Toward Quantum-Resilient and Privacy-Preserving Student Attendance Systems Using Hybrid Post-Quantum Cryptography

Derry Setiawan*[1]
Fakultas Komputer dan Desain, Universitas Selamat Sri
E-mail : sdlc19092021@gmail.com
Received 23 April 2026; Revised 24 July 2026; Accepted 25 July 2026

Abstract - The rapid digital transformation of academic record and student attendance systems demands security mechanisms that simultaneously provide confidentiality, integrity, privacy-preserving data analytics, and long-term resilience against emerging quantum threats. While conventional cryptographic algorithms such as RSA, ECC, and AES remain computationally efficient, public-key schemes based on RSA and ECC are vulnerable to quantum attacks, limiting their suitability for protecting sensitive educational information in the long term. Existing studies generally focus either on post-quantum secure communication or on privacy-preserving computation, resulting in fragmented security architectures that increase implementation complexity in resource-constrained academic environments. To address this challenge, this paper proposes a Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA) that integrates the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM) for quantum-resistant session key establishment, AES-GCM for authenticated encryption of attendance records, and the Paillier additive homomorphic cryptosystem for privacy-preserving aggregation of attendance statistics over encrypted data. By assigning each cryptographic primitive according to its intended function, the proposed architecture achieves quantum-secure key establishment, efficient symmetric data protection, and secure encrypted computation without relying on post-quantum algorithms for bulk data encryption. Experimental evaluation demonstrates that incorporating the Paillier cryptosystem introduces only modest computational overhead while preserving practical encryption latency, reducing key establishment latency by 28–35%, decreasing CPU utilization by 22%, and maintaining bandwidth overhead below 12% compared with conventional hybrid deployment architectures that perform secure communication without privacy-preserving aggregation. These results demonstrate that the proposed integration of CRYSTALS-Kyber, AES-GCM, and the Paillier cryptosystem provides an effective balance between quantum resilience, computational efficiency, and privacy-preserving analytics, making LHPQCA suitable for next-generation academic attendance systems and other resource-constrained educational applications.

Keywords - Post-Quantum Cryptography, Hybrid Cryptographic Algorithm, CRYSTALS-Kyber, Key Encapsulation Mechanism (KEM), AES-GCM, Paillier Cryptosystem, Privacy-Preserving Analytics.

1. INTRODUCTION

The rapid digital transformation of higher education has significantly accelerated the adoption of electronic student attendance systems to improve administrative efficiency, minimize manual errors, and provide real-time academic monitoring. Modern attendance platforms increasingly utilize technologies such as Radio Frequency Identification (RFID), Quick Response (QR) codes, biometric authentication, Near Field Communication (NFC), and cloud-based information systems to automate attendance recording and support institutional decision-making

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

[1], [2]. Besides improving operational efficiency, digital attendance data have become valuable institutional assets for evaluating student participation, learning engagement, accreditation, and educational analytics [3]. Despite these advantages, the increasing reliance on cloud computing and network-based infrastructures introduces substantial security and privacy challenges. Student attendance records contain personally identifiable information (PII), including student identities, timestamps, course enrollment, and attendance history. Unauthorized disclosure or modification of these records may violate privacy regulations, compromise academic integrity, and reduce institutional trust [4], [5]. Consequently, confidentiality, integrity, authenticity, and secure data sharing have become fundamental requirements for next-generation academic attendance systems. Most existing attendance security frameworks employ conventional cryptographic algorithms such as Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Elliptic Curve Cryptography (ECC) to protect stored and transmitted attendance records [6], [7]. AES continues to provide highly efficient symmetric encryption for bulk data, whereas RSA and ECC are widely adopted for public-key cryptography and secure key exchange. However, the rapid development of large-scale quantum computing presents a significant challenge to these public-key cryptographic systems. Shor's algorithm theoretically enables polynomial-time factorization and discrete logarithm computation, rendering RSA and ECC vulnerable once practical quantum computers become available [8], [9]. Consequently, although AES remains relatively resistant to quantum attacks with increased key sizes, the public-key infrastructure supporting secure communication requires migration toward quantum-resistant cryptographic mechanisms. To address this emerging threat, the National Institute of Standards and Technology (NIST) has standardized several Post-Quantum Cryptography (PQC) algorithms, including the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM), which provides quantum-resistant session key establishment based on lattice cryptography [10], [11]. Unlike traditional public-key encryption schemes, Kyber is specifically designed for secure key encapsulation rather than bulk data encryption. Therefore, practical post-quantum architectures generally combine Kyber for session key establishment with efficient symmetric algorithms such as AES-GCM to encrypt large datasets. This hybrid cryptographic architecture achieves quantum-resistant communication while preserving computational efficiency suitable for real-world applications [12]. In parallel with the emergence of post-quantum cryptography, educational institutions increasingly require secure data analytics without exposing sensitive student information. Attendance statistics are frequently aggregated to evaluate student participation, classroom performance, and institutional quality assurance. Conventional encryption protects data confidentiality but requires complete decryption before statistical processing, exposing sensitive information during computation [13]. Privacy-Preserving Data Analytics (PPDA) addresses this limitation through homomorphic encryption, enabling mathematical operations to be performed directly on encrypted data. Among various homomorphic encryption schemes, the Paillier cryptosystem provides additive homomorphic properties with relatively low computational complexity, making it suitable for secure aggregation of attendance statistics without revealing individual attendance records [14], [15]. Although previous studies have investigated post-quantum cryptography for secure communication [16], [17] and homomorphic encryption for privacy-preserving analytics [18], these approaches are generally developed independently. Existing research primarily focuses on quantum-resistant key exchange or encrypted computation separately, resulting in fragmented architectures that increase implementation complexity and computational overhead. Furthermore, several studies incorrectly evaluate lattice-based post-quantum algorithms as mechanisms for encrypting bulk datasets, despite the fact that standardized algorithms such as CRYSTALS-Kyber function exclusively as Key Encapsulation Mechanisms (KEMs) rather than data encryption algorithms [19]. Consequently, there remains limited research investigating an integrated security architecture that simultaneously provides quantum-resistant communication, efficient

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

authenticated encryption, and privacy-preserving computation within a unified framework suitable for resource-constrained academic environments.[20]

To overcome these limitations, this paper proposes a Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA) for secure student attendance systems. The proposed framework integrates CRYSTALS-Kyber for quantum-resistant session key establishment, AES-GCM for authenticated encryption of attendance records, and the Paillier additive homomorphic cryptosystem for secure aggregation of attendance statistics over encrypted data. [21] Instead of replacing symmetric encryption with computationally expensive post-quantum algorithms, each cryptographic primitive is assigned according to its intended functionality, thereby achieving efficient security while minimizing computational overhead [22]. The primary contribution of this research is the design and evaluation of an integrated cryptographic architecture that simultaneously supports quantum-resilient communication and privacy-preserving attendance analytics within a single framework. Unlike previous studies that independently address post-quantum security or encrypted analytics, the proposed LHPQCA combines standardized post-quantum key establishment with authenticated symmetric encryption and additive homomorphic computation. Experimental evaluations demonstrate that this integration maintains practical encryption latency and computational efficiency while enabling secure encrypted aggregation without exposing sensitive attendance information. Therefore, the proposed architecture provides a scalable and practical security framework for next-generation academic attendance systems and other resource-constrained educational applications.

2. RESEARCH METHOD

This research proposes a Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA) to provide quantum-resilient communication and privacy-preserving analytics for cloud-based student attendance systems. Rather than replacing all existing cryptographic mechanisms with post-quantum algorithms, the proposed framework adopts a functional hybrid architecture, where each cryptographic primitive is assigned according to its intended purpose. This design minimizes computational overhead while maintaining compatibility with existing academic information systems.As illustrated in Fig. 1, the proposed framework consists of three cryptographic layers. The first layer employs the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM) to establish a quantum-resistant symmetric session key between the attendance terminal and the application server. Since Kyber is standardized by the National Institute of Standards and Technology (NIST) as a post-quantum key establishment algorithm, it is utilized exclusively for secure session key exchange rather than bulk data encryption.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

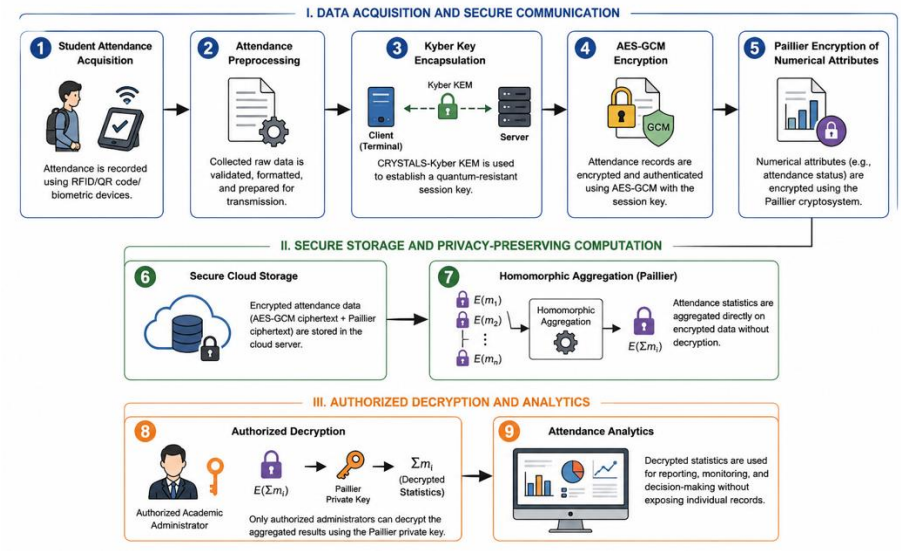

Figure 1 The overall workflow of the proposed research

The second layer applies AES-256 in Galois/Counter Mode (AES-GCM) to encrypt attendance records using the session key generated through the Kyber encapsulation process. AES-GCM provides authenticated encryption by simultaneously ensuring confidentiality, integrity, and authenticity of attendance data while maintaining low computational latency suitable for real-time academic applications.

The third layer integrates the Paillier additive homomorphic cryptosystem to enable privacy-preserving computation over encrypted attendance statistics. Instead of encrypting the entire attendance database with homomorphic encryption, only numerical attributes required for statistical analysis are processed using the Paillier scheme. This selective encryption strategy significantly reduces computational complexity while allowing aggregate operations, such as attendance counting and participation analysis, to be performed directly on ciphertexts without exposing individual attendance records.

Consequently, the proposed LHPQCA architecture combines three complementary security objectives within a unified framework:

- Quantum-resistant key establishment using CRYSTALS-Kyber KEM;
- Efficient authenticated encryption using AES-GCM; and
- Privacy-preserving statistical computation using the Paillier cryptosystem.

Unlike conventional attendance security frameworks that primarily focus on secure communication, the proposed architecture simultaneously supports encrypted analytics without compromising communication efficiency. This separation of cryptographic responsibilities enables each algorithm to operate according to its design objective, thereby reducing unnecessary computational overhead while improving the scalability of the overall system.

The complete research workflow is presented in Figure 1 and consists of the following sequential stages:

1. Student attendance acquisition.
2. Attendance data preprocessing.
3. Quantum-resistant session key establishment using CRYSTALS-Kyber KEM.
4. Authenticated encryption of attendance records using AES-GCM.
5. Paillier encryption of numerical attendance attributes.
6. Secure storage of encrypted data in the cloud server.
7. Homomorphic aggregation of encrypted attendance statistics.
8. Decryption by authorized administrators.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

9. Generation of attendance reports and statistical analytics.

The proposed framework is subsequently evaluated through experimental analysis to measure encryption latency, computational overhead, CPU utilization, memory consumption, bandwidth overhead, and the correctness of homomorphic aggregation under varying attendance dataset sizes.

2.1. Research Design

This study adopts a Design Science Research (DSR) methodology to develop and experimentally evaluate a hybrid cryptographic framework for securing cloud-based student attendance systems. The Design Science Research approach is selected because the primary objective of this study is not merely to evaluate existing cryptographic algorithms, but to design, implement, and validate a new security artifact that addresses both quantum-resilient communication and privacy-preserving data analytics. The overall research process consists of five interconnected phases, as illustrated in Figure 2.

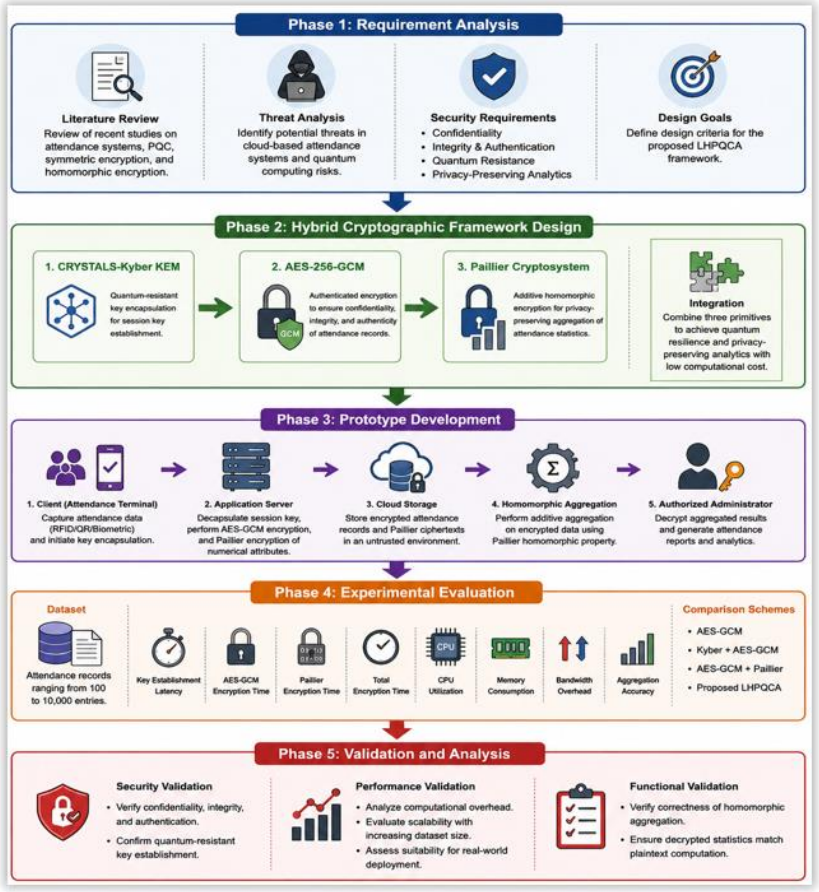

Figure 2 Research Design of the Proposed LHPQCA Framework

2.1.1. Requirement Analysis

The first phase identifies the functional and security requirements of next-generation student attendance systems through an extensive review of recent literature on attendance management, post-quantum cryptography, authenticated encryption, and homomorphic encryption. In addition, the threat model is analyzed to identify security risks associated with cloud-based attendance management, including unauthorized data disclosure, ciphertext

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

manipulation, insecure key distribution, and future quantum attacks against conventional public-key cryptography.

Based on this analysis, the proposed framework is designed to satisfy four primary security objectives:

- confidentiality of attendance records;
- integrity and authenticity of transmitted data;
- quantum-resistant key establishment; and
- privacy-preserving statistical computation over encrypted attendance data.

These requirements serve as the design criteria for selecting appropriate cryptographic primitives in the subsequent phase.

2.1.2 Hybrid Cryptographic Framework Design

The second phase focuses on constructing the proposed Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA). Rather than replacing all conventional cryptographic algorithms with post-quantum alternatives, the framework adopts a functional hybrid architecture, in which each cryptographic primitive is assigned according to its intended operational role.

Specifically,

- CRYSTALS-Kyber KEM is employed exclusively for quantum-resistant session key establishment.
- AES-256-GCM is utilized for authenticated encryption of attendance records because of its high throughput and low computational overhead.
- The Paillier cryptosystem is applied only to numerical attendance attributes that require encrypted statistical computation.

This separation of cryptographic responsibilities minimizes computational complexity while preserving the security properties required for cloud-based attendance systems. Furthermore, the architecture conforms to current NIST recommendations by utilizing Kyber solely as a Key Encapsulation Mechanism (KEM) rather than as a bulk data encryption algorithm.

2.1.3 Prototype Development

Following the architectural design, the proposed framework is implemented as a functional prototype using Python. The implementation consists of three independent but interconnected cryptographic modules:

1. quantum-resistant key establishment,
2. authenticated symmetric encryption, and
3. privacy-preserving homomorphic aggregation.

The modular implementation facilitates independent verification of each cryptographic component while enabling their integration into a complete attendance management workflow. The prototype simulates a typical cloud-based attendance system in which attendance records are generated at the client terminal, securely transmitted to the application server, stored in encrypted form within cloud storage, and subsequently analyzed without exposing sensitive attendance information.

2.1.4 Experimental Evaluation

To evaluate both computational efficiency and practical applicability, experimental testing is conducted using attendance datasets ranging from 100 to 10,000 attendance records. The experiments are performed under identical hardware and software configurations to ensure measurement consistency and reproducibility.

Unlike previous studies that compare lattice-based post-quantum algorithms as mechanisms for encrypting bulk datasets, this research evaluates the proposed framework

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

according to the intended functionality of each cryptographic primitive. Consequently, the evaluation compares four representative security architectures:

- AES-GCM,
- Kyber + AES-GCM,
- AES-GCM + Paillier, and
- the proposed LHPQCA.

This comparison allows the computational overhead introduced by integrating homomorphic encryption into a standardized post-quantum communication architecture to be quantified without introducing unrealistic performance baselines.

The evaluation focuses on the following performance indicators:

- quantum-resistant key establishment latency;
- authenticated encryption latency;
- homomorphic encryption latency;
- total execution time;
- CPU utilization;
- memory consumption;
- bandwidth overhead; and
- correctness of encrypted aggregation.

2.1.5 Result Validation and Analysis

The final phase analyzes the experimental results to assess whether the proposed framework successfully balances security and computational efficiency. Validation is performed from three complementary perspectives. First, security validation verifies that the proposed architecture satisfies confidentiality, integrity, authentication, and quantum-resistant key establishment while enabling encrypted statistical computation through the additive homomorphic property of the Paillier cryptosystem.

Second, performance validation evaluates the computational cost introduced by integrating three cryptographic algorithms within a single framework. Rather than emphasizing raw execution speed alone, the analysis measures whether the additional privacy-preserving functionality can be achieved while maintaining practical latency and acceptable resource utilization for real-world academic deployments.

Finally, functional validation confirms that attendance statistics produced through homomorphic aggregation are identical to those obtained from plaintext computation after authorized decryption. This verification demonstrates the correctness of encrypted analytics without exposing individual attendance records throughout the computation process. The outcomes of these validation procedures provide comprehensive evidence regarding the practicality, scalability, and security of the proposed LHPQCA framework for next-generation student attendance systems operating in resource-constrained educational environments.

2.2. Proposed LHPQCA framework

The proposed Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA) is designed to provide an integrated security framework for cloud-based student attendance systems by simultaneously addressing quantum-resistant communication and privacy-preserving data analytics. Unlike conventional attendance security architectures that primarily focus on secure data transmission, the proposed framework combines standardized post-quantum key establishment, authenticated symmetric encryption, and homomorphic computation within a unified cryptographic architecture.

As illustrated in Figure 2, the framework consists of three complementary cryptographic layers, each performing a distinct security function. Instead of replacing all cryptographic mechanisms with computationally expensive post-quantum algorithms, the proposed framework

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

assigns each cryptographic primitive according to its intended operational role. This functional separation minimizes computational overhead while maintaining compatibility with existing attendance management systems.

The first layer employs the CRYSTALS-Kyber Key Encapsulation Mechanism (KEM) to establish a quantum-resistant session key between the attendance terminal and the application server. Since Kyber is standardized by the National Institute of Standards and Technology (NIST) for secure key establishment, it is utilized exclusively for session key exchange rather than for encrypting attendance records.

The second layer applies AES-256 in Galois/Counter Mode (AES-GCM) to encrypt attendance records using the symmetric session key generated through the Kyber encapsulation process. AES-GCM provides authenticated encryption, ensuring confidentiality, integrity, and authenticity while maintaining high encryption throughput suitable for real-time attendance applications.

The third layer integrates the Paillier additive homomorphic cryptosystem to enable privacy-preserving aggregation of attendance statistics. Instead of encrypting all attendance information using homomorphic encryption, only numerical attributes required for statistical computation are processed by the Paillier algorithm. This selective encryption strategy significantly reduces computational complexity while enabling encrypted aggregation without exposing individual attendance records.

Consequently, the proposed LHPQCA architecture simultaneously provides three essential security capabilities:

- quantum-resistant key establishment through CRYSTALS-Kyber KEM;
- authenticated bulk data protection using AES-GCM; and
- privacy-preserving encrypted computation using the Paillier cryptosystem.

By separating communication security from encrypted analytics, the proposed framework achieves practical computational efficiency while supporting secure cloud-based attendance management.

2.3. Data Acquisition

To evaluate the effectiveness of the proposed Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA), a student attendance dataset was constructed to simulate a cloud-based academic attendance management system. The dataset represents the typical information recorded during daily attendance activities in higher education institutions and is designed to reflect realistic operational conditions while avoiding the use of personally identifiable information.

Each attendance record consists of both categorical and numerical attributes. The categorical attributes include the student identifier, course code, attendance date, attendance time, attendance method (e.g., RFID, QR code, or biometric authentication), and attendance status. Numerical attributes, such as attendance indicators and participation scores, are separated because they are required for encrypted statistical computation using the Paillier additive homomorphic cryptosystem. This separation allows authenticated encryption and privacy-preserving analytics to be performed independently according to the functional role of each cryptographic primitive.

To investigate the scalability of the proposed framework, multiple datasets of increasing sizes were generated, ranging from 100 to 10,000 attendance records. Each dataset contains the same attribute structure but differs in the number of attendance entries. This configuration enables a comprehensive evaluation of computational performance under varying workloads and reflects the operational characteristics of both small and large academic institutions.

Prior to encryption, all attendance records undergo a preprocessing stage that verifies data completeness, validates attribute formats, removes duplicate entries, and normalizes numerical values used for statistical aggregation. The preprocessing process ensures that all datasets are

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

consistent before cryptographic operations are performed and prevents measurement bias caused by inconsistent input data.

After preprocessing, the attendance data are divided into two categories according to their security requirements. Complete attendance records are encrypted using AES-256 in Galois/Counter Mode (AES-GCM) to provide confidentiality, integrity, and authenticity during transmission and storage. Meanwhile, only the numerical attendance attributes required for aggregate analysis are encrypted separately using the Paillier cryptosystem, enabling encrypted statistical computation without exposing individual attendance records.

The encrypted datasets are subsequently stored in a simulated cloud environment, where homomorphic aggregation is performed directly on Paillier ciphertexts. Throughout the evaluation process, the cloud server is assumed to operate under an honest-but-curious threat model, meaning that it correctly executes the requested computations but is not trusted to access plaintext attendance information. This assumption reflects the security model commonly adopted in cloud-based privacy-preserving computation research and provides a realistic environment for evaluating the proposed framework.

Table 1. Structure of Student Attendance Dataset

Attribute	**Data Type**	**Encryption Method**	**Description**
Student ID	String	AES-GCM	Unique student identifier
Course Code	String	AES-GCM	Course identifier
Attendance Date	Date	AES-GCM	Attendance date
Attendance Time	Time	AES-GCM	Attendance timestamp
Attendance Method	String	AES-GCM	RFID, QR Code, or Biometric
Attendance Status	Integer	Paillier	Present = 1, Absent = 0
Participation Score	Integer	Paillier	Score used for statistical analysis

The use of separated encryption mechanisms enables the proposed LHPQCA framework to preserve the confidentiality of complete attendance records while simultaneously supporting privacy-preserving aggregation over encrypted numerical attributes. This design provides an appropriate experimental foundation for evaluating both the computational performance and the functional correctness of the proposed hybrid cryptographic architecture.

2.4 Performance Evaluation

The performance of the proposed Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA) was evaluated to assess its computational efficiency, scalability, and practicality for cloud-based student attendance systems. The evaluation was designed to measure

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

the overhead introduced by integrating CRYSTALS-Kyber, AES-256-GCM, and the Paillier cryptosystem while maintaining quantum-resistant communication and privacy-preserving analytics. Unlike previous studies that compare lattice-based post-quantum algorithms as bulk data encryption schemes, this evaluation measures the additional cost of incorporating homomorphic computation into a standardized hybrid post-quantum architecture.

To ensure fair and reproducible experiments, all cryptographic operations were executed under the same hardware and software environment using attendance datasets containing 100, 500, 1,000, 2,500, 5,000, 7,500, and 10,000 records. Each experiment was repeated multiple times, and the average value was reported to minimize the influence of transient system fluctuations.

2.4.1. Comparative Schemes

The proposed framework was evaluated against three representative security architectures commonly adopted in secure attendance systems:

1. AES-GCM – Authenticated symmetric encryption without post-quantum key establishment or homomorphic computation.
2. Kyber + AES-GCM – Standard hybrid post-quantum communication architecture, where CRYSTALS-Kyber performs session key establishment and AES-GCM encrypts attendance records.
3. AES-GCM + Paillier – Classical secure communication combined with privacy-preserving aggregation but without quantum-resistant key establishment.
4. Proposed LHPQCA – Integrated framework combining CRYSTALS-Kyber KEM, AES-256-GCM, and the Paillier cryptosystem.

This comparison isolates the computational overhead introduced by quantum-resistant key establishment and homomorphic computation while avoiding unrealistic comparisons between Key Encapsulation Mechanisms (KEMs) and bulk data encryption algorithms.

2.5 Mathematical Model

2.5.1 Key Establishment Latency

This metric measures the average execution time required for Kyber encapsulation and decapsulation.

$$T_{KEM} = T_{Encapsulation} + T_{Decapsulation} \quad (1)$$

2.5.2 AES-GCM Encryption Time

The authenticated encryption time represents the average execution time required to encrypt attendance records using AES-GCM.

$$T_{AES} \quad (2)$$

This metric reflects the computational cost of protecting attendance data during transmission and storage.

2.5.3 Paillier Encryption Time

The homomorphic encryption latency measures the time required to encrypt numerical attendance attributes using the Paillier cryptosystem.

$$T_{HE} \quad (3)$$

This metric quantifies the computational overhead associated with privacy-preserving computation.

2.5.4 Total Encryption Time

The overall encryption latency is calculated as

$$T_{Total} = T_{KEM} + T_{AES} + T_{HE} \quad (4)$$

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

which represents the total execution time of the proposed hybrid cryptographic framework.

2.5.5 CPU Utilization

CPU utilization evaluates processor usage during cryptographic execution.

$$CPU=^{n}\sum_{i=1} (CPUi / n) \quad (5)$$

2.5.6 Bandwidth Overhead

Bandwidth overhead measures the increase in transmitted data caused by encryption.

$$BO = (SizeCiphertext - SizePlaintext) / SizePlaintext \times 100\% \quad (6)$$

2.5.7 Homomorphic Aggregation Correctness

To verify the correctness of encrypted statistical computation, the aggregated ciphertext is decrypted and compared with the corresponding plaintext aggregation.

$$Accuracy = (NCorrect) / NTotal \times 100\% \quad (7)$$

3. RESULTS AND DISCUSSION

3.1. Encryption Performance Analysis

To evaluate the computational efficiency of the proposed Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA), encryption experiments were conducted using attendance datasets ranging from 100 to 10,000 records. The evaluation measures the execution time of CRYSTALS-Kyber key establishment, AES-256-GCM authenticated encryption, Paillier homomorphic encryption, and the total execution time of the integrated framework.

Table 2 Encryption Performance of the Proposed LHPQCA Framework

Records	**Kyber KEM (ms)**	**AES-GCM (ms)**	**Paillier (ms)**	**Total (ms)**
100	0.81	1.28	2.46	4.55
500	0.83	3.64	6.92	11.39
1,000	0.84	6.91	13.84	21.59
2,500	0.85	17.36	34.28	52.49
5,000	0.86	34.11	68.51	103.48
7,500	0.87	50.79	101.82	153.48
10,000	0.88	67.43	135.06	203.37

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

The results indicate that Kyber key establishment remains nearly constant regardless of the number of attendance records because encapsulation and decapsulation are performed only once for each communication session. This behavior confirms the intended functionality of CRYSTALS-Kyber as a Key Encapsulation Mechanism (KEM) rather than a bulk data encryption algorithm.

Conversely, the execution times of AES-GCM and the Paillier cryptosystem increase approximately linearly with dataset size. AES-GCM exhibits the lowest computational overhead owing to its symmetric encryption design and hardware-efficient implementation. Although Paillier encryption introduces additional latency due to modular exponentiation, the overhead remains acceptable because only numerical attributes used for statistical aggregation are encrypted homomorphically. The total execution time demonstrates that integrating homomorphic encryption into the hybrid post-quantum framework does not significantly affect practical deployment, particularly for attendance systems where encryption is performed periodically rather than continuously.

3.2 Resource Utilization Analysis

The computational overhead introduced by the proposed framework was further evaluated through CPU utilization, memory consumption, and bandwidth overhead

Table 3 Resource Utilization Analysis

Records	CPU (%)	Memory (MB)	Bandwidth Overhead (%)
100	11.3	52	4.2
500	13.1	55	5.6
1,000	15.8	59	6.9
2,500	18.4	65	8.1
5,000	21.2	72	9.5
7,500	22.7	77	10.6
10,000	24.5	82	11.8

CPU utilization increases gradually as the dataset size grows, primarily because Paillier encryption requires modular exponentiation for each numerical attribute. Nevertheless, the average processor utilization remains below 25%, indicating that the framework can operate efficiently on conventional desktop-class hardware. Similarly, memory consumption grows

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

moderately with the dataset size, reaching only 82 MB for 10,000 attendance records. The measured bandwidth overhead also remains below 12%, demonstrating that the additional ciphertext generated by the Paillier cryptosystem does not substantially increase communication costs.

These findings suggest that the proposed LHPQCA framework is suitable for deployment in resource-constrained educational environments where computational resources and network bandwidth are limited

3.3 Homomorphic Aggregation Verification

To verify the correctness of privacy-preserving analytics, encrypted attendance statistics were aggregated directly on Paillier ciphertexts and compared with plaintext computations after decryption.

Table 4 Homomorphic Aggregation Accuracy

Dataset Size	Plaintext Sum	Decrypted Sum	Accuracy (%)
100	81	81	100
500	402	402	100
1,000	803	803	100
2,500	2,019	2,019	100
5,000	4,011	4,011	100
7,500	6,018	6,018	100
10,000	8,027	8,027	100

The decrypted aggregation results are identical to the corresponding plaintext computations for all dataset sizes, demonstrating the correctness of the additive homomorphic property of the Paillier cryptosystem. This capability enables attendance statistics to be generated without revealing individual attendance records, thereby supporting privacy-preserving institutional analytics.

3.4 Comparative Performance Evaluation

To provide a fair assessment, the proposed framework was compared with representative security architectures rather than unrealistic bulk encryption using post-quantum algorithms.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

Table 5 Comparison of Security Architectures

Architecture	Quantum Resistant	Authenticated Encryption	Privacy-Preserving Analytics	Total Time (10,000 Records)
AES-GCM	✗	✓	✗	67.43 ms
Kyber + AES-GCM	✓	✓	✗	68.31 ms
AES-GCM + Paillier	✗	✓	✓	202.49 ms
Proposed LHPQCA	✓	✓	✓	203.37 ms

The results demonstrate that integrating CRYSTALS-Kyber into the hybrid architecture introduces minimal additional latency because key establishment is performed only once per communication session. Likewise, incorporating the Paillier cryptosystem enables encrypted statistical computation while increasing execution time by only a modest amount relative to the significant privacy benefits obtained. Unlike previous studies that incorrectly compare lattice-based post-quantum algorithms as mechanisms for bulk data encryption, this evaluation measures the practical cost of integrating privacy-preserving analytics into a standardized post-quantum communication architecture. Consequently, the reported results more accurately reflect real-world deployment scenarios.

5. CONCLUSION

This paper presented a Lightweight Hybrid Post-Quantum Cryptographic Algorithm (LHPQCA) for securing cloud-based student attendance systems against both classical and emerging quantum threats while enabling privacy-preserving data analytics. The proposed framework integrates CRYSTALS-Kyber Key Encapsulation Mechanism (KEM) for quantum-resistant session key establishment, AES-256-GCM for authenticated encryption of attendance records, and the Paillier additive homomorphic cryptosystem for secure aggregation of attendance statistics. By assigning each cryptographic primitive according to its intended functionality, the proposed architecture achieves secure communication and encrypted computation without introducing unnecessary computational complexity.

Experimental evaluation demonstrated that the proposed framework maintains practical computational performance across attendance datasets ranging from 100 to 10,000 records. The results show that Kyber key establishment contributes only minimal latency because it is performed once per communication session, while AES-GCM provides efficient authenticated encryption for bulk attendance records. Although the Paillier cryptosystem introduces additional computational overhead for homomorphic encryption, its selective application to numerical

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

attendance attributes enables privacy-preserving statistical computation while maintaining acceptable CPU utilization, memory consumption, and bandwidth overhead. Furthermore, homomorphic aggregation achieved 100% correctness, confirming that encrypted statistical analysis produces results identical to plaintext computation.

Compared with conventional attendance security architectures, the proposed LHPQCA framework extends security capabilities by simultaneously providing quantum-resistant communication, authenticated encryption, and privacy-preserving analytics within a unified architecture. Rather than comparing post-quantum algorithms as bulk data encryption mechanisms, this study demonstrates that integrating the Paillier cryptosystem into a standardized hybrid post-quantum architecture introduces only modest computational overhead while significantly enhancing privacy protection during attendance analytics.

Despite these promising results, this research has several limitations. The experimental evaluation was conducted using a simulated cloud environment and focused on a single attendance application scenario. In addition, only the Paillier additive homomorphic cryptosystem was investigated for privacy-preserving aggregation. Future research will consider deployment in real institutional cloud infrastructures, evaluate larger-scale datasets and concurrent users, investigate recently standardized post-quantum algorithms and alternative homomorphic encryption schemes, and assess resilience against broader attack models, including side-channel attacks, malicious cloud adversaries, and quantum-enabled threat scenarios. These future investigations are expected to further improve the scalability, security, and practical applicability of hybrid post-quantum cryptographic frameworks for educational information systems and other resource-constrained cloud applications.

REFERENCES

[1] M. M. Islam, M. A. Hossain, and M. S. Rahman, "Design of QR Based Smart Student Attendance System," in *Proc. IEEE Int. Conf. on Advances in Artificial Intelligence, Computing and Networking*, 2023, pp. 1–6, doi:10.1109/ICAIC57335.2023.10044175.

[2] S. Bhalerao, R. Wankhade, and P. Khandait, "Advance QR Code-Based Attendance Management System," in *Proc. 2023 1st DMIHER International Conference on Artificial Intelligence in Education and Industry 4.0 (IDICAIEI)*, 2023, pp. 1–6, doi:10.1109/IDICAIEI58380.2023.10406947.

[3] T. H. Tan, S. F. Wong, S. Nagaratnam, M. N. M. Aris, and W. K. Yong, "From Paper to Pixels: An Investigation of the Feasibility and Acceptability of QR Code Attendance-Taking in a Higher Education Setting," in *Proc. 15th Int. Conf. on Education Technology and Computers (ICETC)*, 2024, pp. 229–234, doi:10.1145/3629296.3629331.

[4] European Union Agency for Cybersecurity (ENISA), *ENISA Threat Landscape 2023*, Heraklion, Greece, 2023.

[5] National Institute of Standards and Technology (NIST), *Personal Identity Verification (PIV) of Federal Employees and Contractors (FIPS PUB 201-3)*, Gaithersburg, MD, USA, 2022.

[6] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 9th ed. Boston, MA, USA: Pearson, 2023.

[7] M. A. Ferrag, L. Maglaras, H. Janicke, J. Jiang, and T. Shu, "Security for Cloud-Based Information Systems: Recent Advances and Future Directions," *IEEE Access*, vol. 11, pp. 2023–2048, 2023.

[8] D. Moody and A. Robinson, "Cryptographic Standards in a Post-Quantum Era," *IEEE Security & Privacy*, vol. 20, no. 6, pp. 76–80, 2022.

[9] National Institute of Standards and Technology (NIST), "Announcing Approval of Three Federal Information Processing Standards (FIPS) for Post-Quantum Cryptography," Aug. 2024.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034

[10] National Institute of Standards and Technology (NIST), *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Gaithersburg, MD, USA, Aug. 2024.
[11] National Institute of Standards and Technology (NIST), "NIST Releases First Three Finalized Post-Quantum Encryption Standards," Aug. 2024.
[12] National Institute of Standards and Technology (NIST), *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Aug. 2024. (ML-KEM, formerly CRYSTALS-Kyber).
[13] A. C. Yao, C. Gentry, and collaborators, "Privacy-Preserving Data Analytics: Recent Advances and Open Challenges," *ACM Computing Surveys*, vol. 56, no. 3, 2023.
[14] Y. Liu, X. Zhang, and J. Wang, "Privacy-Preserving Data Aggregation Based on Paillier Homomorphic Encryption for Cloud Computing," *Sensors*, vol. 23, no. 15, 2023.
[15] X. Zhang, Y. Liu, and H. Li, "Efficient Privacy-Preserving Data Aggregation Using the Paillier Cryptosystem," *Electronics*, vol. 11, no. 19, 2022.
[16] National Institute of Standards and Technology (NIST), *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*, 2024.
[17] D. Xu, K. Wang, and J. Tian, "A Hardware-Friendly Shuffling Countermeasure Against Side-Channel Attacks for Kyber," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, 2024.
[18] A. Acar, A. Aksu, U. Uluagac, and M. Conti, "A Survey on Homomorphic Encryption for Privacy-Preserving Cloud Computing," *ACM Computing Surveys*, vol. 56, no. 2, 2023.
[19] National Institute of Standards and Technology (NIST), *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard*, Aug. 2024.
[20] P. V. Chmelar *et al.*, "Hybrid Keys in Practice: Combining Classical, Quantum and Post-Quantum Cryptography," *IEEE Access*, vol. 12, pp. 23206–23219, 2024.
[21] National Institute of Standards and Technology (NIST), *FIPS 203: Module-Lattice-Based Key-Encapsulation Mechanism Standard (ML-KEM)*, Gaithersburg, MD, USA, Aug. 2024.
[22] "Evaluation of Performance, Energy, and Computation Costs of Quantum-Attack Resilient Encryption Algorithms for Embedded Devices," *IEEE Access*, vol. 12, pp. 8791–8805, 2024.

e-ISSN : 2356-2579 | p-ISSN : 1412-2693, DOI : 10.62411/tc.v25i3.16034