A Layered Risk Scoring Model for TLS Connections Against Quantum Threats

Yu-Lim Hyoung[1][0009−0009−7530−6497], Su-Min Jeong[1][0009−0007−9643−4872], Da-Eun Lim[1][0009−0009−4867−8527], Do-Yun Park[1][0009−0002−2201−6161], Su-Been Cho[1][0009−0004−4352−8021], Jae-Hwan Kim[1][0009−0000−3524−5487], Hyun-Ji Kim[1][0000−0001−9828−3894], and Hwa-Jeong Seo[1][0000−0003−0069−9061]

Hansung University, Seoul, South Korea
yulim4hyoung@gmail.com jeong9sumin@gmail.com lima050627@gmail.com rhcp030418@gmail.com chosubin1208@gmail.com jaedol2023@gmail.com khj1594012@gmail.com hwajeong84@gmail.com

Abstract. The advancement of quantum computing threatens public-key cryptographic algorithms used in TLS connections, such as RSA and ECDHE. The *Harvest Now, Decrypt Later* (HNDL) attack exposes long-term confidential data to risk even before quantum computers are practically realized, yet a systematic methodology for immediately quantifying the quantum vulnerability of individual TLS connections remains absent. This paper proposes a layered risk scoring model that quantifies the quantum threat exposure of TLS connections on a 0–100 scale. The model decomposes risk into five independent layers—TLS protocol exposure (L1), legacy public-key vulnerability (L2a), AES-128 Grover weakening (L2b), PQC Level-1 vulnerability (L2c), and certificate expiration urgency (L3)—and incorporates an HNDL global multiplier M that reflects the confidentiality retention period of transmitted data. Applied to 502 real-world TLS sessions across four industry sectors with $M = 1.50$, the domestic average risk score (16.0) is approximately 34% higher than the global average (11.9), with domestic legacy key exchange usage at 77.4% versus 53.5% globally and PQC adoption at 22.6% versus 46.5%. These results quantitatively confirm the elevated quantum risk of domestic network infrastructure, underscoring the urgency of PQC transition.

Keywords: TLS · PQC · Post-Quantum Cryptography · Layered Risk Scoring · HNDL · Quantum Vulnerability Assessment · Crypto-Agility · Real-Time Packet Analysis

1 Introduction

The rapid advancement of quantum computing poses a serious threat to the public-key cryptographic systems that form the foundation of current Internet security. Shor's algorithm [17] has theoretically proven that a quantum computer with sufficient qubits can break RSA and Elliptic Curve Cryptography (ECC) in polynomial time, while Grover's algorithm [8] reduces the effective security strength of symmetric-key ciphers by half. Accordingly, the cryptographic

algorithms widely used in current TLS (Transport Layer Security) connections—RSA key exchange, ECDHE, and AES-128—cannot be guaranteed secure after the advent of quantum computers.

A particularly noteworthy threat is *Harvest Now, Decrypt Later* (HNDL) [14]. HNDL is a strategy in which adversaries collect and store currently encrypted traffic, then decrypt it in the future using quantum computers. This implies that TLS connections handling information with long-term confidentiality requirements are already exposed to risk, even though quantum computers have not yet been practically realized. In practice, connections transmitting data requiring long-term confidentiality in government agencies, financial institutions, and healthcare sectors are insufficiently protected by current security configurations alone.

In response, NIST has completed the standardization of Post-Quantum Cryptography (PQC) [15], and the introduction of hybrid schemes combining PQC algorithms such as ML-KEM and Falcon with existing key exchange methods in TLS 1.3 environments is underway. However, real-world network environments contain a heterogeneous mix of vulnerable connections at varying levels—legacy connections using TLS 1.0 or 1.2, RSA key exchange, and AES-128 cipher suites. Although existing studies such as CVSS v3.1 [6], Baseri et al. [2], and SQOUT [11] have made meaningful contributions in their respective domains, a systematic methodology that directly takes TLS connection parameters as input to immediately quantify quantum vulnerability including the HNDL threat remains absent. A detailed comparison of each study is provided in Section 2.

This paper proposes a layered risk scoring model that quantifies the quantum vulnerability of TLS connections on a 0–100 scale. The proposed model enables the decomposition of risk causes through five independent layers: protocol exposure (L1), legacy cryptographic algorithm vulnerability (L2a), symmetric-key weakening (L2b), PQC Level-1 vulnerability (L2c), and certificate expiration urgency (L3). It is differentiated from existing static evaluation approaches by continuously reflecting the confidentiality retention period of transmitted data in the final score through the HNDL global multiplier M. Furthermore, the proposed model is applied to an existing TLS packet analysis tool to verify its operation in real-world environments.

The main contributions of this paper are as follows.

- We propose a TLS-specific layered risk scoring model that quantifies the HNDL threat as a continuous multiplier M, directly reflecting the data protection period in the risk score.
- We design a hierarchical structure that separates TLS version, key exchange algorithm, cipher suite, PQC adoption status, and certificate state into independent layers, enabling decomposition of risk causes.
- We extend an existing `libpcap`-based TLS packet analysis tool to implement the proposed model and apply it to real-world traffic, validating the feasibility of priority-based response from an operator's perspective.

2 Background

2.1 Preliminaries

TLS Protocol and Key Exchange Methods TLS (Transport Layer Security) is a standard cryptographic protocol that ensures confidentiality, integrity, and authentication of Internet communications [16]. During the TLS handshake, the client and server negotiate the protocol version, cipher suite, and key exchange method.

Various TLS versions coexist in current deployment environments [10]. TLS 1.0 and 1.1 are effectively deprecated due to numerous discovered vulnerabilities such as POODLE and BEAST [13]. TLS 1.2 remains widely used but exhibits varying security levels depending on the key exchange method. TLS 1.3 is the current standard, which eliminates vulnerable cipher suites and simplifies the handshake to 1-RTT (with optional 0-RTT reconnection optimization).

Key exchange methods serve as an important classification criterion from the quantum threat perspective. RSA key exchange does not provide Forward Secrecy (FS), meaning past session keys can be decrypted upon server private key exposure. ECDHE (Elliptic Curve Diffie-Hellman Ephemeral) provides forward secrecy but is vulnerable to quantum attacks as it relies on the discrete logarithm problem [18,**?**]. Recently, hybrid key exchange methods combining post-quantum algorithms such as ML-KEM and Kyber with ECDHE have been deployed in production environments including Chrome and Cloudflare.

Quantum Threats: Shor's Algorithm and Grover's Algorithm The threats that quantum computing poses to current cryptographic systems are primarily explained by two algorithms.

Shor's algorithm [17] solves integer factorization and discrete logarithm problems in polynomial time. This renders all public-key cryptographic algorithms currently used in TLS—including RSA (factorization-based), ECDHE, and DSA (discrete logarithm-based)—ineffective. When a quantum computer with sufficient qubits becomes available, RSA-2048 could be broken within hours [7,**?**].

Grover's algorithm [8] performs unsorted database search in $O(\sqrt{N})$ time, reducing the time complexity of brute-force attacks on symmetric-key ciphers from $O(2^n)$ to $O(2^{n/2})$. Consequently, AES-128's effective security strength is halved to a 64-bit level, making it potentially vulnerable to well-resourced adversaries, whereas AES-256 still maintains 128-bit security strength.

HNDL (Harvest Now, Decrypt Later) Adversaries can collect today's encrypted traffic and decrypt it with future quantum computers. Therefore, even before quantum computers are practically realized, TLS connections requiring long-term confidentiality are already exposed to risk.

No key exchange method is free from the HNDL threat [3]. RSA key exchange lacks forward secrecy, allowing bulk decryption of all captured past sessions once the server private key is obtained. ECDHE, despite providing forward secrecy,

is also unsafe because the session key negotiation process itself is vulnerable to attack via Shor's algorithm.

This implies that most key exchange methods used in current TLS environments are potential targets of HNDL attacks, and a simple protocol upgrade alone cannot fully mitigate the threat.

PQC Standardization Trends To counter these threats, NIST has conducted Post-Quantum Cryptography (PQC) standardization since 2016, finalizing ML-KEM (FIPS 203) [15], ML-DSA (FIPS 204), SLH-DSA (FIPS 205), and FN-DSA (FIPS 206, Falcon-based) as final standards in 2024. NIST IR 8547 further specifies that RSA, ECDH, and DSA shall be deprecated by 2030 and fully prohibited by 2035 [12].

NIST PQC algorithms are classified by security level: Level 1 (AES-128 equivalent), Level 3 (AES-192 equivalent), and Level 5 (AES-256 equivalent). Level 1 algorithms (ML-KEM-512, Falcon-512, etc.) satisfy the minimum security requirement; however, some argue that they may not be sufficient under conservative evaluation criteria when considering symmetric-key strength reduction by Grover's algorithm. Level 3 and above (ML-KEM-768, Dilithium3, etc.) are currently assessed to provide adequate quantum resistance.

In terms of practical deployment, hybrid approaches that introduce PQC while maintaining compatibility with existing systems have been adopted. Chrome 131 and later natively support hybrid key exchange combining ML-KEM-768 with X25519 (group ID `0x11EC`), and Cloudflare has also deployed the same algorithm combination in production environments.

2.2 Related Work

Existing Risk Assessment Frameworks CVSS v3.1. CVSS (Common Vulnerability Scoring System) v3.1 [6] is a general-purpose vulnerability severity scoring system maintained by FIRST. It computes a score on a 0–10 scale by combining attack vector, attack complexity, privilege requirements, and confidentiality/integrity/availability impact. It consists of three metric groups—Base, Temporal, and Environmental—and is applied on a per-vulnerability (CVE) basis.

Baseri et al. Baseri et al. [2] proposed a comprehensive risk assessment framework covering the entire quantum-safe migration process. It applies the STRIDE threat model across three layers—algorithm, certificate, and protocol—at each stage of pre-migration, through-migration, and post-migration, producing qualitative risk ratings of Low/Medium/High.

SQOUT. SQOUT [11] is a threat intelligence platform developed by QuDef, designed exclusively for quantum communication systems. Inspired by MITRE ATT&CK, it organizes attack tactics, techniques, and procedures (TTPs) against QKD systems into a kill chain, and evaluates final risk using an ISO/IEC 27005-based risk matrix. It adopts a structure that assigns threat (T), exposure (E), and multiplier (m) to each attack stage. A detailed comparison is presented in Table 1; distinctions from this work are discussed in the following subsection.

Table 1. Comparison of existing risk assessment frameworks

Criterion	**CVSS v3.1**	**Baseri et al.**	**SQOUT**	**Ours**
Target domain	General vuln.	PQC migration	QKD system	Per-TLS connection
Scoring method	Quant. 0–10	Qual. L/M/H	Quant. kill chain	Quant. 0–100
HNDL	×	Conceptual	×	M quantified
TLS version differentiation	×	Qual. eval.	×	L1 direct input
Certificate expiry	×	Qual. analysis	×	L3 scored
PQC Lv.1 vulnerability	×	Qual. classif.	×	L2c flag
Operational correction m	Env. metric	×	Global M	Per-layer m
Per-connection automation	Manual	Manual	Separate tool	Immediate
Grover/ AES-128	×	Not reflected	×	L2b independent

Limitations of Existing Work and Distinctions of This Study While these three studies have made meaningful contributions in their respective domains, they share the following limitations in immediately quantifying the quantum risk of TLS connections.

CVSS v3.1 is a general-purpose scoring system for known vulnerabilities and does not directly reflect risk differences arising from TLS connection cipher suite combinations or protocol versions. Furthermore, it lacks a mechanism to integrate the future risk of current behavior, such as HNDL, into the score.

The framework by Baseri et al. is useful as a strategic assessment tool for migration roadmap development; however, it does not derive immediate quantitative scores for individual TLS connections, making it difficult to apply for real-time risk monitoring in operational environments.

SQOUT is designed exclusively for QKD systems and cannot be applied to TLS cipher suite-level analysis. While its global multiplier M represents the intensity of the threat environment, it does not provide a quantified mechanism linking the HNDL threat to data protection periods.

This study addresses these limitations by proposing a layered risk scoring model that directly takes TLS connection parameters as input, independently computes risk scores for each layer, and aggregates them. In particular, the HNDL threat horizon is quantified as a continuous global multiplier M, so that the final score increases as the confidentiality retention period of transmitted data grows longer. This directly reflects the temporal dimension of the HNDL threat in the risk score, which is difficult to express through existing qualitative evaluation approaches.

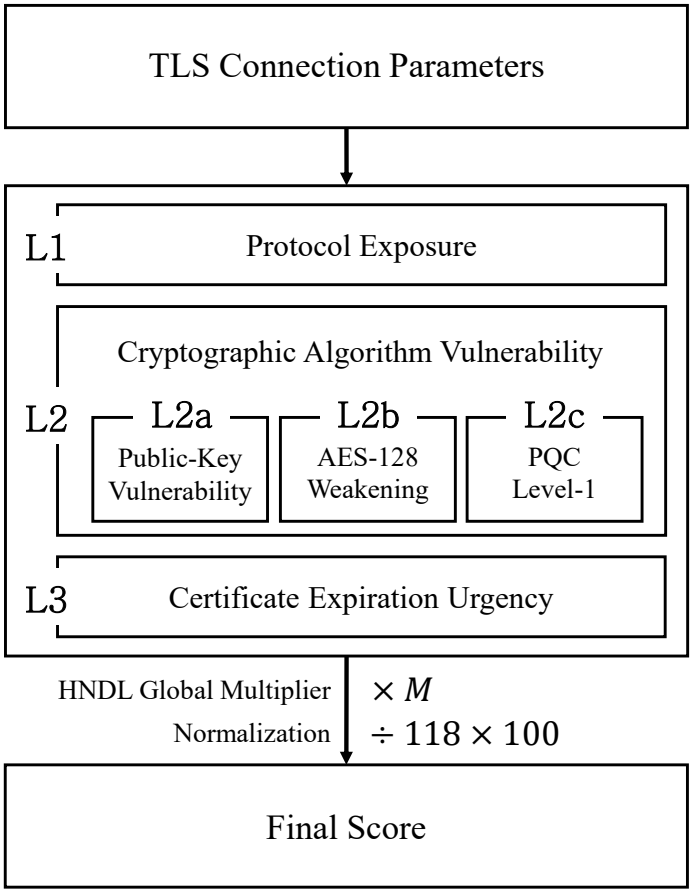

Fig. 1. Overall pipeline architecture

3 Proposed Method

3.1 Design Principles and Overall Architecture

The proposed model takes a single TLS connection as its evaluation unit, decomposes the causes of quantum threats into five independent layers, computes a score for each, and aggregates them. The final score is multiplied by the HNDL global multiplier M and normalized to produce an integer in the range 0–100.

$$\text{Final Score} = (L1 + L2a + L2b + L2c + L3) \times M \tag{1}$$

$$\text{Normalized} = \left\lfloor \frac{\text{Final Score}}{118} \times 100 \right\rfloor \quad \in [0,\, 100] \tag{2}$$

Table 2. Parameter symbol definitions

Symbol	English	Description
T	Threat	Attacker's destructive capability
E	Exposure	Baseline exposure of algorithm/protocol
e	Exposure Factor	Network exposure scope correction
m	Multiplier	Environmental correction multiplier (operational/implementation/key management)
M	HNDL Multiplier	HNDL global multiplier

Each layer addresses a distinct threat dimension. L1 measures the structural exposure of the TLS protocol version, L2a quantifies the quantum vulnerability of legacy public-key algorithms (RSA, ECDHE/DHE), L2b addresses AES-128 weakening by Grover's algorithm, L2c captures the conservative vulnerability of Level-1 algorithms in PQC hybrid deployments, and L3 quantifies certificate expiration urgency.

The parameter symbols of the model are defined in Table 2.

T represents not the difficulty of an attack but the *destructive impact upon successful attack*. Even when the probability of occurrence is low, T is assigned a high value if the destructive impact is large. In principle, T is set by the operator for each layer with reference to Table 4. However, for L2b and L2c, fixed values are used as the required technical level for the corresponding attacks is well-defined. E represents how easily the given algorithm or protocol is exposed to attack. T and E measure different dimensions, and their product forms the baseline risk intensity of the layer [5]. m is a correction coefficient that reflects operational policies (HSTS enforcement, HSM usage, key rotation policy, PQC implementation quality, etc.) not captured by $T \times E$. The reference values of the environmental correction multiplier m for each layer are shown in Table 3.

The scale of T is defined as shown in Table 4.

3.2 Layer 1: TLS Protocol Exposure (L1)

L1 measures the structural vulnerability based on the TLS protocol version and key exchange method. A standard TLS 1.3 connection has no known protocol-level vulnerabilities in its current design, so L1 = 0.

$$L1 = T \times E \times m \tag{3}$$

E is determined by the negotiated TLS version and key exchange method as shown in Table 5. TLS 1.0 has the highest exposure due to multiple publicly disclosed vulnerabilities such as POODLE and BEAST [13,**?**]. TLS 1.2 with ECDHE has lower exposure than TLS 1.2 with RSA key exchange, as it provides forward secrecy. TLS 1.3 + PQC Hybrid is assigned a non-zero value reflecting the residual quantum risk from the classical key exchange component (e.g., X25519 in the hybrid scheme), which remains theoretically vulnerable to Shor's algorithm.

Table 3. Environmental correction multiplier m reference values per layer

Layer	Condition	m
L1	HSTS enforced + Certificate Pinning	0.6
	HSTS applied	0.8
	Default (no correction)	1.0
	No TLS downgrade monitoring	1.2
	Legacy client allowed (mixed environment)	1.4
L2a	HSM used + periodic key rotation policy	0.6
	Periodic key rotation policy only	0.8
	Default (no correction)	1.0
	No key rotation / long-term static key	1.3
	Key compromise history	1.5
L2b	Short session + strong KDF (HKDF, etc.)	0.7
	Periodic session key renewal policy	0.8
	Default (no correction)	1.0
	No KDF / weak key derivation	1.2
	Static key + no session renewal	1.4
L2c	Constant-time implementation verified	0.6
	Audited PQC library used	0.8
	Default (no correction)	1.0
	Unverified custom PQC implementation	1.3
	Implementation with known side-channel vulnerability	1.5

m reflects operational policies that are not captured by TLS version and network exposure. Environments with both HSTS enforcement and Certificate Pinning have reduced downgrade attack potential with $m < 1$, while mixed environments with legacy client allowance policies have increased risk with $m > 1$. Reference values for m are given in Table 3.

3.3 Layer 2: Cryptographic Algorithm Vulnerability (L2a, L2b, L2c)

Layer 2 comprises three sub-layers based on the type of cryptographic algorithm in use. Each sub-layer has independent activation conditions; if the condition is not met, the corresponding score is 0.

L2a: Legacy Public-Key Algorithm Vulnerability L2a applies to connections using legacy public-key algorithms threatened by Shor's algorithm. PQC-only connections skip this layer.

$$L2a = T \times E \times e \times m \tag{4}$$

E is assigned different values for RSA and ECDHE/DHE according to the quantum vulnerability level of the algorithm. RSA key exchange, lacking forward secrecy, is a direct target of HNDL attacks and thus has a higher E.

Table 4. T (attacker destructive capability) scale

Level (T)	Definition
1	Only publicly available automated tools required; no specialized capability needed.
2	Basic hacking tools and moderate technical knowledge required.
3	Advanced classical attack capability or partial quantum technology access required.
4	Practical quantum computer required; applicable to a broad range of sessions upon emergence.
5	Nation-state-level resources and cutting-edge R&D capabilities required.

Table 5. L1 protocol-specific E values

TLS Version	Key Exchange	E
1.0	—	5.0
1.1	—	4.0
1.2	RSA, other	2.0
1.2	ECDHE	1.5
1.3	PQC Hybrid	1.0
1.3	—	0

ECDHE/DHE provides forward secrecy but has the discrete logarithm problem vulnerable to Shor's algorithm, resulting in a relatively lower E. The baseline E values per cryptographic algorithm are shown in Table 6.

e is a coefficient that corrects E by reflecting the network exposure scope of the connection target. Connections to local or private IP ranges require physical access and thus receive a lower e, while Internet port 443 is the most broadly exposed environment with $e = 1.0$. The reference e values per connection target are shown in Table 7.

m reflects key management policies. When HSM usage and periodic key rotation are combined, $m < 1$ mitigates risk; environments with key compromise history or long-term static key usage have $m > 1$ increasing risk. Reference values for m are given in Table 3.

L2b: AES-128 Grover Weakening L2b applies when AES-128 is included in the cipher suite. AES-256 maintains 128-bit security strength even after Grover's algorithm and thus does not activate this layer.

$$L2b = T \times E \times m \tag{5}$$

T is fixed at 4.0, reflecting that executing Grover's algorithm requires a quantum computer with sufficient qubits. E is fixed at 0.5, reflecting that Grover's

Table 6. L2a baseline E values per cryptographic algorithm

Cryptographic Algorithm	Baseline E
RSA	5.0
ECDHE/DHE	3.0

Table 7. L2a exposure scope coefficient e per connection target

Connection Target	e	Effect
Local (127.x, 192.168.x, etc.)	0.25	$E \to \frac{1}{4}E$
Non-standard port / internal network	0.50	$E \to \frac{1}{2}E$
Internet port 443	1.00	$E \to E$

algorithm does not completely break AES-128 but merely reduces its effective security strength from 128 bits to a 64-bit level.

m reflects the key derivation and session management level. Short sessions combined with strong KDF (HKDF, etc.) use $m < 1$; static keys with no session renewal use $m > 1$. Reference values for m are given in Table 3.

L2c: PQC Level-1 Vulnerability L2c applies when PQC hybrid cryptography is in use but the PQC algorithm corresponds to NIST Level-1. L2c is activated only when all three of the following conditions are simultaneously satisfied; if any is unmet, L2c = 0.

1. PQC hybrid cryptography is in use (`is_pqc_hybrid = 1`)
2. The PQC algorithm is Level-1 (`pqc_vuln = 1`)
3. The setting that treats Level-1 as vulnerable is enabled (`pqc_level1_vulnerable = 1`)

$$L2c = T \times E \times m \tag{6}$$

T is fixed at 3.0, reflecting that Level-1 PQC algorithms provide only AES-128-equivalent security strength, which can be threatened by Grover-class quantum operations—requiring partial but not full-scale quantum capability, consistent with the $T = 3$ definition. E is fixed at 2.0: although Level-1 PQC algorithms provide 128-bit classical security, under quantum threats they undergo the same Grover-induced strength reduction as symmetric keys, warranting an exposure value consistent with this conservative assessment.

NIST PQC Level-1 algorithms (ML-KEM-512, Falcon-512, etc.) are designed to provide 128-bit security equivalent to AES-128. However, considering symmetric-key strength reduction by Grover's algorithm, a conservative view exists that Level-1 may not provide sufficient quantum safety. L2c adopts this conservative stance while allowing operators to directly decide whether to activate it through a configuration flag (`pqc_level1_vulnerable`).

Table 8. HNDL global multiplier M by threat horizon h

h (years)	Calculation	M
0	$1.0 + 0/20$	1.00
5	$1.0 + 5/20$	1.25
10	$1.0 + 10/20$	1.50
20	$1.0 + 20/20$	2.00

m reflects the quality of PQC implementation and side-channel defense level. When constant-time implementation is verified, $m < 1$; implementations with known side-channel vulnerabilities use $m > 1$. Reference values for m are given in Table 3.

3.4 Layer 3: Certificate Expiration Urgency (L3)

L3 scores the expiration status of X.509 certificates. It applies only when certificate information is available (`cert_info_available = 1`), and increases linearly based on the number of days remaining until expiration (d).

$$L3 = \begin{cases} 5.0 & d < 0 \quad \text{(already expired)} \\ 5.0 \times \dfrac{30 - d}{30} & 0 \le d < 30 \\ 0 & d \ge 30 \end{cases} \tag{7}$$

An expired certificate receives the maximum L3 = 5.0, while certificates with 30 or more days remaining have L3 = 0. Within the 30-day imminent expiration window, the score increases linearly in inverse proportion to the remaining days. m is not applied to L3, as certificate expiration is an objectively measurable state independent of operational policies.

3.5 HNDL Global Multiplier M

M is a global multiplier that reflects how long the information transmitted over a connection must remain confidential. It is applied as the final multiplication after aggregating all layer scores.

$$M = 1.0 + \frac{h}{20.0}, \quad M \in [1.0,\, 2.0] \tag{8}$$

Here, h is the HNDL threat horizon, representing the period (in years) during which transmitted data must remain confidential. When $h = 0$, $M = 1.0$ with no HNDL weighting; when $h = 20$, $M = 2.0$, doubling the total score. Table 8 shows the variation of M with respect to h.

The design intent of M is as follows. Even though quantum computers do not currently exist, adversaries can collect and store current traffic. The longer the confidentiality retention period of transmitted data, the higher the risk that the traffic will be decrypted in the future. M quantifies this temporal risk dimension as a continuous multiplier and directly reflects it in the final score [9,**?**].

3.6 Final Score Computation

The final score is computed according to Equations (1) and (2). The normalization reference value of 118 is the practical upper bound derived from the worst-case scenario in a legacy TLS environment (TLS 1.0 + RSA + AES-128 + expired certificate), applying the reference threat levels ($T = 3$ for L1, $T = 4$ for L2a and L2b), maximum environmental correction multipliers m per layer, and HNDL threat horizon $h = 20$ ($M = 2.0$). L1 and L2c cannot structurally reach their maxima simultaneously (L1 maximum requires TLS 1.0, while L2c requires TLS 1.3 + PQC hybrid), so this scenario represents the practical maximum. When $M > 1.0$, the normalized score may exceed 100, in which case it is clamped to 100.

Since each layer is computed independently, the final score can be decomposed by layer to identify which factors contribute to elevated risk. This is advantageous over conventional single-score approaches, enabling operators to take priority-based remediation actions.

3.7 Implementation and Demonstration

The implementation of the proposed model and a real-time risk visualization dashboard are publicly available at the following repository:

https://github.com/yulim4hyoung/tls-quantum-risk-scorer

The dashboard provides a browser-based demonstration page for inspecting per-session layer score decomposition, sector-level risk distributions, and HNDL multiplier sensitivity in real time.

4 Experiments and Evaluation

This section establishes the following two research questions to validate the effectiveness of the proposed layered risk scoring model.

- **RQ1.** Does the proposed model meaningfully decompose and quantify the quantum vulnerability of TLS connections by layer?
- **RQ2.** When the proposed model is applied to real-world traffic, does it meaningfully reflect the quantum risk differences between domestic and global companies?

4.1 Experimental Setup

The experiments were conducted based on the quantum-vulnerable TLS automated analysis framework proposed by Cho et al. [4]. This framework automatically extracts cryptographic parameters of TLS connections through packet inspection. The risk scoring model proposed in this paper was applied to this framework for real-world validation. Experiments were performed on Windows

11 and Kali Linux environments, using WinPcap and libpcap for packet capture, respectively. The OQS OpenSSL library was used for PQC-related cryptographic operations.

The analysis targets were real-time TLS traffic from major domestic and international companies and agencies across four industry sectors (Finance, E-commerce/Platform, Public, and Telecom/Media). A total of 502 TLS sessions (by SNI) were collected: 274 domestic and 228 global. The proposed model received the TLS version, key exchange method, cipher suite, and certificate expiration status of each session as input to compute per-layer risk scores. The HNDL threat horizon h was set to 10 years ($M = 1.50$), corresponding to a moderate threat scenario reflecting current predictions for quantum computer emergence.

Table 9. Fixed parameters and rationale for the experiment

Parameter	**Layer**	**Value**	**Rationale**
m (env. multiplier)	L1–L3	1.0	Unobservable operational policies; neutral value
T (threat level)	L1	3.0	Nation-state-level quantum attacker assumed
T, E (RSA)	L2a	4.0, 5.0	Shor compromise + no forward secrecy
T, E (ECDHE)	L2a	4.0, 3.0	Shor compromise; forward secrecy present
e (exposure)	L2a	1.0	All sessions via Internet port 443
T, E	L2b	4.0, 0.5	Grover threat; limited symmetric-key impact
T, E (PQC Lv.1)	L2c	3.0, 2.0	Conservative evaluation mode enabled
h (HNDL horizon)	M calc.	10 yr	Moderate scenario per Mosca timeline

4.2 RQ1: Per-Layer Score Distribution Analysis

The per-layer scores computed for the 502 sessions are summarized in Fig. 2. L1 averaged 2.62 for domestic and 1.67 for global sessions, reflecting the persistence of legacy TLS versions in both groups. L2a showed a higher non-PQC legacy key exchange usage rate in domestic sessions (77.4%) compared to global (53.5%). RSA key exchange sessions produced higher L2a scores than ECDHE, numerically confirming the risk difference based on the presence or absence of forward secrecy. L2b was triggered in sessions using AES-128 cipher suites across both groups (domestic 60.0%, global 73.5%). L2c was 0 across all sessions: 62

domestic (22.6%) and 106 global (46.5%) sessions negotiated PQC Hybrid key exchange, but all used ML-KEM-768 (NIST Level-3), so no Level-1 vulnerability was triggered. L3 scores were low in both groups: domestic avg. 0.15 and global avg. 0.09, confirming that most certificates had more than 30 days remaining.

The independent per-layer computation structure enables decomposition of risk causes that are difficult to identify with a single score, facilitating priority-based operator response.

The parameters for each layer were configured as follows. Table 9 summarizes the fixed parameters and their rationale.

Environmental correction multiplier m (common across all layers). External packet analysis alone cannot observe the target server's operational policies (HSTS enforcement, HSM usage, key rotation policy, etc.). Maintaining a neutral value is more consistent with evaluation reliability than introducing uncertain estimations, so $m = 1.0$ was applied to all layers.

L1 — Threat actor level $T = 3.0$ (fixed). It is reasonable to assume that actors capable of practically operating quantum computers to decrypt TLS sessions are at the nation-state level with substantial resources. Accordingly, $T = 3.0$ was fixed.

L2a — Exposure scope $e = 1.0$ (fixed). All collected sessions were Internet connections via port 443, making local (0.25) and internal network (0.5) scenarios inapplicable, so $e = 1.0$ was fixed. For RSA key exchange, $T = 4.0$ and $E = 5.0$ were applied; for ECDHE, $T = 4.0$ and $E = 3.0$. RSA, lacking forward secrecy, exposes all previously collected ciphertexts to quantum attacks, warranting a higher E value compared to ECDHE.

L2b — $T = 4.0$, $E = 0.5$ (fixed). Grover's algorithm reduces the effective key length of AES-128 from the 128-bit level to the 64-bit level. The threat actor level was set to $T = 4.0$, identical to L2a, but the vulnerability index was fixed at a lower $E = 0.5$, as symmetric-key attacks have limited practical impact compared to asymmetric key exchange compromise.

L2c — Level-1 PQC vulnerability detection enabled. ML-KEM-512 and other NIST Level-1 algorithms provide 128 bit security strength equivalent to AES-128, and their effective strength may be degraded by Grover's attack. The conservative evaluation mode ($T = 3.0$, $E = 2.0$) was enabled to treat this as vulnerable. As all observed PQC Hybrid sessions negotiated ML-KEM-768 (NIST Level-3), no Level-1 vulnerability was triggered, and L2c was computed as 0 throughout the experiment.

HNDL threat horizon $h = 10$ ($M = 1.50$). The quantum threat timeline reports by Mosca and Piani [14,**?**] suggests the possibility of a cryptographically relevant quantum computer emerging within 10 years. Setting $h = 10$ yields $M = 1.0 + (10/20) = 1.50$, corresponding to a moderate threat scenario between optimistic ($h = 5$, $M = 1.25$) and pessimistic ($h = 20$, $M = 2.00$).

4.3 RQ2: Domestic vs. Global Company Risk Comparison

Applying the proposed model to 274 domestic sessions and 228 global sessions revealed a clear difference in final risk scores between the two groups. Domes-

tic sessions had a non-PQC legacy key exchange (RSA/ECDHE) usage rate of 77.4%, higher than the global rate of 53.5%, resulting in elevated L2a scores (8.66 vs. 6.26). With the HNDL global multiplier $M = 1.50$ applied, the average final score of domestic sessions (16.0) was 4.1 points higher than global sessions (11.9), confirming that the temporal risk dimension quantitatively reveals the domestic–global gap.

PQC Hybrid adoption was observed in 62 domestic (22.6%) and 106 global (46.5%) sessions, all negotiating ML-KEM-768 (NIST Level-3), yielding L2c = 0. The substantially higher PQC adoption rate in global traffic reflects early deployment by major CDN and cloud providers, whereas domestic PQC adoption remains concentrated in a small number of platform and media services.

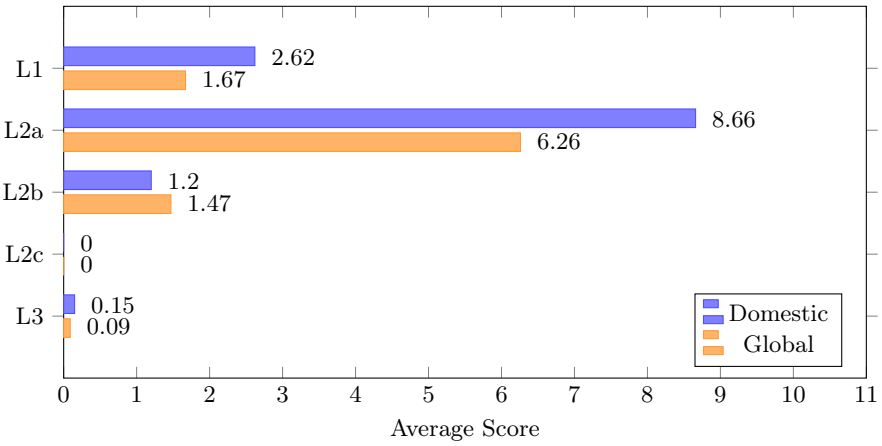

Fig. 2. Per-layer average score distribution (502 sessions, m=1.0)

4.4 Risk Profiles by Industry Sector

To evaluate the model's discriminative capability beyond aggregate averages, we examine per-sector score distributions for both the domestic and global groups.

Domestic Sector Analysis Table 10 summarizes the per-sector layer and final score averages for the domestic group.

Table 10. Domestic per-sector layer score averages

Sector	L1	L2a	L2b	L2c	L3	Final
Finance (n=74)	3.63	8.92	1.00	0.00	0.00	17.3
E-commerce/Platform (n=120)	2.49	8.17	1.42	0.00	0.26	15.6
Public (n=26)	2.88	11.69	0.54	0.00	0.32	19.5
Telecom/Media (n=54)	1.39	7.94	1.30	0.00	0.00	13.5
Total (n=274)	2.62	8.66	1.20	0.00	0.15	16.0

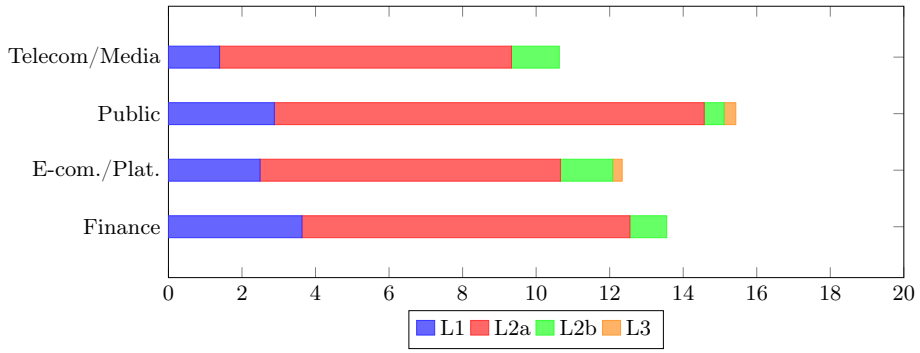

Fig. 3. Domestic per-sector layer score distribution (m=1.0, L2c=0 excluded)

Classifying domestic sessions by industry sector reveals clear patterns of risk concentration. The public sector recorded the highest final score (19.5). TLS 1.2 + static RSA sessions triggered the maximum penalties L1 = 6.0 and L2a = 20.0 simultaneously, producing multiple 33-point sessions at hometax.go.kr (simultaneous L1+L2a activation). Overall, 30.8% of public sector sessions fell in the medium-risk band (30–70 points).

The financial sector ranked second with a final score of 17.3, but exhibits wide intra-sector disparity driven by divergent PQC adoption. Early PQC Level-3 adopters achieved averages as low as 9.4, whereas institutions without PQC transition maintained scores in the 21–24 range. Major financial institutions predominantly use TLS_ECDHE_RSA, providing forward secrecy but still exposing RSA server certificates to Shor's algorithm.

The e-commerce/platform sector (15.6) shows a large intra-sector gap. Institutions with 86.1% PQC adoption averaged 7.2 points, while non-adopters remained in the 19–21 range. Notably, the highest-risk session in the entire domestic dataset—gmarket.co.kr at 35 points—belongs to this sector, combining maximum L1 and L2a penalties (TLS 1.2 + static RSA) with a near-expired certificate ($L_3 = 1.83$).

The telecom/media sector recorded the lowest domestic final score (13.5). An institution with 76.9% PQC adoption achieved 10.2 points, while non-adopters remained in the 16–18 range.

Global Sector Analysis Table 11 summarizes the per-layer and final score averages for each global sector. Global scores are more uniformly distributed across sectors (range: 11.3–13.5), reflecting more homogeneous TLS migration progress compared to the domestic group. The global financial sector recorded the highest final score (13.5), driven by persistent RSA/ECDHE use among major institutions despite partial PQC adoption (35.7%).

Table 11. Global per-sector layer score averages

Sector	L1	L2a	L2b	L2c	L3	Final
Finance (n=42)	1.93	7.71	1.00	0.00	0.07	13.5
E-commerce/Platform (n=77)	1.73	5.77	1.66	0.00	0.08	11.7
Public/Gov (n=18)	1.58	5.67	1.67	0.00	0.10	11.3
Telecom/Media (n=91)	1.52	6.13	1.49	0.00	0.10	11.6
Total (n=228)	1.67	6.26	1.47	0.00	0.09	11.9

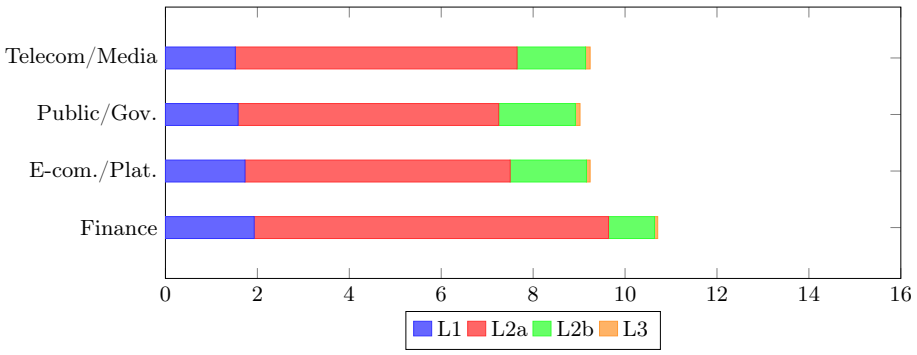

Fig. 4. Global per-sector layer score distribution (m=1.0, L2c=0 excluded)

Global financial institutions show contrasting profiles within the sector. Institutions with 100% PQC adoption recorded averages as low as 6.0, while non-adopters ranged from 15 to 20 points, driving the sector average to 13.5. The e-commerce/platform sector achieved the highest global PQC adoption rate (51.9%), with several institutions reaching 100% Level-3 sessions. Notably, an organization responsible for standardizing PQC algorithms recorded a final score of 18.0 with 0% PQC deployment on its own domains, demonstrating a persistent gap between policy leadership and operational deployment.

Table 12. Average final scores by HNDL threat horizon scenario

Scenario	h	M	Domestic Avg.	Global Avg.	Gap
Optimistic	5 yr	1.25	13.3	10.0	3.3
Baseline	10 yr	1.50	16.0	11.9	4.1
Pessimistic	20 yr	2.00	21.2	15.9	5.3

Cross-Group Comparison Comparing Tables 10 and 11, three observations stand out. First, the domestic public sector (19.5) is the highest-risk group across both datasets, driven by TLS 1.0 + static RSA deployments absent from global traffic. Second, while the domestic financial sector (17.3) exceeds all global sector averages, the global financial sector (13.5) is the highest-risk global sector, reflecting that institutions without PQC adoption carry the heaviest legacy burden. Third, both groups share L2c = 0.00, but for structurally different reasons: domestic traffic remains predominantly non-PQC (77.4%), while global traffic shows higher PQC penetration (46.5%) yet all observed PQC sessions use Level-3 algorithms, triggering no L2c activation in either group.

4.5 HNDL Multiplier Sensitivity Analysis

Since the HNDL threat horizon h is a parameter with high uncertainty, the average score variation was examined across three scenarios: optimistic ($h = 5$, $M = 1.25$), baseline ($h = 10$, $M = 1.50$), and pessimistic ($h = 20$, $M = 2.00$). In the final score formula $S = (\sum L_i) \times M$, since M is a linear multiplier, scenario-specific scores can be computed by multiplying the baseline score by the ratio.

Across the three scenarios, the domestic–global gap ranges from 3.3 to 5.3 points, confirming that domestic risk consistently remains higher regardless of the M value. This suggests that the source of the gap lies not in the HNDL scenario assumptions but in the structural difference in PQC adoption rates and legacy key exchange usage—particularly the static RSA ciphers and low PQC penetration concentrated in the domestic public and financial sectors.

5 Conclusion

This paper proposed a layered risk scoring model that directly takes TLS connection parameters as input to immediately quantify quantum threat exposure on a 0–100 scale. CVSS v3.1 cannot directly reflect TLS cryptographic parameters, the framework by Baseri et al. is not suitable for real-time quantitative evaluation at the individual connection level, and SQOUT is designed exclusively for QKD systems, limiting its applicability to TLS-level analysis. The proposed model fills this gap by specifically identifying risk causes through independent decomposition across five layers, and directly reflecting the temporal dimension of the HNDL threat in the final score via the continuous global multiplier M, clearly differentiating it from existing static evaluation approaches.

In real-world application, the legacy key exchange (RSA/ECDHE) usage rate of domestic companies was 77.4%, higher than the global rate of 53.5%, resulting in elevated L2a scores. The average final risk scores were 16.0 for domestic companies and 11.9 for global companies, quantitatively confirming the domestic–global gap. With the HNDL threat horizon $h = 10$ ($M = 1.50$) applied, the temporal risk dimension was directly reflected in the scores, confirming that the proposed model effectively reveals risk factors that are difficult to capture with single-score approaches.

Even today, when quantum computers have not yet been practically realized, HNDL adversaries may already be harvesting current encrypted traffic. This research provides a practical tool that enables operators to immediately determine, on a per-connection basis, which connections should be prioritized for PQC transition before this threat materializes. The empirical finding that the risk scores of major domestic services are higher than global averages—with PQC adoption at only 22.6% domestically versus 46.5% globally—demonstrates through data that the PQC transition of domestic Internet infrastructure is an urgent task.

Future work considers the following five directions.

1. **Automation of the environmental correction multiplier m.** Currently, m is fixed at a default value of 1.0 because operational policies cannot be observed externally. Automatically estimating m through machine learning models using traffic patterns and side-channel measurement data can directly address this limitation.
2. **Integration with JA4 fingerprinting [1] based on ClientHello.** The current framework already parses SNI, supported groups, and cipher suite lists from ClientHello. Aggregating these into JA4 hashes enables differentiated risk scoring per client for the same server domain.
3. **Full certificate chain tracking.** Currently, L3 reflects only the expiration status of the server certificate. Since RSA keys remaining in intermediate CA certificates are also targets of quantum threats, extending L3 to incorporate the algorithms and expiration status of the entire chain is necessary.
4. **Large-scale real-world validation and protocol extension.** The current experiment is limited to 502 sessions. Validating the model's generalizability with more domains and sessions, and quantitatively measuring the frequency of OID fallback—cases where the server reverts to a classical key exchange group due to an unrecognized PQC hybrid group identifier—is needed. Furthermore, extending the analysis scope to TLS 1.3-embedded protocols such as QUIC (UDP/443) can also be considered.
5. **Extension to other domains.** Although the hierarchical decomposition structure and HNDL multiplier-based temporal risk reflection of this model are designed specifically for TLS, applying the same framework to the entire PKI infrastructure (CA hierarchy, root trust chains) or database access control (DB transport encryption, stored key management) is also feasible. In particular, evaluating quantum vulnerability by signature algorithm and

key length of intermediate CA certificates in PKI environments can directly lead to further research, making it a promising future direction.

References

1. Althouse, J.: JA4+: Network fingerprinting. FoxIO (2023)
2. Baseri, Y., Chouhan, V., Ghorbani, A., Chow, A.: Evaluation framework for quantum security risk assessment: A comprehensive strategy for quantum-safe transition. arXiv preprint arXiv:2404.08231 (2024)
3. Blanco-Romero, J., Mendoza, F.A., Rubio, C.G., Campo, C., Sánchez, D.D.: On the practical feasibility of harvest-now, decrypt-later attacks. arXiv preprint arXiv:2603.01091 (2026)
4. Cho, S.B., Hyoung, Y.L., Kim, H., Sim, M., Chattopadhyay, A., Seo, H.J., Kim, H.: Toward crypto agility: Automated analysis of quantum-vulnerable TLS via packet inspection. In: International Conference on Security, Privacy, and Applied Cryptography Engineering. pp. 114–133. Springer Nature Switzerland, Cham (Dec 2025)
5. ETSI: Quantum-safe cryptography; quantum-safe threat assessment. Group Report GR QSC 004, ETSI (2015)
6. FIRST.Org: Common vulnerability scoring system version 3.1: Specification document. Tech. rep., FIRST (2019)
7. Gidney, C., Ekerå, M.: How to factor 2048-bit RSA integers in 8 hours using 20 million noisy qubits. Quantum **5**, 433 (2021). https://doi.org/10.22331/q-2021-04-15-433
8. Grover, L.K.: A fast quantum mechanical algorithm for database search. In: Proceedings of the 28th Annual ACM Symposium on Theory of Computing. pp. 212–219 (1996)
9. Kagai, F., Branch, P., But, J., Allen, R.: Harvest-now, decrypt-later: A temporal cybersecurity risk in the quantum transition. Telecom **6**(4), 100 (2025). https://doi.org/10.3390/telecom6040100
10. Kotzias, P., Matic, S., Rivera, R., Caballero, J.: Coming of age: A longitudinal study of TLS deployment. In: Proceedings of the ACM Internet Measurement Conference. pp. 415–428 (2018). https://doi.org/10.1145/3278532.3278568
11. Krelina, M., Sorger, T., Dirks, B.: SQOUT: A risk-based threat analysis framework for quantum communication systems. arXiv preprint arXiv:2510.23462 (2025)
12. Moody, D., et al.: Transition to post-quantum cryptography standards. Tech. Rep. NIST IR 8547 ipd, NIST (2024)
13. Moriarty, K., Farrell, S.: RFC 8996: Deprecating TLS 1.0 and TLS 1.1. RFC 8996, IETF (2021)
14. Mosca, M., Piani, M.: 2023 quantum threat timeline report. Tech. rep., Global Risk Institute (2023)
15. National Institute of Standards and Technology: FIPS 203: Module-lattice-based key-encapsulation mechanism standard. Tech. rep., NIST (2024)
16. Rescorla, E.: RFC 8446: The transport layer security (TLS) protocol version 1.3. Tech. rep., IETF (2018)
17. Shor, P.W.: Algorithms for quantum computation: Discrete logarithms and factoring. Proceedings of the 35th Annual Symposium on Foundations of Computer Science (1994)

18. Springall, D., Durumeric, Z., Halderman, J.A.: Measuring the security harm of TLS crypto shortcuts. In: Proceedings of the ACM Internet Measurement Conference. pp. 33–47 (2016). https://doi.org/10.1145/2987443.2987480