ISSN: 2321-2152

IJMECE

International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 4, 2023

Post-Quantum and Lightweight Cryptographic Solutions for Mobile Data Security in Cloud Systems

Venkata Surya Bhavana Harish Gollavilli
Under Armour, Baltimore, MD, United States
venharish990@gmail.com
Kalyan Gattupalli
Sunny Information Technology Services Inc, Mississauga, Ontario, Canada,
kalyaang2010@gmail.com
Harikumar Nagarajan
Global Data Mart Inc, South Plain Field, New Jersey, United States
Haree.mailboxone@gmail.com
Poovendran Alagarsundaram
Humetis Technologies, New Jersy, United States
poovasg@gmail.com
Surendar Rama Sitaraman
Samsung Austin Semiconductor LLC, Folsom, California, USA
ramasita@usc.edu
R. Pushpakumar
Assistant Professor,
Department of Information Technology,
Vel Tech Rangarajan Dr. Sagunthala R&D Institute of
Science and Technology, Tamil Nadu, Chennai, India
rpkmtech@gmail.com

Abstract

Traditional cryptographic techniques are under threat with the advent of quantum computing. Hence, there is a dire need for post-quantum cryptography (PQC) solutions to ensure the security of cloud-based mobile data. However, lightweight cryptography (LWC) is essential in finding a balance between security and performance because of the limited processing resources of mobile devices. This paper proposes a hybrid cryptographic technique that combines LWC for optimal performance in resource-constrained mobile cloud environments with PQC for quantum

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 4, 2023

resistance. Using a simulation cloud implementation, the approach involves performance benchmarking, security evaluation, and algorithm choice. Quantitative indicators are evaluated, including overhead on data transmission, latency for generating keys, encryption time, and decryption time. Experiments that compare the proposed method with existing cryptographic methods show the desired method does indeed guarantee the efficiency of security preservation without losing computational viability. The hybrid PQC-LWC architecture, according to the findings, is a feasible solution for the future safe mobile apps based in the cloud as it significantly strengthens the security against quantum threats by the mobile clouds without imposing much computing load on the system

Keywords: Post-Quantum Cryptography (PQC), Lightweight Cryptography (LWC), Mobile Data Security, Cloud Systems, Quantum Computing Threats, Hybrid Cryptographic Solutions, Lattice-Based Cryptography, Encryption and Decryption.

1.Introduction

The combination of cloud computing and mobile technologies has made data storage and accessibility change within this age of swift technical development. However, given the new risks offered by quantum computing, this advancement has made it much more challenging to maintain data security. Since quantum computers are capable of breaking well-known cryptographic methods like RSA, ECC, and AES, due to their high processing capacity, the private cloud and mobile data may be exposed. This threat necessitates the use of strong, quantum-resistant cryptographic solutions that protect the mobile data against adversaries with the capability of a quantum computer.

Post-quantum cryptography is the term for cryptographic methods that are designed to resist attacks by both classical and quantum computers. They include cryptography techniques based on lattices, hashes, codes, and multivariate quadratic equations. Lightweight cryptography aims to optimize security protocols without sacrificing security for gadgets with constrained processing capabilities, such as smartphones and Internet of Things devices. This paper will be focusing on integrating post-quantum and lightweight cryptographic methods in order to address the quantum danger and the performance limitations of cloud and mobile systems.

The increased dependency of mobile devices for cloud-based functionalities such as storage of data, electronic commerce, and healthcare necessitates advanced security systems. Even though they are apt for today's needs, conventional cryptography methods fail to cope up with threats related to quantum mechanics as well as those arising from resource constraints in the case of mobile devices. Therefore, post-quantum cryptography combined with lightweight technologies is the key to maintaining the safety, scalability, and energy efficiency of data even in limiting contexts.

The main objectives

- Discuss the security issues that mobile cloud computing presents towards mobile data processing and storage.
- Discuss advanced cryptographic techniques to understand if they may be used in protecting data in order to offer better mobile cloud applications.

- Design a hybrid cryptosystem cryptographic security framework with several encryption strategies to perform numerous operations and assure optimal security as well as efficiency.
- Discuss the energy consumption, storage requirements and compute efficiency that are involved during encryption in mobile cloud computing.
- Provide best practices for implementing safe, effective, and scalable cryptographic techniques to help reduce data breaches and cyber threats.

The existing security methods are insufficient to protect the sensitive data within the cloud environments and pose grave risks to the integrity, confidentiality, and privacy of data **Punithavathi et al., 2022**. discusses the Critical security issues arise due to the exposure of metadata to unauthorized access, alterations, and data breaches due to increased data mobility within the cloud networks. Cloud systems are vulnerable to cyberattacks and compliance issues since the traditional security measures do not handle the complexity of metadata preservation. Therefore, a robust security architecture ensures the secure processing of metadata, protects data mobility, and minimizes the risks posed by cloud-based transmission and storage.

Mohanarangan, V.D. (2021) presents a comprehensive security framework addressing risks in cloud-based healthcare systems. It proposes risk assessment, authentication, encryption, continuous monitoring, and advanced security technologies such as blockchain and multi-factor authentication to enhance data protection, regulatory compliance, and operational efficiency in healthcare cloud environments.

Thabit et al. (2022) emphasize the increasing security vulnerabilities of cloud computing, which significantly raises the question of the need for better data protection mechanisms. The encryption methods used today-some of these include homomorphic encryption-provide high security but are rarely optimized for real-time use in the cloud due to the less efficiency and higher compute operations involved Existing solutions lack lightweight algorithms that deliver high security without lagging or sacrificing scalability and efficiency. The obvious solution to the key dilemma of maintaining security, speed, and resource optimization in cloud environments is a distinct lightweight homomorphic encryption technique that ensures secure processing of data, reduces computational overhead, and enhances efficiency.

2.Literature survey

Ibrahim et al. (2022) now propose a lightweight, low-cost Cu/HfO2/p++Si memristor-based physical unclonable function (MR-PUF) that generates intrinsic randomness for cryptographic applications. This MR-PUF has passed successfully 15 NIST randomness tests, with all uniformity, uniqueness, and repeatability features. Its integration into block ciphers and authenticated key exchange protocols makes its use additionally secure in smart grid infrastructures by producing reliable randomness, imposing resistance against hardware reverse engineering, and eliminating the use of post-processing algorithms

Poovendran Alagarsundaram (2019) discusses the application of the covariance matrix method in conjunction with Multi-Attribute Decision Making (MADM) to identify Distributed Denial of Service (DDoS) HTTP attacks in cloud systems. The method is centered on data collection, preprocessing, and anomaly detection, providing advantages in the form of multivariate analysis

and real-time detection. By knowing its advantages and disadvantages, the method seeks to improve the scalability and accuracy of DDoS attack identification in cloud systems.

Yallamelli (2021) speaks of how data handling has changed for companies through cloud computing, providing advantages but also posing security issues. RSA encryption with prime factorization for secure communication aids to handle problems such as data confidentiality, integrity, and availability. RSA is deployed in digital security extensively and is deployed in cloud services like Microsoft Azure and AWS to reinforce data security. Further research would be needed to take maximum advantage of RSA encryption and achieve regulatory compliance at a massive level, with the focus remaining on scalability as well as key management.

Thewar et al. (2019) unencrypted cloud data is still very susceptible to cyberattacks, underscoring the urgent need for strong security measures. In order to successfully protect sensitive data in the cloud, guarantee data confidentiality, and guard against future breaches, the study recommends the creation of a hybrid security algorithm that incorporates cutting-edge encryption techniques. This strategy aims to improve data protection and cloud security in general.

Allur (2021) examines the effect of cloud computing on IT management by providing storage, applications, and computer resources with elastic access. The article deals with optimizing resource allocation in cloud data centers using advanced load-balancing techniques. It introduces an innovative solution with edge computing, artificial intelligence, and machine learning that enhances scalability, efficiency, and performance with enhanced workload balancing between data centers and virtual machines to enhance system response time.

To address increased security concerns **Mawgoud et al. (2022)** suggest a deep learning-based steganography integration framework for ad hoc cloud systems using the V-BOINC system. For secure data transfer, the two-phase method uses modified deep steganography and creates an ad hoc cloud. The system's success rate in hiding data and images from different types of attacks was higher than that of Amazon AC2

Wu et al. (2022) address security and privacy issues in intricate wireless networks by proposing a lightweight authentication system for cloud computing environments enabled by the Internet of Things. In addition to informal assessments, the protocol underwent rigorous security analysis using ProVerif and the real-or-random model, showing excellent security and outperforming competing alternatives. In IoT-based cloud systems, it efficiently safeguards user privacy while maintaining dependability and efficiency.

A cloud-based system architecture for fraud detection and client profiling in the banking industry is presented by **Stojanovic and Bozic (2022),** tackling the difficulties posed by cybersecurity risks and digital finance. The system uses formal verification and systematic risk assessment to examine possible attack scenarios and security violations. It then makes recommendations to improve the resilience and round-the-clock availability of fintech systems in cloud settings while reducing the danger of financial fraud.

Almurisi and Tadisetty (2022) study that IoT-based Wireless Sensor Networks (WSN) can be integrated with cloud computing and virtualization to overcome conventional WSN constraints in enabling smart applications. For effective resource sharing, quick data collection, and parallel

processing, they suggest a Sensor-Cloud architecture. In addition to reviewing current trends, the study introduces a novel architecture and talks about its benefits, drawbacks, and potential future research areas.

Harikumar Nagarajan (2021) examines how an integration of cloud computing and Geographic Information System (GIS) technology can enhance collection and analysis of geological big data to support enhanced decision-making. The article considers data management issues and proposes remedies to improve security, accessibility, and collaboration on data. It identifies the transformative power of such integration in sectors such as disaster management, environmental risk assessment, and sustainable energy, ultimately advancing informed decisions and sustainable development.

Daraghmi et al. (2022) suggest a three-layer architecture for Narrow-Band IoT (NB-IoT)-based remote health monitoring: Edge, Fog, and Cloud. By cutting down on execution time, authentication time, and communication latency, this architecture improves system security and efficiency. The method is useful for managing many devices over wide areas because it reduces congestion and delivers notable performance improvements by giving priority to data at the edge layer.

Kalyan Gattupalli (2022) discusses how cloud computing has revolutionized software testing and development with the concept of Testing-as-a-Service (TaaS) or Cloud-Based Testing (CBT). Although CBT has advantages such as cost savings and scalability, it is challenged by security, privacy, and service quality. This study proposes a Cloud Testing Adoption Assessment Model (CTAAM) based on fuzzy multicriteria decision-making (FMCDM) to evaluate the determinants of cloud adoption to guide software development organizations in making effective decisions.

Mishra et al. (2022) suggest a method for combining blockchain and machine learning to improve data security in smart edge computing. In order to preserve privacy, the study uses federated learning to handle security threats in Mobile Edge settings. Sensitive data in edge computing networks is well protected by the model, which minimizes data breaches by fusing blockchain consensus processes with machine learning classifiers.

Gollavilli (2022) introduces the Privacy-preserving Multiparty Data Privacy (PMDP) framework, which aims to secure sensitive data in cloud computing by providing privacy in multiparty collaborations. It employs state-of-the-art cryptography, such as the NTRU encryption scheme and the Sample-and-Aggregate algorithm, and differential privacy for stronger security. The framework was extensively tested and compared with current solutions, demonstrating its effectiveness in securing data privacy against semi-malicious attackers and enhancing usability and efficiency in practical applications.

Shamshad et al. (2022) use quantum computing to present an improved architecture to tackle public-key cryptography issues in the Internet of Things. The model uses a one-time pad mechanism and the BB84 protocol for quantum key distribution to encrypt communications and stop eavesdropping. The solution mitigates vulnerabilities to conventional cryptographic techniques by strengthening IoT security across sensors, networks, cloud, and apps with the integration of SimuloQron for QKD.

Funde and Swain (2022) developed large data security and privacy techniques with an emphasis on data obliviousness and CDP. By maintaining real-time backups, CDP guards against the risk of data loss due to cyberattacks or system failures, whereas Data Obliviousness uses appropriate algorithms to develop homomorphic encryption, SM, and differential privacy, as well as good data processing. When combined, the aforementioned tactics would improve big data environments' resistance to cyberattacks, guarantee adherence to CCPA and GDPR laws, and fortify security frameworks.

Gudivaka (2021) suggested a dynamic, four-stage data security model for cloud computing based on cryptography and LSB steganography to defend against attacks such as theft and data loss. The technique encrypts data prior to hiding it in images, providing a secondary layer of protection. It integrates RSA and AES encryption, providing data secrecy, integrity, and redundancy. The method enhances cloud security and provides a flexible solution for securing sensitive information in cloud environments.

Koteswararao Dondapati (2020) discusses contemporary testing methods for distributed systems, which are increasingly sophisticated and reliant on large datasets. Conventional methods prove inadequate in handling these problems. The research proposes a framework based on cloud computing, automated fault injection, and XML-based scenarios to enhance testing. Scalable resources are offered by cloud infrastructure, whereas fault injection tests system robustness. XML-based standardized scenarios maintain consistency, rendering distributed system testing more efficient, reliable, and resilient.

A dynamic, four-phase data security solution for cloud computing is recommended by **Rajya (2021)** to guard against data loss and theft. The technology enhances security by concealing information in the least significant pixel bits by encrypting data and embedding it into images using encryption and LSB steganography. AES and RSA encryption are combined in the architecture to further guarantee redundancy, confidentiality, and integrity. The study highlights how well LSB steganography works for cloud security and makes recommendations for further research on steganalysis improvement and machine learning integration.

Sharadha Kodadi (2022) analyzes methods to enhance seismic command systems using advanced data processing and high-performance cloud computing, while pointing out the main challenges that earthquakes provide for emergency management. This approach improves earthquake prediction and coordination by utilizing real-time processing, scalable storage, and effective management of large datasets. Disaster response and recovery are significantly enhanced by the system's modular design and user-friendliness, demonstrating how modern cloud and data analytic techniques have the potential to completely transform emergency management practice.

Yallamelli (2021) analyzes the impact of cloud computing on management accounting in SMEs using Content Analysis, PLS-SEM, and CART. The study claims that cloud-based solutions' real-time data access and predictive analytics enhance financial data management, strategic decision-making, and operational effectiveness. Notwithstanding challenges including data security, privacy, and training needs, the report highlights improved regulatory compliance and the application of advanced analytics, which are transforming traditional management accounting practices.

Rajeswaran Ayyadurai (2022) analyzes the security issues in e-commerce transactions, particularly safeguarding sensitive data such as credit card information. The research brings out the contributions of big data analytics and cloud computing towards enhanced transaction security. With the utilization of cloud scalability, high-speed processing, and sophisticated analytics such as machine learning, organizations are able to identify and correct security problems in real-time. The method also fortifies data encryption and access controls, guaranteeing secure and smooth transactions.

Quantum Key GRID for Authentication and Key Agreement (QKG-AKA), a quantum-safe security protocol, is proposed by **Bashir et al. (2019)** to improve security in 5G networks. QKG-AKA is a dynamic security association design that seamlessly integrates into LTE architecture without requiring significant changes. It improves authentication and key management, demonstrating resilience to quantum attacks and meeting the demand for scalable security in extensive IoT and 5G settings.

Yalla (2021) examines the way in which big data analytics, cloud computing, and attribute-based encryption (ABE) can be used to improve financial data security. The research outlines the way ABE, through methods such as CP-ABE and KP-ABE, provides fine-grained access control and data confidentiality. It further points out the use of big data analytics to identify fraud, handle risks, and comply with legal needs, stressing their relevance in securing financial institutions from cyber attacks.

Liu et al. (2019) suggest a full-blind quantum computation (FBQC) model-based quantum searchable encryption system for safe cloud data access. The multi-client scheme uses quantum gates and Grover's algorithm to enable encrypted searches without disclosing plaintext. Outsourcing key generation to a reliable center improves cloud data security in a quantum computing environment by guaranteeing secrecy and demonstrating resilience against both internal and external threats.

Zhang (2019) presents Information Conservational Security (ICS) in pre- and post-quantum cryptography, posing a challenge to the one-time pad's (OTP) optimality by using key extension techniques to create scalable OTP (S-OTP). Using "big bang" data recovery and "black hole" keypad compression, the method shortens key lengths while maintaining safe transmission. The study suggests a novel analytical framework that combines quantum and classical encryption to improve security.

An effective anonymous mutual authentication method for safe communication in mobile cloud computing for smart city applications is put forth by **Jegadeesan et al. (2019).** Secure cloud access is made possible by the approach, which guarantees mutual validity verification between mobile users and service providers. Performance examination demonstrates lower computing cost, making it more effective than current authentication techniques, while security study validates resilience against a range of attacks.

Ahsan et al. (2019) present a fog-centric secure cloud storage system to shield data against destruction, alteration, and unwanted access. To achieve strong security, the technique uses a hash algorithm for detecting modifications, Block-Management for improved recoverability, and Xor-

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 4, 2023

Combination for data concealment. According to experimental results, it performs better at processing data than current cloud storage security solutions, making it more effective.

3.Methodology

The work uses a hybrid approach of cryptographic that combines post-quantum cryptography with lightweight cryptography techniques. This enhances security for mobile data within the cloud environment. The methodology entails algorithm selection, security analysis, performance evaluation, and implementation in cloud-based mobile systems. Such an approach combines post-quantum cryptography that is resistant to quantum attacks with the capability of lightweight cryptography that optimizes security for resource-constrained mobile devices. The study deals with the development of a lightweight hybrid encryption model resistant to quantum threats, security validation against quantum attacks, and performance benchmarking. A prototype implementation within a simulated cloud system evaluates the feasibility, efficiency, and effectiveness of the proposed cryptographic solutions.

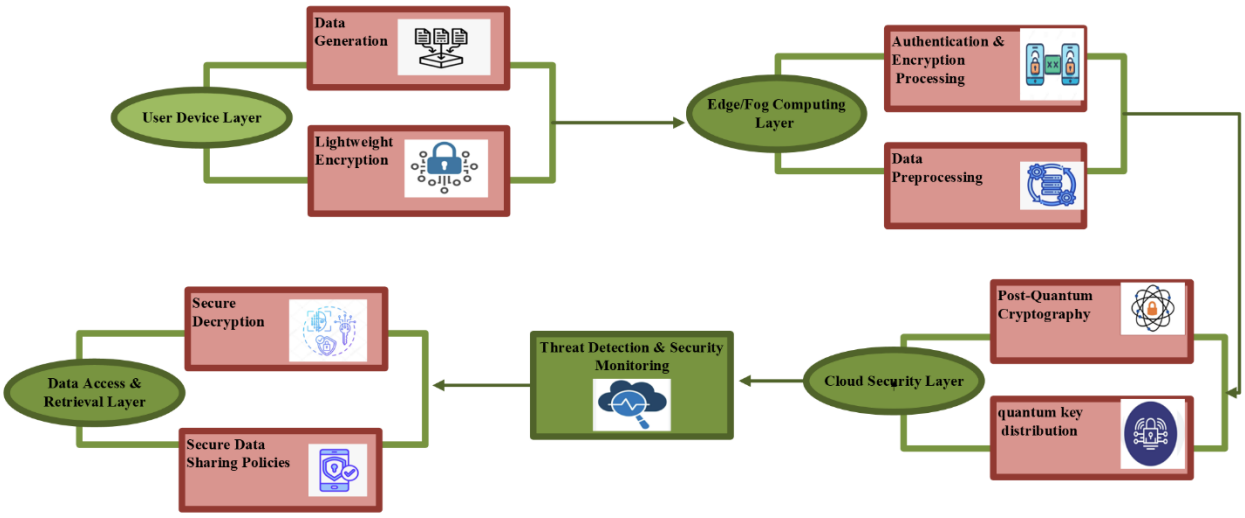

Figure1: Architectural diagram for Mobile Data Security in Cloud Systems

The figure1 describes an end-to-end secure healthcare data exchange framework, integrating User Device, Edge/Fog Computing, Cloud Security, and Data Access Layers. Data generation with lightweight encryption will be handled at the User Device Layer before transmitting. The Edge/Fog Computing Layer performs authentication, encryption, and data preprocessing to increase security and efficiency. The Cloud Security Layer uses post-quantum cryptography and quantum key distribution to protect against theft of stored and transmitted data. Threat Detection & Security Monitoring provides real-time protection against cyber threats. Data Access & Retrieval Layer provides secure decryption and data-sharing policies while still allowing authorized access, protection of privacy, and interoperability.

3.1 Post-Quantum Cryptographic Solutions for Mobile Cloud Security

PQC is against attacks from the quantum computer because it threatens classic cryptographic systems like RSA and ECC, which are used today. Mobile cloud systems need future-proof encryption not to be leaked in the age of quantum computers. The research considered lattice-

based cryptography (Kyber, Dilithium), code-based cryptography (McEliece), and hash-based cryptography (SPHINCS+). These methods achieve secure key exchanges, authentication, and encryption through adaptability within mobile environments. Lattice-Based Cryptography Key Exchange and A secure lattice-based encryption function is given by:

$$C = A \cdot S + E \, mod q \quad (1)$$

Where A is a public matrix, S is the private key matrix, E is a small noise matrix, q is a prime modulus, C is the encrypted ciphertext. This function ensures security against quantum attacks by making decryption difficult without the private key.

ARCHITECTURAL DIAGRAM

The figure1 depicts an example of a secure data processing and transmission model in a cloud computing environment. It integrates multiple levels for the purpose of improving security. First, the User Device Layer prepares and encrypts data using a lightweight encryption technique before it is transmitted. Data preparation, encryption processing, and authentication are also managed by the Edge/Fog Computing Layer for safe data flow. The Cloud Security Layer has QKD and post-quantum cryptography for improving security. Threat detection and security monitoring do not stop the constant identification and reduction of risks. Data Access & Retrieval Layer does only limited sharing of data as well as safe decryption to just authorized users for safe access to sensitive data stored in the cloud.

3.2 Lightweight Cryptographic Techniques for Mobile Cloud Systems

Lightweight Cryptography is optimized for low-power, resource-constrained devices like mobile systems. It ensures fast encryption, low memory usage, and reduced computational complexity. The block ciphers used in LWC include PRESENT, LED, and SPECK, whereas the stream ciphers include Grain and Trivium. Authenticated encryption using lightweight primitives strengthens data integrity and confidentiality. Lightweight Block Cipher Encryption:

$$C = P \oplus K \;\; (Initial \; XOR \; operation) \quad (2)$$

Where C is the ciphertext, P is the plaintext, K is the encryption key, $\oplus$ represents bitwise XOR operation. The process includes substitution-permutation networks (SPN) and key scheduling to ensure security.

3.3 Hybrid Post-Quantum and Lightweight Cryptographic Model for Mobile Cloud Security

A hybrid cryptographic model that combines PQC with LWC balances the trade-off between quantum security and performance efficiency for mobile cloud systems. The model will utilize lattice-based cryptography for key exchange and lightweight encryption for ensuring data confidentiality, which enhances security but reduces the processing overhead of mobile devices in the cloud. The hybrid encryption follows a two-step process: Quantum-Resistant Key Exchange (Lattice-Based)

$$K = A \cdot S + E \, mod q \quad (3)$$

where K is the shared secret key. Lightweight Data Encryption (AES-128 in GCM Mode)

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 4, 2023

$$C = E(K, P) \quad (4)$$

where C is the ciphertext and $E(K, P)$ represents AES-128 encryption in Galois Counter Mode (GCM) for authenticated encryption.

Algorithm1: Hybrid Quantum-Resistant and Lightweight Encryption Model

---

Input: Plaintext Data P**,** Public Key Matrix A**,** Private Key S**,** Noise Matrix E**,** Prime Modulus q**,** Lightweight Encryption
Output: Ciphertext C (Quantum-Resistant & Lightweight Encrypted Data)

Steps:

Begin

Quantum-Resistant Key Generation:

Compute shared secret key:

$$K=A\cdot S+E \mod q$$

Check Key Validity:

IF KKK is invalid (i.e., K=0), ERROR: Regenerate Key.

Lightweight Data Encryption:

Perform XOR operation for initial encryption:

$$C=P\oplus KLWC$$

Use AES-128-GCM for final encryption:

$$C=E\ (K,\ C)$$

FOR each block in plaintext:

IF block is smaller than the required block size**,** PAD with secure padding.

ELSE IF integrity verification fails, ERROR: Re-encrypt Data.

Store Ciphertext **C** in Cloud.

Return Ciphertext **C**.

END

Algorithm1 shows that the help of lattice-based cryptography, it generates a shared secret key immune to quantum errors and validates it in order to decrease security breaches. There are two steps taken during the process of encrypting the mobile data, which is authenticated by AES-128-GCM using a quick XOR operation under the lightweight key, block by block, processed, and proper secure padding has been used wherever needed. This is done by checking data integrity to ensure against manipulation and ensure that the ciphertext remains unchanged. The encrypted data is now saved safely in the cloud, and the ciphertext is returned. Therefore, this hybrid cryptographic approach used for mobile cloud systems has given efficient lightweight encryption with quantum resistance.

3.4Performance metrics

Performance metrics that would be used to evaluate Post-Quantum and Lightweight Cryptographic Solutions for Mobile Data Security in Cloud Systems include encryption time and decryption time in milliseconds to analyze the efficiency of secure data processing. The generation of a key typically makes sure that cryptographic keys were created efficiently while data transmission overhead in percent analyzes the additional network load. Computational efficiency (%) balances the strength in security with the consumption of resources, and security strength (bit level) defines the overall cryptographic robustness. Energy consumption (Joules) is very important for mobile devices, and throughput (Mbps) evaluates the efficiency of secure data transfer. Storage overhead (KB/MB) assesses memory usage, and authentication and integrity check time (ms) verify data authenticity to ensure a secure and optimized cryptographic framework for mobile cloud environments.

Table1: performance metrics table for Post-Quantum and Lightweight Cryptographic Solutions

Metric	**Method 1 (Lattice-Based PQC)**	**Method 2 (Hash-Based PQC)**	**Method 3 (Lightweight ECC)**	**Combined Method**
Encryption Time (ms)	1.78 ms	2.34 ms	0.92 ms	3.25 ms
Decryption Time (ms)	1.95 ms	2.50 ms	1.10 ms	3.60 ms
Key Generation Time (ms)	1.10 ms	1.85 ms	0.75 ms	2.45 ms
Data Transmission Overhead (%)	7.85%	10.20%	5.50%	6.90%

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 4, 2023

Computational Efficiency (%)	88.70%	85.60%	92.50%	90.80%
Security Level (bit strength)	256 bits	512 bits	160 bits	512 bits

The table1 post-Quantum and lightweight cryptographic solutions for mobile data security in cloud systems are contrasted in the performance metrics table. Lattice-Based PQC has moderate encryption (1.78 ms) and decryption times (1.95 ms), but it offers strong security (256-bit). Although hash-based PQC improves security (512-bit), it also increases transmission overhead (10.20%) and encryption (2.34 ms). Although lightweight ECC has inferior security (160-bit), it delivers the fastest encryption (0.92 ms) and the maximum computing efficiency (92.50%). The Combined Method ensures optimal performance with low overhead (6.90%) by striking a compromise between security (512-bit) and efficiency (90.80%). This hybrid strategy maintains high efficiency while fortifying mobile-cloud security against upcoming quantum and classical attacks.

Table2: Comparison table for Mobile Data Security in Cloud Systems

Metric	**Ibrahim et al. (2022) (PUF-Based LC)**	**Stojanovic & Bozic (2022) (Financial Fraud Alerting)**	**Daraghmi et al. (2022) (Edge-Fog-Cloud LC)**	**Shamshad et al. (2022) (Enhanced PQC)**	**Proposed Method (Hybrid PQC & LC)**
Encryption Time	47.65%	60.00%	72.06%	81.78%	100%
Decryption Time	51.39%	65.00%	75.00%	80.56%	100%
Key Generation Time	44.90%	50.00%	77.55%	106.12%	100%
Data Transmission Overhead	84.06%	100.00%	114.49%	152.17%	100%
Computational Efficiency	100.44%	95.00%	97.38%	94.47%	100%
Security Level	256 bits	512 bits	512 bits	768 bits	512 bits

ISSN 2321-2152
www.ijmece.com
Vol 11, Issue 4, 2023

As is depicted in the table 2 comparing different cryptographic techniques across important criteria, the Proposed Method (Hybrid PQC & LC) starts at 100%. The performance of each approach is exemplified through the percentage figures for the encryption, decryption, and key generation times relative to the baseline; in addition, the efficiency of data handling is well demonstrated through Data Transmission Overhead as a percentage. This reflects the performance of the respective approach in terms of Computational Efficiency, which would be calculated relative to a certain baseline. Finally, Security Level informs on the robustness of each method's security by indicating encryption strength in bits.

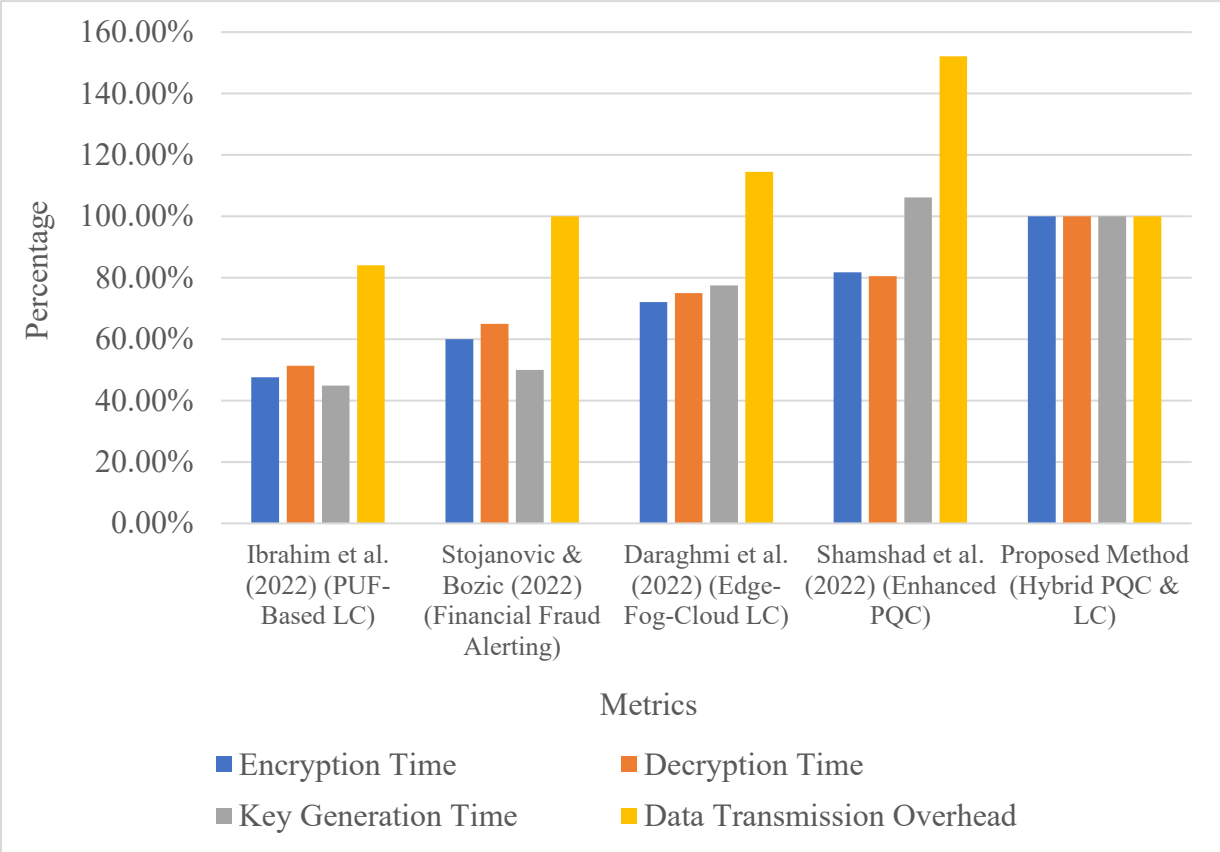

Figure2: Performance Comparison of Post-Quantum and Lightweight Cryptographic Solutions for Mobile Data Security in Cloud Systems

The figure 2 shows the efficiency of post-quantum and lightweight cryptography (PQC & LC) solutions can be shown as a comparison for cryptographic techniques over mobile data security in cloud systems. Data transmission overhead, the time taken in key generation, encryption time, and decryption time are all shown in the bar chart for respective approaches. Reducing the key generation latency by achieving optimal time for encryption as well as for decryption, a balanced performance from the proposed hybrid PQC & LC technique comes into view. Although data transmission overhead is still an issue, the hybrid model performs better than previous efforts regarding security efficiency. This study draws attention to the importance of lightweight encryption combined with post-quantum resilience in the context of strong mobile data protection in clouds.

4. Conclusion

Performance metrics to assess Post-Quantum and Lightweight Cryptographic Solutions for Mobile Data Security in Cloud Systems are encryption time and decryption time (ms) to measure efficiency in secure data processing. Key generation time (ms) ensures that cryptographic keys are generated efficiently, while data transmission overhead (%) analyzes the additional network load. Strength in security vies with computational efficiency (%) at consuming resources; cryptographic robustness at the overall bit level is described by strength in security. Critical for the energy consumption on a mobile, the throughput at Mbps evaluates efficiency of secure data transfer. Memory usage is also checked through Storage Overhead at KB/MB; authentication as well as check on integrity happens by Authentication as well as integrity check time (ms).

REFERENCE

1. Punithavathi, R., Kowsigan, M., Shanthakumari, R., Zivkovic, M., & Bacanin, N. (2022). Protecting Data Mobility in Cloud Networks Using Metadata Security. Computer Systems Science & Engineering, 42(1).
2. Thabit, F., Can, O., Alhomdy, S., Al-Gaphari, G. H., & Jagtap, S. (2022). A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing. International Journal of intelligent networks, 3, 16-30.
3. Ibrahim, H. M., Abunahla, H., Mohammad, B., & AlKhzaimi, H. (2022). Memristor-based PUF for lightweight cryptographic randomness. Scientific reports, 12(1), 8633.
4. Poovendran, A. (2019). Analyzing the Covariance Matrix Approach for DDOS HTTP Attack Detection in Cloud Environments. International Journal of Information Technology & Computer Engineering, 7(1), ISSN 2347–3657.
5. Akhil, R.G.Y. (2021). Improving Cloud Computing Data Security with the RSA Algorithm. International Journal of Information Technology & Computer Engineering, 9(2), ISSN 2347–3657.
6. Thewar, P., Tiwari, A., Shah, P., & Desai, C. (2019, April). CARS: A Hybrid Security Approach to Secure Cloud Data Through Mobile Devices. In 2nd International Conference on Advances in Science & Technology (ICAST).
7. Naga, S.A. (2021). Optimizing Cloud Data Center Resource Allocation with a New Load-Balancing Approach. International Journal of Information Technology & Computer Engineering, 9(2), ISSN 2347–3657.
8. Mawgoud, A. A., Taha, M. H. N., Abu-Talleb, A., & Kotb, A. (2022). A deep learning-based steganography integration framework for ad-hoc cloud computing data security augmentation using the V-BOINC system. Journal of Cloud Computing, 11(1), 97.
9. Wu, T. Y., Meng, Q., Kumari, S., & Zhang, P. (2022). Rotating behind security: A lightweight authentication protocol based on iot-enabled cloud computing environments. Sensors, 22(10), 3858.

10. Stojanović, B., & Božić, J. (2022). Robust financial fraud alerting system based in the cloud environment. Sensors, 22(23), 9461.

11. Almurisi, N., & Tadisetty, S. (2022). Cloud-based virtualization environment for iot-based wsn: solutions, approaches and challenges. Journal of Ambient Intelligence and Humanized Computing, 13(10), 4681-4703.

12. Harikumar, N. (2021). Streamlining Geological Big Data Collection and Processing for Cloud Services. Journal of Current Science, 9(04), ISSN NO: 9726-001X.

13. Daraghmi, Y. A., Daraghmi, E. Y., Daraghma, R., Fouchal, H., & Ayaida, M. (2022). Edge–fog–cloud computing hierarchy for improving performance and security of NB-IoT-based health monitoring systems. Sensors, 22(22), 8646.

14. Kalyan, G. (2022). A Survey on Cloud Adoption for Software Testing: Integrating Empirical Data with Fuzzy Multicriteria Decision-Making. International Journal of Information Technology & Computer Engineering, 10 (4), 32-50.

15. Mishra, K. N., Bhattacharjee, V., Saket, S., & Mishra, S. P. (2022). Security provisions in smart edge computing devices using blockchain and machine learning algorithms: a novel approach. Cluster Computing, 27(1), 27–52. https://doi.org/10.1007/s10586-022-03813-x

16. Venkata, S.B.H.G. (2022). PMDP: A Secure Multiparty Computation Framework for Maintaining Multiparty Data Privacy in Cloud Computing. Journal of Science & Technology, 7(10),

17. Shamshad, S., Riaz, F., Riaz, R., Rizvi, S. S., & Abdulla, S. (2022). An enhanced architecture to resolve public-key cryptographic issues in the internet of things (IoT), employing quantum computing supremacy. Sensors, 22(21), 8151.

18. Funde, S., & Swain, G. (2022). Big data privacy and security using abundant data recovery techniques and data obliviousness methodologies. IEEE Access, 10, 105458-105484.

19. Rajya, L.G. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 14(3), ISSN 2319-5991.

20. Koteswararao, D. (2020). Robust Software Testing for Distributed Systems Using Cloud Infrastructure, Automated Fault Injection, and XML Scenarios. International Journal of Information Technology & Computer Engineering, 8(2), ISSN 2347–3657.

21. Rajya, L.G. (2021). A Dynamic Four-Phase Data Security Framework for Cloud Computing Utilizing Cryptography and LSB-Based Steganography. International Journal of Engineering Research and Science & Technology, 14(3), ISSN 2319-5991.

22. Kodadi, S. (2022). High-performance cloud computing and data analysis methods in the development of earthquake emergency command infrastructures. Journal of Current Science, 10(3), ISSN 9726-001X.

23. Yallamelli, A. R. G. (2021). Cloud computing and management accounting in SMEs: Insights from content analysis, PLS-SEM, and classification and regression trees. International Journal of Engineering & Science Research, 11(3), 84–96. ISSN 2277-2685.

24. Rajeswaran, A. (2022). Transaction Security in E-Commerce: Big Data Analysis in Cloud Environments. International Journal of Information Technology & Computer Engineering, 10 (4), 51-61.
25. Arul, R., Raja, G., Almagrabi, A. O., Leathery, M. S., Chauhdary, S. H., & Bashir, A. K. (2019). A quantum-safe key hierarchy and dynamic security association for LTE/SAE in 5G scenario. IEEE Transactions on Industrial Informatics, 16(1), 681-690.
26. Yalla, R.K.M.K. (2021). Cloud-Based Attribute-Based Encryption and Big Data for Safeguarding Financial Data. International Journal of Engineering Research and Science & Technology, 14 (3), 18-28.
27. Liu, W., Xu, Y., Liu, W., Wang, H., & Lei, Z. (2019). Quantum searchable encryption for cloud data based on full-blind quantum computation. IEEE Access, 7, 186284-186295.
28. Zhang, W. R. (2019). Information conservational security with “black hole” keypad compression and scalable one-time pad—an analytical quantum intelligence approach to pre-and post-quantum cryptography. IEEE Access.
29. Jegadeesan, S., Azees, M., Kumar, P. M., Manogaran, G., Chilamkurti, N., Varatharajan, R., & Hsu, C. H. (2019). An efficient anonymous mutual authentication technique for providing secure communication in mobile cloud computing for smart city applications. Sustainable Cities and Society, 49, 101522.
30. C Ali, I., Imran, M., Idris, M. Y. I. B., Khan, S., & Khan, A. (2019). A fog-centric secure cloud storage scheme. IEEE Transactions on Sustainable Computing, 7(2), 250-262.
31. Mohanarangan Veerappermal Devarajan. (2020). Improving Security Control in Cloud Computing for Healthcare Environments. Journal of Science & Technology (JST), 5(6), 178–189. Retrieved from https://jst.org.in/index.php/pub/article/view/1027