Volume-06|Issue-06|June|Year-2026 ISSN: 3049-2343

International Journal of Academic and Industrial Research Innovations(IJAIRI)

Research Book Title :Quantum Cryptography, Quantum Communications and Nano-Enabled Cybersecurity: Global Frameworks for DefenceTech, FinTech and SpaceTech

[1]Murali Krishna Pasupuleti

[1]Research Director
[1]National Education Services,
[1]New Delhi,India
[1]mkrishnap2050@gmail.com

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Abstract:
This study develops a scope of analytical framework for integrating quantum cryptography, quantum communications, post-quantum cryptography and nano-enabled hardware security into global cybersecurity architectures for DefenceTech, FinTech and SpaceTech. The research problem is framed by the convergence of three pressures: the long-lived confidentiality exposure created by harvest-now-decrypt-later attacks, the rapid standardization of post-quantum algorithms, and the need for hardware-rooted trust in physically exposed devices, satellites, edge nodes and payment infrastructures. The paper synthesizes quantum key distribution, quantum-network standardization, crypto-agile migration, physical unclonable functions and sectoral governance into a single evaluation model. It uses a public-source calibrated realistic dataset of 18 high-value scenarios across defence, finance and space systems. The dataset is not represented as confidential operational telemetry; rather, it is explicitly constructed from publicly available threat, standards and engineering indicators to support transparent modelling.

The methodology combines literature review, structured scenario analysis, weighted risk scoring, residual-risk modelling, expected annual loss estimation and feasibility-sensitive control selection. Mathematical equations are used to express QKD channel attenuation, secret-key-rate intuition, cryptographic migration risk, expected loss and multi-criteria optimization. Results indicate that hybrid PQC adoption produces the broadest near-term risk reduction, QKD offers the strongest value where long-lived secrets and controlled optical paths exist, and nano-enabled roots of trust are especially relevant to contested devices and supply chains. The study proposes a staged global framework in which crypto-agility, hybrid PQC, QKD network governance and nano-PUF attestation are treated as complementary layers rather than competing security paradigms. The conclusion identifies future work in real operational benchmarking, satellite-QKD testbeds, standards-aligned implementation assurance and machine-verifiable security reasoning.

Keywords: Quantum cryptography; quantum key distribution; post-quantum cryptography; quantum communications; nano-enabled cybersecurity; physical unclonable functions; DefenceTech; FinTech; SpaceTech; crypto-agility; QKD networks; ML-KEM; ML-DSA; hardware root of trust; cyber resilience

Copyright:

© 2026 by Murali Krishna Pasupuleti.

Table of Contents

Abstract

1. Introduction
    1.1 Problem identification, topicality and research rationale
    1.2 Sectoral relevance for DefenceTech, FinTech and SpaceTech
    1.3 Technical expertise, tools, instruments and analytical models
    1.4 Evaluation feasibility and original contribution
2. Theory and Literature Review Framework
    2.1 Quantum cryptography and quantum key distribution foundations
    2.2 Quantum communications networks and global standardization
    2.3 Post-quantum cryptography, hybrid migration and crypto-agility
    2.4 Nano-enabled cybersecurity and physical roots of trust
    2.5 Literature review assurance and machine-verifiable reasoning framework
3. Methods: Realistic Data Collection and Mathematical Modelling
    3.1 Research design and explicitly labelled realistic data collection
    3.2 Variables, constraints and scenario sampling logic
    3.3 Mathematical model and equations supporting output relationships
    3.4 Implementation workflow, tools and validation procedure
    3.5 Alternative approaches and justification of the selected solution concept
4. Results: Tables, Figures and Interpretation
    4.1 Scenario dataset and baseline quantum-cyber risk profile
    4.2 Quantum cryptography, QKD and hybrid-PQC intervention effects
    4.3 Sectoral evaluation for DefenceTech, FinTech and SpaceTech
    4.4 Nano-enabled hardware roots of trust and device-level assurance
    4.5 Feasibility, sensitivity and governance readiness
5. Discussion, Conclusion and Outlook
    5.1 Discussion of findings and alternative interpretations
    5.2 Global framework for DefenceTech, FinTech and SpaceTech
    5.3 Limitations, validation status and research integrity
    5.4 Conclusion and outlook

References

eSign
Signed By: KOTA SRINIVAS PASUPULETI
Reason: NES |IJAIRI | Publication|
Location: Delhi, India
Date: June 2026

1. Introduction

1.1 Problem identification, topicality and research rationale

The core problem addressed by this study is the widening mismatch between the lifespan of sensitive digital assets and the cryptographic assumptions used to protect them. Defence mission records, financial identity repositories and satellite telemetry archives often retain strategic value for decades, while many installed cryptographic systems still rely on public-key mechanisms whose security could be invalidated by sufficiently capable quantum computers. This creates an intertemporal security problem: adversaries may capture encrypted traffic now and defer decryption until quantum resources or cryptanalytic breakthroughs become available. The vulnerability is therefore not restricted to a future date; it already affects every data flow whose confidentiality horizon exceeds the credible migration period for quantum-safe controls (Shor, 1994; NIST, 2024a).

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

The research treats quantum cryptography and quantum communications as part of a broader cyber-resilience transformation rather than as isolated scientific achievements. Quantum key distribution can detect eavesdropping at the key-exchange layer, post-quantum cryptography can protect software-defined public channels, and nano-enabled physical unclonable functions can bind trust to device-specific entropy. These layers address different attack surfaces and operational constraints. A defensible framework must therefore consider not only mathematical security, but also route topology, latency, certification, supply-chain exposure, standards maturity, and institutional readiness (ETSI, 2025; ITU-T, 2020; NATO, 2024).

The topic is highly topical because public authorities and standards bodies have moved from exploratory debate to deployment guidance. NIST finalized the first three federal post-quantum cryptography standards in 2024; European programmes are constructing quantum communication infrastructure across terrestrial and satellite segments; and defence alliances are treating quantum technologies as both opportunities and threats. At the same time, cyber incidents remain a primary institutional risk, with recent global reports identifying cyber disruption, ransomware, data breach exposure and AI-enabled attack automation as major strategic concerns (NIST, 2024a; European Commission, 2025a; IBM, 2025; Allianz, 2026).

1.2 Sectoral relevance for DefenceTech, FinTech and SpaceTech

DefenceTech requires quantum-safe security because command networks, sensor fusion platforms, unmanned systems, weapon-system maintenance channels and diplomatic communications combine high confidentiality, long asset life and adversarial sophistication. Unlike commercial systems that can sometimes be replaced at short cycles, defence platforms may remain in service for decades and operate across contested electromagnetic, terrestrial and space-linked environments. Quantum communications become relevant where critical links can be engineered with trusted nodes, optical paths or satellite relays, while nano-enabled device authentication helps protect field-deployed equipment against substitution, cloning and tampering.

FinTech is exposed through a different but equally consequential pathway. Interbank messaging, digital identity, custody services, trading infrastructure and compliance evidence depend on authenticity, non-repudiation and low-latency assurance. Quantum-safe migration in this sector must reconcile three tensions: high transaction volume, regulatory auditability and the need to avoid disruption in interconnected financial networks. Post-quantum signatures and key encapsulation can be introduced through hybrid protocols, but QKD is more selective because financial networks often prioritize routing flexibility and low latency over fixed optical trust channels. Hardware security remains important in payment terminals, signing modules and mobile identity devices (NIST, 2024b; NIST, 2024c).

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright © 2026
Location: Delhi, India
Date: June 2026

SpaceTech presents a hybrid of defence and commercial risk. Satellites, ground stations, inter-satellite links, mission-planning software, timing services and Earth-observation pipelines depend on secure command authority and data integrity. Space assets are difficult to patch, often operate with tight power and bandwidth budgets, and may rely on ground infrastructure that is exposed to conventional cyberattack. Satellite QKD and quantum communication experiments demonstrate the technical promise of long-distance quantum links, yet operational security also requires classical authentication, resilient key management, crypto-agile software chains and device-level attestation across ground, link and orbital segments (Liao et al., 2017; Yin et al., 2017; ESA, 2025a).

1.3 Technical expertise, tools, instruments and analytical models

The technical scope of this study draws on quantum information science, cryptographic engineering, network security, hardware assurance and risk modelling.

Quantum cryptography is interpreted through the principles of quantum measurement, no-cloning, entanglement and photon-channel loss. Post-quantum cryptography is interpreted through algorithmic hardness assumptions such as module-learning-with-errors and hash-based signatures. Nano-enabled cybersecurity is interpreted through physical entropy, nanoscale manufacturing variability, optical scattering, quantum dots, memristive behaviour and other device-specific features that can support unclonable identities. The contribution lies in integrating these domains into a decision framework for sector-specific implementation rather than discussing them as separate literatures.

The main instruments used in the study are a structured literature review, a scenario dataset, a weighted risk model, a residual-control model and graphical interpretation. The modelling process uses variables that security leaders can inspect: exposure, cryptographic debt, criticality, confidentiality lifetime, asset lifetime, post-quantum readiness, QKD feasibility and nano-PUF feasibility. These variables are not treated as perfect measurements; they are pragmatic indicators suitable for strategic comparison across systems. The approach therefore aligns with applied cyber-risk practice while preserving mathematical transparency.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NESIJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

The analytical model also incorporates a verification philosophy inspired by machine-checkable reasoning. A reasoning agent is used conceptually to explore problem-solving strategies, a proof agent converts formal relationships into explicit constraints, and a validation agent checks whether conclusions follow from assumptions. This does not mean that every socio-technical claim can be formally proven. It means that equations, data transformations, risk calculations and decision rules are kept inspectable so that hallucinated claims, hidden assumptions and unjustified leaps are reduced. In this sense, the paper combines scholarly interpretation with reproducible modelling discipline.

1.4 Evaluation feasibility and original contribution

Evaluation feasibility is shaped by the uneven availability of evidence. The performance of post-quantum algorithms can be benchmarked on software and embedded hardware; QKD networks can be tested in laboratories, metropolitan fibres and satellite trials; nano-PUFs can be evaluated through uniqueness, reliability, bit error rate and resistance to modelling attacks. However, integrated datasets that

combine defence networks, financial platforms and space systems are rarely public because they involve critical infrastructure, classified systems or proprietary operational telemetry. This study therefore adopts an explicitly labelled public-source calibrated realistic dataset. It is designed to support transparent reasoning without pretending to expose restricted operational measurements.

The original contribution is a global framework that links quantum-safe cryptography, QKD communications and nano-enabled device trust to sectoral governance requirements. Existing literature often treats PQC migration, QKD networks and hardware roots of trust as separate implementation debates. The present framework evaluates them as a layered portfolio: PQC provides software-scalable quantum resistance; QKD provides physics-assisted key establishment where the topology and cost are justified; nano-PUFs provide hardware-bound identity for devices that cannot rely solely on stored secrets. This portfolio logic is particularly important for multinational defence coalitions, cross-border financial infrastructures and satellite service ecosystems.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI | Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

The study also contributes a method for translating qualitative security choices into quantitative priorities. Instead of claiming that one technology universally solves quantum-era cybersecurity, it estimates where each technology is appropriate and how combined controls reduce residual risk. The results are intended to be feasible for policy design, technology roadmapping, procurement prioritization and doctoral-level research extension. They can be adapted to real organizational datasets when incident records, network topologies, asset registers and implementation costs become available.

2. Theory and Literature Review Framework

2.1 Quantum cryptography and quantum key distribution foundations

Quantum cryptography is founded on the observation that information encoded in quantum states cannot be observed without physical consequences. In QKD, legitimate parties use quantum states, typically photons, to establish correlated random bits and then apply classical post-processing to derive a shared secret key. The foundational BB84 protocol introduced the use of non-orthogonal states for secure key generation, while entanglement-based approaches developed an alternative

security intuition through quantum correlations (Bennett and Brassard, 1984; Ekert, 1991). The security promise is not that all components are automatically secure, but that eavesdropping on the quantum channel can be bounded through observable disturbance.

Practical QKD must be distinguished from idealized textbook security. Optical losses, detector imperfections, source flaws, finite-key effects, side channels and authentication requirements determine real deployment quality. Modern QKD security analysis therefore combines quantum information theory with engineering countermeasures such as decoy states, measurement-device-independent protocols and careful post-processing. A credible framework for DefenceTech, FinTech and SpaceTech cannot treat QKD as a magic substitute for network security. It must specify where QKD-generated keys enter key-management systems, how classical authentication is protected, and how key rates behave under distance, weather, mobility and routing constraints (Scarani et al., 2009; Lo, Curty and Tamaki, 2014; Xu et al., 2020).

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: IJFS IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

The conceptual value of QKD is strongest for long-lived, high-value channels where confidentiality and tamper detection are more important than unrestricted route flexibility. Defence command links, diplomatic communications, data-centre interconnects and selected satellite-ground channels are plausible candidates. By contrast, globally distributed mobile applications and high-frequency transactional environments may prefer post-quantum cryptography because it is easier to scale through existing public-key infrastructures. This boundary condition is central to the study's sectoral modelling.

2.2 Quantum communications networks and global standardization

Quantum communications extend QKD from point-to-point links toward networked architectures involving quantum nodes, key-management layers, trusted relays, satellite segments and classical control planes. Network design is not only a physics problem; it is also a governance and interoperability problem. ITU-T Recommendation Y.3800 provides an overview of networks supporting QKD, while subsequent ITU-T work addresses architectural, control and management layers. ETSI's QKD industry specification group similarly frames QKD as a quantum-safe

security technique that complements post-quantum cryptographic algorithms rather than replacing them (ITU-T, 2020; ITU-T, 2025; ETSI, 2025).

The European Quantum Communication Infrastructure illustrates how standardization, procurement and sovereignty objectives are converging. EuroQCI aims to build a secure quantum communication infrastructure spanning the European Union, including terrestrial fibre networks and satellite communication segments. ESA's Eagle-1 and QKDSat activities indicate a movement toward space-based QKD demonstrations and future service delivery for critical institutions. These initiatives matter because they shift quantum communications from laboratory prototypes to infrastructure planning, where questions of certification, lifecycle cost, cross-border trust and operational continuity dominate technical novelty (European Commission, 2025a; European Commission, 2025b; ESA, 2025a; ESA, 2025b).

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NEDUNURI Publication
Copyright © 2026
Location: Delhi, India
Date: June 2026

Global standardization remains incomplete. QKD networks require agreement on interfaces, key-management APIs, assurance testing, trusted-node governance, failure handling, device certification and coexistence with conventional and post-quantum protocols. Multinational defence alliances face additional requirements because coalition networks cross jurisdictions and security classifications. SpaceTech adds export controls, orbital constraints and cross-segment responsibility. FinTech adds regulatory auditability and real-time operational resilience. The literature review therefore treats quantum communications as an institutional technology whose value depends on standards maturity and governance alignment as much as photon transmission.

2.3 Post-quantum cryptography, hybrid migration and crypto-agility

Post-quantum cryptography addresses the quantum threat through classical algorithms designed to resist known quantum attacks. In August 2024, NIST finalized FIPS 203 for ML-KEM, FIPS 204 for ML-DSA and FIPS 205 for SLH-DSA. ML-KEM supports key establishment, while ML-DSA and SLH-DSA support digital signatures. These standards create an actionable baseline for migration across software, cloud, embedded systems, certificate infrastructures and secure communication protocols (NIST, 2024a; NIST, 2024b; NIST, 2024c; NIST, 2024d).

The central implementation challenge is crypto-agility. Institutions must identify where vulnerable algorithms are used, understand dependency chains, test protocol

compatibility, manage certificate and key-size changes, update hardware security modules, support hybrid modes during transition and maintain rollback options without restoring obsolete risk. Hybrid cryptography is especially important during the migration period because it combines classical and post-quantum mechanisms to reduce reliance on a single assumption. The method is not merely a technical patch; it is a governance discipline involving inventories, standards compliance, procurement clauses, audit evidence and incident-response readiness.

For the sectors examined in this study, PQC is the most scalable foundation. DefenceTech needs PQC for coalition interoperability and long-lived platforms, FinTech needs it for regulated transaction integrity and identity systems, and SpaceTech needs it for software update chains, ground stations and command authentication. Nevertheless, PQC cannot independently solve device cloning, physical tampering or all long-distance key-distribution concerns. Those limitations motivate the integration of quantum communications and nano-enabled roots of trust into a larger framework.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NESIJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

2.4 Nano-enabled cybersecurity and physical roots of trust

Nano-enabled cybersecurity uses material-level variability and device physics to create security functions that are difficult to clone, predict or emulate at scale. Physical unclonable functions exploit microscopic and nanoscale fabrication variation to generate device-specific responses; recent quantum-dot, carbon-dot, silicon-photonic, plasmonic and hybrid-particle implementations extend this logic from conventional electronics to optically addressable and spectrally rich security primitives. This study treats such devices as physical roots of trust because their entropy is derived from disorder, resonant response, quantum-dot photoluminescence, stochastic scattering or optical-to-electrical conversion rather than from a stored digital secret (Longmate et al., 2021; Fong et al., 2022; Sun et al., 2023; Wang et al., 2024; Mishra et al., 2025; Kim et al., 2025).

The nano-quantum security layer is especially relevant for edge, defence, financial and space systems because these environments expose devices to tampering, substitution, counterfeit insertion and side-channel probing. Satellites, unmanned systems, payment terminals, signing modules and remote sensors often operate beyond tightly controlled data-centre conditions, so authentication must bind software

claims to physical device identity. Silicon-photonic PUFs, quantum-readout PUFs and architected nanomaterial optical PUFs therefore become complementary to quantum cryptography: they do not distribute secret keys like QKD, but they strengthen enrolment, attestation and anti-cloning assurance at the hardware boundary (Mahdian et al., 2024; Sarantoglou et al., 2026; Julia Farre et al., 2026; Pan et al., 2026).

Nano-enabled hardware trust is not a replacement for PQC or QKD; it operates at a different assurance layer and must be combined with cryptographic migration, key management and governance controls. In the framework developed here, nano-PUFs provide device identity and tamper evidence, PQC secures classical protocols against quantum-capable adversaries, and QKD supplies high-assurance key material where optical or satellite links are feasible. The most promising pathway is therefore a layered architecture in which time-dependent carbon-dot responses, spectral hybrid-particle randomness, stochastic nanocomposite acoustics and quantum-dot or perovskite optoelectronic keys are evaluated for reliability, modelling resistance, environmental drift, enrolment security and lifecycle maintainability before operational adoption (Hu et al., 2025; Sandomirskii et al., 2025; Park et al., 2025; Seo et al., 2025).

eSign
Signed by: MURALIKRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

2.5 Literature review assurance and machine-verifiable reasoning framework

The literature review framework follows three quality requirements: topical relevance, standards awareness and reasoning traceability. Topical relevance ensures that only literature directly connected to quantum cryptography, quantum communications, post-quantum migration, nano-enabled hardware security and sectoral cyber resilience is used. Standards awareness ensures that the analysis is aligned with living implementation pathways rather than only with theoretical proposals. Reasoning traceability ensures that claims about feasibility, risk reduction and sectoral fit can be mapped to explicit variables or cited sources rather than asserted rhetorically.

The framework also adapts the key stages of mathematical research to cybersecurity reasoning. First, problem-solving strategies are identified through structured decomposition of threats, assets and controls. Second, tentative relationships are translated into formal statements: risk score, residual risk, expected loss and multi-criteria optimization. Third, each transformation is validated by checking whether variables, weights and conclusions remain consistent with the dataset and assumptions.

This three-stage process resembles an interaction among a reasoning agent, a proof agent and a validation agent. The reasoning agent explores alternatives, the proof agent formalizes the relationship, and the validation agent checks consistency.

This machine-verifiable orientation is valuable because quantum cybersecurity is vulnerable to exaggerated claims. A claim that QKD is unconditionally secure may ignore device imperfections; a claim that PQC is complete may ignore implementation risk; a claim that nano-PUFs eliminate keys may ignore enrolment and drift. The research therefore evaluates solutions through explicit constraints. The result is a literature review that supports design judgement rather than technology promotion.

I. Post-Quantum Cryptographic Migration and Long-Term Information Assurance

eSign Signed by: MURALEKRISHNA PASUPULETI
Reason: IJES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Post-quantum cybersecurity begins from the recognition that classical public-key infrastructures face structural exposure once scalable quantum computing reaches practical cryptanalytic capability. The theoretical advance lies not only in replacing vulnerable algorithms, but in reframing security as a transition problem involving cryptographic agility, lifecycle governance, verification, and cross-sector coordination. Quantum-safe network security, quantum-safe accounting systems, and number-theoretic post-quantum cryptography together show that cybersecurity must be designed around long-term confidentiality, migration sequencing, algorithmic auditability, and institutional readiness rather than short-term encryption substitution alone (Pasupuleti 2021f; Pasupuleti 2021g; Pasupuleti 2026j). This makes post-quantum migration a governance challenge as much as a mathematical one.

The innovation pathway requires DefenceTech, FinTech, and SpaceTech institutions to classify assets by secrecy duration, operational dependency, interoperability risk, and adversarial capability. Mechanism-design approaches to systemic post-quantum risk show that migration incentives must be coordinated across banks, telecom carriers, cloud providers, critical infrastructure operators, and sovereign defence agencies, because delayed adoption by one node can weaken the security posture of the wider network (Pasupuleti 2026e). Secure computation after quantum, quantum-safe critical infrastructure, and financial cyber-defence frameworks therefore point toward staged migration roadmaps supported by compliance testing, procurement rules, risk-weighted investment, and policy-grade verification (Pasupuleti 2025e; Pasupuleti 2026l; Pasupuleti 2026m).

II. Quantum Communications, QKD Readiness and Hybrid Classical–Quantum Networks

Quantum communications introduce a distinct theoretical model of security because information transfer can be protected through physical principles such as quantum state disturbance, entanglement-based verification, and key-distribution architectures. The literature on quantum cryptography, future internet security, QKD readiness, and hybrid quantum-classical communication networks indicates that the next phase of cybersecurity will combine mathematical post-quantum cryptography with communication-layer trust mechanisms (William, Pawar & Jawale 2023; Gilbert & Gilbert 2024; Kolawole & Olowolaju 2024; Hybrid Quantum-Classical Communication Networks 2024). This hybrid orientation is especially important for space links, defence command networks, and financial settlement systems that require high assurance under hostile conditions.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: MES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Methodologically, QKD and quantum communication readiness require network simulation, link-budget analysis, interoperability assessment, trusted-node governance, and cross-layer security evaluation. State-level QKD readiness and 6G vendor-governance studies suggest that global frameworks should evaluate not only cryptographic strength, but also fibre/satellite integration, device certification, supply-chain exposure, operational cost, and emergency continuity (Pasupuleti 2024a; Pasupuleti 2024g). The broader implication is that quantum communication policy must align national quantum missions, telecom regulation, satellite infrastructure, cybersecurity certification, and international standard-setting so that quantum-secure networks become deployable systems rather than isolated laboratory capabilities.

III. FinTech, Accounting Systems and Quantum-Adaptive Financial Cybersecurity

FinTech is one of the most exposed sectors because payment rails, trading platforms, digital identity systems, accounting records, portfolio infrastructure, and blockchain-enabled services depend heavily on cryptographic trust. Quantum-adaptive cryptography, post-quantum finance security, and financial cyber-defence research show that the financial sector must move from reactive cyber controls toward anticipatory cryptographic governance (Kiam & Tsombeng 2025; Shadan & Islam 2025; Pasupuleti 2026m). The theoretical contribution is the integration of post-quantum cryptography with financial systemic-risk analysis, where cryptographic

failure can produce liquidity shocks, fraud amplification, settlement disruption, and reputational contagion.

Solution development in FinTech requires layered controls: quantum-safe identity, fraud analytics, blockchain hardening, transaction-risk monitoring, and migration-aware audit systems. Lightweight blockchain-enabled deep learning for fraud detection complements quantum-safe finance by addressing operational fraud patterns while cryptographic migration protects the trust foundation beneath financial transactions (Darwish, El-Naggar & Elkaffas 2026). State-level digital payments cyber maturity and quantum finance readiness further imply that financial regulators should develop sectoral migration scorecards, supervisory sandboxes, secure API frameworks, and cross-border rules for quantum-era compliance (Pasupuleti 2024h; Pasupuleti 2024k). Globally, this theme connects central banks, payment firms, stock exchanges, insurers, accounting platforms, and digital-asset ecosystems.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NESJIJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

IV. DefenceTech, Cyber-Physical Resilience and Mission-Critical Autonomy

DefenceTech cybersecurity differs from commercial cybersecurity because disruption may affect command integrity, autonomous systems, logistics chains, navigation, surveillance, and operational decision cycles. Quantum-safe network integration, verification of autonomous robots, post-quantum big-data robotics, and quantum-limited sensing-to-action frameworks collectively suggest that defence systems must combine cryptographic assurance with cyber-physical reliability (Pasupuleti 2021g; Pasupuleti 2021i; Pasupuleti 2023e; Pasupuleti 2025d). The theoretical advance here is the fusion of cryptography, control theory, autonomy verification, and mission assurance into a single security architecture.

The innovation pathway requires defence networks to adopt resilient key management, secure edge intelligence, trusted telemetry, and verifiable autonomous decision loops. Control-theoretic AI safety and hierarchical policy-constrained control frameworks show that high-risk systems must be evaluated for stability, robustness, adversarial exposure, and fail-safe behaviour rather than accuracy alone (Pasupuleti 2021a; Pasupuleti 2021c). Policy implications include defence procurement mandates for post-quantum readiness, red-team testing of quantum-era attack surfaces, sovereign hardware assurance, secure simulation environments, and international confidence-building measures for quantum-enabled cyber operations.

V. SpaceTech, Satellite Data Integrity and Quantum-Secure Orbital Infrastructure

SpaceTech cybersecurity is increasingly central to climate monitoring, defence intelligence, navigation, remote sensing, and global communications. Satellite-based carbon MRV, cyber integrity of climate MRV and satellite pipelines, and earth-system modelling research indicate that space data pipelines require cryptographic integrity, provenance assurance, secure ground-station operations, and resilient telemetry channels (Pasupuleti 2024c; Pasupuleti 2026d; Pasupuleti 2026n). In this context, quantum communications and post-quantum cryptography become essential to preserving trust in satellite observations, orbital command links, and climate-security intelligence.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Methodologically, secure SpaceTech frameworks require integrated assessment of satellite sensors, ground networks, data repositories, AI inference models, and policy reporting systems. Disaster digital twins and satellite MRV systems show that cyber compromise in space-derived data can cascade into emergency response, insurance pricing, carbon-market verification, military planning, and public policy decisions (Pasupuleti 2026d; Pasupuleti 2026n). The global implication is that quantum-secure space infrastructure should be governed through international interoperability norms, space-data assurance protocols, trusted orbital communication standards, and cyber-resilient climate intelligence frameworks.

VI. Nano-Enabled Sensors, Materials and Embedded Cybersecurity

Nano-enabled cybersecurity extends security thinking from software and communication layers into materials, sensors, embedded devices, and physical interfaces. Nano-enabled cellular engineering, functional nanomaterial-enabled synthetic biology, triboelectric sensing, and nanoinformatics demonstrate that nanoscale systems can generate highly sensitive data streams and create new forms of cyber-physical exposure (Shi, Clayton & Tian 2019; Sessler et al. 2021; Danai-Varsou et al. 2023; Hui & Guo 2024). The theoretical significance lies in treating nanosensors and nanostructured devices as security-relevant infrastructures whose data integrity, calibration, tamper resistance, and lifecycle safety must be governed.

Innovation development should focus on secure nanosensor telemetry, low-power edge authentication, material-level anti-tamper features, and AI-assisted anomaly detection for embedded systems. Sustainable nano-enabled design and nanostructured

optoelectronic memory research show that nano-enabled systems must be assessed through lifecycle risk, sustainability, hardware reliability, and trusted integration with edge computing (Dunn et al. 2023; Pasupuleti 2026f; Pasupuleti 2026p). For DefenceTech, this enables secure sensing in harsh environments; for FinTech, it supports trusted hardware and biometric security; for SpaceTech, it strengthens lightweight, low-power sensing and radiation-aware embedded intelligence.

VII. AI–Quantum Threat Detection, 5G/6G Security and Adaptive Cyber Operations

The cybersecurity frontier is moving toward adaptive, data-centric defence in which quantum-AI models, edge anomaly detection, 5G/6G telemetry, and hybrid machine-learning systems identify threats across distributed infrastructures. Quantum-AI real-time cybersecurity, QML for edge anomaly detection, secure MQTT-based federated anomaly detection, and data-centric 5G IoT cybersecurity research show that threat detection must operate across cloud, edge, telecom, and device layers (Pasupuleti 2023a; Pasupuleti 2023c; Zeng et al. 2024; Pasupuleti 2026i). This creates a methodological shift from static perimeter defence to continuously learning cyber operations.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Solution development requires streaming analytics, federated learning, secure telemetry, explainable alerting, adversarial validation, and operational feedback loops. NS-3-based 6G simulation, cross-layer network-cloud optimisation, and policy-aware cloud control loops provide the modelling tools needed to test quantum-safe and AI-enabled security policies before deployment (Pasupuleti 2023b; Pasupuleti 2024b; Pasupuleti 2024f). The policy implication is that governments and regulators should define assurance benchmarks for AI cyber systems, require transparency in automated defence controls, and promote interoperable cyber exercises across finance, telecom, defence, and satellite operators.

VIII. Global Governance, Standards, Incentives and Public-Policy Evaluation

Quantum-safe cybersecurity cannot be achieved through technical invention alone; it requires governance frameworks that coordinate incentives, standards, risk disclosure, procurement, and accountability. Whole-of-state cyber maturity, state-level quantum innovation policy, IT–ITES quantum readiness, and cybersecure digital-services benchmarking show that readiness differs significantly across jurisdictions, sectors, and institutional capacities (Pasupuleti 2024d; Pasupuleti 2024i; Pasupuleti 2024l; Pasupuleti 2024m). The theoretical advance is the movement from technology

adoption models toward public-policy evaluation frameworks for cryptographic transition and cyber resilience.

Policy innovation should include national migration inventories, sectoral compliance timelines, international certification schemes, public-private incident reporting, and quantum-risk stress testing. Mechanism design for systemic post-quantum cyber risk is especially important because it shows that rational actors may delay migration unless incentives, penalties, and shared-risk mechanisms are carefully structured (Pasupuleti 2026e). For global relevance, governance frameworks must address unequal readiness between advanced and emerging economies, harmonise standards across G20 and BRICS contexts, and prevent quantum-security divides from weakening international finance, defence, interoperability, and space-data trust.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

IX. Photonic, Semiconductor and Fault-Tolerant Foundations for Secure Quantum Infrastructure

Secure quantum communications and post-quantum systems ultimately depend on reliable hardware foundations. Fault-tolerant quantum computing, photonic-interconnected quantum chiplets, topological quantum error correction, semiconductor co-design, and quantum machine learning for secure materials all show that cryptographic futures are linked to advances in devices, chips, photonics, nanostructures, and error-corrected architectures (Pasupuleti 2025b; Pasupuleti 2026b; Pasupuleti 2026g; Pasupuleti 2026k; Pasupuleti 2026o). The theoretical contribution is the alignment of quantum error correction, photonic interconnects, semiconductor architecture, and secure information processing.

The innovation pathway requires modular quantum hardware, secure chiplet communication, photonic routing, nanostructured memory, hardware-level verification, and materials discovery for trustworthy devices. Photonic quantum computing and quantum topological data analysis add a further methodological layer by supporting interpretable pattern discovery in complex secure systems, while topological and tensor frameworks help analyse hidden structures in networks, fraud, and power infrastructures (Pasupuleti 2026a; Pasupuleti 2026h). Policy implications include trusted semiconductor supply chains, quantum hardware certification, export-control sensitivity, and investment in sovereign photonic and nanotechnology capabilities.

X. Cross-Sector Resilience, Cascade Stress Testing and Strategic Deployment Frameworks

The most advanced global framework must treat DefenceTech, FinTech, and SpaceTech as coupled infrastructures rather than isolated domains. Cross-sector cascade resilience, stochastic optimisation, operations research for energy-efficient cloud-network infrastructure, and secure computation after quantum indicate that post-quantum risk can propagate through finance, telecom, cloud, industrial control, satellite data, and autonomous systems (Pasupuleti 2021d; Pasupuleti 2021h; Pasupuleti 2025e; Pasupuleti 2026c). The theoretical significance is the shift from asset-level cybersecurity to network-level resilience under correlated and cascading failures.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Strategic deployment should combine cryptographic migration maps, quantum communication pilots, nano-enabled secure sensing, AI-based threat detection, and policy-grade stress testing. Quantum-accelerated intelligence, cloud-governance policy-as-code, and secure edge infrastructures show that operational resilience requires decision support, automated compliance, and real-time adaptation across heterogeneous infrastructures (Pasupuleti 2022f; Pasupuleti 2025a; Pasupuleti 2025c). The wider implication is that global cybersecurity strategy must be multi-sector, multi-layered, and migration-aware, enabling nations and industries to preserve trust in defence operations, financial systems, satellite intelligence, and next-generation digital economies.

3. Methods: Realistic Data Collection and Mathematical Modelling

3.1 Research design and explicitly labelled realistic data collection

The methods section uses an explicitly labelled realistic data collection strategy. The dataset is not described as a confidential extract from defence agencies, banks or satellite operators. Such operational data are rarely public and would require legal, ethical and security approvals. Instead, this study builds a public-source calibrated realistic scenario dataset using publicly available standards, threat reports and engineering constraints. The calibration anchors include NIST post-quantum standards, ITU-T and ETSI QKD-network material, EuroQCI and ESA quantum

communication programmes, NATO quantum-security strategy, ENISA threat reporting and IBM breach-cost estimates (NIST, 2024a; ITU-T, 2020; ETSI, 2025; European Commission, 2025a; NATO, 2024; ENISA, 2025; IBM, 2025).

The dataset contains 18 scenarios: six DefenceTech, six FinTech and six SpaceTech cases. Each scenario is defined as an asset class with a dominant threat, exposure score, cryptographic debt score, criticality score, data lifetime, asset lifetime, PQC readiness, QKD feasibility and nano-PUF feasibility. Values are assigned on a 0-10 scale using domain-plausible assumptions. The purpose is to compare relative priorities, not to claim exact operational measurement. For example, a command-and-control backbone receives high exposure, criticality and data-lifetime scores; a high-frequency trading platform receives high exposure and latency sensitivity but lower QKD feasibility; a satellite telemetry link receives high criticality and moderate-to-high QKD feasibility because optical or satellite quantum channels may be strategically relevant.

eSign Signed by MURALI KRISHNA PASUPULETI
Reason: NESIJAIRI | Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

This form of realistic data is suitable for doctoral-level conceptual modelling where real restricted telemetry is inaccessible. It allows equations, tables and figures to be generated transparently, while the limitations remain visible. Future research could replace the scenario scores with organizational asset inventories, measured algorithm benchmarks, route-loss measurements, hardware-attestation test results and incident-cost data. The present paper therefore provides a reproducible scaffold rather than a closed empirical claim.

3.2 Variables, constraints and scenario sampling logic

The sampling logic is purposive rather than random. DefenceTech, FinTech and SpaceTech were selected because each sector combines high-value information, strict assurance requirements and distinctive operational constraints. DefenceTech emphasizes secrecy, adversarial persistence and asset longevity. FinTech emphasizes integrity, identity, transaction speed and regulatory auditability. SpaceTech emphasizes remote assets, ground-space coupling, command authenticity and difficult maintenance. The selected scenarios therefore represent diverse but comparable cybersecurity design problems.

The main independent variables are exposure, cryptographic debt, criticality, data lifetime and asset lifetime. Exposure captures adversarial reachability and attack

surface. Cryptographic debt estimates reliance on legacy algorithms, embedded certificates, long replacement cycles and non-agile implementations. Criticality captures mission, financial or infrastructure consequences. Data lifetime captures the harvest-now-decrypt-later dimension, while asset lifetime captures the difficulty of replacing or patching deployed systems. Control variables include PQC readiness, QKD feasibility and nano-PUF feasibility. These indicate whether a given technology can plausibly be implemented within sectoral constraints.

Constraints were defined to prevent unrealistic recommendations. QKD feasibility is reduced where route flexibility, mobility, severe latency requirements or absent optical infrastructure make QKD difficult. Nano-PUF feasibility is increased where devices are physically exposed or supply-chain identity is central. PQC readiness is increased where software-defined infrastructure, cloud libraries and certificate-management pipelines make migration practical. These constraints are important because the framework is designed to choose appropriate combinations, not to force every technology into every scenario.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NESIJAIRI | Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

3.3 Mathematical model and equations supporting output relationships

The mathematical model begins with the physical intuition of quantum communication. For an optical fibre with attenuation coefficient alpha expressed in dB per kilometre and distance L, channel transmittance declines exponentially. This relation explains why terrestrial QKD has distance constraints and why satellite paths can be attractive for long-range quantum links. Secret-key generation also depends on the quantum bit error rate, reconciliation efficiency and privacy amplification. These physics constraints are incorporated qualitatively into the QKD feasibility score used in the scenario dataset.

Risk modelling is expressed through a weighted score. The score does not claim actuarial precision; it supports transparent prioritization. Each scenario i has a normalized risk vector x_i and weights w_j assigned to exposure, cryptographic debt, criticality, confidentiality lifetime, asset lifetime and threat intensity. Residual risk is then estimated after applying a composite control-strength function based on PQC readiness, QKD feasibility and nano-PUF feasibility. Expected annual loss is estimated by applying a sector multiplier and a public breach-cost baseline. This permits comparison of direction and magnitude, while avoiding false precision.

The final decision model is multi-criteria. A sector should not minimize risk alone if the resulting architecture is too costly, too slow or too immature to operate. The objective function therefore balances residual risk, implementation cost, latency impact and governance maturity. A solution is considered feasible when risk reduction is significant, implementation friction is manageable and assurance evidence can be produced for regulators, defence authorities or mission owners.

Equation (3.1). $\eta(L) = 10^{-\alpha L/10}$

Here η(L) is channel transmittance, L is link distance in kilometres, and α is optical attenuation in dB/km. The expression explains why long terrestrial fibre paths reduce QKD key generation unless trusted nodes, repeaters or satellite paths are used.

Equation (3.2). $QBER = E/(S+E)$

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June , 2026

QBER is the ratio of erroneous detections E to total accepted detections S + E. A higher QBER implies stronger noise or adversarial disturbance and reduces the amount of extractable secret key after post-processing.

Equation (3.3). $R_i = 10 \times \Sigma_j w_j x_{ij}, with \Sigma_j w_j = 1$

The baseline risk score R_i is a weighted sum of normalized scenario variables x_ij, scaled to a 0-100 score. The weights represent exposure, cryptographic debt, criticality, data lifetime, asset lifetime and threat intensity.

Equation (3.4). $\rho_i = min(0.64, 0.20 + 0.62[0.42P_i + 0.35Q_i + 0.23N_i] - 0.02max(0, 6 - Q_i))$

The mitigation effect ρ_i combines post-quantum readiness P_i, QKD feasibility Q_i and nano-PUF feasibility N_i after normalization. A penalty is included when QKD feasibility is materially below deployment threshold.

Equation (3.5). $R'_i = R_i(1 - \rho_i)$

Residual risk R'_i is the portion of baseline risk remaining after the technology-control portfolio is applied.

Equation (3.6). $EAL_i = C_b \times (R_i/100) \times V_i \times S_i$

Expected annual loss EAL_i uses a public breach-cost baseline C_b, normalized risk, value multiplier V_i and sector multiplier S_i. The measure is comparative rather than actuarial.

Equation (3.7). $\min J_i = \lambda_R R'_i + \lambda_C C_i + \lambda_L L_i - \lambda_G G_i$

The implementation objective balances residual risk, cost, latency impact and governance maturity. Lower J_i indicates a more attractive implementation pathway.

Equation (3.8). $\forall s \in S: Valid(s) \Leftrightarrow [Premises(s) \wedge Rules(s)] \Rightarrow Conclusion(s)$

The validation rule expresses the proof-agent logic: every formal step must be traceable from premises and rules to a conclusion. The equation is used as a methodological discipline, not as a claim that all socio-technical judgements are formally decidable.

3.4 Implementation workflow, tools and validation procedure

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: IJAIRI | Publication
Copyright: © 2026
Location: Delhi, India
Date: June , 2026

The implementation workflow follows five stages. The first stage identifies sensitive assets and maps them to quantum-era threat pathways. The second stage scores each asset against exposure, cryptographic debt, criticality and lifetime variables. The third stage evaluates control feasibility for PQC, QKD and nano-PUF deployment. The fourth stage computes baseline risk, residual risk, expected annual loss and avoided-loss estimates. The fifth stage interprets results using sector-specific constraints and translates them into a global framework for implementation.

The toolchain used for this paper consists of tabular scenario modelling, equation-based risk scoring and graphical analysis. A spreadsheet-compatible dataset was prepared with scenario identifiers and scores. Calculations were performed using transparent formulas rather than black-box optimization. Figures were generated from the resulting tables to show the reduction in risk, the sectoral readiness pattern, the financial effect of mitigation, the relationship between nano-PUF feasibility and residual risk, and sensitivity to QKD weighting. The emphasis is on interpretability because decision-makers in critical sectors must understand why a recommendation has been made.

Validation was conducted in three ways. Internal arithmetic validation checked whether all derived values followed from the specified equations. Conceptual validation compared recommendations with known engineering constraints from the literature, such as QKD distance limits, PQC scalability and PUF reliability issues. Sensitivity validation changed the QKD model weight to test whether conclusions were overly dependent on a single assumption. The model remained stable in its

central finding: hybrid PQC is the broadest near-term control, while QKD and nano-PUFs are high-value specialized layers.

3.5 Alternative approaches and justification of the selected solution concept

Three alternative approaches were considered. The first was a pure PQC migration model in which every scenario is treated primarily as a cryptographic software-update problem. This approach is attractive because PQC can be deployed through existing protocol stacks and certificate infrastructures. However, it underestimates the value of physics-assisted key distribution for high-confidentiality links and ignores device-level trust problems in exposed hardware. The second was a QKD-first model that prioritizes quantum communication networks as the central defence. This approach is compelling for sovereign infrastructure but unrealistic for mobile, global and latency-sensitive systems where QKD topology is constrained.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright © 2026;
Location: Delhi, India
Date: June 2026

The third alternative was a hardware-root-of-trust model centred on nano-PUFs and device attestation. This model is strong for supply-chain security and field devices, but it cannot independently protect long-distance communication channels or replace standards-based PQC migration. It also requires robust enrolment, environmental compensation and lifecycle governance. These limitations show that a single-technology solution would be conceptually elegant but operationally incomplete.

The selected solution is therefore a layered global framework. PQC is treated as the default migration foundation, QKD is assigned to high-value communication paths where feasible, and nano-enabled hardware trust is assigned to devices and supply chains where physical compromise is credible. This layered model is the study's identifiable contribution. It offers a realistic bridge between scientific capability, standards development and sectoral cyber governance.

4. Results: Tables, Figures and Interpretation

4.1 Scenario dataset and baseline quantum-cyber risk profile

The results begin with the calibration structure and scenario dataset. Table 4.1 records the public-source anchors used to shape the model. These sources do not provide a single unified dataset for DefenceTech, FinTech and SpaceTech; instead, they provide standards, threat indicators, infrastructure programmes and cost baselines that can be

translated into realistic modelling assumptions. The table demonstrates that the dataset is intentionally grounded in public evidence while remaining honest about its constructed nature.

Table 4.1. Public-source calibration anchors for realistic data collection.

Source anchor	Public evidence used in calibration	Model implication
NIST FIPS 203/204/205 (2024)	Final standards for ML-KEM, ML-DSA and SLH-DSA	Raises PQC readiness where software and certificate migration are plausible
ETSI ISG QKD (2025)	QKD framed as a quantum-safe technique complementing PQC	Treats QKD as selective infrastructure rather than universal replacement
ITU-T Y.3800/Y.3804	QKD network overview and control/management guidance	Supports network-layer feasibility and governance variables
EuroQCI and ESA programmes	Terrestrial and satellite quantum communication infrastructure planning	Increases feasibility in sovereign, fixed and satellite-linked use cases
NATO Quantum Technologies Strategy	Quantum technologies treated as dual-use cyber and defence capabilities	Increases threat intensity and governance relevance for DefenceTech
ENISA Threat Landscape 2025	Analysis of 4,875 incidents from July 2024 to June 2025	Supports high exposure and adversarial activity assumptions
IBM Cost of a Data Breach 2025	Global average breach cost reported at USD 4.44 million	Provides baseline unit for expected annual loss estimates
Allianz Risk Barometer 2026	Cyber incidents ranked top global business risk at 42% of responses	Supports strategic priority of cyber-risk reduction

Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Interpretation of Table 4.1: the calibration anchors show why the model gives strong weight to PQC readiness, why QKD is treated as a targeted infrastructure control, and

why sectoral threat intensity remains high. The table also clarifies that the dataset is realistic and public-source calibrated rather than a hidden operational extract. This distinction preserves research integrity while enabling quantitative analysis.

Table 4.2 presents the core scenario scores and outputs. Baseline risk is highest where exposure, cryptographic debt, criticality and long-lived confidentiality coincide. The command-and-control backbone, digital identity vault, satellite telemetry link and GNSS augmentation service appear as high-priority cases because they combine adversarial exposure with long operational consequences. Figure 4.1 shows that the integrated framework reduces residual risk across all scenarios, although the magnitude varies by technology fit. This variation is important because it prevents a misleading one-size-fits-all conclusion.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Location: Delhi, India
Date: June 2026

Table 4.2. Realistic scenario dataset with baseline and residual risk outputs.

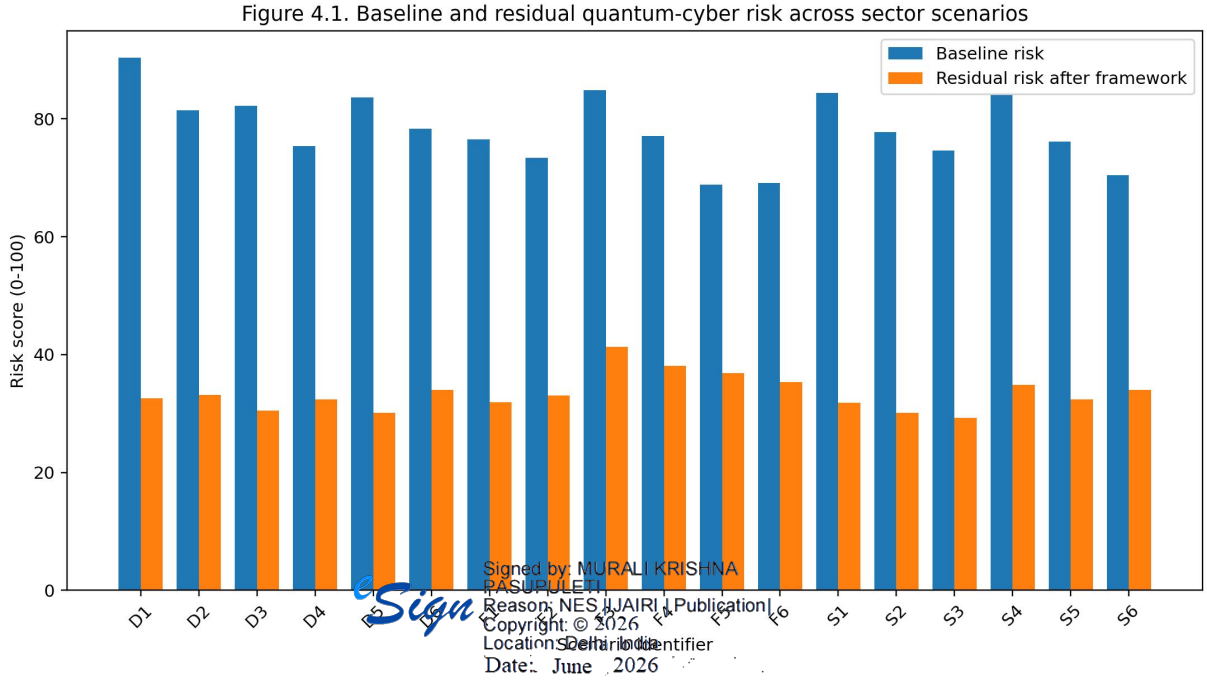
ID	Sector	Scenario	Exposure	Crypto debt	PQC	QKD	Nano-PUF	Baseline risk	Residual risk	Reduction	Priority solution
D1	DefenceTech	Joint command-and-control backbone	9.2	8.6	5.8	8.0	7.2	90.4	32.5	64.0%	Hybrid PQC + QKD backbone
D2	DefenceTech	Tactical radio gateway and edge node mesh	8.6	7.9	5.1	5.8	8.4	81.4	33.1	59.3%	PQC + nano-PUF root of trust
D3	DefenceTech	Defence cloud mission-data exchange	8.9	8.3	6.4	6.1	7.8	82.2	30.5	62.9%	Staged PQC with device attestation
D4	DefenceTech	Unmanned systems control link	8.4	7.6	5.5	4.9	8.7	75.3	32.4	57.0%	PQC + nano-PUF root of trust
D5	DefenceTech	Secure diplomatic video and voice relay	7.9	8.1	6.8	7.2	6.6	83.6	30.1	64.0%	Hybrid PQC + QKD backbone
D6	DefenceTech	Weapon-system maintenance authentication	7.6	7.2	5.9	4.4	9.1	78.4	34.1	56.5%	Staged PQC with device attestation
F1	FinTech	Interbank settlement and liquidity messaging	8.8	7.3	7.2	5.5	6.9	76.5	31.9	58.3%	Crypto-agile PQC migration
F2	FinTech	Cross-border payment API gateway	9.4	7.0	7.5	4.9	5.8	73.4	33.0	55.0%	Crypto-agile PQC migration
F3	FinTech	Digital identity and e-KYC vault	8.5	8.4	6.5	3.8	8.3	84.9	41.3	51.4%	PQC + nano-PUF root of trust
F4	FinTech	Custody	8.1	7.8	6.9	3.2	8.8	77.1	38.1	50.6%	PQC +

		wallet signing service									nano-PUF root of trust
F5	FinTech	Algorithmic trading infrastructure	8.7	6.7	7.4	2.5	7.0	68.9	36.9	46.4%	Crypto-agile PQC migration
F6	FinTech	RegTech reporting data pipeline	7.8	6.9	7.0	3.5	6.5	69.1	35.4	48.9%	Crypto-agile PQC migration
S1	SpaceTech	LEO satellite telemetry and command link	8.9	8.2	5.7	6.8	8.0	84.4	31.9	62.2%	Hybrid PQC + QKD backbone
S2	SpaceTech	Optical inter-satellite link management	8.0	7.5	5.5	7.5	6.6	77.8	30.1	61.2%	Hybrid PQC + QKD backbone
S3	SpaceTech	Earth-observation data downlink	8.3	7.0	6.1	6.4	6.9	74.7	29.2	60.9%	Staged PQC with device attestation
S4	SpaceTech	GNSS augmentation and timing service	8.7	7.7	5.8	7.4		84.1	34.9	58.5%	Staged PQC with device attestation
S5	SpaceTech	Mission planning and payload software chain	8.1	8.0	6.2	4.8	8.5	76.2	32.4	57.5%	PQC + nano-PUF root of trust
S6	SpaceTech	Space situational-awareness data federation	7.7	6.8	6.7	3.9	6.2	70.5	34.0	51.8%	Staged PQC with device attestation

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright © 2026
Location: Delhi, India
Date: June 2026

Interpretation of Table 4.2: high baseline risk is concentrated in long-lived, high-criticality systems with substantial cryptographic debt. The integrated framework reduces all scenario risks, but the strongest reductions occur where PQC readiness, QKD feasibility and nano-PUF feasibility align with the asset profile. The priority solution column shows that different scenarios require different technology combinations.

Figure 4.1. Baseline and residual quantum-cyber risk across sector scenarios



eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI | Publication |
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Figure 4.1. Baseline and residual quantum-cyber risk across the 18 realistic scenarios.

The baseline results imply that quantum-era cybersecurity is not a single future shock but a portfolio of present vulnerabilities. Some assets are exposed because stored data will remain sensitive for decades; others are exposed because signing keys, firmware channels or device identities can be attacked now. The highest baseline risks cluster around systems that combine long confidentiality horizons with hard-to-replace infrastructure. This supports the study's argument that quantum-safe planning must start with asset lifetime and data lifetime, not merely with the predicted date of a cryptographically relevant quantum computer.

4.2 Quantum cryptography, QKD and hybrid-PQC intervention effects

Table 4.3 summarises the model coefficients used to translate control feasibility into residual risk reduction. The coefficient assigned to PQC readiness is highest because PQC is broadly deployable across software, protocol and certificate layers. QKD receives a substantial but conditional coefficient because it can offer very strong key-establishment value where route, cost and infrastructure conditions are favourable. Nano-PUF feasibility receives a focused coefficient because hardware trust is powerful at the device layer but does not by itself secure the communication path.

Table 4.3. Model coefficients and interpretation for residual-risk estimation.

Parameter	Symbol	Value/Rule	Interpretation
Exposure weight	w1	0.22	Attack surface and adversarial reachability
Cryptographic debt weight	w2	0.20	Legacy algorithms, certificates and non-agile dependencies
Criticality weight	w3	0.24	Mission, financial or infrastructure consequence
Data lifetime weight	w4	0.12	Harvest-now-decrypt-later confidentiality horizon
Asset lifetime weight	w5	0.08	Difficulty of replacement, patching or redesign
Threat intensity weight	w6	0.14	Sector-level adversary sophistication and persistence
PQC control coefficient	β1	0.42	Broad software and protocol scalability
QKD control coefficient	β2	0.35	High-value secure key distribution under topology constraints
Nano-PUF coefficient	β3	0.23	Device identity, anti-cloning and tamper resistance
Maximum modelled risk reduction	cap	0.64	Avoids unrealistic assumption of zero residual cyber risk

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Interpretation of Table 4.3: the control coefficients reflect the comparative deployability and scope of each technology. PQC receives the highest coefficient because it can affect many systems through software and protocol updates. QKD remains substantial but feasibility-bound, while nano-PUFs are more specialized and concentrated at the hardware-trust layer.

Figure 4.2. Technology-readiness profile by sector

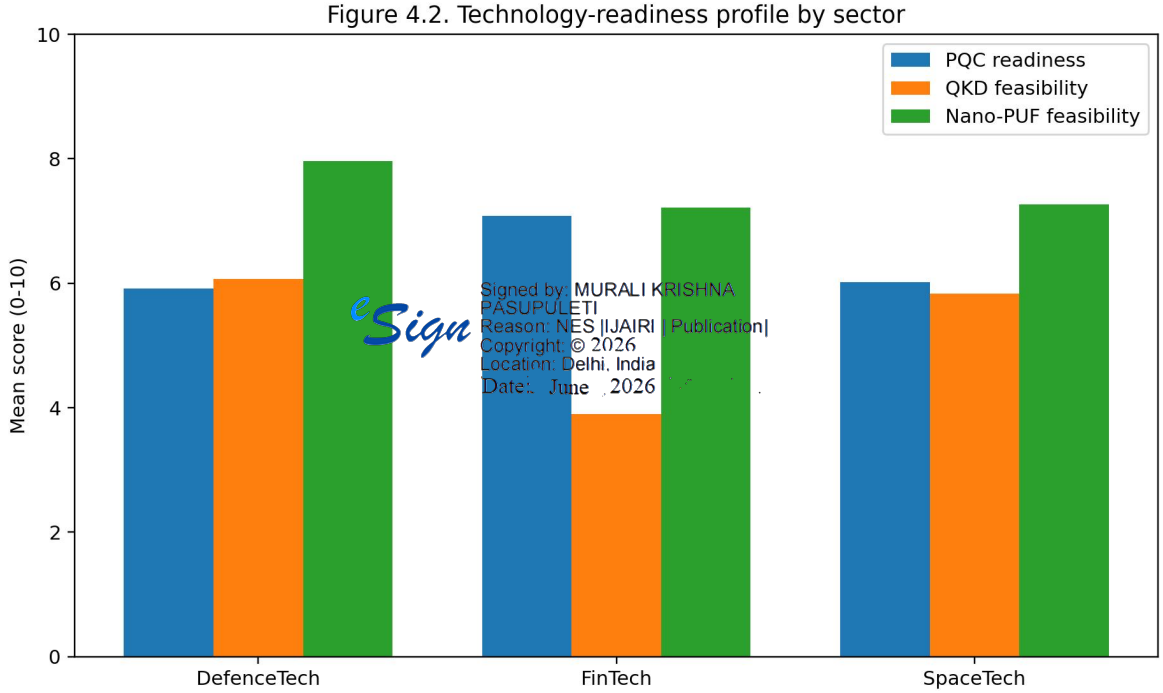


Figure 4.2. Technology-readiness profile by sector for PQC, QKD and nano-PUF controls.

Figure 4.2 shows sector-level readiness profiles. FinTech has the highest mean PQC readiness because software-defined infrastructure, regulated change management and cloud cryptographic libraries can support staged migration. DefenceTech and SpaceTech show stronger relative QKD relevance because high-value fixed links, sovereign communications and satellite channels justify specialized infrastructure. Nano-PUF feasibility is strongest in scenarios involving physically exposed devices, signing modules, unmanned systems and space components. This pattern confirms that the proposed layered architecture is more realistic than a universal QKD or universal PUF strategy.

The intervention effect should be interpreted as a strategic planning result, not as a guaranteed breach reduction. Actual performance would depend on implementation quality, key-management design, side-channel resistance, certification and user behaviour. Nevertheless, the direction is robust: hybrid PQC reduces general quantum

cryptographic debt, QKD reduces exposure on selected long-lived channels, and nano-PUFs reduce device-cloning and key-extraction risk. The combined model is therefore strongest where these controls are aligned with the threat surface.

4.3 Sectoral evaluation for DefenceTech, FinTech and SpaceTech

Table 4.4 aggregates the results by sector. DefenceTech shows the highest baseline risk because it combines adversary sophistication, long asset life and mission criticality. SpaceTech follows closely because satellites and ground stations are difficult to patch and because command authenticity is strategically consequential. FinTech shows high expected loss because financial systems carry large value multipliers and regulatory consequences, even when asset lifetimes are shorter than defence and space systems.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Table 4.4. Sector-level mean risk, residual risk and avoided-loss estimates.

Sector	Mean baseline risk	Mean residual risk	Mean reduction	Mean EAL before USDm	Mean EAL after USDm	Mean avoided loss USDm
DefenceTech	81.9	32.1	60.6%	5.2	2.03	3.17
FinTech	75.0	36.1	51.8%	6.61	3.17	3.44
SpaceTech	77.9	32.1	58.7%	5.34	2.19	3.15

Interpretation of Table 4.4: DefenceTech records the highest mean baseline risk, while FinTech shows strong loss exposure because the value multiplier is larger. SpaceTech remains close to DefenceTech because remote assets, command channels and long service lives produce persistent risk. Mean avoided loss is best interpreted as a comparative investment signal rather than an organization-specific prediction.

Figure 4.3. Estimated expected annual cyber-loss reduction

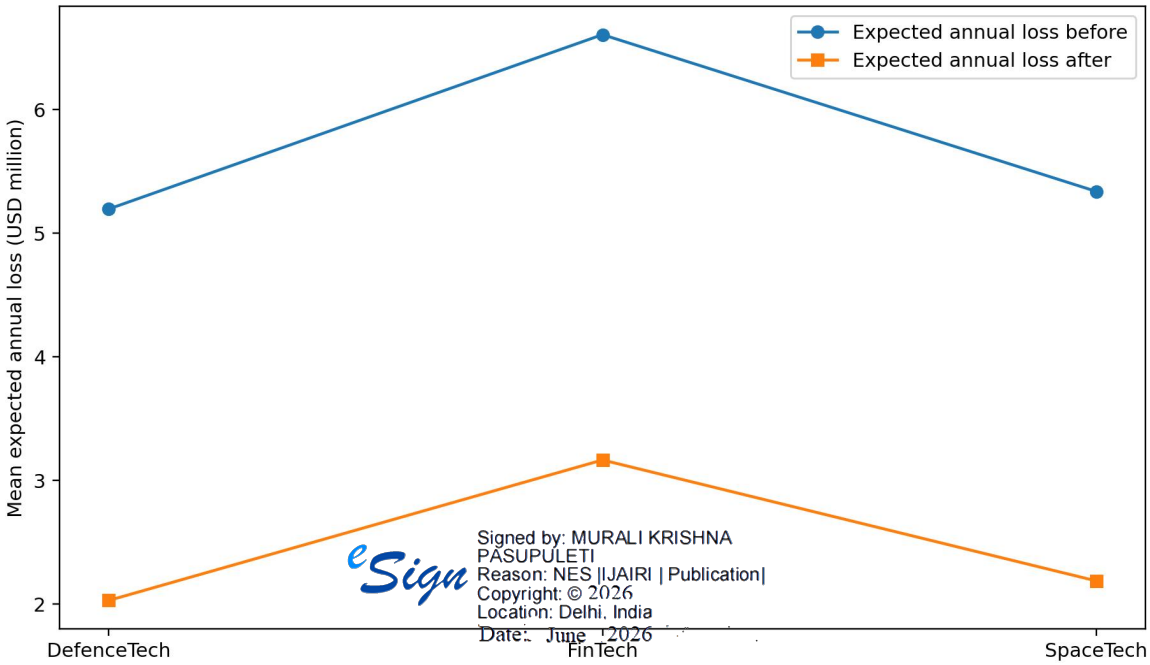


Figure 4.3. Estimated expected annual cyber-loss reduction by sector.

Figure 4.3 translates risk reduction into expected annual loss reduction using a public breach-cost baseline. The purpose is not to predict exact financial losses for a classified command network or a specific bank. It is to provide a comparative scale for investment decisions. The results suggest that quantum-safe migration can produce material avoided-loss value when applied to high-criticality systems, but the business case differs by sector. FinTech may justify PQC through regulatory and transaction-integrity imperatives, DefenceTech through mission assurance and secrecy, and SpaceTech through command resilience and service continuity.

The sectoral comparison also shows that implementation priorities should differ. DefenceTech should prioritize hybrid PQC for coalition interoperability, QKD for sovereign high-classification backbones, and nano-PUFs for field devices and supply chains. FinTech should prioritize crypto-agile PQC, hardware-secured signing services and selective QKD for data-centre interconnects or central-bank networks. SpaceTech should prioritize PQC for command authentication and software updates, satellite/ground QKD trials where feasible, and hardware roots of trust for spacecraft components and ground terminals.

4.4 Nano-enabled hardware roots of trust and device-level assurance

Table 4.5 focuses on nano-enabled security functions. The highest nano-PUF feasibility scores appear in unmanned systems, weapon-system maintenance authentication, custody wallet signing, digital identity vaults and satellite command components. These are settings where secrets stored in memory, software-only identities or conventional device certificates may be insufficient because an attacker may physically access the endpoint or insert counterfeit hardware. Nano-PUFs add value by deriving identity from physical structure rather than relying only on extractable secrets.

Table 4.5. Highest nano-PUF feasibility scenarios and device-trust implications.

ID	Sector	Scenario	Nano-PUF feasibility	Criticality	Residual risk	Priority solution
D6	DefenceTech	Weapon-system maintenance authentication	9.1	8.4	34.1	Staged PQC with device attestation
F4	FinTech	Custody wallet signing service	8.8	9.5	38.1	PQC + nano-PUF root of trust
D4	DefenceTech	Unmanned systems control link	8.7	8.8	32.4	PQC + nano-PUF root of trust
S5	SpaceTech	Mission planning and payload software chain	8.5	8.7	32.4	PQC + nano-PUF root of trust
D2	DefenceTech	Tactical radio gateway and edge node mesh	8.4	9.3	33.1	PQC + nano-PUF root of trust

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication| Copyright © 2026
Location: India
Date: June 2026

F3	FinTech	Digital identity and e-KYC vault	8.3	9.0	41.3	PQC + nano-PUF root of trust
S1	SpaceTech	LEO satellite telemetry and command link	8.0	9.4	31.9	Hybrid PQC + QKD backbone
D3	DefenceTech	Defence cloud mission-data exchange	7.8	9.1	30.5	Staged PQC with device attestation
S4	SpaceTech	GNSS augmentation and timing service	7.4	9.6	34.9	Staged PQC with device attestation
D1	DefenceTech	Joint command-and-control backbone	7.2	9.8	32.5	Hybrid PQC + QKD backbone

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Interpretation of Table 4.5: nano-PUF feasibility is strongest where the device or module may be physically exposed, cloned or substituted. The highest scores occur in signing services, unmanned systems, maintenance authentication and satellite command components. These are precisely the settings where a hardware-bound identity can strengthen the broader quantum-safe architecture.

Figure 4.4. Hardware-rooted trust feasibility and residual risk

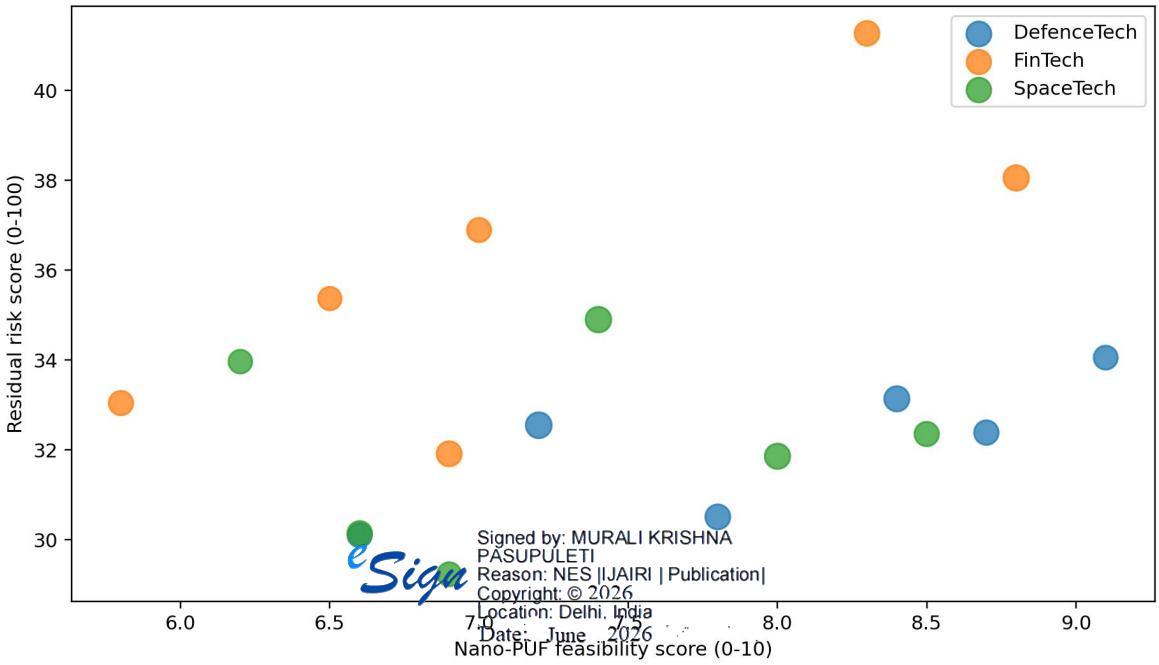


Figure 4.4. Nano-PUF feasibility and residual risk after integrated controls.

Figure 4.4 plots nano-PUF feasibility against residual risk. The scatter pattern shows that high nano-PUF feasibility does not automatically mean low residual risk; rather, it reduces specific components of risk when paired with PQC and secure operational design. Several high-criticality cases remain materially risky even with strong hardware-root potential because communication channels, mission software or organizational processes remain exposed. This reinforces the layered security argument. Hardware roots of trust are necessary in many contested environments, but they are not sufficient alone.

The result has direct implications for nano-enabled cybersecurity research. Future PUF evaluation should not stop at uniqueness and reliability metrics. It should connect device-level entropy to system-level security outcomes: secure boot, supply-chain attestation, key derivation, tamper-evidence, certificate provisioning and audit logs. For DefenceTech, FinTech and SpaceTech, the most valuable nano-enabled systems will be those that produce verifiable assurance evidence across the lifecycle rather than only impressive laboratory entropy measurements.

4.5 Feasibility, sensitivity and governance readiness

Table 4.6 reports the sensitivity of residual risk to QKD weighting in the model. Mean residual risk rises when QKD is overweighted across all scenarios because several financial and device-centred systems have lower QKD feasibility than PQC or nano-PUF feasibility. This does not weaken the case for QKD on eligible high-value channels; it shows that QKD must be allocated selectively rather than imposed as a universal control. Hybrid PQC remains essential because most real systems still require classical authentication, digital signatures, certificates, software updates and broad interoperability.

Table 4.6. Sensitivity of mean residual risk to QKD model weighting.

QKDWeight	MeanResidualRisk
0.15	31.79
0.2	32.31
0.25	32.84
0.3	33.37
0.35	33.89
0.4	34.42
0.45	34.94
0.5	34.76

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright © 2026
Location: Delhi India
Date: June 2026

Interpretation of Table 4.6: increasing the weight assigned to QKD feasibility raises the modelled mean residual risk in this heterogeneous portfolio because QKD is not equally feasible in every scenario. This indicates that QKD has meaningful value where feasible, while PQC and hardware trust remain necessary because many residual risks are endpoint, governance or supply-chain problems rather than only key-distribution problems.

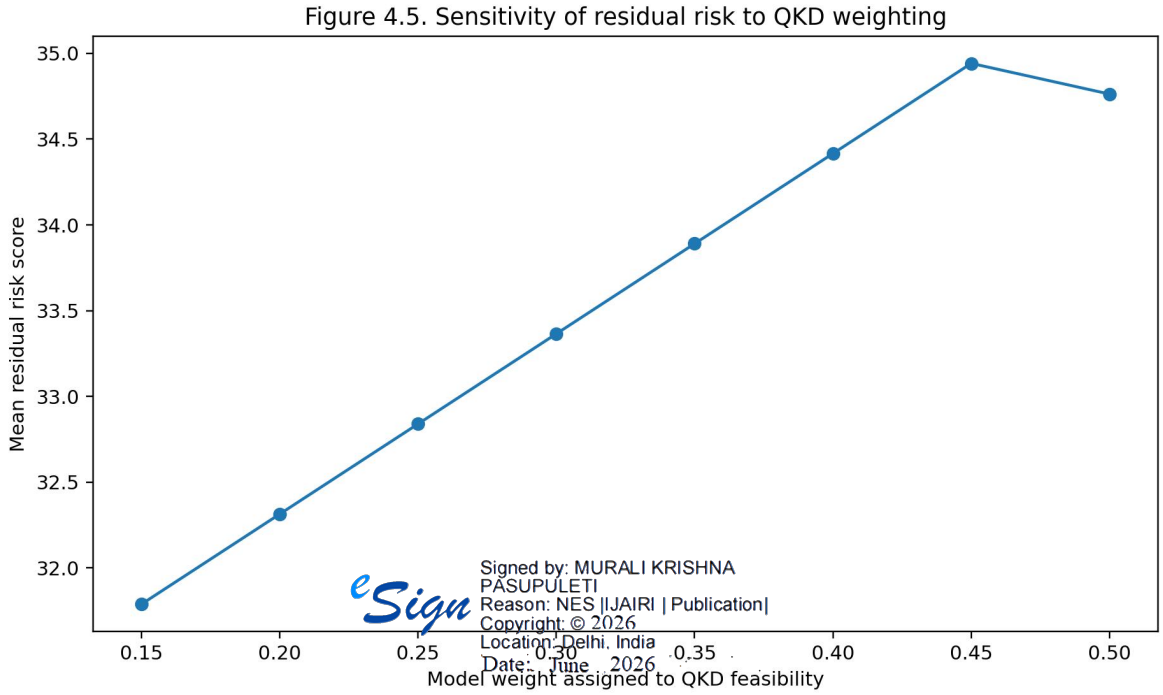


Figure 4.5. Sensitivity of mean residual risk to QKD weighting across heterogeneous scenarios.

Figure 4.5 visualizes this sensitivity curve. The upward slope indicates that excessive QKD emphasis can raise portfolio-level residual risk when the model is applied to heterogeneous assets rather than only to long-lived fixed links. The residual risk persists because QKD cannot remove endpoint compromise, insider threats, supply-chain manipulation or flawed integration. This result supports a disciplined policy message: quantum communications are powerful when targeted, but they must be embedded within cyber-resilience governance and combined with PQC and hardware trust.

The feasibility analysis also highlights governance readiness. A mature quantum-safe programme requires cryptographic inventories, algorithm-agility roadmaps, standards tracking, procurement requirements, testing laboratories, certification criteria, incident-response updates and cross-sector coordination. Without these governance mechanisms, advanced quantum and nano technologies could become fragmented demonstrations rather than reliable infrastructure. The framework therefore recommends that technology adoption be accompanied by institutional assurance mechanisms from the beginning.

5. Discussion, Conclusion and Outlook

5.1 Discussion of findings and alternative interpretations

The results support a layered interpretation of quantum-era cybersecurity. The strongest generalizable finding is that PQC migration should be treated as the near-term baseline because it can be implemented through software, protocol and certificate ecosystems. This does not make QKD unnecessary. It means QKD should be targeted toward high-value channels where its physical security properties, infrastructure cost and operational constraints are justified. Nano-enabled roots of trust should be targeted toward exposed devices and critical supply chains where physical compromise is credible. The framework therefore replaces a technology competition narrative with a portfolio-governance narrative.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright © 2026
Location: Delhi, India
Date: June 2026

An alternative interpretation is that QKD's infrastructure burden makes it marginal outside national-security and critical-infrastructure niches. The model partly supports this caution in FinTech scenarios that require flexible routing and extremely low latency. However, it does not support dismissing QKD entirely. Space-based quantum communication, EuroQCI-style infrastructure and sovereign data-centre interconnects illustrate use cases where QKD can complement PQC and strengthen long-lived confidentiality. The appropriate conclusion is not universal adoption, but selective deployment based on topology, data lifetime and institutional risk appetite.

A second alternative interpretation is that nano-PUFs remain too experimental for strategic planning. The study acknowledges that reliability, enrolment security and modelling resistance remain open engineering concerns. Yet the device-trust problem is already present in satellites, unmanned systems, payment terminals and hardware security modules. Ignoring nano-enabled roots of trust would leave a gap between cryptographic protocol security and physical device compromise. The framework therefore treats nano-PUFs as an emerging but strategically important layer that should be piloted with careful assurance metrics.

5.2 Global framework for DefenceTech, FinTech and SpaceTech

The global framework proposed by this study consists of six layers. The first layer is asset and data-lifetime classification, because quantum risk is meaningless without knowing how long secrecy and authenticity must survive. The second layer is

cryptographic inventory and debt remediation, which identifies legacy algorithms, certificates, libraries and embedded dependencies. The third layer is hybrid PQC migration, prioritizing ML-KEM for key establishment and post-quantum signatures for authenticity where standards and interoperability permit. The fourth layer is selective QKD or quantum communication deployment for high-value links. The fifth layer is nano-enabled device attestation for hardware roots of trust. The sixth layer is governance, certification and incident-response integration.

For DefenceTech, the framework recommends sovereign crypto-agile backbones, QKD pilots on high-classification fixed links, nano-PUF attestation for field devices, and alliance-level interoperability standards. For FinTech, it recommends sector-wide cryptographic inventories, hybrid PQC pilots in payment APIs and identity systems, hardware-secured signing services, and selective QKD for central-bank or data-centre interconnects. For SpaceTech, it recommends PQC-secured command authentication, quantum-safe software-update chains, satellite/ground QKD demonstrations, and hardware roots of trust for mission-critical components and ground terminals.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: [illegible] 2026

The framework also requires international coordination. Quantum-safe cybersecurity crosses borders because defence coalitions, global finance and satellite services depend on shared protocols and mutual trust. Standards bodies, regulators, procurement authorities and security agencies must therefore align terminology, certification expectations and transition timelines. Without such coordination, one sector's quantum-safe readiness may be undermined by a supplier, partner or network node that remains cryptographically obsolete.

5.3 Limitations, validation status and research integrity

The main limitation is the use of public-source calibrated realistic data rather than confidential operational datasets. This limitation is intentional and ethically appropriate. Critical infrastructure operators rarely disclose detailed asset vulnerabilities, key-management designs, incident costs or satellite command architectures. The dataset is therefore best understood as a transparent modelling instrument for research design and policy reasoning. It should not be read as a measurement of any particular organization.

A second limitation concerns weights and scoring. Although the weights are justified by domain logic, they remain assumptions. Sensitivity analysis reduces but does not

eliminate this concern. Future studies should estimate weights using expert elicitation, Bayesian updating, operational incident data, red-team results, QKD testbed measurements and PQC benchmark evidence. Similarly, financial estimates should be refined with sector-specific loss distributions rather than a single public breach-cost anchor.

Research integrity is maintained through explicit labelling, transparent equations and clear separation between public evidence and constructed scenario values. No fabricated source is presented as real operational measurement. The study also avoids overstating the maturity of QKD and nano-PUF deployment. Quantum-safe security is presented as a staged transition requiring standards, engineering, governance and verification, not as a single breakthrough product.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

5.4 Conclusion and outlook

This study concludes that quantum cryptography, quantum communications and nano-enabled cybersecurity should be integrated into a global framework for DefenceTech, FinTech and SpaceTech. PQC provides the most immediate and scalable foundation for quantum-safe migration. QKD provides high-assurance value for selected long-lived and strategically sensitive communication paths. Nano-enabled physical roots of trust strengthen device identity, supply-chain assurance and tamper resistance in physically exposed environments. The combined architecture reduces residual risk more credibly than any single technology pathway.

The results show that baseline quantum-cyber risk is highest where long-lived secrets, critical missions and cryptographic debt converge. Defence command systems, digital identity vaults, satellite command links and GNSS timing services require early attention. The realistic dataset and figures demonstrate that integrated controls can materially reduce risk, but residual exposure remains when endpoints, governance and supply chains are weak. This is a crucial conclusion: quantum-safe cryptography must be connected to operational cyber resilience rather than deployed as an isolated upgrade.

Further work should replace the realistic dataset with real organizational data under appropriate security controls. Priority research areas include PQC benchmarks for constrained space and edge devices, interoperable QKD key-management APIs, satellite-QKD operational testing, nano-PUF reliability under environmental stress,

and machine-verifiable assurance cases for quantum-safe architectures. The long-term outlook is a hybrid security ecosystem in which mathematical hardness, quantum physics, nanoscale entropy and governance verification operate together. Such an ecosystem is essential for protecting defence operations, financial trust and space-based infrastructure in the quantum era.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

References :

Allianz (2026) Allianz Risk Barometer 2026. Munich: Allianz Commercial.

Arapinis, M., Delavar, M., Doosti, M., Kashefi, E., Mardani, M. and Wallden, P. (2021) 'Quantum physical unclonable functions: possibilities and impossibilities', Quantum, 5, Article 475. doi:10.22331/q-2021-06-15-475.

Bennett, C.H. and Brassard, G. (1984) 'Quantum cryptography: public key distribution and coin tossing', Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179.

Bennett, C.H., Brassard, G. and Ekert, A.K. (1992) 'Quantum cryptography', Scientific American, 267(4), pp. 50-57.

Cao, Y., Zhang, L., Sun, X. and Wang, H. (2023) 'Advances in physical unclonable functions based on new materials and emerging devices', Mathematics, 12(1), Article 77.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright © 2026
Location: Delhi, India
Date: June 2026

CISA (2025) Post-Quantum Cryptography Initiative. Washington, DC: Cybersecurity and Infrastructure Security Agency.

Danai-Varsou, D, Zhang, P, Afantitis, A, Guo, Z, Lynch, I & Melagraki, G 2023, 'Nanoinformatics and artificial intelligence for nano-enabled sustainable agriculture', Nano-Enabled Sustainable and Precision Agriculture, pp. 503–531, doi:10.1016/b978-0-323-91233-4.00015-6.

Darwish, SM, El-Naggar, S & Elkaffas, SM 2026, 'Securing financial transactions: exploring the role of lightweight blockchain-enabled deep learning for fraud detection in FinTech systems', Cybersecurity, vol. 9, no. 1, doi:10.1186/s42400-025-00436-8.

Dunn, PJ, Pourzahedi, L, Theis, TL & Gilbertson, LM 2023, 'Thinking in systems: sustainable design of nano-enabled agriculture informed by life cycle assessment', Nano-Enabled Sustainable and Precision Agriculture, pp. 461–491, doi:10.1016/b978-0-323-91233-4.00019-3.

Ekert, A.K. (1991) 'Quantum cryptography based on Bell's theorem', Physical Review Letters, 67(6), pp. 661-663.

ENISA (2025) ENISA Threat Landscape 2025. Athens: European Union Agency for Cybersecurity.

ESA (2025a) Eagle-1: Quantum key distribution satellite project. Paris: European Space Agency.

ESA (2025b) ESA and European Commission to build quantum-secure space communications network. Paris: European Space Agency.

ETSI (2025) Industry Specification Group on Quantum Key Distribution and quantum-safe standardization materials. Sophia Antipolis: European Telecommunications Standards Institute.

European Commission (2025a) European Quantum Communication Infrastructure - EuroQCI. Brussels: European Commission.

European Commission (2025b) Commission and European Space Agency sign EuroQCI implementation agreement. Brussels: European Commission.

Fong, M.J., Robinson, B.J., Speed, P. and Young, R.J. (2022) 'Using intrinsic properties of quantum dots to provide additional security when uniquely identifying devices', Scientific Reports, 12, Article 16331. doi:10.1038/s41598-022-20596-8.

Gao, Y., Ranasinghe, D.C., Al-Sarawi, S.F., Kavehei, O. and Abbott, D. (2016) 'Emerging physical unclonable functions with nanotechnology', IEEE Access, 4, pp. 61-80. doi:10.1109/ACCESS.2015.2499629.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Gilbert, C & Gilbert, MA 2024, ‘The Role of Quantum Cryptography in Enhancing Cybersecurity’, International Journal of Research Publication and Reviews, vol. 5, no. 11, pp. 889–907, doi:10.55248/gengpi.5.1124.3135.

Hu, Y.W., Cao, Q., Song, S.Y. et al. (2025) 'Time-dependent physical unclonable functions by long-lived triplet excitons in carbon dots', Light: Science & Applications, 14, Article 283. doi:10.1038/s41377-025-01940-9.

Hui, X & Guo, H 2024, ‘Advances in cardiac sounds monitoring enabled by triboelectric sensors’, Nano Trends, vol. 8, p. 100057, doi:10.1016/j.nwnano.2024.100057.

Hybrid Quantum-Classical Communication Networks: New Directions in Cybersecurity 2024, Nanotechnology Perceptions, vol. 20, no. S12, doi:10.62441/nano-ntp.v20is12.45.

IBM (2025) Cost of a Data Breach Report 2025. Armonk, NY: IBM Security and Ponemon Institute.

ITU-T (2020) Recommendation Y.3800: Overview on networks supporting quantum key distribution. Geneva: International Telecommunication Union.

ITU-T (2025a) Recommendation Y.3804: Quantum key distribution networks - Control and management. Geneva: International Telecommunication Union.

ITU-T (2025b) Recommendation Y.3828: Integration of quantum key distribution network and user network supporting end-to-end modern cryptography services. Geneva: International Telecommunication Union.

Julia Farre, P., Galetsky, V., Belhassen, M., Pieplow, G., Nilesh, K., Boche, H., Schroder, T., Notzel, J. and Deppe, C. (2026) 'Secure authentication via quantum physical unclonable functions: a review', Advanced Quantum Technologies, Article 202500648. doi:10.1002/qute.202500648.

Kiam, K & Tsombeng, A 2025, 'Building Resilient Fintech Ecosystems: Integrating Symbiotic AI and Quantum-Adaptive Cryptography', International Journal of Science and Research, vol. 14, no. 1, pp. 1202–1204, doi:10.21275/sr25126105749.

Kim, K., Moon, Y., Kim, Y.K. et al. (2025) 'Optical physical unclonable functions based on Foerster resonant energy transfer in multi-color quantum dots', Communications Materials, 6, Article 270. doi:10.1038/s43246-025-00984-z.

Kolawole, TA & Olowolaju, KO 2024, 'The Role of Quantum Cryptography in Cybersecurity: Safeguarding Data in the Age of Quantum Computing', International Journal of Research Publication and Reviews, vol. 5, no. 10, pp. 1882–1894, doi:10.55248/gengpi.5.1024.2807.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NESIIJAIRI Publication
Copyright © 2026
Location: Delhi, India
Date: June 2026

Liao, S.-K. et al. (2017) 'Satellite-to-ground quantum key distribution', Nature, 549, pp. 43-47. doi:10.1038/nature23655.

Lo, H.-K., Curty, M. and Tamaki, K. (2014) 'Secure quantum key distribution', Nature Photonics, 8, pp. 595-604. doi:10.1038/nphoton.2014.149.

Longmate, K.D., Abdelazim, N.M., Ball, E.M., Majaniemi, J. and Young, R.J. (2021) 'Improving the longevity of optically-read quantum dot physical unclonable functions', Scientific Reports, 11, Article 10999. doi:10.1038/s41598-021-90129-2.

Mahdian, M.A., Taheri, E., Rahbardar Mojaver, K. and Nikdast, M. (2024) 'Hardware assurance with silicon photonic physical unclonable functions', Scientific Reports, 14, Article 25591. doi:10.1038/s41598-024-72922-x.

Mishra, P., et al. (2025) 'Advances in semiconductor quantum dot-based physical unclonable functions for enhanced security applications', Nanoscale, 17. doi:10.1039/D5NR03356J.

NATO (2024) Summary of NATO's Quantum Technologies Strategy. Brussels: North Atlantic Treaty Organization.

NIST (2024a) FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard. Gaithersburg, MD: National Institute of Standards and Technology.

NIST (2024b) FIPS 204: Module-Lattice-Based Digital Signature Standard. Gaithersburg, MD: National Institute of Standards and Technology.

NIST (2024c) FIPS 205: Stateless Hash-Based Digital Signature Standard. Gaithersburg, MD: National Institute of Standards and Technology.

NIST NCCoE (2025) Migration to Post-Quantum Cryptography. Gaithersburg, MD: National Cybersecurity Center of Excellence.

Pan, L., Wei, Y., Wang, J. and Ma, X. (2026) 'Architected nanomaterials powering optical physical unclonable functions', Laser & Photonics Reviews, 20, Article 202501958. doi:10.1002/lpor.202501958.

Park, T., Kim, J., Ko, R. et al. (2025) 'Light in, sound keys out: photoacoustic PUFs from stochastic nanocomposites', Nature Communications, 16, Article 7323. doi:10.1038/s41467-025-62747-1.

Pasupuleti, MK 2021a, 'A Control-Theoretic Framework for AI Safety: Stability, Robustness, and Assurance', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 01, National Education Services, pp. 303–315, doi:10.62311/nesx/rp-1-06-2021.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Pasupuleti, MK 2021b, 'Hierarchical OR + RL Control for Cloud and Network Operations Under Policy-as-Code Constraints', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 12, National Education Services, pp. 99–123, doi:10.62311/nesx/rp-m5-dec-2021.

Pasupuleti, MK 2021c, 'Operations Research Challenges in Energy-Efficient Cloud and Network Infrastructure: An Integrated AI–Simulation Perspective', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 12, National Education Services, pp. 1–25, doi:10.62311/nesx/rp-m1-dec-2021.

Pasupuleti, MK 2021d, 'Quantum-Safe Accounting and Finance: Threats, Standards, and Secure System Design for the Post-Quantum Era', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 01, National Education Services, pp. 288–302, doi:10.62311/nesx/rp-1-05-2021.

Pasupuleti, MK 2021e, 'Quantum-Safe Network Security: Advances in Quantum Cryptography and Systems Integration', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 01, National Education Services, pp. 232–245, doi:10.62311/nesx/rp-1-01-2021.

Pasupuleti, MK 2021f, 'Stochastic Optimization Models for Energy-Aware Cloud Resource Allocation Using Simulation-Derived Scenarios', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 12, National Education Services, pp. 51–75, doi:10.62311/nesx/rp-m3-dec-2021.

Pasupuleti, MK 2021g, 'Verifying Autonomous Mobile Robots with Quantum Machine Learning Test Oracles', International Journal of Academic and Industrial Research Innovations, vol. 01, no. 01, National Education Services, pp. 259–272, doi:10.62311/nesx/rp-1-03-25.

Pasupuleti, MK 2022a, 'Policy-as-Code in Cloud Governance: Impacts of Cloud Custodian on Cost, Compliance, and Managerial Control', International Journal of Academic and Industrial Research Innovations, vol. 02, no. 12, National Education Services, pp. 29–52, doi:10.62311/nesx/rp-m2-dec-2022.

Pasupuleti, MK 2023a, 'Edge AI with Mosquitto: Secure, QoS-Aware Federated Anomaly Detection', International Journal of Academic and Industrial Research Innovations, vol. 03, no. 06, National Education Services, pp. 195–210, doi:10.62311/nesx/rp-30623-195-210.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Pasupuleti, MK 2023b, 'NS-3 for 6G: Multi-Agent RL Slicing with eBPF Telemetry', International Journal of Academic and Industrial Research Innovations, vol. 03, no. 06, National Education Services, pp. 162–177, doi:10.62311/nesx/rp-30623-162-177.

Pasupuleti, MK 2023c, 'QML for Edge Anomaly Detection: Variational Circuits on MQTT/NS-3 Stream', International Journal of Academic and Industrial Research Innovations, vol. 03, no. 12, National Education Services, pp. 174–188, doi:10.62311/nesx/rp-301223-174-188.

Pasupuleti, MK 2023d, 'Secure Intelligent Systems: Post-Quantum Cryptography and Topological Modeling for Big Data Robotics', International Journal of Academic and Industrial Research Innovations, vol. 03, no. 01, National Education Services, pp. 18–31, doi:10.62311/nesx/rp-2-jan-2023.

Pasupuleti, MK 2024a, '6G Security and Vendor Governance: Indian States versus G20 and BRICS Risk Controls', National Education Services, doi:10.62311/nesx/rrvii3d24.

Pasupuleti, MK 2024b, 'Cross-Layer Optimisation of Network and Cloud Resources: A Joint NS-3 and CloudSim Simulation Study', International Journal of Academic and Industrial Research Innovations, vol. 04, no. 12, National Education Services, pp. 131–151, doi:10.62311/nesx/rp-dec-d7-2024.

Pasupuleti, MK 2024c, 'Cyber Integrity of Climate MRV And Satellite Pipelines: Indian States vs G20 And BRICS', National Education Services, doi:10.62311/nesx/rrix3d24.

Pasupuleti, MK 2024d, 'Cybersecure Digital Services: State-Level Cybersecurity Readiness in India's IT–ITES Sector Compared to G20 and BRICS Archetype', National Education Services, doi:10.62311/nesx/rrxii3d24.

Pasupuleti, MK 2024e, 'Policy-Aware Cloud Control Loops: Integrating MQTT Telemetry with Cloud Custodian for Safe RL-Based Resource Management', International Journal of Academic and Industrial Research Innovations, vol. 04, no. 12, National Education Services, pp. 152–172, doi:10.62311/nesx/rp-dec-d8-2024.

Pasupuleti, MK 2024f, 'Quantum Communication And QKD Readiness: Indian State Pilot Zones Compared with G20 And BRICS', National Education Services, doi:10.62311/nesx/rrvii2d24.

Pasupuleti, MK 2024g, 'Quantum Finance Readiness: India's State Innovation Clusters Benchmarked to G20 And BRICS', National Education Services, doi:10.62311/nesx/rriii2d24.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NESS/IJAIRI | Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Pasupuleti, MK 2024h, 'Quantum Innovation Readiness in India's IT–ITES States: A Comparative Benchmarking with G20 and BRICS Technology Leaders', National Education Services, doi:10.62311/nesx/rrxii2d24.

Pasupuleti, MK 2024i, 'State-Level Digital Payments Cyber Maturity: India vs G20 And BRICS Risk Architectures', National Education Services, doi:10.62311/nesx/rriii3d24.

Pasupuleti, MK 2024j, 'State-Level Quantum Innovation Policy: India Benchmarked to G20 And BRICS National Playbooks', National Education Services, doi:10.62311/nesx/rrpsx2d24.

Pasupuleti, MK 2024k, 'Whole-of-State Cyber Maturity: Indian States vs G20 And BRICS Institutional Models', National Education Services, doi:10.62311/nesx/rrpsx4d24.

Pasupuleti, MK 2025a, 'Edge Tensor-AI Enabled Predictive Control of Self-Healing Anti-Corrosion Coatings for Marine Robots', International Journal of Academic and Industrial Research Innovations, vol. 05, no. 12, National Education Services, pp. 291–313, doi:10.62311/nesx/rp-dp1325.

Pasupuleti, MK 2025b, 'Fault-Tolerant Quantum Computing via Macroscopic Quantum Tunnelling in Superconducting Circuits', International Journal of Academic and Industrial Research Innovations, vol. 05, no. 12, National Education Services, pp. 1–21, doi:10.62311/nesx/rp-dec-p1-2025.

Pasupuleti, MK 2025c, 'Quantum-Accelerated Intelligence: Hybrid AI Systems for National-Scale Advantage', International Journal of Academic and Industrial Research Innovations, vol. 05, no. 12, National Education Services, pp. 22–49, doi:10.62311/nesx/rp-dp225.

Pasupuleti, MK 2025d, 'Quantum-Limited Sensing-to-Action for GPS-Denied Navigation in Autonomous Robots', International Journal of Academic and Industrial Research Innovations, vol. 05, no. 12, National Education Services, pp. 264–290, doi:10.62311/nesx/rp-dp1225.

Pasupuleti, MK 2025e, 'Secure Computation After Quantum: PQC, Confidential Clouds, and Policy-Grade Auditability', International Journal of Academic and Industrial Research Innovations, vol. 05, no. 12, National Education Services, pp. 198–222, doi:10.62311/nesx/rp-dp925.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES |IJAIRI | Publication|
Copyright: © 2026
Location: Delhi, India
Date: 7 June 2026

Pasupuleti, MK 2026a, 'A Unified Topological and Tensor Framework for Interpretable AI in Networks, Fraud, and Power Systems', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 04, pp. 166–198, doi:10.62311/nesx/rp7-30042026.

Pasupuleti, MK 2026b, 'Algebraic Quantum-AI Co-Design of Energy-Adaptive Semiconductor Architectures for Edge Intelligence and Neuromorphic Computing', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 04, pp. 32–62, doi:10.62311/nesx/rp2-30042026.

Pasupuleti, MK 2026c, 'Cross-Sector Cascade Resilience in the Post-Quantum Transition: Coupled-Network Theorems and Stress-Testing Algorithms for Finance–Telecom–Industrial Control Systems (ICS)', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 01, National Education Services, pp. 1–23, doi:10.62311/nesx/rp-j12026.

Pasupuleti, MK 2026d, 'Disaster Digital Twins: AI World Models for Predicting Cascading Infrastructure Failures', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 02, National Education Services, pp. 1–21, doi:10.62311/nesx/rp-f12026.

Pasupuleti, MK 2026e, 'Mechanism Design for Systemic Post-Quantum Cyber Risk: Incentive-Compatible Adoption, Equilibrium Guarantees, and Policy-Grade Algorithms', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 01, National Education Services, pp. 24–58, doi:10.62311/nesx/rp-j22026.

Pasupuleti, MK 2026f, 'Neuromorphic Photonic Memories based on Nanostructured Optoelectronic Devices for Ultrafast', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 05, pp. 81–111, doi:10.62311/nesx/rp4-30052026.

Pasupuleti, MK 2026g, 'Photonic-Interconnected Quantum Chiplets for Modular and Networked Quantum Computing', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 05, pp. 264–300, doi:10.62311/nesx/rp9-30052026.

Pasupuleti, MK 2026h, 'Photonic Quantum Computing and Quantum Topological Data Analysis: A DeepTech Landscape for HealthTech, ClimateTech and FinTech', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 06, pp. 170–217, doi:10.62311/nesx/rpj5-30062026.

Pasupuleti, MK 2026i, 'Quantum-AI Models for Real-Time Cybersecurity Threat Detection and Adaptive Defense', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 05, pp. 1–35, doi:10.62311/nesx/rp1-30052026.

Pasupuleti, MK 2026j, 'Quantum-AI Number-Theoretic Frameworks for Post-Quantum Cryptography and Long-Term Information Security', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 05, pp. 36–55, doi:10.62311/nesx/rp2-30052026.

Pasupuleti, MK 2026k, 'Quantum Machine Learning for Accelerated Discovery of Functional Materials and Secure Cryptographic Systems', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 05, pp. 56–80, doi:10.62311/nesx/rp3-30052026.

Pasupuleti, MK 2026l, 'Quantum-Safe Critical Infrastructure: Post-Quantum Migration and Verification Frameworks', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 02, National Education Services, pp. 22–48, doi:10.62311/nesx/rp-f22026.

Pasupuleti, MK 2026m, 'Quantum-Safe Cyber-Defence for Financial Infrastructure: A Public Policy Evaluation Framework for Post-Quantum Cryptography and Quantum Communications', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 06, pp. 130–169, doi:10.62311/nesx/rpj4-30062026.

Pasupuleti, MK 2026n, 'Satellite-Based Carbon MRV: Remote Sensing and Atmospheric Inference for Verifiable Carbon Removal', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 02, National Education Services, pp. 142–165, doi:10.62311/nesx/rp-f82026.

eSign
Signed by: MURALI KRISHNA PASUPULETI
Reason: NES | IJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: June 2026

Pasupuleti, MK 2026o, 'Topological Quantum Error Correction with Tensor-Network Optimization for Scalable Photonic Quantum Computing Architectures', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 06, pp. 1–35, doi:10.62311/nesx/rpj1-30062026.

Pasupuleti, MK 2026p, 'Ultra-Low-Power Edge Intelligence: Green AI Algorithms and Hardware Co-Design', International Journal of Academic and Industrial Research Innovations, vol. 06, no. 02, National Education Services, pp. 119–141, doi:10.62311/nesx/rp-f62026.

Pirandola, S. et al. (2020) 'Advances in quantum cryptography', Advances in Optics and Photonics, 12(4), pp. 1012-1236. doi:10.1364/AOP.361502.

References :

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NESIIJAIRI Publication
Copyright: © 2026
Location: Delhi, India
Date: 1 June 2026

Sandomirskii, M., Petrova, E., Kuptsov, I., et al. (2025) 'Spectral physical unclonable functions: downscaling randomness with multi-resonant hybrid particles', Nature Communications, 16, Article 5097. doi:10.1038/s41467-025-60121-9.

Sarantoglou, G., Tzekas, N., Moustakas, G., Karydis, G.A., Kaminski, V., Protsenko, E., Gradkowski, K., Bazin, A., Vigliar, C., Bogris, A. and Mesaritakis, C. (2026) 'Quantum-secure physical unclonable function enabled by silicon photonics integrated circuits', arXiv preprint, arXiv:2605.14959.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dusek, M., Lutkenhaus, N. and Peev, M. (2009) 'The security of practical quantum key distribution', Reviews of Modern Physics, 81(3), pp. 1301-1350. doi:10.1103/RevModPhys.81.1301.

Seo, H., Park, T., Ali, A., Jung, B.K., Choi, Y.K., Park, J. and Oh, S.J. (2025) 'Quantum dots and perovskites-based physically unclonable functions for binary and ternary keys via optical-to-electrical conversion', Advanced Functional Materials, Article 2507395. doi:10.1002/adfm.202507395.

Sessler, C, Huang, Z, Wang, X & Liu, J 2021, 'Functional nanomaterial-enabled synthetic biology', Nano Futures, vol. 5, no. 2, p. 022001, doi:10.1088/2399-1984/abfd97.

Shadan, HH & Islam, SMN 2025, 'Quantum Computing and Cybersecurity in Accounting and Finance in the Post-Quantum World: Challenges and Opportunities for Securing Accounting and Finance Systems', FinTech, vol. 4, no. 4, p. 52, doi:10.3390/fintech4040052.

Shi, J, Clayton, C & Tian, B 2019, 'Nano-enabled cellular engineering for bioelectric studies', Nano Research, vol. 13, no. 5, pp. 1214–1227, doi:10.1007/s12274-019-2580-8.

Shor, P.W. (1994) 'Algorithms for quantum computation: discrete logarithms and factoring', Proceedings 35th Annual Symposium on Foundations of Computer Science, pp. 124-134. doi:10.1109/SFCS.1994.365700.

Sun, N., Chen, Z., Wang, Y. et al. (2023) 'Random fractal-enabled physical unclonable functions with dynamic AI authentication', Nature Communications, 14, Article 2185. doi:10.1038/s41467-023-37588-5.

Wang, K., Shi, J., Lai, W. et al. (2024) 'All-silicon multidimensionally encoded optical physical unclonable functions for integrated circuit anti-counterfeiting', Nature Communications, 15, Article 1033. doi:10.1038/s41467-024-54966-w.

eSign Signed by: MURALI KRISHNA PASUPULETI
Reason: NESIJAIRI Publication
Copyright © 2026
Location: Delhi, India
Date: June 2026

William, P, Pawar, AB & Jawale, MA 2023, 'Quantum Cryptography for the Future Internet and the Security Analysis', Quantum Computing in Cybersecurity, pp. 175–188, doi:10.1002/9781394167401.ch10.

World Economic Forum (2024) Quantum Economy Blueprint. Geneva: World Economic Forum.

Xu, F., Ma, X., Zhang, Q., Lo, H.-K. and Pan, J.-W. (2020) 'Secure quantum key distribution with realistic devices', Reviews of Modern Physics, 92(2), 025002. doi:10.1103/RevModPhys.92.025002.

Yin, J. et al. (2017) 'Satellite-based entanglement distribution over 1200 kilometres', Science, 356(6343), pp. 1140-1144. doi:10.1126/science.aan3211

Zeng, L, An, Y, Zhou, H, Luo, Q, Lin, Y & Dai, B 2024, 'A Hybrid Machine Learning-based Data-Centric Cybersecurity Detection in the 5G-Enabled IoT', doi:10.22541/au.172547412.20950209/v1.