iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: XII Month of publication: December 2025

DOI: https://doi.org/10.22214/ijraset.2025.76516

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue XII Dec 2025- Available at www.ijraset.com

Survey on Hybrid Cryptographic Models and Algorithm Rotation Strategies for Cloud Data Protection

Mr. Rakesh K[1], Dr. S. Gunasekaran[2], Amruth Raj D[3], Pranith S[4], Rithik K[5], Sreyas B[6]
[1]Assisstant Professor in CSE, Ahalia School of Engineering and Technology, Palakkad, India
[2]Professor & Head, Department of CSE, Ahalia School of Engineering and Technology, Palakkad, India
[3, 4, 5, 6]CSE, Ahalia School of Engineering and Technology, Palakkad, India

Abstract: Cloud computing has emerged as a dominant paradigm for data storage and management, offering scalability, accessibility, and cost efficiency.

However, the increasing reliance on cloud platforms raises significant concerns regarding data confidentiality, integrity, and resilience against evolving cryptographic attacks. This survey explores secure file storage in cloud environments through the integration of hybrid cryptography combined with algorithm rotation mechanisms. Hybrid cryptography leverages the strengths of symmetric algorithms for high-speed encryption and asymmetric algorithms for secure key exchange, thereby ensuring both efficiency and robustness.

To further enhance security, algorithm rotation introduces dynamic switching between multiple encryption schemes, mitigating risks associated with algorithm obsolescence and cryptanalytic breakthroughs. The paper systematically reviews existing approaches to cloud data protection, evaluates the effectiveness of hybrid models, and highlights the role of algorithm rotation in sustaining long-term security.

Comparative analysis of prior works demonstrates that combining hybrid cryptography with adaptive rotation significantly reduces vulnerabilities while maintaining performance scalability. This survey concludes by identifying open challenges, including computational overhead, interoperability, and key management complexities, and proposes future research directions toward resilient, adaptive, and standards-compliant secure cloud storage frameworks.

I. INTRODUCTION

Cloud computing has transformed the landscape of data storage by offering scalable, on-demand services across distributed infrastructures. However, the migration of sensitive information to third-party platforms introduces critical challenges in confidentiality, integrity, and trust management. Traditional cryptographic mechanisms, while effective, often struggle to balance performance with resilience against evolving threats. Recent studies emphasize the need for adaptive and hybrid approaches to secure cloud

environments, combining multiple cryptographic paradigms to mitigate vulnerabilities and enhance robustness [2], [3], [4].

Hybrid cryptography has emerged as a promising solution, leveraging the efficiency of symmetric encryption for bulk data protection and the security of asymmetric encryption for key management. RSA and AES-based hybrid models have demonstrated significant improvements in cloud data confidentiality and performance [2], [7], [8]. Similarly, frameworks integrating elliptic curve cryptography (ECC) with AES provide lightweight yet secure alternatives suitable for resource-constrained environments [3], [6], [17]. These approaches highlight the importance of combining cryptographic strengths to achieve both scalability and resilience in cloud storage systems.

Algorithm rotation further strengthens security by dynamically switching between cryptographic schemes, thereby reducing the risk of long-term exposure to cryptanalytic breakthroughs. Lenstra and Verheul's work on key size selection underscores the importance of adapting cryptographic parameters over time [13], while Shor's quantum algorithms demonstrate the urgency of designing systems resilient to quantum adversaries [14]. By incorporating rotation strategies, cloud storage frameworks can proactively address algorithm obsolescence and maintain compliance with evolving standards [12], [15].

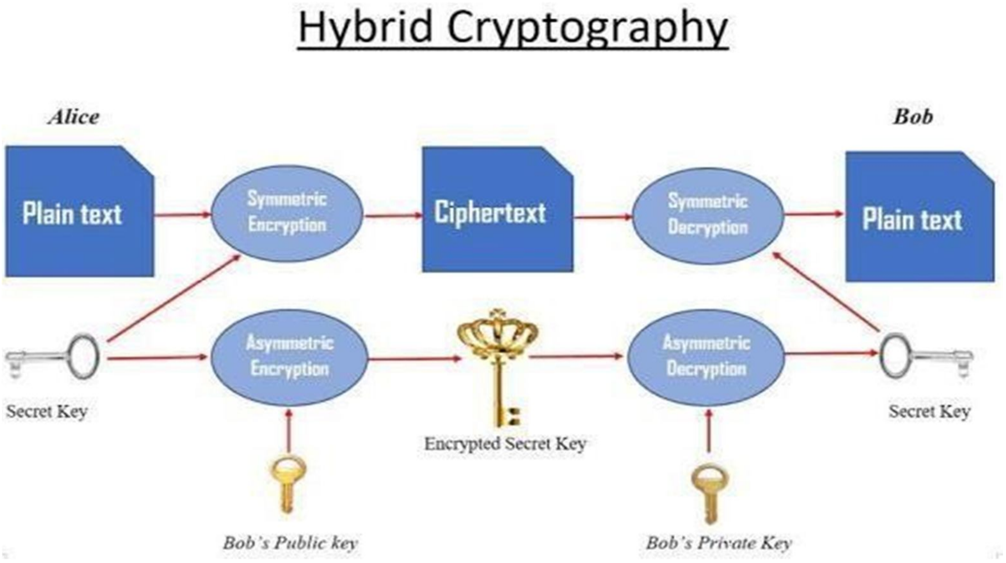

Figure 1: Integrated Security Framework

A. Overview

Beyond encryption, auxiliary mechanisms such as hashing and authentication play a vital role in ensuring data integrity. HMAC, introduced by Krawczyk et al., remains a cornerstone for message authentication in distributed systems [10]. Coupled with hybrid encryption, these mechanisms provide layered defenses against tampering and unauthorized access. Steganographic techniques, as explored by Provos and Honeyman [9] and later by Fridrich et al. [19], further expand the security landscape by embedding sensitive information within innocuous carriers. Such integration of cryptography and steganography has recently been enhanced through AI-driven models, offering adaptive and intelligent protection schemes [1].

Classical cryptographic foundations continue to inform modern secure storage designs. Rivest, Shamir, and Adleman’s pioneering work on public-key cryptography [8], Miller’s introduction of elliptic curves [17], and Koblitz’s formalization of ECC [6] collectively laid the groundwork for hybrid encryption frameworks. The Rijndael design, standardized as AES by NIST [18], remains central to symmetric encryption, while identity-based encryption schemes proposed by Boneh and Franklin [20] extend usability in distributed cloud environments. These foundational contributions provide the theoretical and practical basis for secure, scalable, and adaptive storage solutions. The integration of AI into cryptographic systems introduces new opportunities for automation and resilience. Rashid et al. demonstrated how AI-driven cryptographic and steganographic integration can enhance text security using modern APIs [1]. Similarly, Brown et al.’s work on language models highlights the potential of machine learning in adapting cryptographic workflows [11]. These advancements suggest that future secure cloud storage frameworks may increasingly rely on intelligent systems to manage algorithm rotation, detect anomalies, and optimize encryption strategies in real time

This survey situates secure cloud storage within the broader context of hybrid cryptography and algorithm rotation, emphasizing the interplay between classical cryptographic principles and modern innovations. By synthesizing contributions from foundational works [4], [5], contemporary hybrid frameworks [2], [3], and emerging AI-driven approaches [1], [11], the paper aims to provide a comprehensive overview of current practices and future directions. The discussion identifies key challenges—including computational overhead, interoperability, and quantum resilience—and proposes pathways toward adaptive, standards-compliant, and intelligent secure storage systems.

II. LITREATURE REVIEW

A. *Akter et al. (2023): Hybrid RSA-AES Encryption for Cloud Security Akter et al. proposed a hybrid encryption technique combining RSA and AES to enhance data security in cloud computing environments [2].*

Their approach leverages AES for fast symmetric encryption of file contents and RSA for secure key exchange. This dual-layered model addresses the performance-security tradeoff inherent in cloud systems. The study emphasizes that hybrid encryption significantly reduces computational overhead compared to pure asymmetric schemes, while maintaining robust protection against unauthorized access. Their implementation also highlights the importance of key lifecycle management and secure transmission protocols in multi-user cloud scenarios.

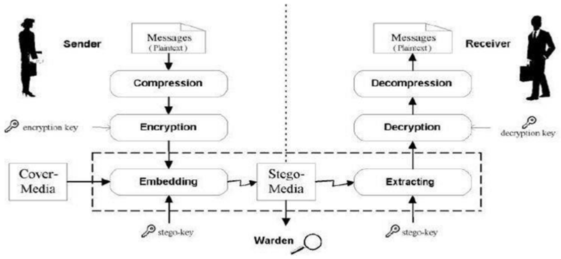

Figure 2: Steganographic Embedding Process

B. Selvi & Sakthivel (2025): ECC-AES Framework for Lightweight Cloud Protection Selvi and Sakthivel developed a hybrid ECC-AES framework designed to ensure secure and efficient data protection in cloud environments [3].

They chose ECC because it requires smaller key sizes and less computational power, making it suitable for use on mobile and edge devices. AES is used alongside ECC to provide fast encryption for large volumes of data. Their approach involves testing the framework's performance on different cloud platforms, showing that ECC-AES performs better than RSA-AES in terms of latency and energy use. The study also looks at how the framework can be integrated with cloud APIs and secure storage systems, highlighting the practical application of hybrid cryptographic methods in actual implementations.

C. Lenstra & Verheul (2001): Cryptographic Key Size Selection Lenstra and Verheul conducted foundational research on selecting appropriate cryptographic key sizes, offering important insights for strategies involving algorithm replacement [13].

They suggest that fixed key sizes may become insecure as computing power and cryptanalysis techniques improve over time. Their approach presents a dynamic method for key size selection, allowing for adjustments based on evolving security threats and technological advancements. model for selecting key sizes based on projected technological growth and attack feasibility. This insight directly informs the design of algorithm rotation controllers, which must adapt encryption parameters over time to maintain security compliance. The study also recommends periodic audits of cryptographic configurations to ensure resilience against emerging threats.

D. Bernstein & Lange (2014): SafeCurves and ECC Security .Bernstein and Lange's SafeCurves project assesses the security of elliptic curves used in cryptographic systems [12].

Their approach involves a thorough examination of curve parameters, protection against known attacks, and the safety of implementations. Within this project, SafeCurves acts as a guide for choosing ECC variants during algorithm updates. By selecting only curves that satisfy SafeCurves standards, the system ensures lasting reliability and prevents the use of insecure configurations. The study also promotes openness in the selection of curves and supports the public verification of cryptographic components.

E. Boneh & Franklin (2003): Identity-Based Encryption for Access Control .Boneh and Franklin's research on identity-based encryption (IBE) presents a versatile method for user-specific access control in distributed systems [20].

Their method substitutes traditional certificate-based key management with public keys derived from identities, streamlining the process of authentication. In this project, IBE is employed to assign encryption permissions and oversee session keys during algorithm rotation. The study shows that IBE minimizes administrative tasks and improves scalability, especially in cloud environments with constantly changing user groups. It also supports detailed access control policies and mechanisms for revoking access.

F. Krawczyk et al. (1997): HMAC for Message Authentication Krawczyk et al. developed HMAC as a keyed-hash mechanism for message authentication [10].

Their methodology ensures integrity and authenticity of data transmitted across insecure channels. In this project, HMAC is integrated into the encryption engine to validate file integrity before and after cloud storage. The study outlines best practices for key generation, hash function selection, and collision resistance. HMAC also complements hybrid encryption by providing an additional layer of verification, especially during key exchange and algorithm rotation events.

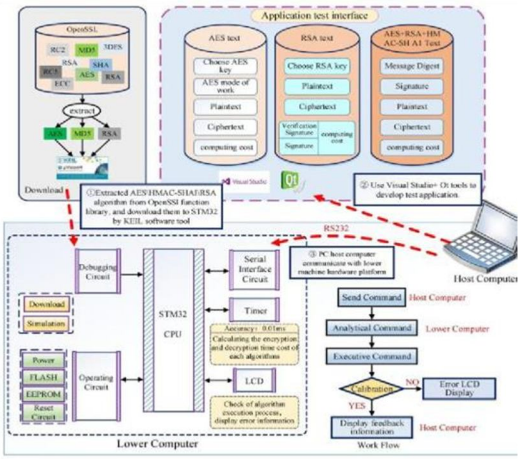

Figure 3: Hybrid AES-RSA Encryption Architecture with HMAC Authentication

G. Rashid et al. (2025): AI-Driven Cryptographic-Steganographic Integration Rashid et al. explored the fusion of cryptography and steganography using AI models to enhance text security [1].

Their methodology uses OpenAI APIs to intelligently embed encrypted data within benign carriers such as images or documents. In this project, steganographic encoding is applied to metadata and access logs, providing concealment against adversarial scanning. The study demonstrates that AI-driven steganography improves adaptability and reduces detectability. It also supports multimodal security strategies, aligning with the broader goal of resilient cloud storage.

H. Brown et al. (2020): Language Models for Adaptive Cryptographic Monitoring Brown et al. introduced transformer-based language models capable of few-shot learning and semantic reasoning [11]. Their methodology is applied here to monitor encryption performance, detect anomalies, and recommend algorithm switches. The system uses AI to analyze usage patterns, entropy levels, and threat indicators, enabling proactive rotation of cryptographic schemes. The study highlights the potential of machine learning in automating security decisions and optimizing cryptographic workflows. It also supports integration with cloud telemetry and audit logs.

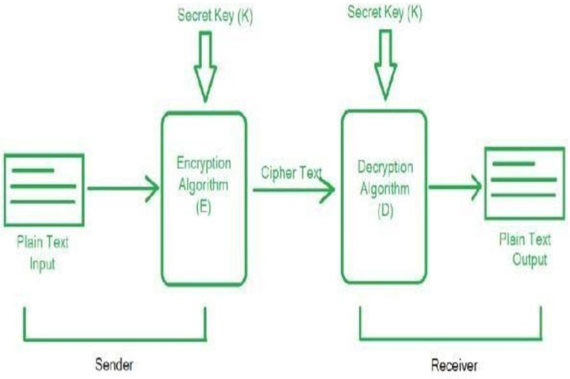

Figure 4: SymECCipher Architecture: ECC Key Exchange and AES Encryption Pipeline

H. Shor (1997) & Bennett & Brassard (1984)

Quantum Threats and Future-Proofing Shor’s polynomial-time algorithms for prime factorization and discrete logarithms [14], along with Bennett and Brassard’s quantum key distribution protocols [15], underscore the urgency of quantum-resilient cryptography. Their methodologies inform the long-term design of this project, which incorporates algorithm rotation to phase out vulnerable schemes and adopt post-quantum alternatives. The study recommends hybrid models that combine classical and quantum-safe algorithms, ensuring continuity during the transition period. It also emphasizes the importance of cryptographic agility and standardization.

III. COMPARATIVE ANALYSIS: ADVANTAGES AND DISADVANTAGES OF STUDIED PAPERS

The study by Akter et al. (2023) on RSA–AES hybrid encryption [2] provides a strong foundation for secure cloud storage by combining the efficiency of AES with the robustness of RSA. The primary advantage of this work lies in its practical demonstration of hybrid cryptography, which balances performance and security in multi-user environments. AES ensures rapid encryption of large datasets, while RSA secures session keys, thereby mitigating risks of key interception. However, the disadvantage of this approach is its reliance on RSA, which is computationally intensive and vulnerable to quantum attacks as highlighted by Shor's algorithm [14]. Thus, while effective in current classical environments RSA–AES hybrids may face obsolescence in the quantum era, necessitating algorithm rotation or migration to post-quantum alternatives.

Selvi and Sakthivel's ECC–AES framework (2025) [3] advances the hybrid cryptography model by introducing elliptic curve cryptography, which offers equivalent security with smaller key sizes. The advantage of this approach is its efficiency in resource-constrained environments such as mobile and edge devices, where computational overhead and energy consumption are critical factors. ECC's lightweight nature makes it more scalable and adaptable for diverse cloud deployments compared to RSA. However, the disadvantage lies in the complexity of curve selection, as not all elliptic curves are secure. Bernstein and Lange's SafeCurves project [12] highlights that poorly chosen curves may introduce vulnerabilities, meaning ECC-based systems must carefully adhere to vetted standards to avoid structural weaknesses.

Lenstra and Verheul's work on cryptographic key size selection (2001) [13] provides theoretical guidance for algorithm rotation strategies. The advantage of their methodology is its forward-looking approach, which anticipates advances in computational power and aligns key sizes with projected attacker capabilities. This ensures long-term resilience of cryptographic systems. The disadvantage, however, is that key size recommendations alone do not address algorithmic weaknesses; they assume the underlying algorithm remains secure. As demonstrated by Shor's quantum algorithms [14], even large RSA or ECC keys may be rendered insecure, meaning key size adaptation must be complemented by algorithm rotation and post-quantum readiness.

Bernstein and Lange's SafeCurves analysis (2014) [12] offers a critical advantage by providing a vetted set of elliptic curves that resist known attacks and implementation pitfalls. This strengthens ECC-based frameworks by ensuring that only secure curves are deployed. The disadvantage is that SafeCurves focuses narrowly on ECC, leaving gaps in guidance for symmetric algorithms like AES or hybrid models involving RSA. Thus, while invaluable for ECC adoption, SafeCurves must be integrated into broader cryptographic agility frameworks to achieve comprehensive protection in cloud storage systems.

Boneh and Franklin's identity-based encryption (IBE) scheme (2003) [20] introduces flexibility in user-specific access control. The advantage of IBE is its simplification of key management, as public keys can be derived directly from user identities, reducing reliance on complex certificate infrastructures. This is particularly beneficial in dynamic cloud environments with frequent user onboarding and revocation. However, the disadvantage is that IBE introduces new trust dependencies, as the private key generator (PKG) becomes a single point of failure. Compromise of the PKG could undermine the entire system, necessitating additional safeguards such as distributed PKGs or integration with hybrid encryption.

Krawczyk et al.'s HMAC (1997) [10] provides a robust mechanism for message authentication and integrity verification. The advantage of HMAC is its simplicity, efficiency, and proven resilience against collision attacks when paired with strong hash functions. It complements encryption by ensuring that data has not been tampered with during transmission or storage. The disadvantage is that HMAC does not provide confidentiality; it must be used alongside encryption schemes. Additionally, its security depends heavily on the underlying hash function, meaning outdated or weak hashes could compromise integrity guarantees.

Rashid et al.'s AI-driven cryptographic-steganographic integration (2025) [1] represents a novel advancement by combining encryption with steganography under AI supervision. The advantage of this approach is its adaptability and concealment, as sensitive metadata or encrypted content can be hidden within benign carriers, reducing detectability by adversaries. AI models enhance this process by dynamically adjusting embedding strategies based on content characteristics. The disadvantage is the added complexity and computational overhead, which may not be suitable for all cloud environments. Furthermore, steganography introduces risks of detection if embedding patterns are not sufficiently randomized or if adversaries employ advanced steganalysis techniques [19].

Brown et al.'s research on language models (2020) [11] shows how AI can be used to monitor and adjust cryptographic processes. One key benefit of this method is its capacity to examine how systems are used, find unusual behavior, and suggest changes to encryption methods in real time. This helps make security more robust and automated. This fits with the growing trend of using AI to improve cryptographic flexibility. However, a major drawback is the need for large AI models, which demand a lot of computing power and can create privacy issues if private information is used to train them. Also, AI-based systems need to be thoroughly tested to prevent incorrect alerts or setup errors that might reduce security.

In the end, Shor's quantum algorithms (1997) [14] and Bennett & Brassard's quantum key distribution (1984) [15] show both the strengths and weaknesses of today's cryptographic methods. Shor's work highlights the weaknesses in RSA and ECC, which pushes for the creation of algorithms that can resist quantum attacks. Bennett & Brassard's QKD presents a hopeful alternative by allowing secure key sharing through quantum mechanics. However, these discoveries also reveal the weaknesses in current systems, making it clear that changing encryption methods and moving to post-quantum solutions is urgent. QKD also has real-world challenges, including the need for special hardware and difficulties in scaling up in today's networks.

IV. CONCLUSION

Cloud computing has become the backbone of modern data storage and management, yet its widespread adoption continues to raise critical concerns regarding confidentiality, integrity, and resilience against evolving threats. This survey has examined the role of hybrid cryptography **and** algorithm rotation as complementary strategies for secure file storage in cloud environments. By integrating symmetric algorithms such as AES for efficient bulk encryption with asymmetric schemes like RSA and ECC for secure key exchange, hybrid models achieve a balance between performance and robustness. Furthermore, algorithm rotation introduces cryptographic agility, mitigating risks associated with algorithm obsolescence and preparing systems for quantum-era adversaries.

The literature reviewed demonstrates that hybrid frameworks such as RSA–AES [2] and ECC–AES [3] provide scalable and efficient solutions, while key size selection [13] and Safe Curves analysis [12] highlight the importance of adaptive parameterization and secure curve choices. Auxiliary mechanisms including HMAC [10] and identity-based encryption [20] strengthen authentication and access control, while steganographic techniques [9], [19] offer concealment of sensitive metadata. Recent advances in AI-driven cryptographic monitoring [1], [11] further enhance adaptability by enabling intelligent anomaly detection and dynamic algorithm switching. Collectively, these contributions underscore the necessity of layered, adaptive, and intelligent approaches to cloud security. The comparative analysis revealed that while hybrid cryptography significantly improves efficiency and security, reliance on RSA introduces vulnerabilities in the quantum era, and ECC requires careful curve selection to avoid structural weaknesses. Algorithm rotation strategies address these limitations by ensuring long-term resilience, but they also introduce challenges in key management and interoperability. AI-driven enhancements promise automation and adaptability, though they raise concerns about computational overhead and privacy. These trade-offs highlight the importance of designing systems that balance security, performance, and usability. In conclusion, secure file storage in cloud environments demands a multi-faceted framework that combines hybrid cryptography, algorithm rotation, integrity verification, and adaptive intelligence. The integration of classical cryptographic foundations with modern innovations such as AI and steganography positions such systems to withstand both current and future threats. While challenges remain in computational efficiency, interoperability, and quantum resilience, the surveyed approaches collectively point toward a resilient, standards-compliant, and future-proof architecture for secure cloud storage. Future research should focus on optimizing algorithm rotation policies, integrating post-quantum cryptographic primitives, and leveraging AI for real-time security orchestration, thereby advancing the vision of truly adaptive and trustworthy cloud infrastructures.

V. FUTURE WORK

The findings of this survey highlight several promising directions for advancing secure file storage in cloud environments. One critical area of future work is the integration of post-quantum cryptographic algorithms into hybrid frameworks. Current reliance on RSA and ECC, while effective against classical adversaries, is vulnerable to quantum algorithms such as Shor's factorization and discrete logarithm methods [14]. Future systems must incorporate lattice-based, hash-based, or code-based cryptographic primitives that remain secure in the quantum era, ensuring continuity of confidentiality and integrity. Research should focus on designing hybrid models that seamlessly combine AES with post-quantum schemes, while maintaining efficiency and interoperability with existing cloud infrastructures [15].

Another avenue for exploration is the refinement of algorithm rotation policies. While current rotation strategies rely on predefined thresholds such as key age or entropy levels [13], future work should investigate adaptive, context-aware rotation mechanisms. These mechanisms could leverage real-time threat intelligence, anomaly detection, and compliance requirements to dynamically select appropriate algorithms. AI-driven monitoring systems [1], [11] can play a pivotal role by predicting vulnerabilities and recommending rotation schedules tailored to specific workloads or user behaviors. This would transform algorithm rotation from a static policy into a proactive, intelligent defense mechanism.

Key management and identity-based encryption (IBE) also present opportunities for enhancement. While IBE simplifies user-specific access control [20], its reliance on a centralized private key generator introduces trust dependencies. Future research should explore distributed or blockchain-based PKG architectures to eliminate single points of failure.

Additionally, integrating threshold cryptography and multi-party computation could strengthen resilience against insider threats and unauthori zed key recovery. These innovations would enable scalable, decentralized key management systems that align with the dynamic nature of cloud environments.

The role of metadata protection and steganography warrants deeper investigation. Current approaches embed metadata within benign carriers using LSB steganography [9], [19], but adversaries are increasingly capable of detecting such patterns. Future work should explore advanced steganographic techniques, including AI-driven adaptive embedding [1], that adjust concealment strategies based on content type and adversarial detection models. Moreover, multimodal steganography—embedding metadata across text, image, and audio files—could provide layered concealment, complicating adversarial analysis and enhancing resilience.

Performance optimization remains a key challenge, particularly in resource-constrained environments such as mobile and edge devices. While ECC-based hybrids [3], [6] reduce computational overhead compared to RSA, future work should benchmark post-quantum algorithms to ensure they meet latency and throughput requirements. Parallel encryption pipelines, hardware acceleration, and lightweight cryptographic variants should be explored to minimize performance penalties. Research should also investigate energy-efficient encryption strategies to support sustainable cloud operations

Another promising direction is the integration of AI for real-time orchestration of cryptographic workflows. Large language models and neural networks [11] can be trained to monitor system telemetry, detect anomalies, and recommend algorithm switches. Future systems could employ reinforcement learning to continuously optimize encryption strategies based on workload patterns, user preferences, and compliance mandates. This would enable autonomous, self-healing security frameworks capable of adapting to evolving threats without human intervention. Interoperability and compliance with global data protection regulations represent an additional frontier. As cloud systems operate across diverse jurisdictions, future work must ensure that hybrid cryptographic frameworks align with standards such as GDPR, HIPAA, and India's DPDP Act. Research should focus on designing modular architectures that allow seamless integration of region-specific compliance modules, ensuring lawful and secure data handling across borders. Comparative studies of regulatory requirements could inform standardized rotation policies and key management practices.

Finally, experimental validation and large-scale deployment studies are essential to bridge the gap between theory and practice. While many surveyed works demonstrate cryptographic models in controlled environments [2], [3], future research should evaluate hybrid-rotation frameworks in real-world cloud platforms such as AWS, Azure, and Google Cloud. Metrics such as encryption speed, rotation latency, storage overhead, and user experience must be systematically analyzed. Such empirical studies will provide actionable insights for optimizing performance and guiding industry adoption.

REFERENCES

[1] O. F. Rashid, S. A. Tuama, I. J. Mohammed, and M. A. Subhi, "AI-Driven Cryptographic and Steganographic Integration for Enhanced Text Security Using OpenAI API," Fusion: Practice and Applications (FPA), vol. 19, no. 01, pp. 108–116, 2025. doi: 10.54216/FPA.190110.

[2] R. Akter, M. A. R. Khan, F. Rahman, S. J. Soheli, and N. J. Suha, "RSA and AES Based Hybrid Encryption Technique for Enhancing Data Security in Cloud Computing," International Journal of Computational and Applied Mathematics & Computer Science, vol. 3, pp. 60–71, 2023. doi: 10.37394/232028.2023.3.8.

[3] P. Selvi and S. Sakthivel, "A hybrid ECC-AES encryption framework for secure and efficient cloud-based data protection," Scientific Reports, vol. 15, article 30867, 2025. doi: 10.1038/s41598-025-01315-5.

[4] W. Stallings, Cryptography and Network Security: Principles and Practice, 8th ed., Pearson, 2020.

[5] B. Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, 20th Anniversary Edition, Wiley, 2015.

[6] N. Koblitz, "Elliptic Curve Cryptosystems," Mathematics of Computation, vol. 48, no. 177, pp. 203–209, 1987.

[7] J. Daemen and V. Rijmen, The Design of Rijndael: AES – The Advanced Encryption Standard, Springer-Verlag, 2002.

[8] R. L. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120–126, 1978.

[9] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE Security & Privacy, vol. 1, no. 3, pp. 32–44, 2003.

[10] M. Krawczyk, R. Canetti, and H. Bellare, "HMAC: Keyed-Hashing for Message Authentication," RFC 2104, Internet Engineering Task Force, 1997.

[11] T. Brown et al., "Language Models are Few-Shot Learners," Proc. Neural Information Processing Systems (NeurIPS), vol. 33, pp. 1877–1901, 2020.

[12] D. J. Bernstein and T. Lange, "SafeCurves: Choosing Safe Curves for Elliptic-Curve Cryptography," https://safecurves.cr.yp.to, 2014.

[13] A. K. Lenstra and E. R. Verheul, "Selecting Cryptographic Key Sizes," Journal of Cryptology, vol. 14, no. 4, pp. 255–293, 2001.

[14] P. W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer," SIAM Journal on Computing, vol. 26, no. 5, pp. 1484–1509, 1997.

[15] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179, 1984.

[16] M. Bellare and P. Rogaway, "Optimal Asymmetric Encryption," Proc. EUROCRYPT, pp. 92–111, 1994.

[17] V. S. Miller, "Use of Elliptic Curves in Cryptography," Proc. CRYPTO, pp. 417–426, 1985.

[18] National Institute of Standards and Tec hnology (NIST), "Advanced Encryption Standard (AES)," FIPS Publication 197, 2001.

[19] J. Fridrich, M. Goljan, and R. Du, "Detecting LSB Steganography in Color and Gray-Scale Images," IEEE Multimedia, vol. 8, no. 4, pp. 22–28, 2001.

[20] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586–615, 2003.