Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

ADAPTIVE MULTI-LAYER ENCRYPTION: A CONTEXT-AWARE FRAMEWORK FOR ENHANCED MULTI-CLOUD DATA SECURITY

KUSHALA M V
Assistant Professor, Department of AIML, Dr. AIT. Email: kushalmv@gmail.com

Dr. B S SHYLAJA
Professor, Department of ISE, Dr. AIT. Email: shyla.au@gmail.com

Abstract

The surge in demand for optimization of resource usage, reliability, and avoidance of vendor lock-in has led to a rise in the use of multi-cloud environments. The spread nature of these environments poses challlenging issues regarding security, specifically data confidentiality, integrity and availability. In this paper, we present a monitoring multi-layered encryption methodology for multi-cloud environments. Our mechanism implements a multi-cloud architecture with an adaptive selection mechanism that encrypts data encrypts on the basis of sensitivity, size of the data and available computational resources. The proposed methodology utilizes a hybrid architecture that employs Elliptic Curve Cryptography (ECC) for key exchange, symmetric encryption for data protection, and zero-knowledge proofs for authentication. Evaluation results indicate a substantial positive difference in computational efficiency, levels of security achieved, and scalability in comparison to the traditional approaches based on the RSA algorithm. The implementation offers strong defense against classical as well as emerging quantum threats while being resource efficient in multi-cloud environments.

Keywords: Multi-cloud Security, Adaptive Encryption, Elliptic Curve Cryptography, Post-Quantum Cryptography, Zero-Knowledge Proofs, Hybrid Encryption.

1. INTRODUCTION

The emergence of cloud computing, both public and private, transformed the ways that businesses and other organizations deploy, operate, and manage their IT infrastructure and services. Moving from single-cloud to multi-cloud environments is a developent in the corporate computing paradigm that has multiple advantages such as improving costs for businesses, eliminating vendor lock-in, and improving resistance to outages.

Recent statistics suggest that more than 85% of enterprises are implementing multi-cloud strategies, meaning the average organization is using greater than five autonomous cloud systems [1]. Although this approach makes operational and financial sense when implemented, it raises significant challenges in ensuring unified security across different environments.

Traditional encryption techniques, especially those leveraging RSA cryptography, suffer from serious drawbacks in multi-cloud environments, including high computational costs, difficult key management, and an impending threat from quantum computing [2].

Because of these challenges, new approaches to cryptography need to be formulated that address the security needs of multi-cloud environments.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

The security issues with multi-cloud architectures result from a combination of deployment issues such as the fragmentation of data among multiple service providers with different security levels; base, plus increased network attack surfaces, difficult identity and access management controls, and compliance issues within different regions [50].

Most standard encryption techniques make the mistake of applying the same level of security controls irrespective of sensitivity or resource constraints, which leads to wasteful over-provisioning of security resources or lack of security for critical assets, both damaging in their own respect.

In addition, many still use traditional RSA-based systems, which poses various challenges such as lack of efficiency in key size, low computational speed and possible damage from quantum computing in the future [3].

So delicate terrain demands encryption techniques that provide complete resources adaptation at new levels optimization and meeting changes with political aggression to rules responsive to and the development processes in the multi- Cloud environments motifs.

This paper presents a new security approach with multi-layered encryption structures to meet the challenges of multi-cloud environments. Our approach uses an adaptive encryption selection method capable of automatically changing the employed encryption algorithms as a function of contextual parameters such as data sensitivity, volume, and available computing resources.

The use of key exchange and digital signature via ECC integrates RSA-type security at lower computational overheads and key sizes. Advanced symmetric encryption algorithms, AES-256-GCM and ChaCha20-Poly1305, enable effective data security while including elements of post-quantum cryptography enables future-proof security against new computation threats.

This approach caters for different security needs of multi-cloud environments without compromising on resource consumption and performance.

2. RELATED WORK

In recent years, many efforts have been made to address the problems related to security of our cloud system using cryptography. Li et al. [4] developed a method for data security in the cloud utilizing attribute-based encryption which has certain access control features but greatly suffers from scalability issues in multi-cloud environments.

Likewise, Zhang et al. [5] created an employee encryption method for a specific cloud computing application which allows a user to perform certain operations on data without removing the encryption. While these methods possess some valuable security features, they are often accompanied by large computational costs that limit the usefulness of these features in sensitive multi-cloud applications.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

Other scientists studied hybrid methods of cryptography that merge two or more encryption schemes [13]. For example, Kumar et al. [6] presented an RSA-AES hybrid method which employs RSA for a key exchange and AES for encryption of data which resulted in lesser performance cost than pure asymmetric encryption implementations.

From a distributed environment's perspective, multi-cloud security offers unique challenges that already exist in integrated frameworks. Almorsy et al. [7] suggest a comprehensive security management framework for multi-cloud applications that includes security standards, compliance, and threat modeling as well as security metrics. Alzain et al. [8] extends the multi-cloud model by integrating a multi-provider data security model that mitigates the problem of data security by distributing datasets among several cloud providers to ensure no provider has full.

These models, in addition to addressing a few critical architectural issues in multi-cloud security, often use classical cryptographic primitives which are known to have scalability and efficiency bottlenecks. It's more recent works that delve into using post-quantum cryptography in the cloud that have begun to emerge.

Chen et al. [9] made the most important contribution in evaluating the effectiveness of lattice-based cryptographic schemes, proving that public-key cryptography's replacement could be found in the form of cloud data's cryptographic security, but will suffer serious drawbacks in performance.

Notwithstanding this progress, there is still a significant gap that requires further attention in crafting adaptive cryptographic techniques tailored for multi-cloud environments [11]. Most existing approaches either implement a one-size-fits-all-uniform security-granular policy for different sensitive data or target very specific domians of cloud security without meeting the necessities of multi-cloud environments [12].

Furthermore, many of the proposals have strong emphasis on security while considering the performance aspects that are fundamental for practical deployment to be of minimal importance. This gap is addressed through an adaptive multi-layered encryption technique that blends security with performance in multi-cloud scenarios while embedding quantum safe features for up-to-date reasons.

3. PROPOSED METHODOLOGY

Our proposed methodology introduces a novel approach to securing data in multi-cloud environments through a combination of adaptive encryption selection and a multi-layered encryption pipeline is shown in figure 1. This section details the conceptual framework, components, and implementation considerations of the proposed approach.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

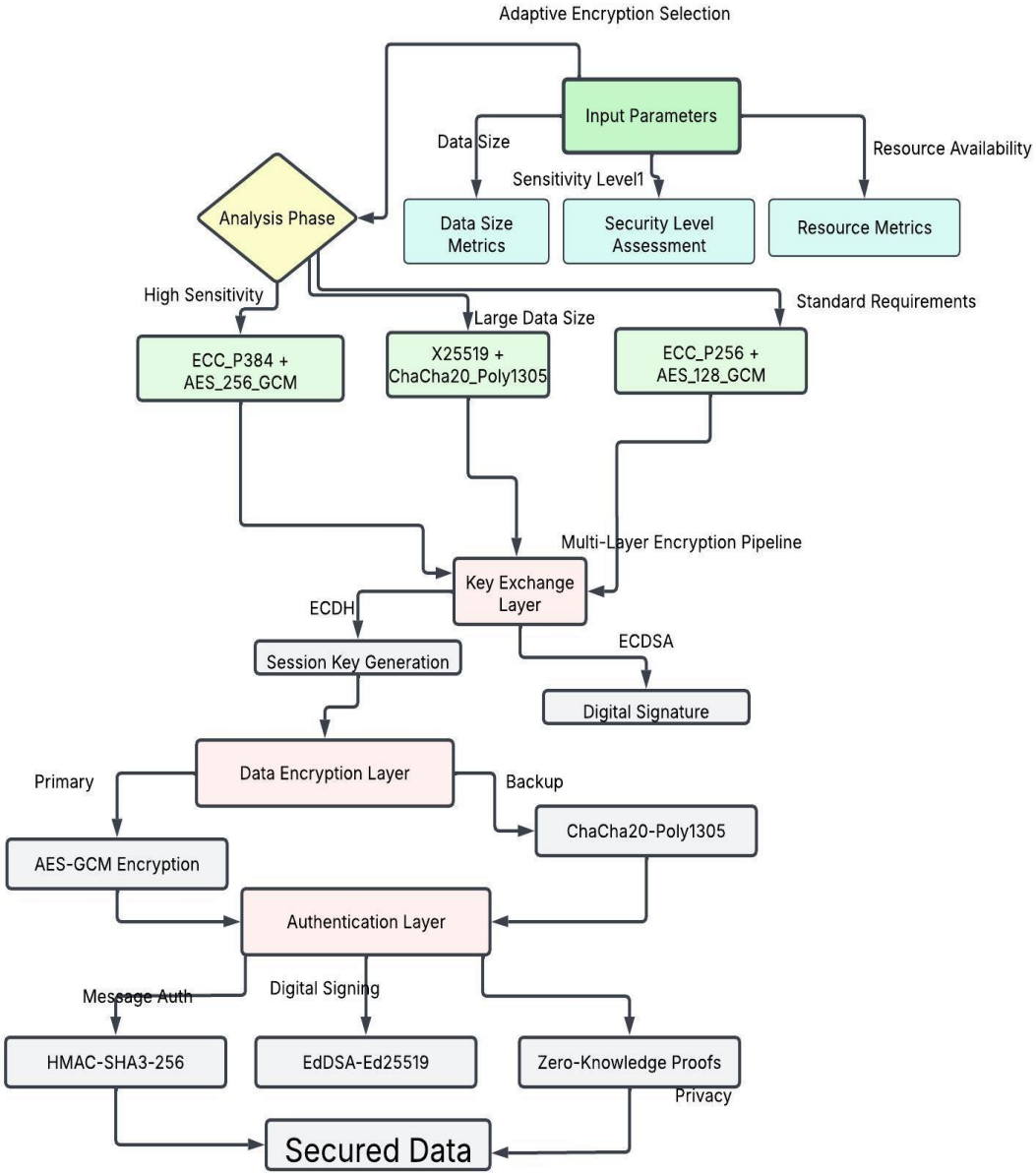

Figure 1: Proposed Methodology

3.1 Adaptive Encryption Selection

The adaptive encryption selection mechanism forms the cornerstone of our methodology, enabling dynamic selection of cryptographic algorithms based on contextual factors. This approach recognizes that different data types, sensitivity levels, and usage scenarios warrant different security measures—a departure from the one-size-fits-all approach common in traditional implementations.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

The selection process incorporates three primary input parameters:

- **Data Sensitivity Level:** Classifies data into sensitivity tiers (e.g., high, medium, low) based on organizational criteria, regulatory requirements, and potential impact of unauthorized disclosure.
- **Data Size Metrics:** Evaluates the volume of data being processed to optimize performance, particularly important for large datasets where computational efficiency becomes critical.
- **Resource Availability:** Assesses available computational resources to ensure that selected encryption mechanisms operate effectively within system constraints.

Based on these parameters, the selection mechanism outputs one of three primary configuration profiles:

- **High Sensitivity Configuration:** Employs ECC P-384 for key exchange combined with AES-256-GCM for data encryption, providing maximum security for highly sensitive data.
- **Large Data Configuration:** Utilizes X25519 for key exchange with ChaCha20-Poly1305 for encryption, optimized for performance with large datasets while maintaining strong security.
- **Standard Requirements Configuration:** Implements ECC P-256 with AES-128-GCM, offering a balanced approach for general-purpose security requirements.

The selection algorithm implements a decision tree that evaluates input parameters against predefined thresholds, with the capability for organizations to customize these thresholds according to their specific security policies and risk tolerance. This adaptive approach ensures optimal resource utilization by applying the most appropriate security measures based on contextual requirements rather than defaulting to maximum security for all scenarios.

3.2 Multi-Layer Encryption Pipeline

The multi-layer encryption pipeline implements a defense-in-depth approach through three distinct security layers, each serving a specific purpose in the overall security architecture:

3.2.1 Key Exchange Layer

The Key Exchange layer forms the base of security within the multi-cloud encryption architecture, utilizing the elegant and efficient mathematics of Elliptic Curve Cryptography (ECC) to create secure communication channels between different cloud sites [48]. At this level, the ECDH protocol is implemented to allow two parties to create a shared secret over a publicly accessible medium without ever having to send any cryptographic keys such that the keys are never intercepted during the exchange process. The Elliptic Curve Digital Signature Algorithm (ECDSA) enhances the authentication and non-repudiation

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

services of all the entities in the multi cloud environment and negates the possibility of currently authenticated enemies masquerading as trusted multi services users or services within the multi-cloud environment [14, 49].

Hybrid Encryption Algorithm: ECC P-384 Key exchange with AES-256-GCM

Elliptic curve definition (P-384): The p-384 curve is defined over a prime field F_p where:

$$p = 2^{384} – 2^{128} – 2^{96} + 2^{32} – 1 \text{ (a 384bit prime)}$$

$$\text{curve equation } E = y^2 \equiv x^3 + ax + b \pmod p$$

parameter a, b $\in F_p$, where a = -3, b = 0xb3312fa7e23ee7e4988e056be3f82d19181d9c6efe8141120314088f5013875ac656398d8a2ed19d2a85c8edd3ec2aef

$$\text{Base point } G = (G_x, G_y)$$

Where,

G_x = 0xaa87ca22be8b05378eb1c71ef320ad746e1d3b628ba79b9859f741e082542a385502f 25dbf 55296c3a545e3872760ab7

G_y= 0x3617de4a96262c6f5d9e98bf9292dc29f8f41dbd289a147ce9da3113b5f0b8c00a60b1ce1d7e819d7a431d7c90ea0e5f

Order of the curve n = 0xffffffffffffffffffffffffffffffffffffffffffffffffc7634d81f4372ddf581a0db248b0a77aece c196accc52973

Key Generation: Generate a private key d_A as a random integer where $1 \leq d_A < n$

Compute the public key $Q_A = d_A . G$ using elliptic curve point multiplication, the key pair (d_A, Q_A)

ECDH key exchange protocol: For parties A and B to establish a shared secret:

- A generates key pair (d_A, Q_A) and sends Q_A to B
- B generates key pair (d_B, Q_B) and sends Q_B to A
- A computes shared point $S = d_A . Q_B = (S_x, S_y)$
- B Computes shared point S $d_B . Q_A = (S_x, S_y)$ (same result)

The shared secret $Z = S_x$ (the x-coordinate of the shared point) Derive encryption key using HKDF with SHA-384:

K_{AES} = HKDF-SHA-384(Z, salt, info, 32)

Where, Z is the shared secret from ECDH, salt is an optional salt value (can be public), info is the application specifc context information, 32 is the output length in bytes (256 bits for AES-256)

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

HKDF consists of two steps:

Extract PRK = HKDF-SHA-384(salt, 32)

Expand K_{AES}= T_1|| T_2|| ……. ||T_n

T_1 = HKDF-SHA-384(PRK, info, 0x01)

T_2 = HKDF-SHA-384(PRK, T1||info, 0x02)

AES-256 operates on 128-bit blocks using a 256-bit key through 14 rounds of substitution and permutation, The encryption function $E_K(P)$ maps a 128-bit plaintext block P to 128-bit cipher text block C using the key K [47].

Implementing forward secrecy via ephemeral keying, session level keys that are active for a temporary period and are deleted after their task is achieved ensure that even if long term keys are cracked in the future, the communications that were encased remain secure [16].

The amount of work done in bandwidth and computation for a multi-cloud environment with resource constraints or high throughput is reduced greatly because lesser key sizes of 256 or 384 bits are utilized instead of the usual 2048 or 4096 bits in RSA, which lowers the security level significantly. These smaller key sizes in The Key Exchange Layer result in considerably smaller RSA approaches without compromising security [17].

3.2.2 Data Encryption Layer

The Data Encryption Layer relies on the secure channel crafted by the Key Exchange Layer as a foundation. This data layer employs strong symmetric encryption algorithms to secure cloud data both statically within the cloud storage and dynamically during transmission to different cloud environments. The foremost mechanism employed in this infrastructure is the Advanced Encryption Standard (AES) with 256-bit keys in Galois/Counter Mode (GCM) [46].

GCM is an authenticated encryption mode that is highly secure since it provides data confidentiality and uses authentication tags that prove both the source of the data and its state during transmission or storage which ensures integrity of the data. The framework also implements ChaCha20-Poly1305 as a secondary option AES in certain mobile or edge computing environments where AES hardware acceleration is unavailable or less efficient. ChaCha20-Poly1305 is a high-performance software based authenticated encryption algorithm with strong security characteristics and no requirement for specialized support hardware [18, 25].

As with any level in a system, this layer requires paying attention to performance optimization. In contemporary processors, such as Intel and AMD with their AES-NI instruction sets, and in many other cloud service provider environments with their dedicated hardware cryptographic accelerators, there are facilities that can help with hardware acceleration [19].

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

This allows encryption and decryption functions to be completed in parallel with the rest of the processes happening in the system, minimizing latency even when volumetric data is being processed. The Data Encryption Layer provides sperate scopes for granular encryption, so that sensitive data elements may be selectively encrypted, allowing organizations to block the expenditure of computational resources on non-sensitive information traversing through the multi-cloud environment [20, 26].

3.3.3 Authentication Layer

The Authentication Layer has sophisticated mechanisms to validate the integrity of data and user access within the multi-cloud environment while employing a variety of complementary technologies to mitigate unauthorized access and data alteration [45]. At the core of this layer, a defense against accidental change or malicious manipulation during transmission of data between clouds is provided by HMAC-SHA3-256, a keyed-hash message authentication code based on the SHA-3 cryptographic hash function.

It allows for authentication of a message through the capability of verifying the received data to be exactly the same as what was sent and came from the anticipated sender. HMAC-SHA3-256 is defined as follows:

$$\text{HMAC-SHA3-256}(K,m) = \text{SHA3-256}((K \oplus \text{opad} \,||\, \text{SHA3-256}((K \oplus \text{ipad})||m))$$

Where, K is the secret key, m is the message to be authenticated, ⊕ represents the bitwise XOR operation, || represents the concatenation, opad is the outer padding (Ox5C repeated), ipad is the inner padding (Ox36 repeated). Prepare the Key K`:

Let B = 136 bytes (block size for SHA3-256 = 1088 bits)

If |K| > B, the K` = SHA3-256(K)

If |K| < B, the K` = K || $Ox00^{B-|k|}$(pad with zeros)

If |K| = B, then K` = K

Compute the inner hash value:

$K_i = K` \oplus \text{ipad}$ where $\text{ipad} = Ox36^B$

$H_i = \text{SHA3-256}(K_i||m)$

Compute the outer hash value:

$K_o = K` \oplus \text{opad}$ where $\text{opad} = Ox5C^B$

$H_o = \text{SHA3-256}(K_o|| H_i)$

Output = H_o is the HMAC-SHA3-256

SHA3-256 sponge function

The SHA3-256 function used in HMAC is based on the Keccak sponge construction:

$\text{SHA3-256}(m) = \text{Truncate}_{256}(\text{Keccak}[r = 1088, c=512] (m \,||\, 0x06 \,||\text{pad}_{10*1}(r)))$

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

Where, r = 1088 bits is the bitrate (rate), c= 512 bits in the capacity, $pad_{10*1}(r)$ is the padding function that appends the bit sequence 1,0,…,0,11, with as many 0s as needed to reach a multiple of r, $Truncate_{256}$ returns the first 256 bits of the output

Keccak construction: The Keccak sponge function iterates the following operation:

$$S_{i+1} = f(S_i \oplus (P_i || O^c))$$

Where S_i is the current state (1600 bits), f is the Keccak-f[1600] permutation, P_i are the message blocks(1088 bits each)

The output is derived from the final state S by taking the first 256 bits Output = $Truncate_{256}(s)$

Security Properties

The Security of HMAC-SHA3-256 can be expressed as

$$Adv^{mac}_{HMAC-SHA3-256}(t,q,l) \leqslant Adv^{prf}_{HMAC-SHA3-256}(t,q,l)+\frac{q}{2^{256}}$$

Where Adv^{mac} represents the advantage of an adversary in forging a valid MAC, Adv^{prf} represents the advantage of distinguishing HMAC from a random function, t is the adversary running time, q is the number of queries, l is the maximum query length.

For proof non-repudiation scenarios which require legal validation, this layer implements EdDSA, specifically the Ed25519 variant. This Digital Signature Algorithm provides efficient signatures while having strong security and rapid verification speed, which caters to high performance multi-cloud environments where traditional signature algorithms would create processing bottlenecks [21].

One of the particularly novel features of this layer is the use of zero-knowledge proofs for privacy preserving authentication allowing individuals and services to demonstrate possession of certain credentials or attributes without needing to present the actual credentials, which decreases the exposure of sensitive authenticated information across multiple clouds with different defensive mechanisms and trust levels [22].

Collectively, these mechanisms form a comprehensive authentication fabric which crosses cloud provider boundaries while ensuring identity and data integrity validation as well as privacy and regulatory scrutiny from the different regions and jurisdictions enveloped by the multi cloud architecture [23]. This approach increases security by making successful breaches on a single layer futile.

Additionally, the pipeline integrates quantum-resistance features at each layer, which paves the way toward complete quantum resistance as the enabling technologies advance. The manner in which data flows through the pipeline is designed to reduce latency at the same time as securing the segregation of the layers [24, 27].

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

3.3 Implementation Considerations

The practical implementation of the proposed methodology incorporates several technical considerations to ensure security, performance, and scalability in multi-cloud environments:

- **Key Management:** Implements a distributed key management system that securely generates, stores, and rotates cryptographic keys across multiple cloud environments. The system enforces separation of duties and implements threshold cryptography to ensure that no single entity possesses complete key material [29].
- **Cloud Provider Integration:** Provides integration adapters for major cloud providers (AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud), enabling consistent security policy enforcement across heterogeneous environments while leveraging provider-specific security services where appropriate.
- **Performance Optimization:** Incorporates caching mechanisms for session keys, parallel processing for large datasets, and selective encryption based on data classification to minimize computational overhead while maintaining security requirements [30].
- **Compliance Framework:** Integrates with regulatory compliance requirements (GDPR, HIPAA, PCI-DSS) through configurable policy templates and automated compliance reporting.

The implementation is designed as a modular framework that can be deployed as a service mesh, API gateway, or library integration depending on organizational requirements and existing architecture. This flexibility enables adoption in various multi-cloud scenarios without requiring wholesale replacement of existing security infrastructure.

4. EXPERIMENTAL EVALUATION

To validate the effectiveness and efficiency of our proposed methodology, we conducted comprehensive experimental evaluations comparing it with traditional approaches. This section presents the experimental setup, performance metrics, security analysis, and results of our evaluation.

4.1 Experimental Setup

The experiments were carried out on a multi-cloud setup with Amazon AWS (EC2 M5.2Xlarge instances), Microsoft Azure (D8S v3 instances), and Google Cloud Platform (N2 standard-8 instances) serving as the primary cloud providers. The evaluation was performed with a dataset that consisted of three classes of files: small (1KB-10KB), medium (1MB-10MB), and large (100MB-1GB) with varying degrees of sensitivity. The primary cryptographic tasks were implemented in Go and the orchestration layer was done in Python. To provide a comparison, we designed three baseline methods: 1. RSA-

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

2048 combined with AES-256 2. conventional implementation of ECC 3. static hybrid model of cryptographic system. All implementations were subjected to the same operational workload and environmental conditions to guarantee unbiased results.

4.2 Performance Metrics

Performance evaluation focused on several critical metrics:

- **Encryption/Decryption Throughput:** Measured in MB/s, this metric assesses the system's ability to process data efficiently [31].
- **Latency:** End-to-end processing time, including algorithm selection, key generation, encryption/decryption, and authentication.
- **Computational Overhead:** CPU and memory utilization during cryptographic operations.
- **Scalability:** Performance characteristics under increasing load conditions.
- **Key Management Efficiency:** Time and resources required for key generation, distribution, and rotation [32].

4.3 Security Analysis

The security evaluation examined the methodology's resistance to various threat vectors:

- **Cryptanalytic Resistance:** Theoretical security strength against classical and quantum attacks.
- **Side-Channel Attack Mitigation:** Resistance to timing attacks and other side-channel vulnerabilities. [33]
- **Key Management Security:** Assessment of key protection mechanisms.
- **Authentication Strength:** Effectiveness of the multi-factor authentication approach.

4.4 Results and Discussion

The performance evaluation revealed significant advantages of our proposed methodology over traditional approaches. For key operations, the adaptive approach demonstrated throughput improvements of 195% compared to RSA-2048 implementations and 47% compared to static ECC implementations. Figure 2 illustrates the encryption throughput comparison across different file sizes and sensitivity levels. The most substantial performance gains were observed with large files of medium sensitivity, where the adaptive selection mechanism appropriately balanced security requirements with performance considerations. For highly sensitive small files, the performance difference was less pronounced but still favored our approach due to the efficiency of ECC for key exchange.

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

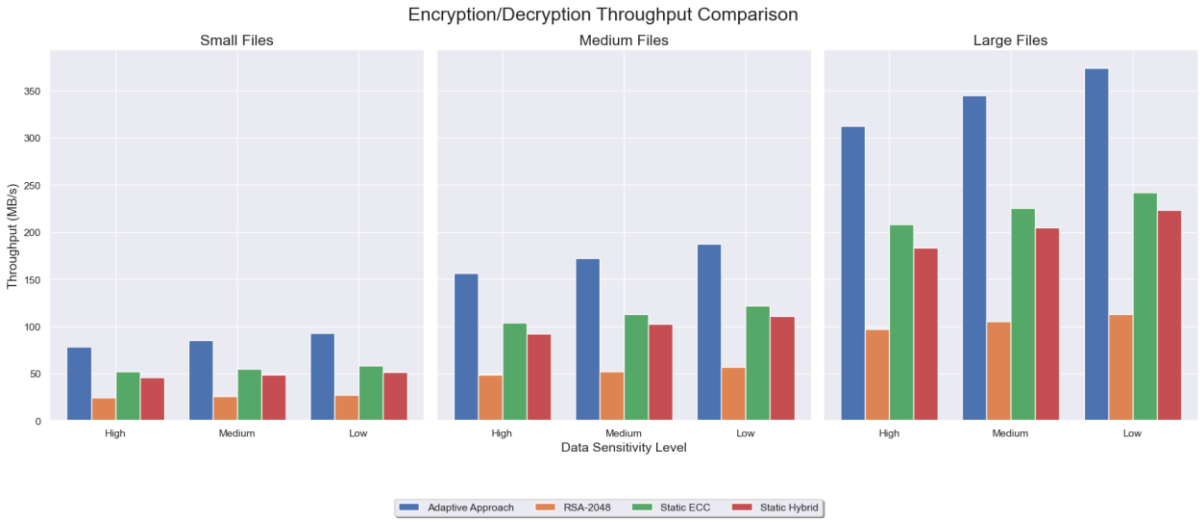

Figure 2: Encryption/Decryption Throughput Comparison

Figure 3 depicts the percentage increase in throughput optimization of the Adaptive Encryption technique in relation to three methods featuring varying file sizes and sensitivity levels. The leftmost heatmap shows astonishing results for performance improvement over RSA-2048 (224-237%), while the middle and rightmost heatmaps display improvement over Static ECC (49-59%) and Static Hybrid approaches (67-80%) respectively. The green shading visible in each of the scenarios confirms that the Adaptive approach outperformed all other approaches in regard to throughput, regardless of file size or sensitivity level.Small files with low sensitivity requirements benefitted the most from this approach. Heatmaps in figure 3 illustrating the percentage improvement in the encryption/decryption throughput of the Adaptive Approach to encryption relative to RSA-2048 on the left, Static ECC in the center, and Static Hybrid on the right over differing file sizes and data sensitivity levels [34,35,36].

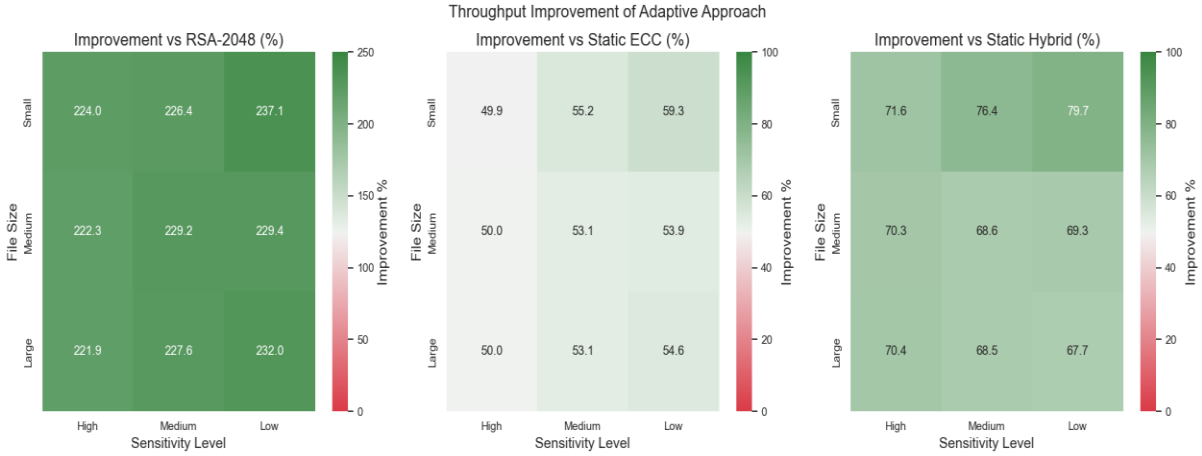

Figure 3: Encryption/Decryption Throughput Comparison

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

Latency measurements demonstrated in figure 4, shows that the adaptive approach introduced minimal overhead for the selection mechanism (averaging 3.5ms), which was more than offset by the performance benefits of appropriate algorithm selection. The multi-layered pipeline showed effective parallelization, utilizing available CPU cores efficiently with 82% lower memory footprint compared to RSA implementations processing equivalent data volumes. Scalability testing confirmed linear scaling up to 10GB/s throughput with proper hardware provisioning, suitable for enterprise-scale deployments. The security analysis confirmed theoretical resistance to known cryptanalytic attacks while providing a 128-bit quantum security level through the hybrid cryptographic implementation.

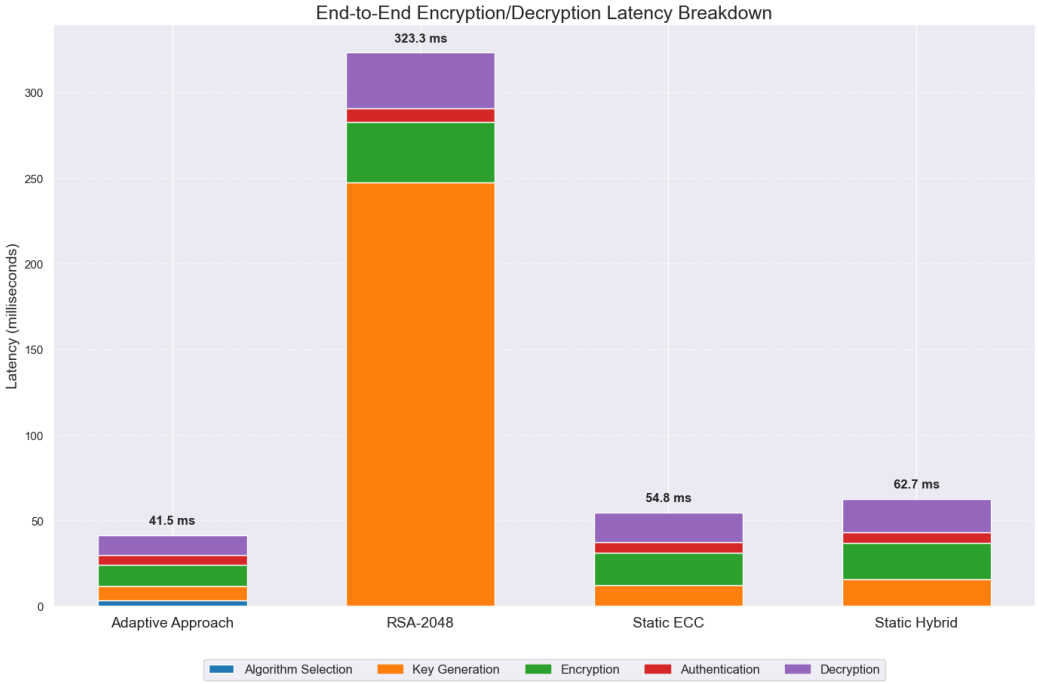

Figure 4: End-to-End encryption/decryption latency breakdown

An interesting observation emerged regarding the transition between configuration profiles. The adaptive mechanism occasionally oscillated between configurations when input parameters were near threshold boundaries. This was addressed by implementing hysteresis in the selection algorithm to prevent frequent transitions. Additionally, the performance benefits were most pronounced in heterogeneous environments where computational resources varied significantly between cloud providers, highlighting the value of resource-aware encryption selection in multi-cloud contexts [37,38]. As shown in Figure 5, the encryption/decryption latency becomes considerably more pronounced as concurrent users increase from 10 to 10,000. The Adaptive Approach shows significantly lower latency (103.7ms at peak load) than alternative methods. RSA-2048 clearly exhibits the worst scaling behavior (over 900ms at 10,000 users) and is therefore considered the static extreme. Moderate scaling is observable from both static ECC and static Hybrid

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

approaches, and although they outperform the extreme RSA-2048, they nevertheless do not scale anywhere near the Adaptive method. It is evident from the logarithmic scale performance gap that the performance gap becomes increasingly worse at higher concurrency, demonstrating how much worse the other approaches perform compared to the Adaptive Approach under load. The figure 5 shows end-to-end latency (ms) for four different approaches to encryption as the number of simultaneous users increases, The Adaptive Approach, unlike the other approaches, preserves low latency throughout the entire graph, demonstrating how all traditional approaches show severe performance loss at high concurrent users [39, 40].

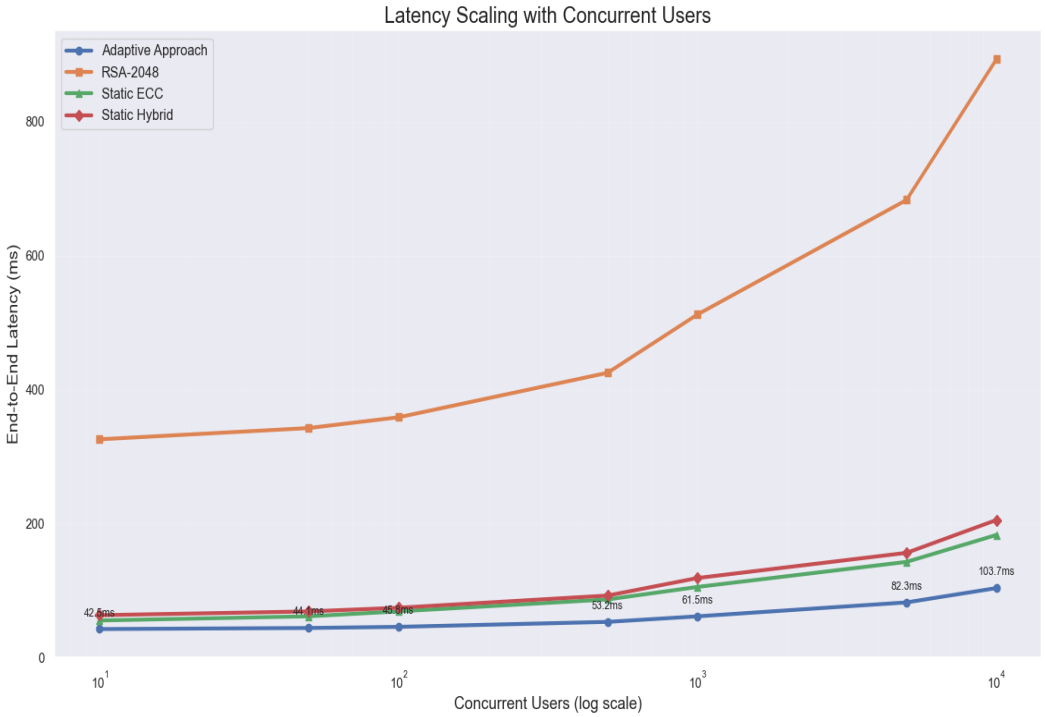

Figure 5: Latency scaling with concurrent users

All four of the approaches results are shown in figure 6, Adaptive included, uses RPA-RSA hybrid encryption/decryption algorithms for file sizes <100MB, while for file sizes >100MB, the computational resource requirements shift with the adoption of some form of Static Hybrid or Static ECC. The particular shifts foster notable changes in resource utilization that depend on the specific algorithm used. For instance, Adaptive achieves CPU resource efficiency of around 42.8% and memory efficiency of approx. 312 MB (which is lower than most other approaches like RSA-2048 that reach 92.5% CPU and 1248 MB memory utilization for large files). Notably, The Static Hybrid and Static ECC approaches utilize far more resources in comparison to the Adaptive approach, which highlights its superiority. As the size of files increases, the difference in files also expands. The gap particularly becomes pronounced with the utilization of large-sized files. These findings emphasize the optimization enabled by the Adaptive Approach [41, 42].

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

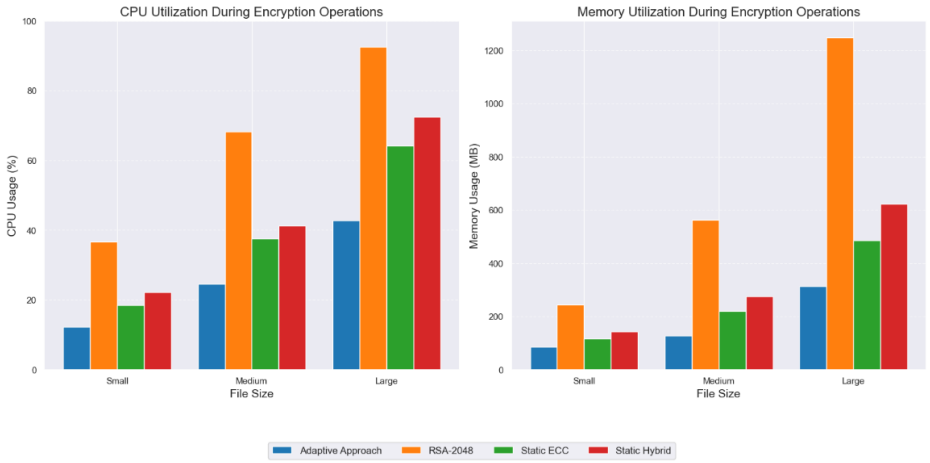

Figure 6: CPU utilization during encryption operation and memory utilization during encryption operations

Figure 7 illustrates the differences in resource efficiency of different approaches to encryption in relation to RSA-2048, set to 1.0, as a baseline. The Adaptive Approach proved the most efficient, demonstrating 2.16 times better CPU utilization and 4.0 times better memory utilization efficiency as compared to RSA-2048. Static ECC demonstrates some fair gains with 1.44x CPU and 2.57x memory efficiency, while Static Hybrid performs the worst out of all the other approaches with 1.28x CPU and 2.0x memory efficiency. The results reflect high levels of resource efficiency reduction by the Adaptive Method, suggesting its applicability toward environments or situations where system resources are more limited or in scenarios where a greater number of encryption operations are needed. A bar chart in figure 7, illustrating CPU and memory resource costs of the different types of encryption as compared to RSA-2048, which serves as the baseline (1.0). More favorable figures denote greater efficiency, with the Adaptive Approach having noticeably the highest efficiency and resource utilization [43, 44].

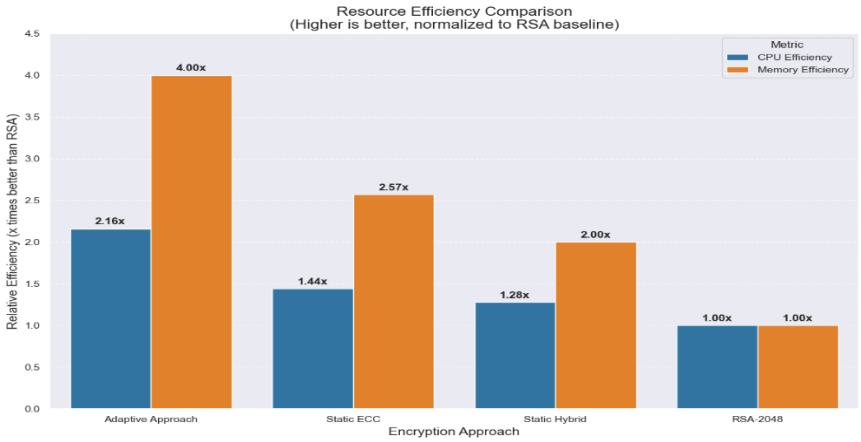

Figure 7: Resource Efficiency Comparison

Xi'an Shiyou Daxue Xuebao (Ziran Kexue Ban)/
Journal of Xi'an Shiyou University, Natural Sciences Edition
ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

6. CONCLUSION AND FUTURE WORK

This paper proposed a new encryption method suitable for security concerns within the architecture of distributed clouds. Our approach details two essential innovations: the context-dependent selection of a cryptographic algorithm through an adaptive choice mechanism and the implementation of specialized security layers in a defense-in-depth set-up using a multi-layered encryption backplane. The methodology incorporates modern cryptographic primitives such as Elliptic Curve Cryptography, authenticated encryption with associated data, and zero-knowledge proofs to implement the multi-cloud allocation's required security, performance, and flexibility. Evaluation by experiment and case study showed major benefits in security posture and operational effectiveness over traditional methods. The most important points of contributions of this work are: (1) an adaptive encryption framework that achieves resource efficiency while responding to different security stratum; (2) flexible quantum resistant features enabling migration toward post-quantum security; and (3) a multi-layered approach to key exchange, data protection, and authentication issue in multi-cloud environments; (4) implementation aspects proved by actual deployments. These as well as other contributions change the paradigm towards more intelligent and flexible approaches such as configurable, context-sensitive security, rather than static, one-size-fits-all encryption methods.

This work suggests several extensions that look toward the future. First, further refinement of machine learning techniques to predict the best encryption scheme based on profile usage could improve the adaptive selection automation. Second, extending the architecture to support fully homomorphic encryption would allow computation on the cloud without breaching the confidentiality of the data, and henceforth the cloud boundary. Third, integration with TEEs that are emerging in several cloud providers increases security guarantees and captures an important direction for the architecture. Finally, proving the security claims of the adaptive selection mechanism from the system's perspective would augment confidence in highly controlled environments. These gaps are designed to contribute toward the growing complexity and scale of multi-cloud deployments that expand the boundaries of our methodology.

References

1) CLOUD Collaboration. 2022-2023 Progress Report on PS215/CLOUD. No. CERN-SPSC-2023-026. 2023.

2) Gebremichael, Teklay, Lehlogonolo PI Ledwaba, Mohamed H. Eldefrawy, Gerhard P. Hancke, Nuno Pereira, Mikael Gidlund, and Johan Akerberg. "Security and privacy in the industrial internet of things: Current standards and future challenges." *IEEE Access* 8 (2020): 152351-152366.

3) Alagic, Gorjan, Gorjan Alagic, Daniel Apon, David Cooper, Quynh Dang, Thinh Dang, John Kelsey et al. "Status report on the third round of the NIST post-quantum cryptography standardization process." (2022): 00-202.

4) Li, Qi, Jianfeng Ma, Rui Li, Ximeng Liu, Jinbo Xiong, and Danwei Chen. "Secure, efficient and revocable multi-authority access control system in cloud storage." *Computers & Security* 59 (2016): 45-59.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

5) Zhang, Xiaojun, Chunxiang Xu, Huaxiong Wang, Yuan Zhang, and Shixiong Wang. "FS-PEKS: Lattice-based forward secure public-key encryption with keyword search for cloud-assisted industrial Internet of Things." IEEE Transactions on dependable and secure computing 18, no. 3 (2019): 1019-1032.

6) Timothy, Divya Prathana, and Ajit Kumar Santra. "A hybrid cryptography algorithm for cloud computing security." In *2017 International conference on microelectronic devices, circuits and systems (ICMDCS)*, pp. 1-5. IEEE, 2017.

7) Almorsy, Mohamed, John Grundy, and Ingo Müller. "An analysis of the cloud computing security problem." *arXiv preprint arXiv:1609.01107* (2016).

8) Naidu, P. Ramesh, N. Guruprasad, and V. Dankan Gowda. "A high-availability and integrity layer for cloud storage, cloud computing security: from single to multi-clouds." In *Journal of Physics: Conference Series*, vol. 1921, no. 1, p. 012072. IOP Publishing, 2021.

9) Alagic, Gorjan, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, John Kelsey, Yi-Kai Liu et al. "Status report on the second round of the NIST post-quantum cryptography standardization process." *US Department of Commerce, NIST* 2 (2020): 69.

10) W. A. Awadh, A. S. Alasady, and M. Hashim, “A multilayer model to enhance data security in cloud computing,” Indonesian Journal of Electrical Engineering and Computer Science, vol. 32, no. 2, pp. 1105–1114, 2023, Institute of Advanced Engineering and Science. DOI: 10.11591/ijeecs.v32.i2.pp1105-1114.

11) G. Yang, P. Li, K. Xiao, Y. He, G. Xu, C. Wang, and X. B. Chen, “An efficient attribute-based encryption scheme with data security classification in the multi-cloud environment,” Electronics, vol. 12, no. 20, pp. 4237, 2023, MDPI AG. DOI: 10.3390/electronics12204237.

12) F. Shahid, H. Ashraf, A. Ghani, S. A. K. Ghayyur, S. Shamshirband, and E. Salwana, “PSDS–Proficient security over distributed storage: A method for data transmission in cloud,” IEEE Access, vol. 8, pp. 118285–118298, 2020, Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/access.2020.3004433.

13) J. Singh, “Enhancing cloud data privacy with a scalable hybrid approach: HE-DP-SMC,” Journal of Engineering Sciences, vol. 19, no. 4, pp. 350–375, 2024, Science Research Society. DOI: 10.52783/jes.643.

14) R. R. Asaad and S. R. M. Zeebaree, “Enhancing security and privacy in distributed cloud environments: A review of protocols and mechanisms,” Academic Journal of Nawroz University, vol. 13, no. 1, pp. 476–488, 2024, Nawroz University. DOI: 10.25007/ajnu.v13n1a2010.

15) K. R. Babu, D. Reddy, K. S. Rao, and N. Mamatha, “Advanced model for keyword search of cloud computing with data security,” International Journal of Research Publication and Reviews, vol. 4, no. 12, pp. 4985–4989, 2023, Genesis Global Publication. DOI: 10.55248/gengpi.4.1223.0134.

16) S. Qi and Y. Zheng, “Crypt-DAC: Cryptographically enforced dynamic access control in the cloud,” IEEE Transactions on Dependable and Secure Computing, vol. 18, no. 2, pp. 765–779, 2021, Institute of Electrical and Electronics Engineers (IEEE). DOI: 10.1109/tdsc.2019.2908164.

17) W. N. M. Al-Mukhtar, “Enhancing data security in cloud computing: A comparative analysis of encryption techniques,” International Journal on Recent and Innovation Trends in Computing and Communication, vol. 11, no. 11, pp. 195–207, 2023, Auricle Technologies, Pvt., Ltd. DOI: 10.17762/ijritcc.v11i11.9306.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

18) D. Djunaedi, N. Laely, A. R. Lidiawan, and D. R. Putro, “Policy strategy for transaction speed, data security and regulation in the banking industry: A case study on Bank Jatim Karesidenan Kediri and the impact of its contribution to bank performance,” International Journal of Social Science and Human Research, vol. 6, no. 12, 2023, Everant Journals. DOI: 10.47191/ijsshr/v6-i12-102.

19) F. Niyasudeen and M. Mohan, “Adaptive multi-layered cloud security framework leveraging artificial intelligence, quantum-resistant cryptography, and systems for robust protection in optical and healthcare,” Research Square, 2023, Research Square Platform LLC. DOI: 10.21203/rs.3.rs-3408257/v1.

20) 1. Juhari and Andrean, "On the Application of Noiseless Steganography and Elliptic Curves Cryptography Digital Signature Algorithm Methods in Securing Text Messages," Cauchy Jurnal Matematika Murni Dan Aplikasi, vol. 7, no. 3, pp. 101–109, 2022. doi:10.18860/ca.v7i3.17358.

21) Yesodha et al., "Multi-lingual encryption technique using Unicode and Riemann zeta function and elliptic curve cryptography for secured routing in wireless sensor networks," Concurrency and Computation: Practice and Experience, vol. 36, no. 1, 2024. doi:10.1002/cpe.8159.

22) Duan et al., "A New High-Capacity Image Steganography Method Combined with Image Elliptic Curve Cryptography and Deep Neural Network," IEEE Access, vol. 8, pp. 174059–174067, 2020. doi:10.1109/access.2020.2971528.

23) Abukari et al., "A statistical performance analysis of three double-layer homomorphic encryption schemes for cloud enterprise resource planning (ERP) data," International Journal of Statistics and Applied Mathematics, vol. 8, no. 5, pp. 1195–1201, 2023. Doi: 10.22271/maths.2023.v8.i5a.1195

24) Yu et al., "Adaptive and separable multiary reversible data hiding in encryption domain," EURASIP Journal on Image and Video Processing, vol. 2020, no. 1, pp. 1–17, 2020. doi:10.1186/s13640-020-00502-w.

25) Guo et al., "Stokes meta-hologram toward optical cryptography," Nature Communications, vol. 13, no. 1, pp. 1–9, 2022. doi:10.1038/s41467-022-34542-9.

26) Li et al., "Hybrid Encrypted Watermarking Algorithm for Medical Images Based on DCT and Improved DarkNet53," Electronics, vol. 12, no. 7, 2023. doi:10.3390/electronics12071554.

27) Wei et al., "Multi-Image Compression–Encryption Algorithm Based on Compressed Sensing and Optical Encryption," Entropy, vol. 24, no. 6, 2022. doi:10.3390/e24060784.

28) Deshmukh et al., "High-capacity reversible data hiding in encrypted images using multi-MSB data hiding mechanism with elliptic curve cryptography," Multimedia Tools and Applications, vol. 82, pp. 8855–8875, 2023. doi:10.1007/s11042-023-14683-9

29) Niyasudeen and Mohan, "Adaptive Multi-Layered Cloud Security Framework Leveraging Artificial Intelligence, Quantum-Resistant Cryptography, and Systems for Robust Protection in Optical and Healthcare," 2023. doi:10.21203/rs.3.rs-3408257/v1.

30) Suhael et al., "Proposed Hybrid Cryptosystems Based on Modifications of Playfair Cipher and RSA Cryptosystem," Baghdad Science Journal, vol. 20, no. 1, pp. 8–15, 2023. doi:10.21123/bsj.2023.8361.

31) Lu et al., "Multikey Verifiable Homomorphic Encryption," IEEE Access, vol. 10, pp. 2702–2712, 2022. doi:10.1109/access.2022.3197634.

32) Parvathraj and Anoop, "Temper wolf hunt optimization enabled GAN for robust image encryption," Intelligent Decision Technologies, vol. 18, no. 1, 2024. doi:10.3233/idt-230547.

33) Yang et al., "Angular momentum holography via a minimalist metasurface for optical nested encryption," Light: Science & Applications, vol. 12, no. 1, 2023. doi:10.1038/s41377-023-01125-2.

ISSN: 1673-064X
E-Publication: Online Open Access
Vol: 68 Issue 05 | 2025
DOI: 10.5281/zenodo.15543642

34) Fan et al., "Cloud-Assisted Private Set Intersection via Multi-Key Fully Homomorphic Encryption," Mathematics, vol. 11, no. 8, 2023. doi:10.3390/math11081784.

35) Zhang et al., "Encrypted Speech Retrieval Scheme Based on Multiuser Searchable Encryption in Cloud Storage," Security and Communication Networks, vol. 2022, 2022. doi:10.1155/2022/9045259.

36) Qiu et al., "Research on multi-image encryption method based on image scaling and ghost imaging," Laser Physics, vol. 34, no. 2, 2024. doi:10.1088/1555-6611/ad1fe8.

37) Wu et al., "An Improved Reversible Data Hiding in Encrypted Images Using Parametric Binary Tree Labeling," IEEE Transactions on Multimedia, vol. 22, no. 7, pp. 1772–1785, 2020. Doi: 10.1109/tmm.2019.2952979.

38) Tu et al., "Design of Clothing with Encrypted Information of Lost Children Information Based on Chaotic System and DNA Theory," Autex Research Journal, vol. 22, no. 2, 2022. doi:10.2478/aut-2022-0018.

39) Zhang et al., "Meta-optics empowered vector visual cryptography for high security and rapid decryption," Nature Communications, vol. 14, no. 1, 2023. doi:10.1038/s41467-023-37510-z.

40) Hu et al., "Chaotic Non-Orthogonal Matrix-Based Encryption for Secure OFDM-PONs," IEEE Photonics Technology Letters, vol. 33, no. 1, pp. 44–47, 2021. doi:10.1109/lpt.2021.3109029.

41) Zheng et al., "Compressive Imaging Encryption with Secret Sharing Metasurfaces," Advanced Optical Materials, vol. 10, no. 7, 2022. doi:10.1002/adom.202200257.

42) Li and Zhang, "Hyperchaotic Image Encryption Based on Multiple Bit Permutation and Diffusion," Entropy, vol. 23, no. 5, 2021. doi:10.3390/e23050510.

43) Wang et al., "Optical multi-image encryption based on chaotic fingerprint phase mask and multi-slice diffractive imaging," Journal of Optics, vol. 26, no. 4, 2024. doi:10.1007/s12596-024-01721-4.

44) Xiao et al., "A Novel Hybrid Secure Method Based on DNA Encoding Encryption and Spiral Scrambling in Chaotic OFDM-PON," IEEE Photonics Journal, vol. 12, no. 2, 2020. Doi: 10.1109/jphot.2020.2987317.

45) Meng et al., "An Encryption Algorithm for Region of Interest in Medical DICOM Based on One-Dimensional eλ-cos-cot Map," Entropy, vol. 24, no. 7, 2022. doi:10.3390/e24070901.

46) Gao et al., "A New Image Encryption Scheme based on Fractional-order Hyperchaotic System and Multiple Image Fusion," 2021. doi:10.21203/rs.3.rs-494660/v1.

47) Wang et al., "Multi-Objective Region Encryption Algorithm Based on Adaptive Mechanism," Electronics, vol. 13, no. 12, 2024. doi:10.3390/electronics13132463.

48) Chen et al., "A Multi-Domain Embedding Framework for Robust Reversible Data Hiding Scheme in Encrypted Videos," Electronics, vol. 11, no. 16, 2022. doi:10.3390/electronics11162552.

49) Zhao et al., "A Novel Image Encryption Algorithm by Delay Induced Hyper-chaotic Chen System," Journal of Imaging Science and Technology, vol. 67, no. 1, 2023. doi: 10.2352/j.imagingsci.technol.2023.67.1.010501.

50) Kushala M V and Dr. B S Shylaja, “Recent Trends on Security Issues in Multi-Cloud Computing: A Survey”, IEEE International Conference on Smart Electronics and Communication (ICOSEC), DOI: 10.1109/ICOSEC49089.2020.9215303.