encryption, and side-channel attacks. Studies were included if they provided: empirical measurements of cryptographic performance or breach impact; theoretical security proofs or standardisation documentation; or systematic reviews of cryptographic deployment in specific sectors. Studies were excluded if they focused exclusively on mathematical cryptanalysis without practical deployment relevance, or predated the 2020 regulatory and standardisation period that defines the paper's scope.

C. Analytical Framework

The primary analytical instrument is the original Cryptographic Strength-Vulnerability (CSV) framework, applied across eight security dimensions: confidentiality, data integrity, authentication, key management, protocol security, side-channel resistance, post-quantum transition readiness, and regulatory compliance. For each dimension, the framework maps the theoretical cryptographic strength available through correctly deployed controls against the corresponding implementation vulnerability documented in the empirical literature. This dual-column structure enables the identification of the implementation gap as a function of dimension-specific failure modes rather than overall cryptographic inadequacy. The full CSV framework is presented in Appendix C (Table C1). Sector-level breach cost differentials were derived by synthesising IBM Security (2023, 2024) reported cost ranges for organisations with and without fully deployed encryption as a primary data control, disaggregated by sector. These figures are presented as indicative estimates based on reported survey ranges rather than as precise cost measurements, consistent with the methodology stated in both IBM Security and Thales Group publications. Regulatory mapping was conducted by cross-referencing the cryptographic requirements of each framework against the algorithm-level and operational controls assessed in

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

the CSV framework, identifying alignment gaps and areas where regulatory requirements lag technical best practice.

D. Limitations

Several limitations apply. First, industry survey data from IBM Security and Thales Group are based on self-reported organisational responses, which may be subject to selection bias toward organisations with more mature security practices. Second, breach cost figures represent sector-level averages and do not capture the full distribution of outcomes within sectors. Third, the post-quantum timeline projections cited from Kinyua (2025) and NSA CNSA 2.0 represent strategic planning estimates rather than precise technical predictions. These limitations are acknowledged in the interpretation of findings throughout the results section, and findings are qualified accordingly.

IV. RESULTS AND DISCUSSION

This section presents the findings of the CSV framework assessment, the empirical breach cost analysis, and the cross-domain deployment evaluation, with discussion of implications.

A. The Demonstrated Significance of Cryptographic Protection

The empirical case for cryptographic protection is established through two convergent bodies of evidence. IBM Security (2024) found that organisations with fully deployed encryption sustained average breach costs USD 1.25 million lower than those without encryption, with healthcare and government demonstrating the largest differentials. Thales Group (2023) reported that 37% of organisations suffering a breach confirmed that affected data had been rendered unreadable to attackers through encryption, effectively neutralising the confidentiality impact of the event. The GDPR Article 34 notification exemption has created a measurable regulatory incentive: European Data Protection Board guidance (2023) clarifies that the exemption applies when encryption of appropriate standard was applied to the data prior to the breach, reducing the reputational and notification costs that constitute a significant component of total breach cost.

Table 1 presents comparative breach cost data by sector for encrypted versus non-encrypted systems, synthesised from IBM Security (2023, 2024) and Thales Group (2023).

Table 1: Comparative Breach Impact: Encrypted vs. Non-Encrypted Systems (Average Cost, USD Millions, 2023-2024)

Sector	Avg Cost: Encrypted (USD M)	Avg Cost: Not Encrypted (USD M)	Cost Differential
Healthcare	$2.2M	$9.8M	$7.6M differential (highest across all sectors)
Financial Services	$2.0M	$6.1M	$4.1M differential
Technology	$1.3M	$4.6M	$3.3M differential
Government	$1.6M	$7.2M	$5.6M differential
Retail / E-commerce	$0.9M	$3.2M	$2.3M differential
Critical Infrastructure	$1.8M	$7.8M	$6.0M differential

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

Note. Values for encrypted systems represent organisations with fully deployed encryption as primary data control. Data synthesised from IBM Security (2023, 2024) and Thales Group (2023). Figures are indicative estimates based on reported sector differentials.

Across all sectors, the breach cost differential between encrypted and non-encrypted systems is substantial and consistent. Healthcare exhibits the most dramatic disparity, a USD 7.6 million differential, reflecting direct harm mitigation from encrypted data being unusable by recipients, alongside the GDPR Article 34 regulatory notification cost reduction. The consistency of differentials across sectors, from retail (USD 2.3 million) to critical infrastructure (USD 6.0 million), establishes cryptographic investment as a high-return risk management intervention regardless of industry context.

B. CSV Framework Assessment: Strengths and Implementation Vulnerabilities

The application of the eight-dimension CSV framework (Appendix C, Table C1) reveals a consistent pattern across all dimensions: the vulnerabilities most consequential in practice are not failures of the underlying cryptographic mathematics but failures of implementation, key management, and operational process. This finding aligns with Verizon (2024) attribution data, which identified configuration errors, weak or reused credentials, and supply chain vulnerabilities, not cryptanalytic weaknesses, as the majority drivers of financially damaging breaches in 2024.

In the confidentiality dimension, AES-256-GCM provides 256-bit classical security and IND-CCA2 security under standard assumptions, yet IV/nonce reuse, weak key derivation, and hardcoded keys in source code routinely nullify these guarantees in deployed systems. In the key management dimension, FIPS 140-3 validated HSMs and cloud KMS with CMEK provide robust technical controls, yet Thales Group (2023) found that 87% of organisations identified key management as their most significant encryption challenge, spanning insufficient rotation intervals, insecure storage mechanisms, and the absence of automated revocation. In the post-quantum transition dimension, NIST FIPS 203/204/205 standardise ML-KEM, ML-DSA, and SLH-DSA as technically sound post-quantum replacements, yet harvest-now-decrypt-later attacks on current RSA/ECC traffic represent an active threat for organisations with long data retention requirements. The protocol security dimension illustrates the gap particularly sharply. TLS 1.3 eliminates all non-AEAD cipher suites and mandates ECDHE for forward secrecy, providing strong theoretical guarantees. Yet legacy TLS 1.0/1.1 configurations remain present in embedded systems and operational technology environments, and weak cipher suite negotiation in TLS 1.2 deployments continues to create practical downgrade attack exposure (Verizon, 2024).

C. Key Management as the Critical Operational Weakness

Among all operational challenges in cryptographic deployment, key management consistently emerges as the most consequential. NIST SP 800-57 Part 1 Rev. 5 (Barker, 2020) provides comprehensive key lifecycle guidance covering generation, distribution, storage, use, rotation, and destruction, yet industry surveys indicate that full compliance with these recommendations remains the exception rather than the rule. Hardware security modules (HSMs), providing FIPS 140-3 validated tamper-resistant key storage, represent the gold standard for enterprise key management. Cloud-hosted HSM services (AWS CloudHSM, Azure Dedicated HSM, Google Cloud HSM) have substantially reduced the barrier to entry. Ding et al. (2024) demonstrated that TPM-based key storage in IoT deployments provides a practical equivalent of HSM-level security

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

for constrained environments, protecting key material even when the device operating system is compromised.

D. Side-Channel Vulnerabilities in Deployed Systems

Side-channel attacks represent a distinct category of implementation failure that operates independently of algorithm selection. Lipp et al. (2020) demonstrated in the Meltdown disclosure that speculative execution in modern processors creates cache-timing side channels capable of recovering kernel memory, including cryptographic key material, from user-space processes on shared cloud infrastructure. The implications for multi-tenant cloud environments are significant: cryptographic workloads run alongside potentially adversarial tenant workloads. Amrita et al. (2024) documented that many resource-constrained IoT implementations trade constant-time properties for performance optimisations, creating practical side-channel exposure in physically accessible devices. The tension between performance and side-channel resistance persists as one of the more difficult problems in constrained-environment cryptographic engineering.

E. The Post-Quantum Transition Imperative

The finalisation of FIPS 203, 204, and 205 in August 2024 provides the technical foundation for migration, but the operational challenge of replacing all RSA and ECC cryptographic infrastructure across heterogeneous enterprise environments is substantial (National Institute of Standards and Technology, 2024a, 2024b, 2024c). The harvest-now-decrypt-later attack model is particularly pressing for sectors with long data retention requirements, including healthcare, legal, government, and financial services. An adversary capturing TLS 1.3 session traffic today can archive it and decrypt it once a quantum computer capable of running Shor's algorithm becomes available. For data that must remain confidential for ten to twenty years, this threat is present now, making immediate cryptographic agility investment non-optional (Kinyua, 2025).

F. Cross-Domain Deployment Discussion

The cross-domain analysis reveals sector-specific challenges that qualify the aggregate findings. In cloud computing environments, customer-managed encryption key (CMEK) schemes provide tenant-controlled key hierarchies that technically resolve the cloud provider trust problem, yet key management complexity remains the dominant barrier to effective deployment (Rafiq et al., 2022). In IoT and mobile systems, the cryptographic capability gap between enterprise and constrained environments has narrowed substantially through the selection of ASCON as a lightweight cryptographic standard and the availability of hardware-accelerated AES-128 on ARM Cortex-M processors, though a meaningful gap remains, particularly for public-key operations (El-Hajj et al., 2023). Mobile platforms benefit from hardware-isolated secure enclaves, providing FIPS 140-level key isolation that renders key extraction infeasible even for operating-system-level attackers. In healthcare and financial systems, the results confirm a divergence: financial services organisations (87% full encryption deployment) consistently outperform healthcare organisations (73%), despite healthcare bearing the highest average breach costs. This divergence reflects the difference in regulatory enforcement intensity between PCI DSS v4.0's prescriptive cryptographic mandates and HIPAA's addressable encryption standard for data at rest, which has historically allowed clinical organisations to defer implementation. Blockchain and digital identity systems demonstrate a complementary pattern: while foundational cryptographic primitives (SHA-256 hash chaining, ECDSA/Ed25519 signatures) provide strong immutability guarantees, the GDPR

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

right to erasure creates a structural tension with blockchain immutability that can only be resolved through cryptographic means, specifically crypto-shredding (Vanin et al., 2023).

Taken together, the results establish that the implementation gap between theoretical cryptographic guarantees and operational security outcomes is the defining challenge of cryptographic practice in the 2020-2025 period, not algorithmic inadequacy. Addressing this gap requires concurrent investment in key management infrastructure, protocol modernisation, workforce capability, and post-quantum transition planning.

V. CONCLUSION

This paper has critically assessed the significance of cryptographic techniques in personal data security across modern information system domains through a structured eight-dimension Cryptographic Strength-Vulnerability (CSV) framework, comparative sector-level breach cost analysis, and systematic regulatory mapping, yielding three overarching conclusions with corresponding practical imperatives. Cryptographic protection is empirically validated as the most reliable mechanism for limiting the exploitability of exfiltrated data: the IBM Security (2024) breach cost differential of USD 1.25 million between fully encrypted and non-encrypted organisations, combined with the GDPR Article 34 notification exemption (European Data Protection Board, 2023), establishes encryption deployment as a high-return investment for any organisation processing personal data at scale, and organisations should therefore implement cryptographic algorithm abstraction layers enabling agile algorithm substitution, mandate TLS 1.3 across all production services with immediate retirement of TLS 1.0 and 1.1, and embed end-to-end and client-side encryption as architectural defaults consistent with GDPR Article 25. The most consequential vulnerabilities in deployed systems are not mathematical weaknesses but operational failures in key management, protocol configuration, and implementation quality—Thales Group (2023) identified key management as the leading challenge for 87% of organisations—requiring as a priority the adoption of FIPS 140-3 validated HSM-backed key management as a baseline standard, supported by workforce investment in secure cryptographic API usage and automated audit tooling capable of detecting nonce reuse, weak key derivation parameters, and deprecated configurations within continuous integration pipelines. Third and most urgently, the post-quantum transition represents the defining strategic challenge of the 2024–2035 period: the harvest-now-decrypt-later attack model means that organisations with long data retention requirements cannot defer action until quantum capability is realised, and must instead conduct an immediate cryptographic inventory, deploy hybrid TLS key exchange combining X25519 with ML-KEM on all externally facing endpoints, and complete full migration to NIST FIPS 203 (ML-KEM) and FIPS 204 (ML-DSA) standards aligned to the NSA CNSA 2.0 2030 milestone, while future research should evaluate hybrid classical and post-quantum TLS performance at internet scale, develop automated cryptographic agility assessment frameworks, and examine the security and performance characteristics of fully homomorphic encryption in production healthcare analytics workloads, as the combined pressures of AI-assisted cryptanalysis, advancing quantum computing, and expanding IoT attack surfaces will demand sustained investment in applied cryptography to consistently realise the strong theoretical guarantees that current standards provide.

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

REFERENCES

Adeniyi, A. E., Jimoh, R. G., & Awotunde, J. B. (2024). A systematic review on elliptic curve cryptography algorithm for internet of things: Categorization, application areas, and security. Computers & Electrical Engineering, 114, Article 109062. https://doi.org/10.1016/j.compeleceng.2024.109062

Alagic, G., Cooper, D. A., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., & Smith-Tone, D. (2022). Status report on the third round of the NIST post-quantum cryptography standardization process (NIST IR 8413). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8413

Alshudukhi, J. S., Al-Mekhlafi, Z. G., & Mohammed, B. A. (2021). A lightweight authentication with privacy-preserving scheme for vehicular ad hoc networks based on elliptic curve cryptography. IEEE Access, 9, 15633-15642. https://doi.org/10.1109/ACCESS.2021.3049986

Amrita, Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight cryptography for internet of things: A review. EAI Endorsed Transactions on Internet of Things, 10. https://doi.org/10.4108/eetiot.5565

Barker, E. (2020). NIST Special Publication 800-57 Part 1 Rev. 5: Recommendation for key management. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-57pt1r5

Bernstein, D. J., & Lange, T. (2020). Post-quantum cryptography: State of the art. In B. Preneel & F. Vercauteren (Eds.), Cyber security cryptography and machine learning (LNCS 12161, pp. 23-33). Springer. https://doi.org/10.1007/978-3-030-49785-9_2

Cremers, C., Duzlu, S., Fiedler, R., Fischlin, M., & Janson, C. (2022). BUFF security of digital signature schemes in the multi-user setting with corruptions. In Advances in Cryptology: EUROCRYPT 2022 (LNCS 13275, pp. 3-32). Springer. https://doi.org/10.1007/978-3-031-06944-4_1

Cremers, C., Fischlin, M., Kissner, L., Peters, Z., & Stebila, D. (2021). A cryptographic analysis of the TLS 1.3 handshake protocol. Journal of Cryptology, 34(4), Article 37. https://doi.org/10.1007/s00145-021-09384-1

Ding, Z., Li, Y., Li, J., Chen, X., & Zhu, H. (2024). A lightweight and secure communication protocol for the IoT environment. IEEE Transactions on Dependable and Secure Computing, 21(3), 1050-1067. https://doi.org/10.1109/TDSC.2023.3267979

El-Hajj, M., Mousawi, H., & Fadlallah, A. (2023). Analysis of lightweight cryptographic algorithms on IoT hardware platform. Future Internet, 15(2), 54. https://doi.org/10.3390/fi15020054

European Data Protection Board. (2023). Guidelines 9/2022 on personal data breach notification under GDPR version 2.0. https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202209_personal_data_breach_notification_v2.0_en.pdf

European Parliament and Council. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data (General Data Protection Regulation). Official Journal of the European Union, L 119, 1-88. https://eur-lex.europa.eu/eli/reg/2016/679/oj

IBM Security. (2023). Cost of a data breach report 2023. IBM Corporation. https://www.ibm.com/reports/data-breach

IBM Security. (2024). Cost of a data breach report 2024. IBM Corporation. https://www.ibm.com/reports/data-breach

ISO/IEC. (2022). ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection. International Organization for Standardization. https://www.iso.org/standard/82875.html

Jager, T., & Schwenk, J. (2021). On the tight security of TLS 1.3: Theoretically sound cryptographic parameters for real-world deployments. Journal of Cryptology, 34(3), Article 30. https://doi.org/10.1007/s00145-021-09388-x

Kiesel, R., Lakatsch, M., Mann, A., Lossie, K., Sohnius, F., & Schmitt, R. H. (2023). Potential of homomorphic encryption for cloud computing use cases in manufacturing. Journal of Cybersecurity and Privacy, 3(1), 44-60. https://doi.org/10.3390/jcp3010004

Kinyua, C. G. (2025). The impact of quantum computing on cryptographic systems: Urgency of quantum-resistant algorithms and practical applications in cryptography. European Journal of Information Technologies and Computer Science, 5(1), 1-10. https://doi.org/10.24018/ejcompute.2025.5.1.146

Kumar, D., & Kumar, M. (2024). Hybrid cryptographic approach for data security using elliptic curve cryptography for IoT. International Journal of Computer Network and Information Security, 16(2), 42-54. https://doi.org/10.5815/ijcnis.2024.02.04

Lipp, M., Schwarz, M., Gruss, D., Prescher, T., Haas, W., Fogh, A., Horn, J., Mangard, S., Kocher, P., Genkin, D., Yarom, Y., & Hamburg, M. (2020). Meltdown: Reading kernel memory from user space. Communications of the ACM, 63(6), 46-56. https://doi.org/10.1145/3357033

Mahadik, S. S., Pawar, P. M., Muthalagu, R., Prasad, N. R., Hawkins, S.-K., Stripelis, D., Rao, S., Ejim, P., & Hecht, B. (2024). Digital privacy in healthcare: State-of-the-art and future vision. IEEE Access, 12, Article 10549909. https://doi.org/10.1109/ACCESS.2024.3404432

Majumder, S., Ray, S., & Sadhukhan, D. (2021). ECC-CoAP: Elliptic curve cryptography based constraint application protocol for internet of things. Wireless Personal Communications, 116(3), 1867-1896. https://doi.org/10.1007/s11277-020-07763-w

National Institute of Standards and Technology. (2024a). Federal Information Processing Standard (FIPS) 203: Module-lattice-based key-encapsulation mechanism standard (ML-KEM). NIST. https://doi.org/10.6028/NIST.FIPS.203

National Institute of Standards and Technology. (2024b). Federal Information Processing Standard (FIPS) 204: Module-lattice-based digital signature algorithm (ML-DSA). NIST. https://doi.org/10.6028/NIST.FIPS.204

National Institute of Standards and Technology. (2024c). Federal Information Processing Standard (FIPS) 205: Stateless hash-based digital signature algorithm (SLH-DSA). NIST. https://doi.org/10.6028/NIST.FIPS.205

National Institute of Standards and Technology. (2024d). Cybersecurity framework (CSF) 2.0. NIST. https://doi.org/10.6028/NIST.CSWP.29

Payment Card Industry Security Standards Council. (2022). PCI DSS v4.0: Payment Card Industry Data Security Standard. PCI Security Standards Council. https://www.pcisecuritystandards.org/document_library/

Rafiq, F., Awan, M. J., Yasin, A., Nobanee, H., Zain, A. M., & Bahaj, S. A. (2022). Privacy prevention of big data applications: A systematic literature review. SAGE Open, 12(2), 1-18. https://doi.org/10.1177/21582440221096445

Rana, M., Mamun, Q., & Islam, R. (2022). Lightweight cryptography in IoT networks: A survey. Future Generation Computer Systems, 129, 77-89. https://doi.org/10.1016/j.future.2021.10.035

Rescorla, E. (2018). The Transport Layer Security (TLS) Protocol Version 1.3 (RFC 8446). Internet Engineering Task Force. https://doi.org/10.17487/RFC8446

Thabit, F., Can, O., Aljahdali, A. O., Al-Gaphari, G. H., & Alkhzaimi, H. A. (2023). Cryptography algorithms for enhancing IoT security. Internet of Things, 22, Article 100759. https://doi.org/10.1016/j.iot.2023.100759

Thales Group. (2023). 2023 Thales data threat report: Global edition. Thales. https://cpl.thalesgroup.com/data-threat-report

Ullah, S., Zheng, J., Din, N., Hussain, M. T., Ullah, F., & Yousaf, M. (2023). Elliptic curve cryptography: Applications, challenges, recent advances, and future trends: A comprehensive survey. Computer Science Review, 47, Article 100530. https://doi.org/10.1016/j.cosrev.2022.100530

Vanin, F. N. S., Policarpo, L. M., Righi, R. R., Heck, S. M., da Silva, V. F., Goldim, J., & da Costa, C. A. (2023). A blockchain-based end-to-end data protection model for personal health records sharing: A fully homomorphic encryption approach. Sensors, 23(1), 14. https://doi.org/10.3390/s23010014

Verizon. (2024). 2024 data breach investigations report. Verizon Enterprise. https://www.verizon.com/business/resources/reports/dbir/

Wibawa, F., Catak, F. O., Kuzlu, M., Sarp, S., & Cali, U. (2022). Homomorphic encryption and federated learning based privacy-preserving CNN training: COVID-19 detection use-case. In Proceedings of the 2022 European Interdisciplinary Cybersecurity Conference (EICC) (pp. 85-90). ACM. https://doi.org/10.1145/3528580.3532845

Zhang, H., Ji, Z., & Liu, Y. (2022). Privacy-preserving cloud computing using multi-key homomorphic encryption. Journal of Information Security and Applications, 65, Article 103098. https://doi.org/10.1016/j.jisa.2022.103098

Appendix A

Table A1

Comparison of Major Data Protection Regulations and Cryptographic Requirements

Regulation	In Force	Cryptographic Requirements	Non-Compliance Penalties	Enforcement Strength
GDPR (EU 2016/679)	2018	Art. 32: pseudonymisation and encryption of personal data as appropriate technical measures; Art. 25: encryption by design and default	Fines up to 4% of global annual turnover; Art. 83 enforcement; cumulative fines exceeded EUR 6.7 billion by 2025	Strong; DPA supervisory oversight
HIPAA Security Rule (USA)	1996 / Updated 2013	Encryption of ePHI in transit (required) and at rest (addressable); AES-256 recommended; TLS 1.2+ for transmission	Civil penalties USD 100 to 50,000 per violation; up to USD 1.9M/year per violation category	Strong for covered entities; HHS Office for Civil Rights enforcement
PCI DSS v4.0	2022 (fully effective 2025)	TLS 1.2+ mandatory for all cardholder data in transit; AES-256 for stored PANs; explicit cryptographic agility requirements	Fines USD 5,000 to 100,000/month; card brand penalties; potential loss of card acceptance	Strong; mandatory for all entities handling payment card data
CCPA / CPRA (USA)	2020 / 2023	Encryption encouraged as reasonable security; CPRA strengthens sensitive data provisions and audit requirements	Statutory damages USD 100 to 750/consumer/incident; up to USD 7,500 for intentional violations	Moderate; enforcement by CA AG and California Privacy Protection Agency
ISO/IEC 27001:2022	2022	Annex A Control 8.24 mandates use of cryptography policy; key management procedures required; algorithm selection criteria specified	Certification and contractual obligation; loss of certification for non-conformance	Voluntary but widely required in supply chains; over 70,000 certified organisations globally
NIST CSF 2.0 (USA)	2024	PR.DS-2: data-in-transit encryption; PR.DS-5: data-at-rest encryption; references NIST SP 800-57 key management guidance	Non-mandatory for private sector; mandatory for US federal agencies under FISMA	High for federal sector; influential voluntary standard for critical infrastructure

Note. PCI DSS v4.0 effective date for all new requirements is 31 March 2025. NIST CSF 2.0 was released in February 2024. Cumulative GDPR enforcement fines exceeded EUR 6.7 billion across over 2,600 enforcement actions as of late 2025 (EDPB, 2023). ISO/IEC 27001:2022 Annex A Control 8.24 specifically requires a documented cryptography policy and key management procedures. FISMA = Federal Information Security Modernization Act; DPA = Data Protection Authority; HHS = US Department of Health and Human Services.

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

Appendix B

Table B1

Comparison of AES, RSA, ECC, and NIST Post-Quantum Algorithms

Algorithm	Key Size (bits)	Security Level (bits)	Performance	Primary Use Case	Post-Quantum Resilience
AES-128	128	128 (classical); 64 (quantum)	Very High (HW acceleration)	Bulk data encryption, VPNs, storage	Partial (Grover halves key length)
AES-256	256	256 (classical); 128 (quantum)	High (slight overhead vs AES-128)	Government, financial, cloud encryption	Moderate (128-bit post-Grover security)
RSA-2048	2048	112	Moderate; slow for large data	Key exchange, digital signatures, TLS handshake	None; broken by Shor's algorithm
RSA-4096	4096	140	Low (computationally expensive)	High-assurance PKI, code signing	None; broken by Shor's algorithm
ECC P-256 (ECDSA/ECDH)	256	128	High; compact keys	TLS, IoT, mobile, blockchain auth	None; broken by Shor's algorithm
ML-KEM / CRYSTALS-Kyber (FIPS 203)	768 (Level 2)	128 (quantum-resistant)	High; competitive with RSA	Post-quantum key encapsulation mechanism	Designed for post-quantum resistance
ML-DSA / CRYSTALS-Dilithium (FIPS 204)	1312 (Level 2)	128 (quantum-resistant)	Moderate; larger signatures than ECC	Post-quantum digital signatures	Designed for post-quantum resistance
SLH-DSA / SPHINCS+ (FIPS 205)	32 (seed)	128 (Level 1)	Low (slow signing); hash-based	Post-quantum signature backup (no lattice)	Designed for post-quantum resistance

Note. Security levels expressed in bits of classical security. Post-quantum security accounts for Grover's algorithm against symmetric ciphers and Shor's algorithm against RSA/ECC. ML-KEM = Module-Lattice Key-Encapsulation Mechanism (FIPS 203); ML-DSA = Module-Lattice Digital Signature Algorithm (FIPS 204); SLH-DSA = Stateless Hash-Based Digital Signature Algorithm (FIPS 205). All three standards were finalised by NIST in August 2024. Sources: NIST (2024a, 2024b, 2024c); Alagic et al. (2022); Barker (2020).

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491

Appendix C

Table C1

Cryptographic Strength-Vulnerability (CSV) Framework: Eight-Dimension Assessment

Dimension	Cryptographic Strength	Implementation Vulnerability
Confidentiality	AES-256-GCM provides 256-bit classical security and 128-bit post-quantum security (Grover); IND-CCA2 secure under standard assumptions	IV/nonce reuse in GCM nullifies confidentiality; weak key derivation; storing keys in application memory; hardcoded keys in source code
Data Integrity	AEAD modes (GCM, CCM, ChaCha20-Poly1305) prevent undetected tampering; HMAC-SHA256 provides strong MAC under all classical attacks	Misuse of unauthenticated encryption modes (e.g., raw AES-ECB/CBC); length-extension attacks on MD5/SHA-1 in legacy HMAC implementations
Authentication	PKI/X.509 certificates; mutual TLS (mTLS); Ed25519 / ML-DSA digital signatures; FIDO2/WebAuthn for user authentication	Certificate mis-issuance; weak CA practices; accepting expired or self-signed certs; MITM via missing hostname verification
Key Management	FIPS 140-3 validated HSMs; cloud KMS with CMEK; Shamir secret sharing for key escrow; automated rotation via CryptoAgility APIs	Hardcoded keys; insecure PBKDF2/bcrypt iteration counts; missing key rotation; key material in log files or environment variables
Protocol Security	TLS 1.3 eliminates all non-AEAD cipher suites; mandatory ECDHE ensures forward secrecy; explicit version; no renegotiation downgrade	Legacy TLS 1.0/1.1 still present in embedded systems; POODLE/BEAST exploitable on downgrade; weak cipher suite negotiation in TLS 1.2
Side-Channel Resistance	Constant-time AES using AES-NI hardware; Montgomery blinding for RSA/ECC; data-independent timing in Curve25519	Power analysis attacks (DPA) on non-hardened smart cards; cache-timing attacks (Flush+Reload) on shared cloud VMs; Spectre/Meltdown variants
Post-Quantum Transition	NIST FIPS 203/204/205 standardise ML-KEM, ML-DSA, SLH-DSA; hybrid schemes provide dual-algorithm security during transition	Harvest-now-decrypt-later attacks on current RSA/ECC traffic; slow migration of embedded systems; cryptographic agility gaps in legacy software
Regulatory Compliance	GDPR Art. 32 safe harbour for encrypted breaches; PCI DSS v4.0 mandates TLS 1.2+; HIPAA addressable standard for ePHI encryption	Compliance-driven minimum encryption not matched to threat level; audit failures to detect key management deficiencies; checkbox compliance mentality

Note. AEAD = Authenticated Encryption with Associated Data; GCM = Galois/Counter Mode; PBKDF2 = Password-Based Key Derivation Function 2; mTLS = Mutual TLS; FIPS = Federal Information Processing Standard; DPA = Differential Power Analysis; ML-KEM = Module-Lattice Key Encapsulation Mechanism. Post-quantum threat timeline references NSA CNSA 2.0 target dates and NIST PQC guidance (Alagic et al., 2022; NIST, 2024a).

Volume 2, Issue 1, 2026
https://doi.org/10.5281/zenodo.18904491