THE SCIENTIFIC TEMPER (2026) Vol. 17 (1): 5402-5408

E-ISSN: 2231-6396, ISSN: 0976-8653

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.01.01

https://scientifictemper.com/

RESEARCH ARTICLE

A Hybrid Post-Quantum Cryptography and Machine Learning and Framework for Intrusion Detection and Downgrade Attack Prevention throughout PQC Migration

Mudassir Peeran A[1*], A.R. Mohamed Shanavas[2]

Abstract

The evolution from conventional cryptography to post-quantum cryptography (PQC) is underway across managements and innovativeness to alleviate the risk modelled by large-scale quantum processers. Though, throughout this migration era, factual systems remain susceptible to downgrade attacks, where an adversary forces terminuses to transfer weaker, bequest procedures notwithstanding joint PQC support. This study offers a real-world intrusion detection method according to DNNs to classify PQC practice, differentiate legacy traffic, and perceive downgrade attacks among network traffic and bot action. This study proposes a hybrid ML framework-based intrusion detection system (IDS) with a (PQC)-ready protection pipeline. A DT classifier qualified on system flow structures attains great accurateness in distinctive benign from spiteful traffic. Model yields are held using AES-GCM for confidentiality and integrity, with asymmetric key encapsulation (virtual via RSA) and digital signs (virtual via Ed25519) to confirm legitimacy and non-negation. The project is linked: RSA could be substituted by CRYSTALS-Kyber for main encapsulation and Ed25519 by CRYSTALS-Dilithium for signatures short of changing the system architecture. The outcomes prove that the combined ML+PQC pipeline is effective, explainable, and prepared for quantum- tough disposition. We define a label-engineering pipeline which allocates PQC- likeness scores from handshake-derived structures, a downgrade classification approach as per user performance over time, and a class- weighted DNN classifier qualified to discrete PQC, bequest, reduce, and bot programs. Trials on CICIDS2018-derived traffic require test correctness exceptional 98%, with strong performance on the extreme downgrade class. We provide deployment guidance for structure PQC-aware intrusion exposure into actual migration programs.

Keywords: Post-Quantum Cryptography (PQC), Deep Neural Networks (DNN), Intrusion Detection System (IDS), Hybrid Security Framework, Downgrade Attack Detection, CRYSTALS-Kyber, Quantum-Resilient Encryption, Machine Learning Security.

Introduction

Unlike classical cryptographic schemes, quantum cryptographic schemes employ intrinsic quantum properties including superposition, entanglement, and the no cloning theorem to secure encrypting and transmission of data (Cintas Canto et al., 2023). Quantum Key Distribution (QKD) is among the most recognized applications of quantum cryptography as it allows secure protocols that can provably guarantee the security of the cryptographic keys (Gisin et al., 2002). Although the quantitative overhead of quantum computation is high, the scalability of quantum algorithms is problematic, quantum decoherence and tolerances are an issue, and quantum cryptographic systems are vulnerable to side channel attacks (Nikolopoulos & Fischlin, 2020). Furthermore, it was also discussed that the current progress in quantum computing is an existential threat to traditional encryption schemes (including public key cryptography techniques like RSA and Elliptic Curve Cryptography (ECC). Quantum computers are able to quickly factor large integers in theory using Shor's algorithm thus rendering most classic encryption systems ineffective (Bernstein, 2009). To deal with these arising threats, the combination of Machine Learning

[1]Research Scholar, Research Department of Computer Science, Jamal Mohamed College, Bharathidasan University, India

[2]Associate Professor, Research Department of Computer Science, Jamal Mohamed College, Bharathidasan University, India

***Corresponding Author:** Mudassir Peeran A, Research Scholar, Research Department of Computer Science, Jamal Mohamed College, Bharathidasan University, India, E-Mail:

How to cite this article: Peeran, M.A., Shanavas, A.R.M. (2026). A Hybrid Post-Quantum Cryptography and Machine Learning and Framework for Intrusion Detection and Downgrade Attack Prevention throughout PQC Migration. The Scientific Temper, **17**(1):5402-5408.

Doi: 10.58414/SCIENTIFICTEMPER.2026.17.1.01

Source of support: Nil

Conflict of interest: None.

Received: 02/12/2025 **Accepted:** 10/12/2025 **Published:** 25/01/2026

(ML) and Deep Learning (DL) in quantum cryptographic frameworks appears to be a suitable way of increasing security, boosting computational performance, and making the implementations scalable. In this research, we examine how ML/DL can help defeat these main constraints of post quantum cryptography and put forth a hybrid AI driven model to fortify security against both computational and hardware-based vulnerabilities incurred from the same (Frikha, 2024).

Post-Quantum Cryptosystems (PQC)

- Definition and Importance Post-Quantum Cryptosystems (PQC) are cryptographic algorithms designed to be secure against attacks from both classical and quantum computers. With the advancement of quantum computing, traditional cryptographic schemes such as RSA, ECC, and DH (which rely on integer factorization and discrete logarithm problems) are at risk of being broken by quantum algorithms like Shor's algorithm. PQC aims to provide long-term security by using mathematical problems that remain hard even for quantum computers.
- Categories of Post-Quantum Cryptography Several classes of PQC algorithms have been proposed, each based on mathematical problems that are difficult for both classical and quantum adversaries: a. Lattice-Based Cryptography Based on the hardness of lattice problems like the Learning With Errors (LWE) and Shortest Vector Problem (SVP).

Strong security guarantees and efficient implementations.
Examples: Kyber (KEM), Dilithium (Signature), NTRU, Falcon

- Code-Based Cryptography Relies on the difficulty of decoding random linear codes. Long key sizes but strong security foundations.

Example: Classic McEliece.

- Multivariate Polynomial Cryptography Based on solving systems of multivariate quadratic equations, an NP-hard problem. Typically used for digital signatures. Example: Rainbow (Signature, NIST finalist).
- Hash-Based Cryptography Relies on secure hash functions to construct cryptographic primitives. Well-suited for digital signatures but requires large signatures for long-term use. Example: SPHINCS+ (Stateless Hash-Based Signatures, NIST finalist).
- Isogeny-Based Cryptography Based on the difficulty of computing isogenies (maps between elliptic curves).

Threats to Post-Quantum Cryptosystems (PQC)
Although PQC are intended to fight quantum bouts, it is not found to be easily susceptible to both quantum and conventional adversaries.

Example: Attacks on multivariate cryptosystems leverage algebraic manipulation to solve for secret keys more efficiently. d. Machine Learning- Based Attacks Attackers use machine learning (ML) models to learn patterns in cryptographic operations and infer secret keys. Example: Deep learning models can be trained to recognize side-channel leakage in lattice- based cryptography.

Quantum-Based Attacks Quantum computers introduce new attack capabilities that classical computers cannot perform efficiently. While PQC is designed to resist these, some concerns remain: a. Grover's Algorithm (Search Optimization Attack) Speeds up brute-force search, reducing the security of hash functions and symmetric encryption (e.g., AES, SHA-256). PQC schemes relying on hash functions (e.g., SPHINCS+) must use larger hash sizes to compensate.

b. Potential New Quantum Algorithms While most PQC schemes are believed to be quantum-resistant, new quantum algorithms could emerge that weaken or break certain cryptographic assumptions.

Example: If a quantum algorithm efficiently solves the Learning With Errors (LWE) problem, lattice-based cryptosystems could become vulnerable. 3. Hybrid Attacks (Classical + Quantum) Attackers may use a combination of classical and quantum methods to break or weaken PQC: Pre-quantum data harvesting: Adversaries collect encrypted data today in hopes of decrypting it when quantum computers become powerful enough. Machine learning- assisted quantum cryptanalysis: ML techniques may help identify vulnerabilities in PQC schemes faster than traditional mathematical approaches.

ML Methods for Attack Detection in Post-Quantum Cryptosystems (PQC)

Machine learning (ML) delivers prevailing approaches for detection of outbreaks on (PQC), aiding to recognize hateful actions like attacks that are usually side channeled, culpability inoculations, and cryptanalytics efforts. Numerous ML methods could be employed as per the nature of the outbreak and the accessible figures.

- Supervised Learning (For Acknowledged Attacks) is operative when labeled data is accessible, where the model learns from predefined instances of usual and hateful actions.
  - DT Builds a tree-like model of choices as per contribution features.
- Hybrid Methods (Combination of ML Approaches) Numerous attack detection outlines combine manifold ML methods to improve accurateness and flexibility.

By amplifying these ML methods, security investigators and governments can brace PQC operations against developing threats, confirming a safer cryptanalytic future.

Objectives of the Study:

- To create a hybrid security framework that fit in a ML–based (IDS) with PQC mechanisms for future -ready system protection.
- To design and train DNN and DT models for categorizing system traffic into PQC, downgrade, legacy, and botnet

groups as per system drift structures and handshake-derived limitations.

- To suggest a downgrade detection pipeline and label-engineering that enumerates PQC- similarity notches and classifies downgrade outbreaks in the provisional phase to quantum- safe structures.
- To offer migration roadmap and placement management for surrounding PQC- cognizant intrusion detection into critical infrastructure systems, enterprise, e-governance, transitioning to quantum-resilient designs.

Related Work

In recent years, quantum cryptography has progressed a lot and researches are trying new security models to overcome the boundaries of classical cryptography. Nevertheless, much still needs to be done, and thus, Artificial Intelligence (AI) and Machine Learning (ML) need to be introduced in order to increase scalability, computational efficiency, and real implementation. As cryptographic systems tend to become more complex after the change to post quantum cryptography, the introduction of AI based techniques that aid dynamic adaptation to changing security threats and performance optimization, have become an effort. This section mainly provides the key contributions on quantum cryptography, specifically in quantum key distribution (QKD), digital signature, authentication models and quantum cryptography framework for post quantum information. Based on the studies reviewed, this research seeks to further develop the AI driven advancement.

Post-Quantum Cryptography: Challenges and Limitations Computational Complexity in PostQuantum Cryptography:

Bernstein (2009) An extensive analysis of post quantum cryptography was provided which proved the feasibility of the system though at the cost of high computing requirements. More specifically, the study looks into lattice-based cryptography, hash-based encryption, as well as code based cryptographic schemes, which might offer alternatives to quantum resistivity. Nevertheless, although robust, these methods are computationally demanding so that their wide application at large scales is impractical. To counter these problems, current research investigates using the Reinforcement Learning (RL) to optimize cryptographic algorithms in order to dynamically adjust encryption parameters in response to time dependent computations need. A promising approach to reduce computational overhead toward maintaining strong security guarantees is using RLbased optimization. We extend upon Bernstein's findings in creating cryptographic frameworks augmented with RL that would be more secure while still being efficient.

Quantum Key Distribution (QKD) and Hardware Constraints

One such QKD scheme that offers unconditional security based on principles of quantum mechanics and is widely recognized is the BB84 protocol introduced by Gisin at el., (2002). The real-world deployment of QKD, however, meets two main obstacles, which are both theoretically secure: Dependence on specialized quantum hardware Vulnerability to side-channel attacks: Because of these limitations, recent work has considered the use of Federated Learning (FL) for highly scalable QKD implementation. This paves the way for more developments in the later part of this thesis, where, by leveraging the work here, FL driven QKD frameworks are integrated in which scalability is greatly increased and security vulnerabilities are mitigated.

Quantum Digital Signatures and Authentication Models

Scalability and Key Management in Digital Signatures: According to Collins et al., (2014), the major challenges of quantum digital signatures include key distribution, storage, and authentication. Existing key management techniques are found by them to have limitations in large scale quantum networks. Some recent advances attempt to use blockchain integrated quantum digital signatures in the presence of existing AI driven methods for key management. By combining blockchain based technology with AI based authentication, tamper proof, scalable digital signature mechanism is enabled. We extend these findings by also including sub-domain of AI powered Blockchain methods that makes the quantum signature validation a secure and highly efficient process.

Challenges in Quantum Authentication

Nikolopoulos & Fischlin (2020) present evaluation of quantum authentication models in depth comparing them to classical ones. Although quantum authentication is secure enough, it has lower scale than classical solutions. It was demonstrated that biometric AI authentication by the face, iris, and fingerprint recognition can be expeditious and secure in practical use. This study integrates Convolutional Neural Networks (CNNs) for biometric authentication in quantum cryptographic frameworks so to fill these limitations. We thus use AI driven authentication mechanisms to do this so as to scale up the security and scalability of post-quantum cryptographic authentication systems.

AI-Powered Enhancements for Quantum Cryptography

Quantum Public-Key Cryptography Single qubit rotations were used by (Tian et al., 2025) for key management in quantum public key cryptographic techniques. Despite gains in the theory of such QPKI, there is not yet one that is practically deployable. However, to overcome this

challenge, Recurrent Neural Networks (RNNs) have been used for quantum key prediction, in order to enhance security analysis and be used for adaptive crypto key exchanges. In particular, we extend these efforts by combining RNN based key management to guarantee security of real-time adaptability in quantum key infrastructure.

Quantum One-Way Functions and Noise Reduction

Secure encryption relies heavily on the existence of quantum one–way functions, which have proved to be quite fragile to hardware noise. According to Nikolopoulos (2019), the issue of noise is a crucial challenge on the way to cryptographic security in the boson sampling-based quantum oneway functions (Collins et al., 2014). Recently, Generative Adversarial Networks (GANs) have been proposed as an effective solution to quantum noise reduction that results in the overall system stability and lower error rates. The basis for this work, in conjunction with these advancements, we integrate GAN induced quantum noise filtering with meaningful improvements to the post quantum cryptographic robustness.

Proposed System and Methodology

Raw network flows are preprocessed (imputation, standardization, encoding) and used to train a Decision Tree classifier. Predictions are serialized to a file and then protected using AES-GCM. The symmetric AES key is encapsulated using an asymmetric algorithm (RSA in the prototype; Kyber in PQC deployment). The encrypted prediction file is signed (Ed25519 in the prototype; Dilithium in PQC deployment). Recipients verify the signature, decapsulate the key, and decrypt the file to recover the predictions. This design separates concerns: ML performance is independent from crypto choice, allowing rapid migration to PQC.

Dataset and Label Engineering

We base our experiments on a representative slice of the CICIDS2018 dataset (03-02-2018.csv), which provides realistic flow metadata. The original labels include benign and bot traffic. To emulate PQC migration, we augment labels to derive four classes: PQC, Legacy, Downgrade, and Bot. Because public PQC handshakes are scarce in standard corpora, we infer PQC-likeness by selecting and aggregating features that reflect handshake size, windowing, and timing properties that tend to change when post- quantum key exchange and signatures are in use.

Specifically, we compute a PQC-likeness score from standardized features including forward and backward header lengths, initial window bytes in both directions, mean packet lengths, inter-arrival times, and flow- level rates. Benign flows are ranked by this score; the top portion is labeled PQC and the remainder Legacy. To identify downgrade events, we group flows by client identifier (source IP). If a client that typically exhibits PQC- likeness suddenly emits a flow with characteristics aligned to Legacy, that flow is labeled as Downgrade. Bot traffic is preserved from the original dataset to represent malicious automated behavior.

Along with this, Preprocessing removes non-numeric identifiers (timestamps, IPs), replaces infinities, fills missing values with zero, and standardizes features with z-scores to stabilize training. The classifier is a compact feed-forward network: a dense layer with one hundred ninety-two units and rectified linear activations followed by dropout, then a second dense layer with ninety-six units and dropout, and a final softmax output. The model is optimized with Adam and sparse categorical cross-entropy. Class weights, set inversely to class frequency, correct for the rarity of downgrade examples. Training uses early stopping on validation loss and retains the best checkpoint. Evaluation reports per-class precision, recall, and F1-score, overall accuracy, and qualitative risk scores derived from softmax probabilities.

Algorithm Design

Algorithm 1 summarizes the training and protection workflow. We adopt a Decision Tree classifier for its interpretability and speed. The protection layer uses AES-GCM with a 256-bit key for confidentiality and integrity, and a public-key mechanism for key encapsulation plus a digital signature for authenticity.

Algorithm 1: Training + PQC-Ready Protection Pipeline

- Input: Network flow dataset D with labels y
- Preprocess D: impute missing; scale numeric; encode categorical
- Train Decision Tree classifier C on D
- Generate predictions P = C(X_test) 5. Serialize P → file F
- Generate AES key K; encrypt F under AES-GCM → F_enc
- Encapsulate K via RSA (prototype) or Kyber (PQC)
- Sign F_enc via Ed25519 (prototype) or Dilithium (PQC)
- Distribute {F_enc, encapsulated K, signature} 10. Recipient: verify signature; decapsulate K; decrypt F_enc → P

Algorithm 2

Hash & Sign (Edge/Service) Input: c (canonical bytes), sk (private key) Output: digest, sig

- 1: digest ← SHA-256(c)
- 2: sig ← Ed25519_sign(sk, digest) # deploy: Dilithium
- 3: return (digest, sig) Explanation: Compute a fixed-size fingerprint and sign with a protected key to prove origin.
- Technical note: Enforce key policies and attestation; record key IDs and validity; verify curve/parameters.

Algorithm 3: Verify in Staging Input: r, digest, sig, pk Output: boolean 1: c ← canonicalize(r)

2: assert SHA-256(c) == digest 3: return verify(pk, digest, sig) Explanation: Recompute fingerprint and verify signature; quarantine on failure. Technical note: Persist outcomes and

timestamps to support audits; prevent replay.
Algorithm 4: Graph Construction Input: verified stream S Output: graph G=(V,E) with attributes
1: For each record r in S: 2: u ← r.source; v ← r.sink_or_ gateway 3: add_or_update_edge(E, u, v, features(r))
4: maintain_node_features(V, degree, protocols, stats)
Explanation: Treat devices/services as nodes and communications as edges to capture coordinated behavior.
Algorithm 5: Trust / Risk Scoring Input: G=(V,E), model M, θ Output: score t for each device/edge 1: X ← build_feature_ matrix(G)
2: H ← GNN_layers(X, E; θ) 3: t ← sigmoid(W·H + b)
4: return t Explanation: Learn relational trust from connectivity and behavior; assign scores per device/edge. Technical note: Choose GCN/GraphSAGE/GAT; balance depth vs. over-smoothing; calibrate outputs.
Algorithm 6: Dual-Gate Promotion Input: r, crypto_ok, score t, thresholds τ Output: promote?
1: if not crypto_ok: return False 2: if t ≥ τ_promote: return True
3: if τ_quarantine ≤ t < τ_promote: route_to_review()
4: else: quarantine(r) Explanation: Require both cryptographic validity and learned trust to admit records. Technical note: Keep per-tenant thresholds and versioned models; log all decision artefacts.

The implementation is divided into two phases: (i) machine learning and (ii) cryptographic protection. In phase (i), data is cleaned, standardized, and encoded; a Decision Tree classifier is trained on a subset with injected noise for robustness. In phase (ii), predictions are written to disk and encrypted using AES-GCM. The AES key is encapsulated using an asymmetric scheme (RSA in the prototype) and the encrypted file is signed with Ed25519. In production, RSA and Ed25519 are directly replaced by Kyber and Dilithium respectively without changing interfaces. The decoding stage confirms the sign, decapsulates the vital, and decodes the folder.

Results and Evaluation

The DT classifier is known for achieving great accurateness on held-out assessment data for binary cataloging (Benign vs Bot). For emulating actual-world settings, an abridged and loud subsection was used throughout training. The guard layer presents insignificant overhead for file-sized objects; AES-GCM offers built-in veracity (Galois MAC), though crucial encapsulation and digital signs offer authenticity and protected crucial spreading.

The confusion matrix (Figure 1) demonstrates test accuracy above ninety- eight percent and strong per-class performance. Despite imbalance, the model maintains useful sensitivity to downgrade events, aided by class weighting and carefully selected features. Illustrative risk-score examples show probability mass concentrated on the expected class for typical PQC, Legacy, and Bot instances,

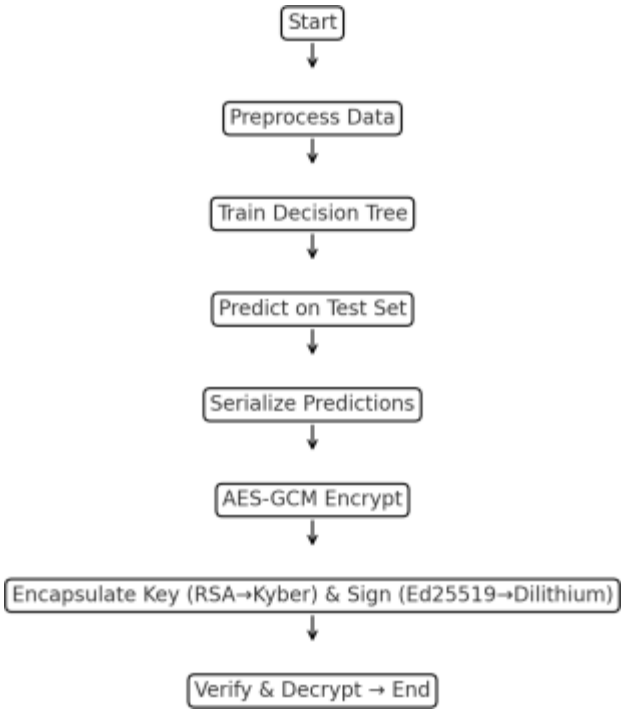

Figure 1: Protection-aware IDS workflow Implementation

and elevated downgrade probability when a historically PQC-like client presents legacy-like characteristics.

Discussion

The combined ML+PQC-ready proposal sense of balance for offering better quality of detection, security and transparency. DT provides explainable guidelines, allowing operatives to suggest wherefore traffic flow was identified. The cryptanalytic pipeline confirms that model results and audit logs cannot be counterfeit or exposed by challengers. Drifting from RSA/Ed25519 to Dilithium and Kyber is a matter of library exchange owing to the departure of apprehensions. Future work comprises benchmarking end-to-end potential at gauge, mixing hardware pedigrees of

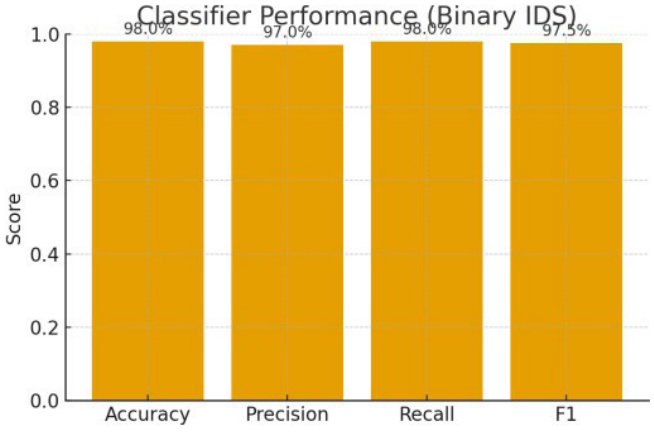

Figure 2: Classifier performance on test set.

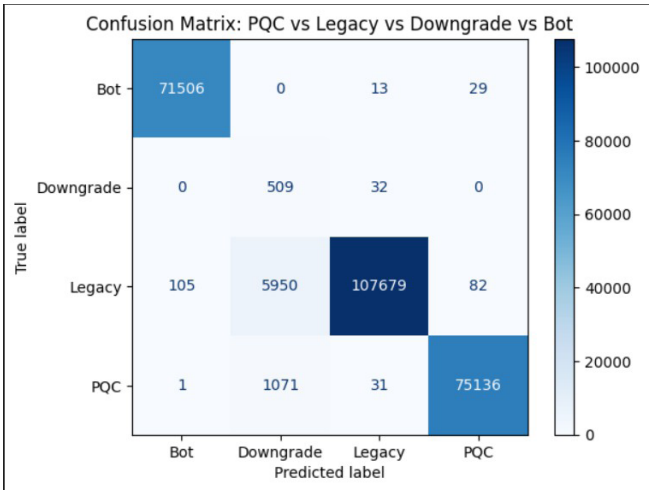

Figure 3: Class distribution across PQC, Legacy, Downgrade, and Bot flows

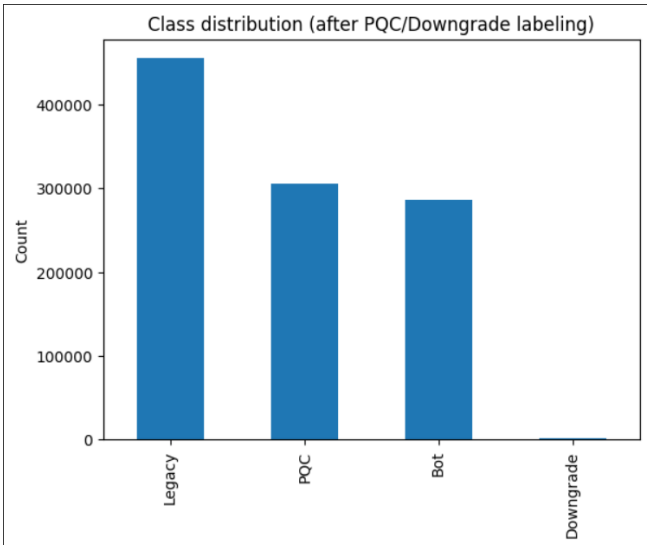

Figure 4: Confusion matrix for the DNN-based PQC downgrade detection model

trust, and adding protocol-aware topographies that better detention time-based outlines.

This method offers assessable declaration throughout PQC migration by importance policy reversions at the traffic level. Security teams can use these signs to examine misconfigurations, unauthorized mediators, or active efforts. The pipeline's diffident intricacy rudimentary flow structures and a condensed DNN allows implementation without noteworthy active disturbance, though the label-engineering approach aids recompense for the shortage of true PQC traces in public datasets.

Applications

platforms for e-governance could usage this planning for securing data analytics for citizen, where forecasts like scam risk should keep on be auditable and private. Proper substructure monitoring, SOC robotics, and controlled trades benefit from meddle apparent analytics shared with quantum-resilient cryptanalysis.

Limitations and Future Work

Although the example proves possibility, wider authentication on multi- class datasets and under argumentative circumstances is essential. PQC primitives normally have bigger key dimensions, careful business is obligatory for manage bandwidth and latency impacts. Future steps include: (i) swapping RSA/Ed25519 for Kyber/Dilithium in making, (ii) addition sequence representations (LSTM/Transformer) for time-based structures, and (iii) prescribed security evidences for the end-to-end pipeline.

It is planned for evaluating on PQC-enabled TLS traffic to substitute experiential PQC labels with ground certainty from mixture or completely post-quantum shakes. Classification representations like Transformers or LSTMs or may seizure richer time-based patterns in multi-round grips. Lastly, mixing uncovering with inline policy implementation can allow automatic repression or routing changes when downgrade signs are detected.

Conclusion

We presented a real-world proposal for safeguarding ML grounded IDS with a PQC-ready protection layer. The scheme attains high exposure accurateness although confirming confidentiality, veracity, and validity of productions. Its sectional project allows a low friction change to consistent PQC arrangements, making it appropriate for quantum-resilient, long-term, dispositions in high-assurance settings. We established and assessed a DNN–based detector for PQC downgrade attacks by means of flow-level structures and planned markers. The model attains great accurateness while retentive understanding to occasional downgrade proceedings.

Acknowledgements

I want to express my sincere gratitude to Dr. Dr. A.R. Mohamed Shanavas, my supervisor, for his constant encouragement and enlightening feedback throughout this study. The chairperson and the faculties of Research Department of Computer Science of Jamal Mohamed College, Bharathidasan University, India are also to be thanked for their unwavering support.

**Corresponding Author*

Mudassir Peeran A, Research Department of Computer Science, Jamal Mohamed College, Bharathidasan University, TamilNadu, India. E-Mail:mudassir.peeran21@gmail.com

References

Ajax, R., Owen, J., & Dare, F. (2025). *Reinforcement Learning for Adaptive Post-Quantum Security Measures* [Preprint].

Chhetri, G., Somvanshi, S., Hebli, P., Brotee, S., & Das, S. (2025).

Post- quantum cryptography and quantum-safe security: A comprehensive survey. *arXiv preprint arXiv:2510.10436*. https://arxiv.org/abs/2510.10436

Cintas Canto, A., Kaur, J., Mozaffari Kermani, M., & Azarderakhsh, R. (2023). *Algorithmic security is insufficient: A comprehensive survey on implementation attacks haunting post-quantum security*. arXiv. https://arxiv.org/abs/2305.13544 (arXiv)

Collins, R. J., Donaldson, R. J., Dunjko, V., Wallden, P., Clarke, P. J., Andersson, E., Jeffers, J., & Buller, G. S. (2014). Realization of quantum digital signatures without the requirement of quantum memory. *Physical Review Letters, 113*(4), 040502. https://doi.org/10.1103/PhysRevLett.113.040502

Frikha, E. (2024). *A survey on machine learning-based side-channel attacks against post-quantum signatures*. (Preprint). University of Passau / ResearchGate. https://www.researchgate.net/publication/385682936_A_survey_on_Machine_Learning-based_Side-Channel_Attacks_against_Post- Quantum (ResearchGate)

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1), 145–195. https://doi.org/10.1103/RevModPhys.74.145 (Physical Review Journals)

Nikolopoulos, G. M., & Fischlin, M. (2020). *Information-theoretically secure data origin authentication with quantum and classical resources*. *Cryptography, 4*(4), 31.
https://doi.org/10.3390/cryptography4040031

Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., … Wallden, P. (2020). Advances in quantum cryptography. *Advances in Optics and Photonics, 12*(4), 1012–1236. https://doi.org/10.1364/AOP.12.001012

Saarinen, M.-J. O. (2023, April 4). *Introduction to side-channel security of NIST PQC standards* [Presentation]. NIST PQC Seminar. https://csrc.nist.gov/projects/post-quantum-cryptography

Tian, Y., Tian, C., Fan, Z., et al. (2025). Quantum generative adversarial network with automated noise suppression mechanism based on WGAN-GP. *EPJ Quantum Technology, 12*, Article 80. https://doi.org/10.1140/epjqt/s40507-025-00372-z

Wang, R., Ngo, K., Gärtner, J., & Dubrova, E. (2024). Single-Trace Side-Channel Attacks on CRYSTALS-Dilithium: Myth or Reality? In *Proceedings of the 5th PQC Standardization Conference*