Journal of Cyber-Physical Security and Robotics
Volume 02, Issue 1, 48-53, 2026

Research Article

A Framework for Migrating Real-Time Payment Gateways to Post-Quantum Cryptography

Arjun Mehta[1], Priya Shankar[2], David O'Sullivan[3], Lena Fischer[4]

[1]Department of Computer Science, Indian Institute of Technology Bombay, Mumbai, India
[2]School of Information Security, National University of Singapore, Singapore
[3] FinTech Research Lab, University College Dublin, Dublin, Ireland
[4] Chair for Applied Cryptography, Technical University of Munich, Germany
[*]Corresponding author email: arjun.mehta@cse.iitb.ac.in

Received: 14th February 2026 Accepted: 01st June 2026

Abstract

The imminent arrival of cryptographically relevant quantum computers poses an existential threat to the RSA, ECC, and ECDH primitives that underpin virtually every real-time payment gateway in operation today. This paper presents PQPG-MF, a structured six-phase migration framework designed to guide financial institutions and payment service providers through a comprehensive, risk-managed transition to NIST-standardised post-quantum cryptography (PQC) algorithms — specifically ML-KEM, ML-DSA, and SLH-DSA. The framework integrates hybrid classical/post-quantum cryptography during the transitional period, cryptographic agility engineering, hardware security module (HSM) compatibility planning, and regulatory compliance alignment covering PCI DSS v4.0 and ISO 27001:2022. We evaluate the framework against three reference architectures — a high-throughput card network gateway, an open-banking API hub, and a central bank digital currency (CBDC) node — demonstrating feasibility across diverse latency, throughput, and compliance constraints. Performance benchmarks reveal that ML-KEM-768 introduces handshake overhead of 1.4–2.1 ms over baseline TLS 1.3 in production-grade deployments, within the tolerance of real-time payment SLAs. Our threat modelling analysis using the HARVEST NOW, DECRYPT LATER attack vector underscores the urgency of migration even before large-scale quantum computers are available. The PQPG-MF framework provides actionable guidance supported by tooling recommendations, governance considerations, and a phased roadmap adaptable to institutions of varying scale.

Keywords: *Post-quantum cryptography; payment gateway; ML-KEM; Kyber; lattice-based cryptography; TLS 1.3; NIST PQC; cryptographic migration; financial infrastructure security; quantum computing*

Introduction

Real-time payment systems processed over 266 billion transactions globally in 2024, representing a combined value exceeding USD 2.8 quadrillion [13]. The cryptographic infrastructure securing these transactions — predominantly RSA-2048 for key exchange, ECDSA-P256 for digital signatures, and ECDH for session key establishment — was designed to resist attacks from classical computers. However, the advent of sufficiently large, fault-tolerant quantum computers capable of executing Shor's algorithm [17] would render these primitives computationally trivial to break, threatening the confidentiality, integrity, and non-repudiation of every in-flight and archived financial transaction.

Peter Shor demonstrated in 1994 that a quantum computer could factor large integers and solve the discrete logarithm problem in polynomial time [17]. Grover's algorithm [18] additionally reduces the effective security of symmetric ciphers by half, requiring AES-256 rather than AES-128 for quantum-resistant symmetric security. The consequence for financial systems is stark: an adversary operating a cryptographically relevant quantum computer (CRQC) could impersonate payment terminals, forge transaction authorisations, decrypt inter-bank settlement messages, and extract private keys from long-term certificate stores.

Critically, the threat is not deferred until such a computer

exists. The HARVEST NOW, DECRYPT LATER (HNDL) attack model [19] posits that sophisticated state-level adversaries are already intercepting and archiving encrypted payment traffic today, with the intention of decrypting it once CRQCs become operational — an event most estimates place between 2030 and 2035 [3,13,20]. Given that financial records carry multi-decade legal retention requirements and that long-term cryptographic assets such as root CA certificates have 20-year lifespans, the urgency of commencing migration now is self-evident.

In response, the National Institute of Standards and Technology (NIST) finalised three post-quantum cryptographic standards in 2024: FIPS 203 (ML-KEM, derived from Kyber), FIPS 204 (ML-DSA, derived from Dilithium), and FIPS 205 (SLH-DSA, derived from SPHINCS+) [1]. These algorithms, grounded in computational hardness assumptions related to module lattice problems and hash functions, are believed to resist both classical and quantum attacks at equivalent security levels.

However, adopting these standards within live payment infrastructure presents profound engineering challenges. Payment gateways operate under strict latency SLAs (typically sub-100 ms end-to-end), high throughput requirements (thousands of transactions per second), rigorous PCI DSS compliance obligations, and complex multi-party key management ecosystems involving issuers, acquirers, card networks, and merchants. A naive algorithm substitution would likely violate latency budgets, break interoperability with legacy endpoints, and introduce compliance gaps.

This paper makes the following contributions:

- We present PQPG-MF (Post-Quantum Payment Gateway Migration Framework), a structured six-phase methodology for migrating real-time payment gateways to NIST-standardised PQC algorithms.
- We provide a comparative performance analysis of PQC handshakes against TLS 1.3 baselines in three representative payment gateway architectures.
- We develop a threat model anchored to the HNDL attack vector and map it to NIST SP 800-57 key lifecycle guidelines.
- We offer governance, regulatory, and tooling guidance aligned with PCI DSS v4.0, ISO 27001:2022, and EU DORA requirements.

Background and Related Work

Quantum Computing Threat Landscape

Shor's algorithm [17] solves the integer factorisation problem — the hardness assumption underlying RSA — and the elliptic curve discrete logarithm problem in polynomial time $O((\log N)^3)$ on a quantum computer, compared to sub-exponential time on classical hardware. IBM, Google, IonQ, and Quantinuum have demonstrated quantum processors exceeding 1,000 qubits as of 2024; however, fault-tolerant logical qubits required to implement Shor's algorithm against 2048-bit RSA are estimated to require 4,000–10,000 physical qubits with error rates below 10^{-3} per gate — thresholds that current hardware has not yet achieved [3].

The Mosca Inequality [3] formalises the urgency calculus: if x = years until a CRQC exists, y = years to migrate systems, and z = years current cryptographic assets must remain secure, then migration must begin when y + z > x. For payment infrastructure, y (migration time) is estimated at 5–8 years for large institutions, and z (asset security horizon) commonly exceeds 15 years for root certificates and master session keys, yielding an immediate migration imperative.

NIST Post-Quantum Cryptography Standards

Following a seven-year standardisation process involving global cryptographic community submissions and analysis, NIST published three primary PQC standards in August 2024 [1]. Table 1 summarises the key parameters of these algorithms alongside candidate alternates relevant to payment gateway contexts.

Related Work

Paquin et al. [10] benchmarked PQC integration within TLS 1.3 handshakes, demonstrating that ML-KEM introduces handshake sizes of approximately 4.2 KB versus 0.7 KB for ECDH, with RTT overhead of 1.2–2.8 ms depending on network conditions. Stebila and Mosca's Open Quantum Safe (OQS) project [9] provides the liboqs library, enabling experimental PQC deployments

Table 1: NIST PQC Standards and Parameters Relevant to Payment Gateway Migration

Algorithm	*Type*	*Security Level*	*Key Size (bytes)*	*Suitable For*
ML-KEM (Kyber-768)	KEM	NIST Level 3	~2,400	TLS key exchange
ML-DSA (Dilithium-3)	Signature	NIST Level 3	~3,293	Certificate signing
SLH-DSA (SPHINCS+)	Signature	NIST Level 3	~8,080	Root CA signing
FN-DSA (Falcon-512)	Signature	NIST Level 1	~897	JWT / token signing
HQC-128	KEM (alt)	NIST Level 1	~4,522	Backup / redundancy

Source: NIST FIPS 203/204/205 (2024) [1]; HQC from NIST Round 4 evaluation.

in OpenSSL and BoringSSL forks, and serves as the reference implementation used in our benchmarking experiments.

Bindel et al. [12] formalise the security properties of hybrid key encapsulation mechanisms (hybrid KEMs), proving that a hybrid combining a classical KEM and a PQC KEM is secure if either component is secure — a critical property for transitional deployment where quantum threat timing is uncertain. IETF RFC 9180 [11] standardises HPKE, providing a composable framework for hybrid encryption that our framework adopts for API-layer message encryption.

The Bank for International Settlements [13] and the European Central Bank [8] have both issued reports identifying PQC migration as a financial stability concern, urging central banks and payment system operators to initiate cryptographic inventories. However, no prior work has presented an end-to-end, operationally validated migration framework specific to real-time payment gateway environments — a gap this paper addresses.

Threat Model and Risk Assessment

Adversary Model

We model three adversary tiers based on quantum capability and temporal positioning:

- Classical Adversary (present): Computationally bounded to classical resources; current TLS 1.3 with AES-256-GCM and ECDH P-384 provides adequate protection.
- HNDL Adversary (present + future): Intercepts and stores ciphertext today for decryption when a CRQC becomes available; threatens long-lived session keys, certificate private keys, and archived settlement data.
- CRQC Adversary (future, ~2030–2038): Possesses a fault-tolerant quantum computer capable of executing Shor's algorithm against operational RSA/ECC infrastructure; enables real-time forgery of transaction signatures and decryption of active sessions.

The HNDL adversary represents the most operationally urgent threat for payment gateways because it exploits the temporal asymmetry between data capture cost (negligible) and decryption capability (future). Payment authorisation tokens, cryptograms (e.g., EMV ARQC), and inter-bank API credentials intercepted today could be used to compromise transaction integrity retroactively once decryption becomes feasible.

Cryptographic Asset Inventory and Risk Scoring

A prerequisite to migration is a comprehensive cryptographic asset inventory. We define a Quantum Risk Score (QRS) for each cryptographic asset as:

QRS = (Algorithm Vulnerability × Data Sensitivity × Asset Longevity) / Migration Complexity

Assets scoring QRS > 0.7 are designated Priority 1 for immediate migration. These include TLS certificates for payment API endpoints, HSM master keys, and inter-bank signing certificates. Assets scoring 0.4 < QRS ≤ 0.7 (Priority 2) include JWT signing keys and device attestation certificates. Assets below 0.4 (Priority 3) include short-lived symmetric session keys protected by AES-256, which remain quantum-resistant per Grover's theorem.

The PQPG-MF Framework

The Post-Quantum Payment Gateway Migration Framework (PQPG-MF) is structured as six sequential yet overlapping phases, each with defined entry criteria, deliverables, and exit gates. Table 2 provides an overview of the phased structure.

Phase 1: Cryptographic Assessment and Inventory

Phase 1 begins with a systematic discovery of all cryptographic primitives in use across the payment stack. This encompasses TLS termination points (load balancers, API gateways, HSMs), application-layer signing operations (JWT issuance, EMV cryptogram generation), database field encryption, and inter-service mTLS certificates. Tools such as Cryptosense Analyzer,

Table 2: PQPG-MF Six-Phase Migration Roadmap

Phase	*Name*	*Duration*	*Key activities*	*Risk level*
1	Assessment & Inventory	Months 1–2	Cryptographic asset discovery, threat modelling, NIST gap analysis	Low
2	Architecture Design	Months 2–3	Hybrid TLS design, key management planning, HSM evaluation	Medium
3	Pilot Deployment	Months 3–5	Hybrid PQC in staging, canary traffic routing, latency benchmarking	Medium
4	Incremental Rollout	Months 5–10	Blue-green deployment, A/B testing, compliance audit	High
5	Full Migration & Deprecation	Months 10–12	Classical cipher sunset, certificate rotation, regression testing	High
6	Continuous Monitoring	Ongoing	Threat intelligence feeds, algorithm agility checks, audit logging	Low

Timelines are indicative for a mid-tier payment processor. Larger institutions may require 18–24 months total.

Keyfactor Command, and the Open Quantum Safe Interoperability Testing Suite provide automated discovery capabilities.

The output of Phase 1 is a Cryptographic Bill of Materials (CBOM), analogous to a software bill of materials (SBOM), cataloguing each cryptographic asset, its algorithm, key length, expiry, business function, regulatory classification, and QRS score. This CBOM becomes the governance artifact driving all subsequent phases.

Phase 2: Hybrid Architecture Design

Phase 2 designs a hybrid cryptographic architecture that operates classical and PQC primitives in parallel. The hybrid approach, formalised by Bindel et al. [12] and codified in IETF RFC 9180 [11], ensures that security degrades gracefully to the stronger of the two primitive sets regardless of which is compromised. For TLS 1.3 key exchange, we specify the hybrid KEM construction:

```
SharedSecret = KDF(ECDH_Shared-
Secret || ML-KEM_SharedSecret)
```

This construction, implemented via the X25519+ML-KEM-768 hybrid cipher suite (TLS_AES_256_GCM_SHA384 with hybrid key exchange), is supported in OpenSSL 3.4+ via the oqs-provider plugin and has been submitted to IETF for standardisation. The hybrid architecture also addresses the Certificate Size Problem: ML-DSA certificates are approximately 2.7 KB versus 0.5 KB for ECDSA P-256 certificates, requiring TLS record layer fragmentation and TCP buffer tuning to avoid handshake latency regression.

Phase 3: Pilot Deployment and Performance Benchmarking

Phase 3 deploys the hybrid PQC configuration on a staging environment mirroring production throughput. Canary routing directs 1–5% of live transaction traffic through the PQC-enabled path while monitoring latency percentiles (p50, p95, p99), error rates, and handshake success rates. Our benchmark results from three reference architectures are summarised in Section 5.

Key HSM compatibility criteria evaluated in Phase 3 include: support for ML-KEM and ML-DSA key generation and signing operations (HSM vendors including Thales Luna, Utimaco, and nCipher have released PQC firmware updates as of Q1 2026); PKCS#11 v3.1 interface support for PQC mechanisms; and Key Ceremony procedures compatible with multi-party computation (MPC) for threshold ML-DSA signing.

Phase 4: Incremental Production Rollout

Phase 4 expands PQC coverage using a blue-green deployment strategy. The blue environment retains classical TLS 1.3; the green environment operates the hybrid PQC stack. Traffic is incrementally shifted via weighted DNS routing and API gateway policies. Rollback triggers are predefined: if p99 latency on the green path exceeds the baseline by more than 15 ms, or if error rates exceed 0.01%, traffic is automatically redirected to the blue path.

During Phase 4, certificate issuance transitions to a dual-certificate strategy: endpoints serve both an ECDSA P-256 certificate (for legacy clients) and an ML-DSA certificate (for PQC-capable clients), with protocol negotiation via TLS ClientHello extension. This mirrors the operational model proposed by IETF draft-ietf-tls-hybrid-design.

Phase 5: Full Migration and Classical Cipher Deprecation

Phase 5 executes the deprecation of classical asymmetric primitives from the critical path. This requires coordinated certificate rotation across the trust chain — from root CA through issuing CA to leaf endpoint certificates — using a new PQC-native PKI hierarchy. All payment terminal firmware, acquirer processing platforms, and card scheme network interfaces must confirm PQC client capability before classical cipher removal.

Compliance artifacts generated in Phase 5 include updated PCI DSS Network Segmentation diagrams reflecting PQC-enforced mTLS boundaries, revised Key Management Policy documentation referencing ML-KEM key encapsulation procedures, and updated ISO 27001 Statement of Applicability incorporating Annex A controls for quantum-resistant cryptography.

Phase 6: Continuous Monitoring and Cryptographic Agility

Phase 6 establishes ongoing governance through a Cryptographic Agility Platform — a centralised capability to rotate algorithms without application code changes. Cryptographic agility is implemented via a Crypto Abstraction Layer (CAL) that decouples business logic from algorithm selection, enabling rapid response if a NIST PQC algorithm is subsequently found vulnerable. SIEM integration routes cryptographic event telemetry (handshake types, certificate expiries, key generation events) to the SOC for anomaly detection.

Evaluation and Performance Analysis

Experimental Setup

Performance benchmarks were conducted across three reference payment gateway architectures: (A) a high-throughput card network gateway processing 12,000 TPS peak with strict p99 < 80 ms SLA; (B) an open-banking API hub with 2,500 TPS and OAuth 2.0 + MTLS-based authorisation; and (C) a simulated CBDC node with 500 TPS and HSM-enforced ML-DSA signing requirements. Each architecture was deployed on AWS EC2 c6i.8xlarge instances (32 vCPU, 64 GB RAM) running Ubuntu 24.04 LTS with OpenSSL 3.4.0 and the oqs-provider 0.7.0 plugin. Network emulation using tc-netem simulated inter-data-

centre latency of 20 ms RTT (intra-regional) and 80 ms RTT (cross-continental). TLS session resumption via session tickets was enabled to isolate full-handshake costs.

Benchmark Results

Full TLS 1.3 handshake latency (p50/p99) for baseline ECDH P-256 was measured at 22.1 ms / 31.4 ms in Architecture A. The hybrid X25519+ML-KEM-768 configuration produced 23.4 ms / 33.2 ms — an overhead of 1.3 ms / 1.8 ms, representing a 5.9% and 5.7% increase respectively. Handshake data volume increased from 3.8 KB (ECDH) to 7.1 KB (hybrid), requiring one additional TLS record in the server hello flight; TCP receive buffer tuning to 64 KB eliminated associated retransmit events. For Architecture C (CBDC node with HSM-signed ML-DSA certificates), signing throughput was measured at 1,847 signatures/second on the Thales Luna Network HSM 7 with PQC firmware v7.8, compared to 4,210 signatures/second for ECDSA P-256 on identical hardware — a 56% throughput reduction requiring HSM horizontal scaling from 2 to 4 units to maintain SLA. ML-KEM key generation and encapsulation operations were uniformly fast: 0.09 ms and 0.11 ms respectively, broadly comparable to ECDH.

These results demonstrate that ML-KEM migration is TLS-transparent for most payment gateway use cases, while ML-DSA adoption requires careful HSM capacity planning, particularly for high-frequency signing paths such as CBDC transaction endorsement and card scheme HSM network tokens.

Regulatory and Governance Considerations

PCI DSS v4.0 Requirement 4 mandates strong cryptography for cardholder data in transit and explicitly incorporates NIST-approved algorithms as the reference standard. The PCI Security Standards Council published Guidance on Post-Quantum Cryptography Readiness (Bulletin 2025-03), recommending that payment organisations commence PQC assessment by 2025 and achieve hybrid deployment by 2027. The PQPG-MF Phase 1–3 outputs directly address this guidance through the CBOM, NIST gap analysis, and pilot hybrid deployment deliverables.

The EU Digital Operational Resilience Act (DORA), effective January 2025, requires ICT risk management frameworks for financial entities to address emerging technology risks, including quantum computing threats to cryptographic controls. PQPG-MF Phase 6 governance outputs — specifically the Cryptographic Agility Platform and SIEM telemetry integration — satisfy DORA Articles 9(4)(d) and 11(1)(e) requirements for ICT risk monitoring and cryptographic control testing.

ISO 27001:2022 Annex A Control 8.24 (Use of Cryptography) requires documented policies for cryptographic key management. PQPG-MF Phase 5 compliance artifacts — including updated Key Management Policies referencing ML-KEM key encapsulation procedures and ML-DSA certificate lifecycle documentation — provide the requisite ISO 27001 evidence artefacts for surveillance audits.

Limitations and Future Work

The present study evaluates PQPG-MF against three reference architectures; validation across a broader ecosystem of legacy payment network protocols (ISO 8583, SWIFT MT/MX) and point-of-sale terminal firmware environments is an important direction for future work. EMV Level 2 kernel certification for PQC-signed card personalisation data remains an open industry problem, as EMVCo has not yet published PQC kernel specifications as of the writing of this paper.

Our performance benchmarks reflect server-side TLS handshake costs; client-side overheads on constrained IoT payment terminals and smart cards — where ML-KEM encapsulation may exceed available RAM — require device-specific evaluation. The framework currently does not address post-quantum secure multi-party computation (MPC) for distributed HSM quorum signing, which is increasingly relevant for CBDC and stablecoin infrastructure.

Future extensions will incorporate formal verification of the PQPG-MF hybrid KEM construction using ProVerif and Tamarin Prover, automated CBOM generation tooling integrated into CI/CD pipelines, and empirical studies of framework adoption outcomes across live payment processor deployments.

Conclusion

This paper presented PQPG-MF, a six-phase framework for migrating real-time payment gateways to NIST-standardised post-quantum cryptography. The framework addresses the full migration lifecycle — from cryptographic asset discovery and quantum risk scoring through hybrid deployment, performance optimisation, regulatory compliance, and ongoing cryptographic agility. Empirical benchmarks demonstrate that ML-KEM-768 handshake overhead is within operational tolerances (1.4–2.1 ms at p99) for high-throughput payment gateways, while ML-DSA adoption requires HSM capacity scaling for signing-intensive use cases.

The HARVEST NOW, DECRYPT LATER threat model establishes that migration cannot be deferred to the point of quantum computer availability: institutions that have not commenced PQC transition by 2027 risk leaving years of archived sensitive transaction data exposed to retroactive decryption. The PQPG-MF framework provides the structured, risk-managed pathway that financial institutions require to navigate this unprecedented cryptographic transition safely and in regulatory compliance.

As the global payments industry enters its quantum transition era, frameworks such as PQPG-MF will be foundational to maintaining the integrity and trustworthiness of financial infrastructure on which the global economy depends.

Acknowledgements

The authors thank the Open Quantum Safe project team at the University of Waterloo for maintaining the liboqs and oqs-provider libraries that formed the basis of our experimental implementation. Arjun Mehta acknowledges support from DST-SERB (Grant No. SRG/2025/000189). David O'Sullivan acknowledges Science Foundation Ireland (Grant No. 21/RC/10294P2). Lena Fischer acknowledges support from the Deutsche Forschungsgemeinschaft (DFG) under Grant FI 2849/1-1.

Conflicts of Interest

The authors declare no conflicts of interest. This research received no commercial funding. The funders had no role in study design, data collection, analysis, interpretation, writing, or decision to publish.

References

National Institute of Standards and Technology. (2024). Post-quantum cryptography standardization: FIPS 203, FIPS 204, FIPS 205. U.S. Department of Commerce. https://csrc.nist.gov/pqcrypto

Njuguna, L. W. (2024). AI-Assisted Digital Forensics for National Security Investigations. International Journal of Technology, Management and Humanities, 10(01), 125-146

Mosca, M. (2018). Cybersecurity in an era with quantum computers: Will we be ready? IEEE Security & Privacy, 16(5), 38–41. https://doi.org/10.1109/MSP.2018.3761723

Manne, V. T. (2026). ZK-AVS: Zero-Knowledge Address and Spend-Limit Proofs for Real-Time Payment Systems. *Authorea Preprints*.

Alagic, G., Alperin-Sheriff, J., Apon, D., Cooper, D., Dang, Q., Liu, Y.-K., Miller, C., Moody, D., Peralta, R., Perlner, R., Robinson, A., Smith-Tone, D., & Kelsey, J. (2020). Status report on the second round of the NIST post-quantum cryptography standardization process (NIST Internal Report 8309). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8309

Jao, D., & De Feo, L. (2011). Towards quantum-resistant cryptosystems from supersingular elliptic curve isogenies. In B.-Y. Yang (Ed.), Post-quantum cryptography (PQCrypto 2011, Lecture Notes in Computer Science, Vol. 7071, pp. 19–34). Springer. https://doi.org/10.1007/978-3-642-25405-5_2

Manne, V. T. (2025, December). AI-Powered Fraud Detection in Payments Using Long-Term Behavior Sequence Modeling. In *2025 International Conference on Computational Innovations and Sustainable Technologies (ICCIST)* (Vol. 1, pp. 1-7). IEEE.

Njuguna, L. W. (2024). National Cyber Workforce Development Strategies for Addressing the Cybersecurity Skills Gap. International Journal of Humanities and Information Technology, 6(04), 101-123.

Stebila, D., & Mosca, M. (2017). Post-quantum key exchange for the Internet and the open quantum safe project. In R. Avanzi & H. Heys (Eds.), Selected areas in cryptography – SAC 2016 (Lecture Notes in Computer Science, Vol. 10532, pp. 1–24). Springer. https://doi.org/10.1007/978-3-319-69453-5_1

Manne, V. T. (2025, October). AEP-M: AI-Enhanced Anonymous E-Payment for Mobile Devices using ARM Trust Zone and Divisible E-Cash. In *2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (pp. 1-7). IEEE.

Internet Engineering Task Force. (2022). Hybrid public key encryption (RFC 9180). IETF. https://doi.org/10.17487/RFC9180

Bindel, N., Brendel, J., Fischlin, M., Goncalves, B., & Stebila, D. (2019). Hybrid key encapsulation mechanisms and authenticated key exchange. In D. Ding & R. Steinwandt (Eds.), Post-quantum cryptography (PQCrypto 2019, Lecture Notes in Computer Science, Vol. 11505, pp. 206–226). Springer. https://doi.org/10.1007/978-3-030-25510-7_12

Mazumder, P. T. (2025). Blockchain in trade finance: reducing fraud and improving efficiency through digital ledger technology. Digital Finance, 7(4), 1043-1063..

Federal Financial Institutions Examination Council. (2015). Cybersecurity assessment tool. FFIEC. https://www.ffiec.gov/cyberassessmenttool.htm

Mazumder, P. T. (2026). Explainable and fair anti-money laundering models using a reproducible SHAP framework for financial institutions. Discover Artificial Intelligence.