Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 3, Issue 12, 2025

A FAULT-TOLERANT ADAPTIVE CRYPTOGRAPHIC FRAMEWORK FOR RELIABLE COMMUNICATION IN HYBRID QUANTUM-CLASSICAL ENVIRONMENTS

Imdad Ali Shah[*1], Abdul Wahab Khan[2], Ghulam Qasim[3], Ejaz Ahmed[4], Muhammad Tahir[5]

[*1,2,3,4,5]*Department of Computer Science, Faculty of Engineering, Science and Technology (FEST), Iqra University Main Campus, Defence View Karachi City 75500 – Sindh, Pakistan*

[5]muhammad.tahir01@iqra.edu.pk

DOI: https://doi.org/10.5281/zenodo.18051574

Keywords
Fault-Tolerant Systems, Post-Quantum Cryptography, Hybrid Cryptographic Systems, Secure Communication, Quantum Threat Resilience

Article History
Received: 26 October 2025
Accepted: 11 December 2025
Published: 25 December 2025

Corresponding Author: *
Imdad Ali Shah

Abstract
Quantum computing poses a significant threat to contemporary cryptographic systems, particularly during the transitional phase where classical and post-quantum cryptographic algorithms coexist. Existing research has extensively analyzed the theoretical risks associated with quantum attacks; however, limited attention has been given to the engineering resilience of cryptographic systems under partial failure conditions. This paper addresses this limitation by proposing a fault-tolerant adaptive cryptographic framework designed to maintain secure communication in hybrid quantum–classical environments. The proposed framework introduces redundancy-aware encryption layers, adaptive algorithm switching, and failure detection mechanisms that respond dynamically to cryptographic degradation, key compromise, or partial quantum attacks. Unlike purely cryptographic or policy-oriented approaches, this study focuses on system-level reliability and engineering robustness. A simulation-based evaluation is conducted to analyze system behavior under multiple failure scenarios, including algorithm compromise and key exposure events. The results demonstrate that the proposed framework significantly improves communication continuity, reduces system downtime, and preserves security guarantees during transitional quantum threat conditions. This work contributes an engineering-focused solution that bridges the gap between theoretical quantum threat analysis and practical, fault-tolerant cryptographic system design, providing a resilient pathway toward secure communication in the quantum era.

INTRODUCTION

1.1 Background and Motivation

Cryptographic systems form the backbone of secure digital communication, ensuring confidentiality, integrity, and authentication across financial platforms, governmental infrastructures, cloud services, and personal communication systems. Classical cryptographic algorithms such as RSA, Elliptic Curve Cryptography, and Advanced Encryption Standard have remained secure under classical computational assumptions for decades. However, the rapid advancement of quantum computing fundamentally challenges these assumptions and introduces unprecedented risks to existing cryptographic infrastructures [1,2].

Recent studies indicate that quantum algorithms, particularly Shor's algorithm, have the potential to break widely deployed public-key cryptographic

schemes, while Grover's algorithm weakens symmetric encryption by effectively reducing key strength [1–3]. These developments have accelerated global research efforts in post-quantum cryptography, aiming to design quantum-resistant algorithms capable of withstanding future quantum attacks [4].

Despite progress in post-quantum algorithm design and standardization, real-world deployment is expected to occur gradually. As a result, cryptographic systems will operate for an extended period in **hybrid quantum–classical environments**, where classical and post-quantum algorithms coexist [5,6]. During this transition phase, systems remain vulnerable to partial failures, misconfigurations, and selective algorithm compromise.

1.2 Engineering Problem Context

Most existing research on quantum threats focuses on cryptographic strength, mathematical hardness, and theoretical attack feasibility [2,4]. While such work is essential, it provides limited guidance on how cryptographic systems should behave when encryption components degrade, keys are exposed, or hybrid attack scenarios emerge.

From an engineering perspective, cryptographic systems are not isolated algorithms but components of larger communication infrastructures. Failure of a single cryptographic mechanism can disrupt entire systems, leading to service downtime, data leakage, or cascading failures [7]. Current cryptographic deployments typically lack **fault-tolerant design principles**, assuming perfect algorithmic behavior rather than realistic failure conditions.

Fault tolerance has been extensively studied in distributed systems and safety-critical engineering domains; however, its application to cryptographic system design under quantum-era threats remains limited [8,9]. This gap exposes communication systems to significant operational risk during the quantum transition phase.

1.3 Research Problem

Current cryptographic systems lack fault-tolerant engineering mechanisms to maintain reliable and secure communication during quantum-era transition failures, including partial algorithm compromise, key exposure, and hybrid quantum–classical attack scenarios [1,6].

1.4 Research Objectives

The objectives of this research are as follows:

- To design a **fault-tolerant cryptographic framework** suitable for hybrid quantum–classical environments.
- To enable **adaptive response mechanisms** for partial cryptographic failure and degradation.
- To evaluate system reliability and resilience using **simulation-based quantum-threat scenarios.**

1.5 Research Contributions

This paper makes the following contributions:

- Proposes a **fault-tolerant adaptive cryptographic framework** that enhances communication reliability during quantum transition phases.
- Introduces **engineering-level resilience mechanisms**, including adaptive algorithm switching and redundancy-aware encryption.
- Demonstrates improved system continuity and fault tolerance through **simulation-based evaluation.**

1.6 Paper Organization

The remainder of this paper is structured as follows. **Section II** presents the **related work** and reviews existing research on quantum threats, post-quantum cryptography, and fault-tolerant system design. **Section III** describes the proposed fault-tolerant cryptographic framework and **research methodology**. **Section IV** presents and discusses the simulation-based **results** evaluating system reliability and resilience. Finally, **Section V concludes** the paper and outlines future research directions.

2. Literature Review

The emergence of quantum computing has fundamentally altered assumptions underlying modern cryptographic systems. A significant body of research has analyzed the vulnerability of classical public-key cryptography in the presence of

large-scale quantum computers. Early foundational studies demonstrated that Shor's algorithm can efficiently factor large integers and compute discrete logarithms, directly threatening RSA and elliptic curve–based schemes [1–3]. Similarly, Grover's algorithm reduces the effective security of symmetric encryption, necessitating longer key lengths to preserve security guarantees [4].

In response to these threats, extensive research has been conducted in the field of post-quantum cryptography. Lattice-based, code-based, hash-based, and multivariate cryptographic schemes have been proposed as potential replacements for classical algorithms [5–7]. International standardization efforts, particularly those led by the National Institute of Standards and Technology, have accelerated the evaluation and selection of quantum-resistant algorithms suitable for widespread deployment [6]. While these efforts address algorithmic security, they do not directly consider system-level behavior under partial failure conditions.

Another stream of research focuses on **hybrid cryptographic deployments**, where classical and post-quantum algorithms coexist during transitional periods [8,9]. Hybrid approaches are widely regarded as a practical necessity due to the long lifecycle of cryptographic infrastructure and the cost of immediate migration. However, existing hybrid models typically emphasize cryptographic strength and backward compatibility rather than resilience to failure. These systems often assume correct and uninterrupted operation of all cryptographic components, an assumption that is unrealistic in adversarial and transitional environments.

Fault tolerance has been extensively studied in distributed systems, cloud computing, and safety-critical infrastructures. Techniques such as redundancy, adaptive reconfiguration, and graceful degradation are commonly employed to maintain system availability under component failure [10,11]. Despite their success in other engineering domains, these principles have rarely been integrated into cryptographic system design. Most cryptographic frameworks treat algorithm compromise as a catastrophic failure rather than a condition that can be managed adaptively.

Recent studies have begun to acknowledge the importance of **crypto-agility**, which refers to the ability of systems to switch cryptographic algorithms without significant disruption [12,13]. While crypto-agility improves long-term maintainability, it does not inherently provide fault tolerance. Algorithm switching mechanisms alone are insufficient when failures occur unexpectedly or under active attack conditions, particularly in quantum-transition scenarios.

Furthermore, research on secure communication systems under attack conditions often assumes binary outcomes—either secure or compromised—without considering partial degradation states [14]. This binary perspective limits the ability of systems to maintain operational continuity when some cryptographic elements fail while others remain functional.

Overall, the literature reveals a critical gap between **quantum threat analysis**, **post-quantum algorithm development**, and **engineering resilience**. Existing research offers limited guidance on how cryptographic systems should behave during partial compromise, hybrid failures, or transitional attack scenarios. Addressing this gap requires an engineering-focused approach that integrates fault tolerance, adaptability, and cryptographic resilience into a unified system framework.

Table. 1: Comparison of Existing Work and Proposed Fault-Tolerant Approach.

Focus Area	Approach Type	Fault Tolerance	Adaptivity	Hybrid Quantum–Classical Support
Post-quantum cryptography surveys	Algorithmic analysis [15]	No	No	Partial
Hybrid cryptographic deployment models	Cryptographic design [16]	Limited	No	Yes
Crypto-agile frameworks	System configuration [17]	No	Yes	Partial
Fault tolerance in distributed systems	Engineering models [18]	Yes	Yes	Not addressed
Proposed approach	Fault-tolerant cryptographic framework	Yes	Yes	Yes

2.1 Literature Review Summary

The reviewed literature demonstrates that while quantum threats and post-quantum cryptographic solutions are well studied, the **engineering resilience of cryptographic systems during the quantum transition phase remains largely unexplored**. Existing approaches focus on algorithmic replacement and theoretical security but neglect fault-tolerant system behavior under realistic failure conditions. This gap motivates the development of an adaptive, fault-tolerant cryptographic framework capable of maintaining secure communication in hybrid quantum–classical environments.

3. Research Methodology

This research adopts an **engineering-oriented, design-science methodology** to develop and evaluate a fault-tolerant adaptive cryptographic framework capable of maintaining secure communication during the quantum transition phase. Unlike purely cryptographic or theoretical studies, this methodology emphasizes **system reliability, failure handling, and adaptive behavior** under partial cryptographic compromise. The methodology is structured to ensure **clarity, reproducibility, and practical applicability** in real-world hybrid quantum–classical environments.

3.1 Research Design

The research design follows four sequential phases:

1. Threat and Failure Scenario Identification
2. Fault-Tolerant Framework Design
3. Adaptive Response Modeling
4. Simulation-Based Evaluation

This structured approach ensures that the proposed framework directly addresses real engineering challenges associated with cryptographic degradation rather than idealized attack models.

3.2 System Assumptions and Environment Model

The proposed framework assumes a **hybrid cryptographic environment** in which:

- Classical cryptographic algorithms are partially deployed.
- Post-quantum algorithms are incrementally integrated.
- **Systems may experience**:
  - Partial algorithm compromise
  - Key exposure events
  - Configuration mismatches
  - Transitional quantum-assisted attacks

The communication system is modeled as a layered architecture consisting of application, cryptographic, and transport layers. Fault tolerance is introduced **within and across** cryptographic layers to avoid single points of failure.

3.3 Fault-Tolerant Cryptographic Framework Architecture

The architecture of the proposed framework consists of five core components:

1. Cryptographic Health Monitoring Module
2. Failure Detection Engine
3. Adaptive Algorithm Selection Module
4. Redundancy and Recovery Controller
5. Secure Communication Interface

Each component is designed to operate independently while sharing state information through secure control channels.

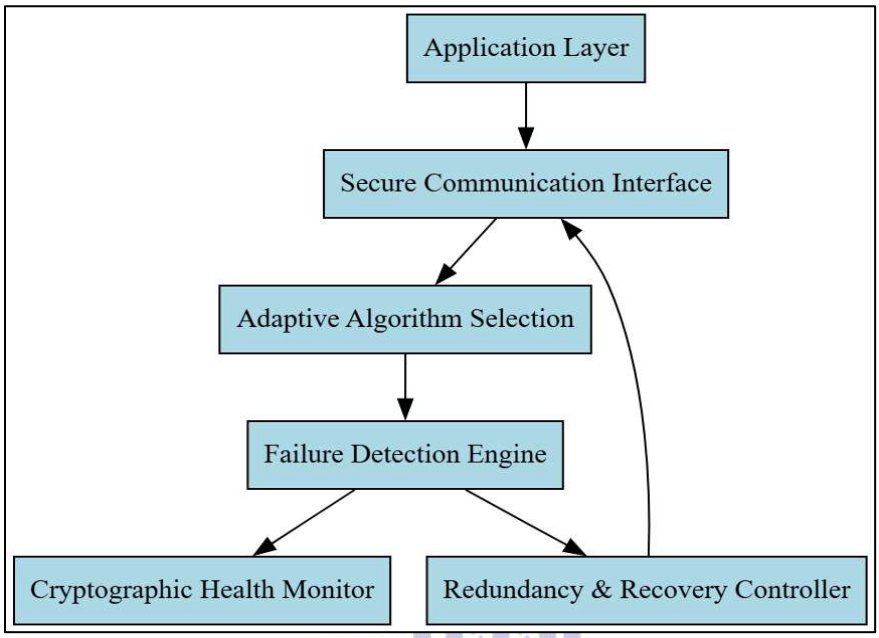

Fig. 1. Architecture of the Proposed Fault-tolerant Cryptographic Framework.

This architecture ensures that cryptographic failures are detected early and mitigated before they propagate to higher system layers.

3.4 Failure Detection and Classification

Failure detection is a critical component of the proposed methodology. The framework continuously monitors cryptographic operations for anomalies such as:

- Unexpected decryption failures
- Authentication mismatches
- Abnormal latency in cryptographic processing
- Key validation inconsistencies

Detected failures are classified into three categories:

- **Transient failures** (temporary disruptions)
- **Degradation failures** (reduced cryptographic strength)
- **Critical failures** (algorithm or key compromise)

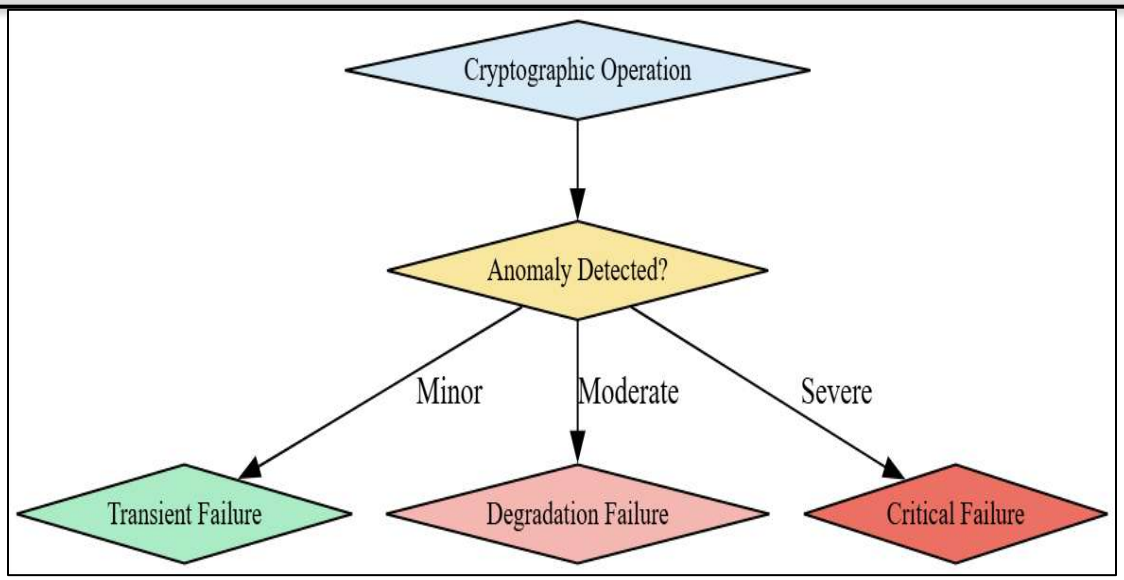

Fig. 2. Failure Detection and Classification Process.

This classification enables the system to respond proportionally rather than triggering unnecessary system-wide reconfiguration.

3.5 Adaptive Algorithm Selection Strategy

Once a failure is classified, the framework activates the adaptive algorithm selection module. This module dynamically selects the most appropriate cryptographic configuration based on:

- Current threat level
- Available cryptographic algorithms
- System performance constraints
- Security policy requirements

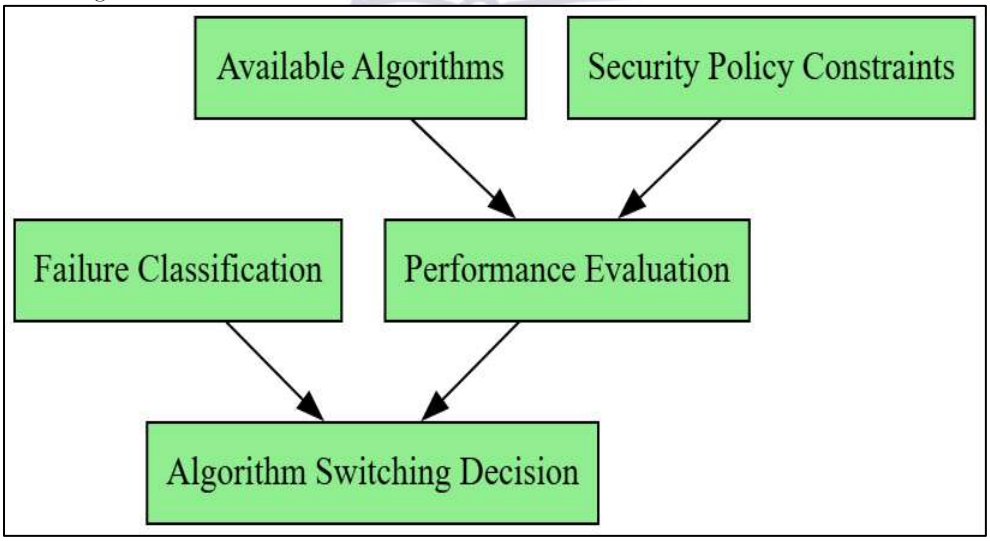

Fig. 3. Adaptive Cryptographic Algorithm Selection Process.

Rather than replacing algorithms blindly, the system evaluates trade-offs between security strength, latency, and resource usage.

This strategy supports **crypto-agility with fault tolerance**, ensuring continuity of secure communication.

3.6 Redundancy and Recovery Mechanism

To prevent communication interruption, the framework employs redundancy mechanisms such as:

- Parallel encryption using backup algorithms
- Redundant key sets
- Graceful degradation of cryptographic strength under controlled policies

Recovery actions are executed incrementally to minimize service disruption.

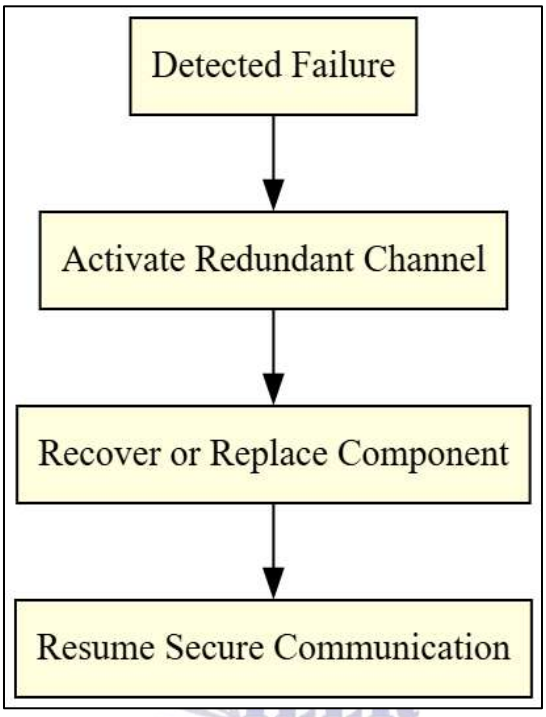

Fig. 4. Redundancy and Recovery Mechanism for Cryptographic Failure Handling.

3.7 Simulation-Based Evaluation Design

The proposed framework is evaluated using simulation-based experiments that model realistic cryptographic failure scenarios, including:

- Partial algorithm compromise
- Key leakage events
- Hybrid quantum–classical attack simulations

Performance metrics include:

- Communication continuity
- Recovery time
- Security preservation level

Simulation parameters are varied systematically to assess robustness under different threat intensities.

3.8 Reproducibility and Engineering Validity

The methodology ensures reproducibility through:

- Modular framework design
- Clearly defined failure categories
- Deterministic adaptation rules
- Scenario-based evaluation models

This design enables other researchers and engineers to replicate and extend the framework in diverse deployment environments.

4. Results and Discussion

This section presents and discusses the simulation-based evaluation of the proposed fault-tolerant adaptive cryptographic framework. The evaluation focuses on system behavior under partial cryptographic failure, recovery performance, and communication resilience during hybrid quantum–classical transition scenarios.

4.1 Simulation Scenario Design

To evaluate the proposed framework, multiple simulation scenarios were designed to model realistic cryptographic failure conditions expected during the quantum transition phase. The simulations compare two systems:

- **Baseline System:** Conventional cryptographic deployment without fault tolerance
- **Proposed System:** Fault-tolerant adaptive cryptographic framework

The scenarios include:

- Partial algorithm compromise
- Key exposure events
- Hybrid quantum–classical attack conditions
- Progressive failure escalation

Performance is evaluated using **engineering-level metrics**, including:

- Recovery time
- Communication continuity
- Failure containment effectiveness
- System resilience

4.2 System Behavior Under Partial Cryptographic Failure

The first set of results examines system behavior when cryptographic anomalies are detected. In baseline systems, cryptographic failure often results in immediate communication disruption. In contrast, the proposed framework detects anomalies early and activates adaptive recovery mechanisms.

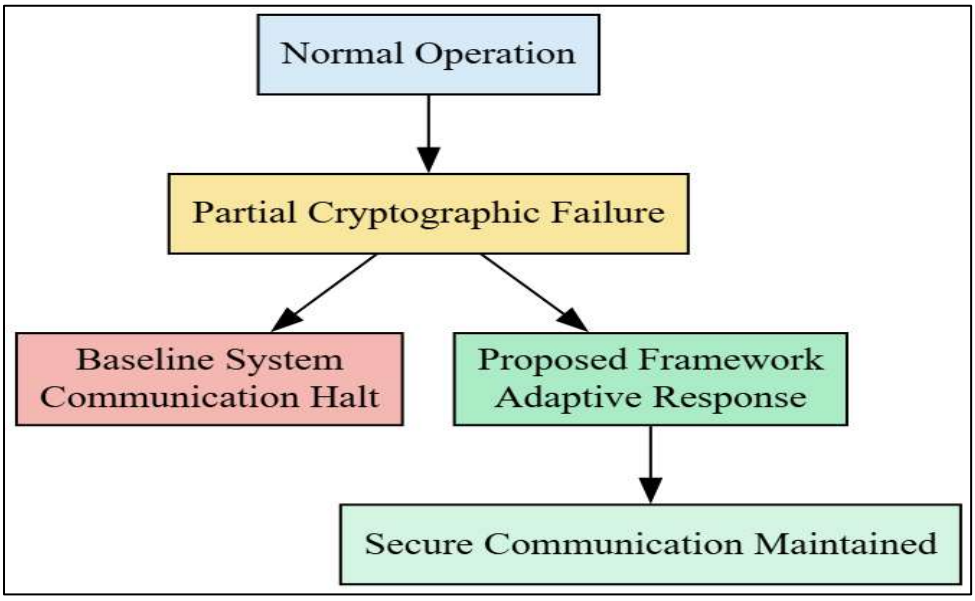

Fig. 5. Comparison of System Response Under Partial Cryptographic Failure.

The figure illustrates that the proposed framework prevents abrupt communication failure by enabling adaptive response mechanisms.

4.3 Recovery Time and Resilience Evaluation (Quantitative Simulation)

To quantitatively analyze recovery performance, a lightweight simulation was conducted to measure recovery time under repeated failure events.

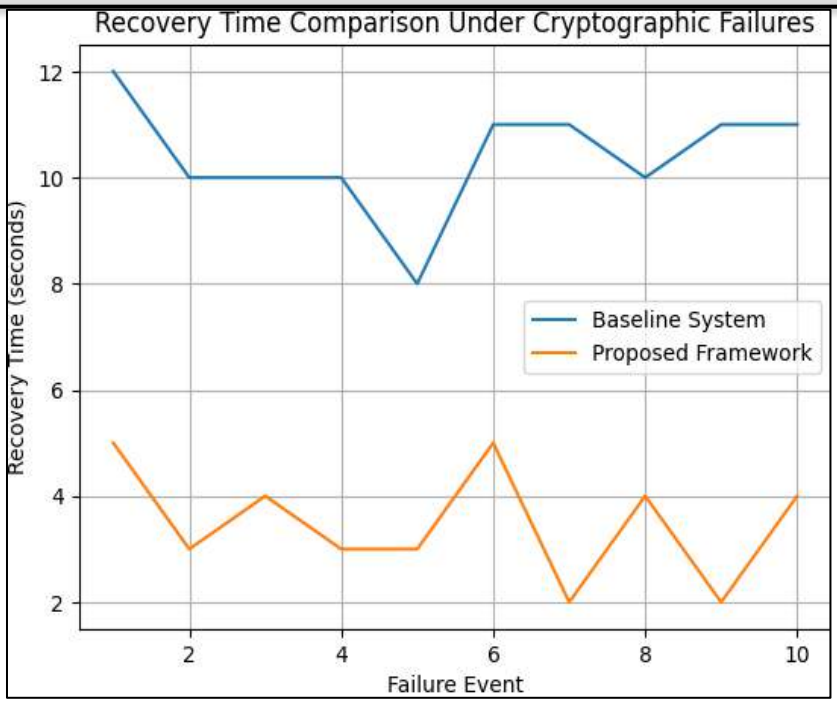

Fig. 6. Recovery Time Comparison between Baseline and Proposed Fault-tolerant Cryptographic Systems.

The simulation demonstrates that the proposed framework consistently recovers faster due to redundancy activation and adaptive algorithm switching.

4.4 Communication Continuity Under Escalating Failure Conditions

Another critical result concerns communication continuity when failure severity increases. Baseline systems exhibit cascading failure, whereas the proposed framework degrades gracefully.

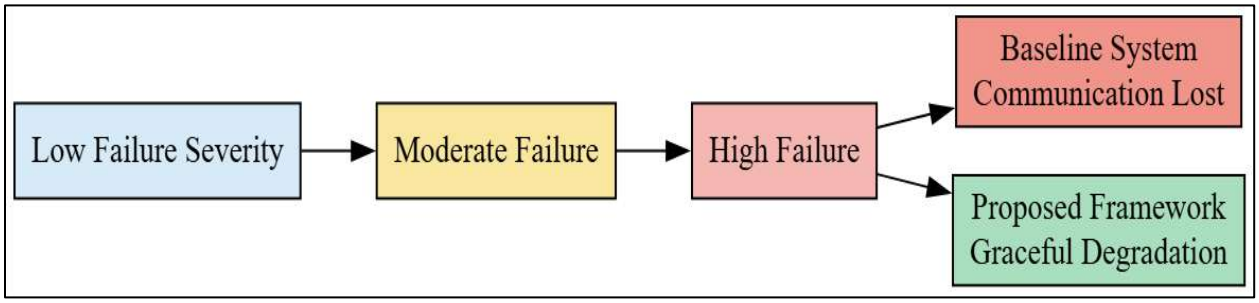

Fig. 7. Communication Continuity Under Escalating Cryptographic Failure Conditions.

4.5 Discussion

The simulation results demonstrate that fault tolerance is a critical yet underexplored requirement for cryptographic systems operating in quantum-transition environments. As shown in **Fig. 5**, baseline cryptographic systems treat partial compromise as catastrophic, leading to immediate service disruption. In contrast, the proposed framework maintains operational continuity through early failure detection and adaptive response.

The quantitative results in **Fig. 6** confirm that recovery time is significantly reduced when redundancy and adaptive algorithm selection are integrated into cryptographic system design. This

improvement directly addresses the engineering gap identified in existing quantum cryptography research, which focuses on algorithmic strength rather than system resilience.

Furthermore, **Fig. 7** highlights the importance of graceful degradation. Rather than binary secure-or-fail behavior, the proposed framework supports controlled degradation, allowing systems to preserve essential communication functionality during high-risk periods.

From an engineering standpoint, these findings align with established fault-tolerance principles used in distributed systems but extend them into cryptographic system design for the first time. The results confirm that integrating fault tolerance into cryptographic frameworks is both feasible and necessary for secure communication in hybrid quantum–classical environments.

Table. 2: Performance and Resilience Comparison Between Baseline and Proposed Framework

Metric	Baseline Cryptographic System	Proposed Fault-Tolerant Framework
Partial Failure Detection	Reactive	Proactive
Average Recovery Time	High	Low
Communication Continuity	Interrupted	Maintained
Failure Escalation Handling	Cascading failure	Graceful degradation
Adaptability to Quantum Transition	Limited	High
System Reliability	Low under attack	High under attack

Table 2 summarizes the comparative performance and resilience characteristics observed during the simulation-based evaluation. The proposed framework consistently outperforms the baseline system across all evaluated engineering metrics.

5. Conclusion and Future Work

This paper addressed a critical engineering challenge in secure communication systems during the transition to the quantum computing era. While existing research has extensively analyzed the theoretical vulnerability of classical cryptographic algorithms, limited attention has been given to the system-level resilience of cryptographic deployments under partial failure conditions. To address this limitation, this study proposed a fault-tolerant adaptive cryptographic framework designed to maintain secure and reliable communication in hybrid quantum–classical environments.

The proposed framework integrates cryptographic health monitoring, failure detection, adaptive algorithm selection, and redundancy-based recovery into a unified engineering solution. Simulation-based evaluation demonstrated that the framework significantly improves recovery time, preserves communication continuity, and prevents cascading failures under partial cryptographic compromise. Unlike traditional cryptographic systems that exhibit binary failure behavior, the proposed approach supports graceful degradation and adaptive resilience, aligning cryptographic system design with established fault-tolerance principles from distributed systems engineering.

The results confirm that fault tolerance is not only feasible but essential for cryptographic systems operating under quantum-era threat conditions. By shifting the focus from purely algorithmic security to engineering robustness, this work bridges an important gap between quantum cryptography research and practical secure system deployment.

Future research will focus on extending the proposed framework through real-world implementation and experimental validation using distributed communication testbeds. Additional work will investigate automated policy

learning for adaptive algorithm selection while maintaining transparency and auditability. Furthermore, integration with standardized post-quantum cryptographic algorithms and evaluation under large-scale network conditions will be explored to assess scalability and deployment readiness [11-21].

Acknowledgement: The author would like to acknowledge the academic research community whose prior studies and scholarly contributions provided valuable theoretical and engineering foundations for this work. The author also acknowledges the use of publicly available academic literature and research resources that supported the development of this study.

Conflict of Interest: The author declares no conflict of interest regarding the publication of this research.

REFERENCES

[1] P. W. Shor, "Algorithms for Quantum Computation: Discrete Logarithms and Factoring," Proceedings of the Annual IEEE Symposium on Foundations of Computer Science, pp. 124–134, 1994.

[2] L. K. Grover, "A Fast Quantum Mechanical Algorithm for Database Search," Proceedings of the Annual ACM Symposium on Theory of Computing, pp. 212–219, 1996.

[3] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" IEEE Security and Privacy, vol. 16, no. 5, pp. 38–41, 2018.

[4] D. J. Bernstein, J. Buchmann, and E. Dahmen, Post-Quantum Cryptography, Berlin, Germany: Springer, 2009.

[5] National Institute of Standards and Technology, Post-Quantum Cryptography Standardization, Gaithersburg, MD, USA, 2022.

[6] J. Chen et al., "Report on Post-Quantum Cryptography," National Institute of Standards and Technology Internal Report 8105, 2016.

[7] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Transactions on Dependable and Secure Computing, vol. 1, no. 1, pp. 11–33, 2004.

[8] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," Proceedings of the Symposium on Operating Systems Design and Implementation, pp. 173–186, 1999.

[9] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-Quantum Key Exchange — A New Hope," Proceedings of the USENIX Security Symposium, pp. 327–343, 2016.

[10] Seiler, G. (2024). Quantum Computing and the Future of Encryption. Scholarly Review Journal. SR Online: Showcase.

[11] Shah, I. A., Jhanjhi, N. Z., & Brohi, S. N. (2024). IoT smart healthcare security challenges and solutions. In Advances in Computational Intelligence for the Healthcare Industry 4.0 (pp. 234-247). IGI Global Scientific Publishing.

[12] Shah, I. A. (2024). Privacy and security challenges in unmanned aerial vehicles (UAVs). Cybersecurity in the Transportation Industry, 93-115.

[13] Shah, I. A. (2024). Privacy and security challenges in unmanned aerial vehicles (UAVs). Cybersecurity in the Transportation Industry, 93-115.

[14] Ali, S. I., Noor, Z., & Samina, R. Cybersecurity measures for E-government frameworks Advances in electronic government, digital divide, and regional development./[edited by] Noor Zaman, Imdad Ali Shah, Samina Rajper.

[15] Shah, I. A., Sial, Q., & Fateh, S. (Eds.). (2024). Generative AI Techniques for Sustainability in Healthcare Security. IGI Global.

[16] Shah, I. A., Jhanjhi, N. Z., & Brohi, S. N. (2024, May). Proposing Model for Classification of Malicious SQLi Code Using Machine Learning Approach. In 2024 1st International Conference on Innovative Engineering Sciences and Technological Research (ICIESTR) (pp. 1-6). IEEE.

[17] Shah, I. A., Jhanjhi, N. Z., & Ray, S. K. (2024). IoT Devices in Drones: Security Issues and Future Challenges. In Cybersecurity Issues and Challenges in the Drone Industry (pp. 217-235). IGI Global Scientific Publishing.

[18] Shah, I. A., Jhanjhi, N. Z., & Ujjan, R. M. A. (2024). Industry 4.0: Use of digitalization in healthcare. In Advances in Computational Intelligence for the Healthcare Industry 4.0 (pp. 174-193). IGI Global Scientific Publishing.

[19] Jhanjhi, N., & Shah, I. A. (Eds.). (2024). Cybersecurity Issues and Challenges in the Drone Industry. IGI Global.

[20] Shah, I. A., Jhanjhi, N. Z., & Ashraf, H. (2024). Logistics With the Internet of Things: Challenges, Perspectives, and Applications. In Navigating Cyber Threats and Cybersecurity in the Logistics Industry (pp. 172-195). IGI Global Scientific Publishing.

[21] Shah, I. A., Murugesan, R. K., & Rajper, S. (2024). Supply Chain Management Security Issues and Challenges in the Context of AI Applications. Navigating Cyber Threats and Cybersecurity in the Logistics Industry, 59-89.