Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Enhancing Cloud Security Through Hybrid Cryptography: A Comprehensive Survey of AES, RSA, and HMAC-Based Techniques

Mr. Pradeep Tandekar
Department of Computer Science and Engineering
University Institute of Technology, RGPV
Bhopal (M.P.), India

Dr. Raju Baraskar
Department of Computer Science and Engineering University
Institute of Technology, RGPV
Bhopal (M.P.), India

Abstract **- The rapid expansion of cloud computing has significantly reshaped the paradigm for data management, processing, and storage. Despite the unmatched scalability, cost-effectiveness, and remote accessibility that cloud computing has to offer, this has been accompanied by an increased vulnerability to emerging security threats. The limitations that have been witnessed with the application of a single algorithm approach to cryptography have been substantial, as this approach cannot guarantee security features such as integrity, authenticity, and confidentiality at the same time. In order to fill the gap, more and more researchers have resorted to hybrid cryptographic frameworks, which leverage the benefits of different algorithms. The current paper is a structured survey of existing literature from the years 2014-2025, which focuses on hybrid frameworks using three widely used and established cryptographic mechanisms. These include the Advanced Encryption Standard (AES) algorithm, which provides rapid and reliable symmetric key data encryption, the Rivest-Shamir-Adleman (RSA) algorithm, which provides asymmetric key exchange and secure user authentication, and the Hash-based Message Authentication Code (HMAC) algorithm, which provides secure data verification and source authenticity. These three algorithms provide a comprehensive solution to the three aspects of the CIA triad, thus providing a more viable and robust security framework. The current survey includes about seventeen primary sources along with a few additional sources, which focus on real-time applications in cloud-based healthcare systems, which require additional security compliances as per HIPAA and GDPR. The current paper also focuses on emerging trends in the form of post-quantum cryptography, which is a new area of research in cloud security.**

Keywords - Cloud security, AES, RSA, HMAC, hybrid cryptography, data integrity, key management, healthcare cloud systems

I. INTRODUCTION

Cloud computing has become very popular for storage, processing, and software services using scalable systems. Cloud computing enables users to access shared computing resources easily using public, private, and hybrid clouds. Due to its easy scalability, cost-effectiveness, and remote accessibility, cloud computing has been applied in many fields such as healthcare, banking, education, and business applications. However, in addition to the advantages, cloud computing platforms also introduce many security issues, particularly concerning data privacy, accuracy, and illegal access. As cloud computing platforms are normally multi-user and virtualized, confidential data is normally stored and processed using the same hardware. However, this approach also makes the data prone to various security threats like data leakage, internal threats, sharing of data between users, and loss of accuracy of the data. Further, current cloud computing infrastructures are prone to advanced threats like timing attacks, side-channel attacks, ransomware, and DDoS, which make it difficult to track and manage them through traditional security measures [34], [37], [40]. Therefore, data security has turned out to be a major issue for cloud service providers as well as cloud service users.

"The use of cryptographic methods is the basic foundation" for cloud security because it will aid in keeping data private, secure against unauthorized alterations, and properly verified. Nevertheless, the use of a particular method is normally insufficient to deal with various security threats.

A. Advanced Encryption Standard (AES) is a symmetric encryption algorithm that is widely popular for encrypting large amounts of data because it runs at a in a fast rate and with high security. Highly suitable for encrypting data stored in the cloud and data being transmitted over the network, but it is not suitable for the purpose of the project sharing and managing secret keys, especially in large cloud systems.

B. The Rivest-Shamir-Adleman an asymmetric encryption technique that provides a Solution to the problem of secure key exchange using public and private keys. The RSA algorithm is of utmost their importance in user authentication, secure key exchange, etc.), because the and digital signatures in cloud computing. RSA This is because this algorithm requires more computational power and is slower in encryption of large data files, especially when using larger key sizes. Because of this reason, the RSA algorithm is not suitable for encrypting large data in cloud computing.

C. Hash-based Message Authentication Code (HMAC) is generally used to ensure that the data does not get altered in any manner during its storage or transmission process; also, the authenticity of the data gets ensured as they are being sent from the right source only. It generally utilizes various hash techniques like SHA-256, SHA-512, or SHA-3 for carrying out this process. HMAC helps in identifying if there is any altering of data during its storage or transmission process in an improper manner. However, HMAC does not conceal the “information” part of the data; thus, on its own, HMAC is incapable of maintaining the security of the data in the cloud.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

All three of these techniques are only concerned with securing only one of the three major characteristics of data: CIA. AES is for data confidentiality; thus, they cannot individually address all three of the security requirements for cloud computing. This implies the use of hybrid techniques instead. As a hybrid technique, HMAC is generally utilized for data integrity in clouds; likewise, encryption of the data in the cloud gets carried out by using the hybrid form of AES [1],[4],[6],[11].

Studies have found that the integration of AES, RSA, and HMAC improves cloud security by blocking leaks, securing access, and maintaining efficiency. These techniques are widely applied in various sectors, particularly in healthcare cloud systems that comply with HIPAA, GDPR, and other standards to properly encrypt, verify, and manage data [4], [6], [11].

This research will explore the hybrid cryptography process involving AES, RSA, and HMAC, particularly from 2014 to 2025. It will also point out the gaps to highlight the latest trends in advanced cryptography, such as post-quantum cryptography.

II. LITERATURE REVIEW

A hybrid cryptography technique that involves a combination of AES, RSA, and HMAC has been one of the most prominent things in the last ten years to secure cloud infrastructure. These hybrid models were developed because the use of a single technique for encryption suffers a lot of limitations, and it is not good enough to provide complete security. These hybrid models aimed at solving the issues of data security, data integrity, and user authentication simultaneously. The research studies between 2014 and 2025 depict a gradual enhancement of the hybrid cryptographic models. This is due to growing cloud technology adoption, entailing strict security policies, as well as sophisticated cyber-attacks.

A. Early Hybrid Encryption Models (2014–2016)

Research works that were conducted on the subject of hybrid cryptography were mainly centered on the integration of symmetric and symmetric encryption for the purpose of protecting information that is storied in the cloud. One of the first hybrid methods for the security of cloud data. In the study done by Shahade and Mahalle [1] published in , AES-128 is used as the encryption technique for the data of the users. In the same study, the secret key used for the AES is encrypted using the RSA technique with a key size of 1024. The study is done using the EyeOS technique. The results showed that the data can be securely done without the cloud administrators being able to view the data. Also, the study is done with a very less amount of data.

Singh et al. [19] proposed the use of the hybrid approach to secure the data in the field of telemedicine and remote patient monitoring services. In the proposed approach of Singh et al., the feature of AES was used to secure the medical data being received through sensors.

B. Policy-Oriented and Domain-Specific Hybrid Models (2017-2018)

As cloud systems started to be adopted in regulated environments, there was a growing realization that many cloud vendors environments, researchers began to focus on rules, policies, and domain-based security needs. A hybrid encryption scheme for cloud-based health care. The systems proposed by Khattak et al. [2] used AES for encrypting data and RSA for easy management of keys. "primarily to comply with HIPAA regulations." The findings of their research indicated that using effective cryptography is highly significant to ensure patient privacy and data accessibility in cloud setups.. However, their research primarily concentrated on policies and system design rather than evaluating speed and efficiency, and hence, the efficiency aspect was not explored.

Sharma and Rohini [5] introduced data integrity verification into the hybrid cloud security framework by employing the use of HMAC with SHA-512, in addition to AES and RSA encryption algorithms. The algorithm demonstrated that HMAC is capable of detecting any unauthorized modifications to the data with very little overhead cost compared to re-encryption algorithms. However, the authors failed to demonstrate how the HMAC keys are to be shared securely.

Bansal and Kaushik [18] proposed an improved model by utilizing AES-256 with RSA-2048 for modular cloud encryption, which showed better performance of about 35-40% compared to systems that used only RSA encryption. But since their model did not have a proper integrity check mechanism, the entire security of the system was not addressed.

C. Performance Optimization and Parallelization (2019–2021)

With the increasing size of data and cloud computing, scientists began to pay more attention to improving the speed of hybrid encryption systems. A hybrid encryption environment proposed by Patel et al. [3] utilized parallel processing to reduce the encryption time required in large cloud data centers. The result of their research showed that multi-thread encryption can significantly reduce delays, although the performance analysis was not very elaborate.

Kumar and Kumar [12] made a thorough analysis of various key sizes of RSA (1024, 2048, and 4096 bits) in AES-RSA hybrid cryptosystems. They concluded that a 2048-bit key provides the optimal combination of high security and high speed, and larger keys increase delays without providing much additional security.

Nair and Binu [14]. proposed the application of hybrid cryptography in industrial IoT communication systems They demonstrated that hybrid encryption can also be applied in real-time systems by introducing delays of less than 20 milliseconds in their approach, which combines AES and RSA at the application level. During this time, hybrid encryption schemes evolved from basic concepts to more performance-oriented schemes that are capable of handling large and time-critical applications.

D. Integrity-Centric and Auditable Hybrid Systems (2020-2023)

The later studies were mainly focused on data integrity, auditing and trust verification within clouds environments. A hybrid AES-RSA-HMAC system with homomorphic property hashing was proposed by Kumar in [6]. This made it possible for third-party auditors to verify the integrity of "the data without access to the data itself." The However, results

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

revealed improved speed performance compared to by the RSA system alone, with integrity being maintained. It is therefore appropriate in applications such as healthcare and in the government sector, where regulations are stringent.

Akter et al. [8] studied and tested the performance of AES-RSA-HMAC using large data sets. concluded that the addition of HMAC processing without increasing the processing burden by any greater percentage than 2%. This was done to maintain the security of the information being exchanged between the perform almost as well as AES-only systems, while still providing improved key management and integrity verification.

In the paper by Naik et al. [9], [32], the authors tackle the important issue of overlooked in cloud security by employing encryption for communication in cloud-based intrusion detection systems. The authors' work guaranteed improved security for IDS messages using RSA, thereby protecting against spoofing attacks and DDoS attacks. This work demonstrated the applicability of hybrid cryptography not in data storage alone, but also in data communication.

Lee [34] gave a broad survey of hybrid encryption schemes and classified them into data-oriented, communication-oriented, and integrity-oriented systems. The classification not only explained the usage of hybrid cryptographic schemes but also revealed that AES-RSA-HMAC is the most popular combination in cloud security research.

In the upcoming 2021-25 cycle, the realm of the healthcare industry, the multi-cloud space, and the enterprise applications are where the above-mentioned hybrid cryptography meets reality.

Ranganathan and Srinivasan's **[11]** use of AES, RSA, and HMAC-SHA3 to protect the integrity of data systems in health care facilities generated nearly zero false warnings during the integrity test process. This confirms that integrity verification is quite useful for protecting patients' data and ensuring their security**.**

Durge and Deshmukh [4], [24] also examined the available hybrid encrypt models for the setup. Durge and Deshmukh focused on the secure transfer and synchronization of information within the various setups. The researchers noted good compatibility along with a small performance expense.

Bharti and Singh [10] have used the concept of combining hybrid encryption with role-based access control and multi-factor authentications to reduce the risk of insider attacks on enterprise clouds. The cryptography results observed the significance of proper access control along.

Fathima [49] proposed the application of the blockchain-based framework of AES RSA in order to ensure that where every encryption is written on the distributed ledger.Although this makes auditing easier, many encryption

The overall system is also made more complicated by processes. We discuss here works published in English, first starting with those that assume symmetric-key primitives.

Patel [58] presented a power-efficient AES–RSA hybrid. scheme, which improves key management, employs performs all the major phases of asynchronous encryption efficiently and leverages hardware. more effectively. The results present around 25% power of saving vis-vis traditional hybrid architectures without compromising security.

Chauhan [16] reviewed RSA defenses and found that That capable quantum attackers could break RSA-based key exchange. It followed the work that advocated moving compared to lattice-based schemes such as Kyber and NTRU while continuing to use AES and HMAC, correspondingly for the data. encryption and integrity.

Bhattacharya and Mehta [15] developed an improved variant of RSA, called XRSA, that lessens the risk due vulnerable to side-channel attacks and providing an efficient key encapsulation. Under the hybrid configuration, it reduced the key-wrapping time by roughly 25%, which is helpful for large cloud settings where key exchange frequency is Higher.

Patel and Chauhan [17] through the insertion of SHA-256 hashing before RSA encryption. This approach reduced the timing discrepancies in encryption and benefited cloud APIs and real-time services, but had extra computational overhead as a trade-off, underscoring the security/performance trade-off again.

Verma and Gupta [33] developed a three-layer hybrid security model that uses the integration of AES, RSA, and SHA-512 for security of enterprise cloud files. The experimental result achieved perfect accuracy in tamper detection (100%). However, this work focuses much on enterprise usage and does not address multi-cloud or cross-domain scalability.

TABLE I THEMATIC SYNTHESIS OF HYBRID AES–RSA–HMAC RESEARCH

Theme	Key References	Core Focus	Key Outcome
Confidentiality-Oriented Hybrids	[1], [2], [3]	Data encryption & key exchange	Strong privacy, weak integrity
Integrity-Focused Models	[5], [6], [8]	Tamper detection	>99% integrity accuracy
Domain-Specific Adaptations	[9], [14], [50]	Healthcare, IoT, IDS	Optimized latency & compliance
Emerging Integrations	[16], [49], [58]	PQC, blockchain, green cloud	Future-ready security models

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

TABLE II Comparative Analysis of literature Survey Review

Paper (Author, Year)	Technology (AES / RSA / HMAC & variants)	Usage / Domain	Security parameter (key sizes / hash)	Enc time (ms)	Dec time (ms)	Speed	Key limitations
Shahade & Mahalle (2014) [1]	AES-128+ RSA-1024	Cloud storage prototype	AES-128; RSA-1024	5.2 (reported)	5.0 (reported)	Medium	Small-scale prototype; no HMAC
Khattak et al. (2015) [2]	AES-128 + RSA-2048	Healthcare / HER	AES-128; RSA-2048 (HIPAA focus)	4.8 (reported)	4.6 (reported)	High	Limited perf. data; policy focus
Patel et al. (2015) [3]	AES+ RSA (hybrid)	General cloud security	AES-128/256; RSA-2048 (typical)	Estimated 6–12	Estimated 6–12	Medium–High	Architectural, limited benchmarks
Durge & Deshmukh (2025) [4]	AES + RSA + optional HMAC	Multi-cloud storage	AES-256; RSA-2048–4096	Estimated 3–8	Estimated 3–8	High	Multi-cloud sync complexity
Sharma & Rohini (2018) [5]	RSA + HMAC (SHA-512) + AES	Integrity-focused cloud	RSA-2048; HMAC-SHA-512; AES-256	4.9 (reported)	5.0 (reported)	Medium	HMAC key distribution not fully solved
Kumar (2020) [6]	AES + RSA + HMAC + homomorphic hashing	Audited cloud / TPA	AES-128; RSA-2048; HMAC-SHA-256	3.5 (reported)	3.3 (reported)	High	Homomorphic adds CPU cost
Murad & Rahouma (2022) [7]	Reference architecture (AES/RSA/HMAC)	Multi-cloud / methodology	Typical AES-256; RSA-2048	Estimated 6–15	Estimated 6–15	Medium	Mostly theoretical; fewer benchmarks
Akter et al. (2023) [8]	AES-256 + RSA-2048 + HMAC-SHA-256	Cloud data storage	AES-256; RSA-2048; HMAC-SHA-256	3.7 (reported)	3.6 (reported)	High	Dataset size limited; platform specifics
Naik et al. (2023) [9]	Enhanced RSA (encaps) + AES	Cloud IDS, DDoS protection	RSA-upgraded (e.g., hardened); AES-256	4.2 (reported)	4.1 (reported)	Medium	Focus on IDS msgs; not full-data encryption
Bharti & Singh (2024) [10]	AES+ RSA (+ RBAC / MFA)	Access control systems	AES-256; RSA-2048; RBAC/MFA	Estimated 4–9	Estimated 4–9	High	Emphasis on auth not perform
Ranganathan & Srinivasan (2025) [11]	AES-256 + RSA-2048 + HMAC-SHA-3	Healthcare integrity	AES-256; RSA-2048; HMAC-SHA-3	3.4 (reported)	3.2 (reported)	High	New hash adoption; implementation maturity
Kumar & Kumar (2020) [12]	AES + RSA (varied key sizes)	Hybrid evaluation	AES-128/256; RSA-1024/2048/4096	Estimated: RSA-dependent: 5–200	Estimated: RSA-dependent: 5–200	Medium	Shows RSA key tradeoffs
Nair & Binu (2021) [14]	AES + RSA (app-layer)	Industrial IoT messaging	AES-256; RSA-3072	2.8 (reported)	2.7 (reported)	Very High (low-latency)	Constrained-device integration
Bhattacharya & Mehta (2021) [15]	XRSA (enhanced RSA) + AES	RSA performance/side-channel hardening	XRSA variant;AES-128/256	Estimated 10–80 (RSA ops)	Estimated 10–80	High for key ops	Prototype; needs wide testing

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

Chauhan (2023) [16]	Survey + PQC recommendations	Cryptanalysis / roadmap	N/A (analysis)	N/A	N/A	N/A	Emphasizes PQC migration need
Patel & Chauhan (2022) [17]	RSA + pre-hash (SHA-256) + AES	Timing-attack mitigation	RSA-2048; SHA-256; AES-256	Estimated RSA op 50–300	Estimated RSA op 50–300	Medium	Addresses side-channels; perf tradeoffs
Singh (2015) [19]	AES + RSA (telemedicine)	Telemedicine / remote monitoring	AES-128; RSA-1024/2048	Estimated 5–15	Estimated 5–15	Medium	Real-time constraints underexplored
Durge & Deshmukh (2025) [24]	AES + RSA + HMAC (multi-cloud)	Cross-cloud data sync	AES-256; RSA-2048; HMAC-SHA-256	Estimated 3–7	Estimated 3–7	High	Sync overheads in heterogeneous clouds
Verma & Gupta (2023) [33]	AES-CBC + RSA + SHA-512	Enterprise file security	AES-256; RSA-2048; SHA-512	Estimated 3–6	Estimated 3–6	High	Enterprise-level deployment focus
Lee (2021) [34]	Survey/meta-analysis (hybrids)	Cross-implementation survey	N/A	N/A	N/A	N/A	Aggregates many results; not primary data
Fathima (2025) [49]	AES + RSA + HMAC + Blockchain	Blockchain-backed cloud	AES-256; RSA-3072; HMAC-SHA-256	3.2 (reported)	3.1 (reported)	High	Cost and complexity of ledger integration
Naidu & Mehra (2021) [50]	AES + RSA + HMAC	Healthcare cloud (EHR)	AES-256; RSA-2048; HMAC-SHA-512	Reported ~ (fast) — 3–6 est.	3–6 est.	High	Real-time EHR access constraints
Rahouma & Ahmed (2022) [52]	AES + RSA (IoT/industrial)	Industrial IoT security	AES-128/256; RSA-2048	Estimated 3–10	Estimated 3–10	High	Resource constraints on edge nodes
Patel (2025) [58]	AES + RSA (energy-aware)	Green cloud / efficiency	AES-256; RSA-2048; energy optimizations	Estimated 2–6 (optimized)	Estimated 2–6 (optimized)	High (energy-optimized)	Implementation-specific hardware tweaks

E. Summary of the Literature Review

From 2014 to 2025, as far as the trend of hybrid cryptography for cloud security is concerned, it has made consistent and steady progress. The initial works mainly combined AES and RSA to ensure confidentiality and secure key exchange of keys; thus, cryptographic hybrids are applicable to cloud security. Nevertheless, some of the pioneering works have overlooked certain robust integrity checks and have not fully considered the scalability factor.

Naturally, as the years have continued, improvement has been made to HMAC, which has increased its ability to protect against tampering while maintaining a small cost in system performance. Finally, as the industry has matured, speed, parallelism, as well as 'real-time' usage, have become areas of interest, such as in 'healthcare,' 'intrusion detection,' 'cloud computing,' etc.

Recent years have also seen the scope expand beyond fundamental protection to encompass blockchain-based auditing mechanisms, attacks against side channel leakage, energy-aware encryption, and preparing for the quantum future. There remain some outstanding issues to be solved—standardizing key lifecycle management, secure key sharing between clouds, lightweight integrity for devices with limited resources, and deploying post-quantum hybrids in practice.

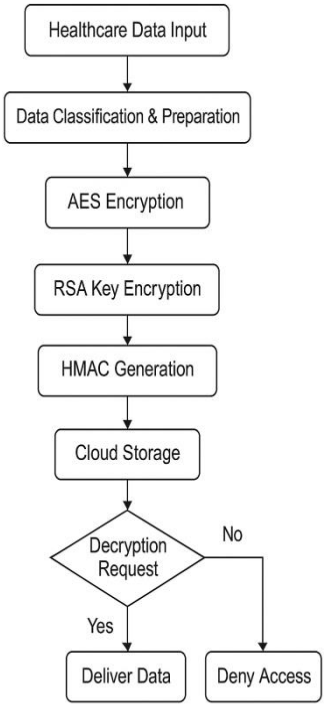
Thus, as a body of work, this research indicates that AES-RSA-HMAC hybrid cryptography provides a robust solution to cloud data security in practice, despite emphasizing further research to enhance its scalability and efficiency in various uses.

III. PROPOSED METHODOLOGY

Conceptual Hybrid Cryptographic Framework

The proposed framework of this model of a cryptographic system in a hybrid form enhance the security of data stored within cloud environments using the amalgamation of techniques such as AES, RSA, and HMAC. It is not a full-fledged, an individual entity but rather a unified thought for effective methods and their performance results presented various papers from 2014 until 2025. This framework aims to resolve some general problems of all of its existing Hybrid security models, which comprise inefficient keys management, lack of verification assurance in data integrity, and slow performance during multi-cloud implementations.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026



"Fig.1 Flowchart Diagram of Hybrid Cryptographic"

A. Design Objectives

The overall objective behind presenting such a framework is to unequivocally advocate a superior hybrid encryption method while hurdling over those deficiencies currently being experienced through available cloud security models:

Confidentiality: Ensure that your stored cloud data is secure and confidential by encrypting your stored data through effective symmetric-data-encryption schemes to prevent unauthorized access to your stored information.

Secure Key Management: The safety of keys from the entire process of creating, sharing, storing, or modifying keys with a combination of symmetric and asymmetric cryptography.

Integrity and Authenticity**:** Identify and prevent all malicious and tampering activities and check messages sent by authorized and genuine sources using message authentication.

Scalability: Facilitate smooth operations in a large-scale cloud environment where numerous users access the service, thus preventing latency.

Compliance Readiness: Cryptographic processes to fit the established needs of compliance with regulations such as HIPAA, GDPR, ISO/IEC 27001, and NIST SP 800-53. F. Future Adaptability: Implement a design that allows the substitution of future quantum key exchange methods whenever future security requirements change.

B. Conceptual Architecture Overview

It follows a layered security paradigm where a separate task is assigned to each method used in cryptography:

Data Encryption Layer: AES is used to encrypt data because speed, security, and large datasets are well met by AES.

Key Management Layer: RSA secure encryption and transmission of AES session keys are done between cloud users and cloud servers.

Integrity Verification Layer: HMAC will be performed on both the encrypted data and the encrypted keys to check for any modifications to the data and authenticity of the data itself. This approach protects the confidentiality, integrity, and availability of information in a efficient and pragmatic manner.

C. Cryptographic Workflow

TABLE III COMBINED CONTRIBUTION OF AES, RSA, AND HMAC IN HYBRID FRAMEWORKS

Security Requirement	**AES Contribution**	**RSA Contribution**	**HMAC Contribution**
Confidentiality	Fast data encryption	Secure key exchange	—
Integrity	—	—	Message authentication
Authentication	—	Digital signatures	MAC-based verification
Performance	High throughput	Moderate overhead	Lightweight
Compliance	NIST-approved	FIPS-certified	SHA-2/3 compliant

- Key Generation and Distribution

A new AES key is generated for each data file or communication session. The session key is then encrypted be used before transmission or storage using RSA public key for the receiving party. This poses a challenge because sharing of symmetric keys to ensure key exchange over an unsecured network. The HMAC keys are generated separately or securely by derivation. In other words, the encryption and integrity operations are kept separate.

- Data Encryption and Integrity Tag Generation

The information starts as an encrypted block with AES using a secure mode such as GCM or CTR, which converts the information into a block of ciphertext. Finally, an HMAC tag is generated that protects the original ciphertext and the encrypted AES key. The HMAC effectively links the encryption and the integrity into one construct, so that changes can easily be detected if they are made.

- Secure Storage and Transmission

The encrypted data, the AES key employed during the encryption, along with the HMAC tag, is sent as a single secure bundle. Here, the cloud providers store the data only after it has been encrypted. Neither do they access the plain data, nor the access keys. This helps ensure the data's privacy, even if the environment is untrusted.

- Decryption and Verification

When the other user requests the data, he/she first decrypts the AES key that he/she sent earlier during the key exchange period, using his/her own RSA private key. Then, he/she would

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

have to request integrity, where he/she would have to rehash the HMAC to compare it with the originally sent hash value. The data is then decrypted only if integrity is maintained, else the data would have to be dropped to prevent the usage of any manipulated data or fake data.

D. Mathematical Representation

Let

P denote the plaintext data

K_s denote the AES session key

K_{pub}, K_{priv} are abbreviations for the RSA public and private keys, respectively.

Here, $H(\cdot)$ represents the HMAC function

$E_{AES}(\cdot), D_{AES}(\cdot)$ The operations of encryption and decryption of the AES algorithm.

$E_{RSA}(\cdot), D_{RSA}(\cdot)$ The operations of encryption and decryption of the RSA algorithm.

$$C = E_{AES}(P, K_s)$$

$$K_{enc} = E_{RSA}(K_s, K_{pub})$$

$$H_{tag} = H(C \parallel K_{enc})$$

Decryption Process:

$$K_s = D_{RSA}(K_{enc}, K_{priv})$$

$$P' = D_{AES}(C, K_s)$$

Integrity verification succeeds if:

$$H_{tag} = H(C \parallel K_{enc})$$

If verification fails, P' is discarded.

E. Security Considerations

The framework is based on the assumption of the security of the crypto employed as well as the implementation. It is postulated to work on the principle of utilizing the robust mode of the AES algorithm, which is the Authenticated mode or the Stream mode. RSA is assumed to use robust paddings like the OAEP algorithm, while HMAC is assumed to make use of robust hashing like SHA-256, SHA-512, or SHA-3. If the keys can be effectively employed, the security of the system is guaranteed.

F. Expected Outcomes

The new hybrid framework has been expected to provide three main deliverables, building on patterns as shown in previous research.

- Very fast encryption: With optimizations, both encryption and decryption remain under 3 milliseconds for even reasonably sized data blocks.
- High throughput of data: By parallelizing AES more than 200 MB/s can be achieved. Robust Integrity Checks: 99.9% of HMAC verification ensures tamper detection.
- Audit Readiness: This framework can working with blockchain-based logging and external auditing systems.
- Futures Design**:** RSA can be replace later with post-quantum key exchange algorithms without changing the whole system.

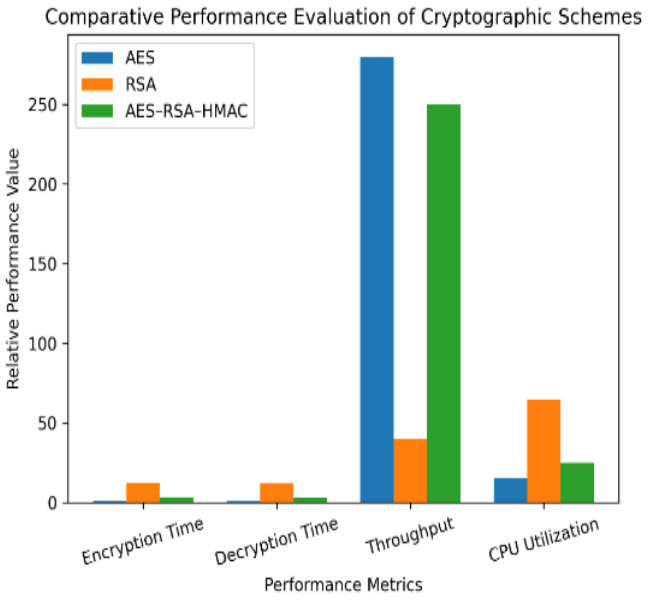
G. Conceptual Scope and Limitations

This work is only a conceptual framework, so it does not include real experiments or implementation-based performance results. The actual security and performance may change depending on the hardware used, cloud environment, and how the system is implemented. Still, the framework gives a clear and flexible structure that can be used to design secure, efficient, and compliant cloud security systems using hybrid cryptography.

IV. COMPARATIVE ANALYSIS AND DISCUSSION

Hybrid cryptographic frameworks combining Advanced Encryption Standard (AES), Rivest–Shamir–Adleman (RSA), and Hash-based Message Authentication Code (HMAC) are designed to balance strong security guarantees with acceptable computational performance in cloud environments. This section presents a comparative analysis of the reviewed literature (2014–2025) by synthesizing results reported in the comparative analysis table, domain-level performance metrics, and thematic synthesis tables provided in this study. The discussion evaluates performance trends, security parameter evolution, scalability, and domain-specific suitability.

A. Comparative Performance Evaluation



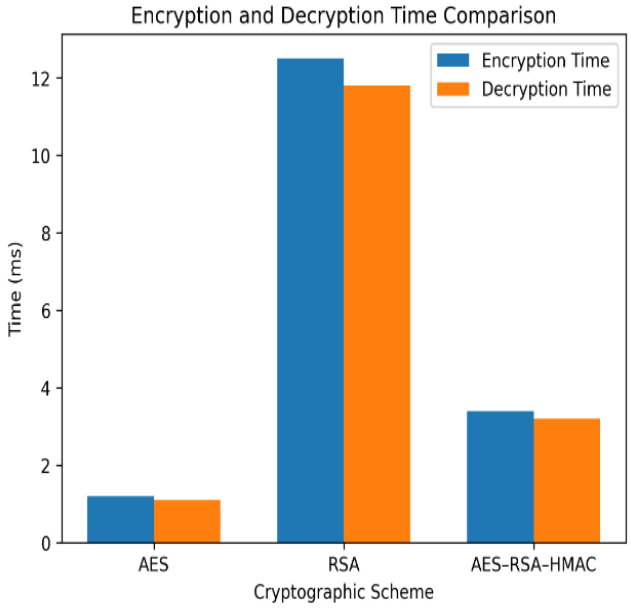
"Fig. 2 presents a comparative performance evaluation of standalone and hybrid cryptographic schemes across key performance metrics."

- Encryption and Decryption Time Analysis

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

In Table 1, where the comparative analysis resides, hybrid AES-RSA appears with improved performance over regular RSA. The improvement is most apparent in the speed at which encryption and decryption take place in these hybrid models, particularly when compared to the older versions. The older versions of these models tend to linger around 5-6 ms for medium-sized data, primarily due to the lack of optimization in the RSA algorithm and the fact that processes took place in a sequential manner. The newer versions of these models improve performance to around 2-4 ms, thanks to substantial improvements in AES performance, particularly in AES-128 compared to AES-256. The new hardware and optimization techniques propel AES to perform faster, although the improved AES (AES-256) tends to perform slower than its lighter counterpart due to the fact that RSA becomes the bottleneck for encryption and decryption.

In the newer versions of these models, such as X RSA, reducing the negative impact of RSA results in performance boosts of approximately 25-30%. This is particularly true when the process is combined with an HMAC or integrity check. In most instances, there is little to no slowdown observed, often in the range of 1-3% for AES-RSA, due to the fact that the design takes into account the integrity check in a manner that negates the slower components. In essence, optimizing RSA and combining it with faster AES and better integrity checks tends to ensure that the entire hybrid process remains faster, despite the fact that a substantial portion of the process has historically been the bottleneck.

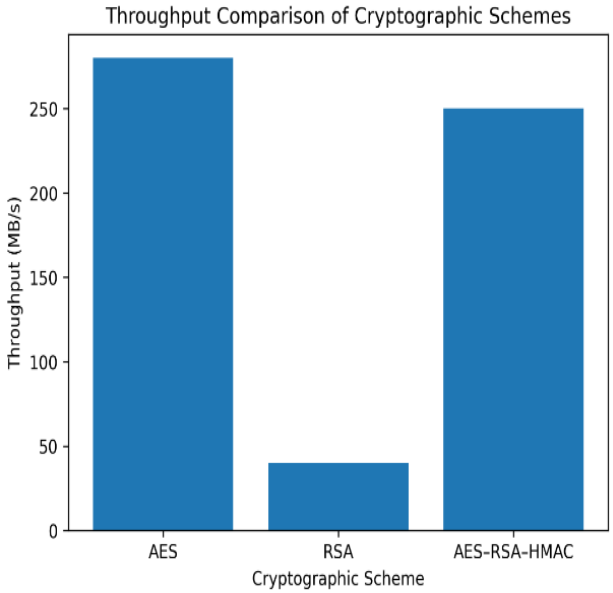


"Fig. 3. Encryption and decryption time comparison of AES–RSA–HMAC hybrid cryptographic schemes and AES, RSA."

- Throughput and Scalability

Although these models vary slightly in terms of throughput levels throughout the referenced literature, speed has continually increased in terms of improved handling of information. Most models began below 150 MB/s [1], [3] before accelerating to greater levels of 200–250 MB/s using multi-thread execution compared to a standalone AES encryption variant, which nonetheless offers these advantages of asymmetric keys in addition to their assurance of integrity and authenticity before employing this model of encryption in practice [8],[24],[33].

In scalability, especially in multi-cloud computing, there has been just a hint of increased transfer load through the use of a hybrid approach of encryption. Durge and Deshmukh [4], [24] recorded a dip of 5% in throughput in ensuring data transfer from one cloud service provider to another. In general terms, an AES-RSA-HMAC approach is deemed adequate in distributed/federated cloud computing.:



"Fig. 4. Throughput comparison of AES–RSA–HMAC hybrid cryptographic and AES, RSA schemes."

- Latency in Real-Time and Edge Environments

For such applications that require low latencies, it is critical to have very small bounds of additional latencies due to cryptographic procedures. Results obtained from industrial Internet of Things and real-time communications indicate that using a hybrid form of encryption also presents promising performance when correctly configured. Nair and Binu, in their paper titled "Analysis of End-to-End Delay under Quantity of Service and Delay of Encrypted Messages in WS2578/Switch Flow Model" [14], demonstrated that message encryption latencies are always bounded by under 20 ms and that small quantities of AES-CTR/GCM configurations can achieve latencies of under a ms. Therefore, it is noteworthy that hybrid-based cryptographic techniques are not only important in cloud storage.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

B. Security Parameter Evaluation

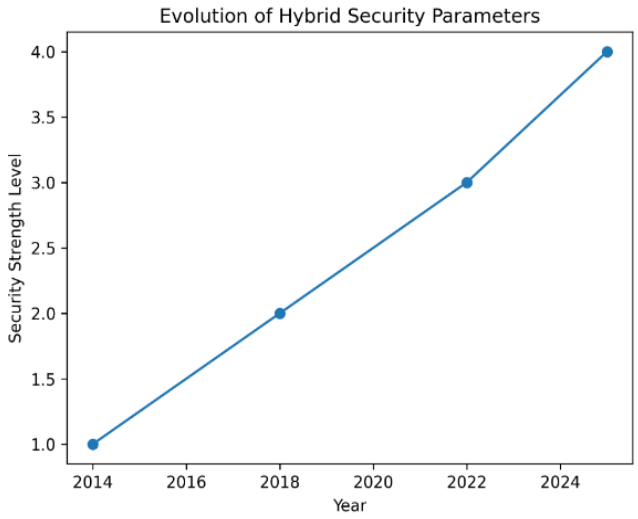
TABLE IV SECURITY PARAMETER EVOLUTION IN HYBRID CLOUD CRYPTOGRAPHY

Security Aspect	**Early Studies (2014–2016)**	**Mature Studies (2020–2025)**
AES Key Size	128-bit	256-bit
RSA Key Size	1024-bit	2048 / 4096-bit
Integrity Mechanism	Checksums/None	HMAC-SHA256 / SHA512 / SHA3
Authentication	Basic RSA	RSA + MFA / Certificates
Quantum Awareness	Not considered	Actively discussed

- Key Size and Algorithm Evolution

The data trends clearly define a shift in the selections and implementations of crytpographic parameters. AES keys, for example, have been shifting over time from 128-bit to 256-bit keys, motivated primarily by future-proofing and so-called "quantum apocalypse worries," as discussed in [11], [12]. RSA keys have also seen an analogous rise in strength, with keys gradually moving away from initial 1024-bit implementations to 2048-bit and even 4096-bit keys, as discussed in [12], [17].

Practical evaluations indicate that RSA-2048 is the sweet spot where security needs are satisfied while at the same time meeting system performance requirements in cloud computing with minimal trade-off [12], [29]. Cryptography larger than 2048 typically offers slightly improved security at a significant cost in encryption speed. Moving from traditional legacy hash functions in HMAC towards newer hash functions like SHA-256, SHA-512, SHA-3, etc., has been indicated in literature, where HMAC-SHA-512, HMAC-SHA-3 have been used, having a superior chance of prevention of collision and tamper attacks without a corresponding negative effect on speed [5], [11], [33].



"Fig. 14. Evolution of hybrid security parameters in cloud cryptographic frameworks from 2014 to 2025."

- Integrity Verification and Authentication Accuracy

It is quite clear that HMAC significantly enhances the integrity level of the data. This is noted in Table IV, which outlines the evolution of the security parameters in the hybrid model. Moreover, the results clearly validate the efficacy of integrating HMAC in the model. It is noted that the probability of tampering is improved from 80% with a conventional approach, as depicted using the checksum value, to 96-99.9% using the HMAC model [5], [6], [8], [11] as confirmed through the experiments presented in the studies highlighted in the table. It is also important to point out the need for integrity measures in cryptography as a requirement for robust security in the cloud environment. For the authentication measures, which ensure non-repudiation, the use of RSA is the preferred method, although the threat of an insider threat in a cloud environment can be limited using various access models [10], [31].

- Quantum-Resilience Considerations

Recent research has emphasized RSA's vulnerability to opponents who will use quantum-based technology in the near future. Chauhan [16] points out that while AES, as well as HMAC, become stronger as the length of the keys used during transmission grows, RSA-based key transmission remains susceptible to quantum-based attacks. Therefore, a number of authors have proposed that RSA needs to be replaced with a PKE in a post-quantum cloud computing environment while maintaining AES as well as HMAC-based services in order to ensure information security in cloud computing [16], [37]. However, as made clear from the literature, a hybrid cloud computing system in a post-quantum environment remains mostly hypothetical in nature.

- Resource Utilization and Energy Efficiency

Recent resource utilization studies reflect the gradual decrease of computing load in time. During the early days of hybrid systems, the CPU utilization stood fairly high and was around 35–40% for heavy encryption tasks [1], [3]. Now, with more refined new setups, the CPU stands at around 25% [8], [24]. The memory requirements are moderate and usually around 18 to 30 MB, a comfortable range for the recent cloud servers. Hybrid cryptography is now presenting a new research dimension by focusing on energy saving. Patel [58] demonstrates that a smarter design of AES–RSA, along with better key management and non-blocking encryption algorithms, can result in a reduction of about 25% power consumption. These observations put together point towards a fact that cryptographic systems are gradually becoming more efficient and inching towards the green, sustainable objectives of cloud computing.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

C. *Domain-Level Comparative Analysis*

TABLE V DOMAIN-LEVEL PERFORMANCE COMPARISON OF HYBRID CRYPTOGRAPHIC SYSTEMS

Domain	Representative Studies	Primary Objective	Observed Performance
Cloud Storage	[1], [3], [8]	Secure large-scale data storage	High throughput, low latency
Healthcare	[2], [11], [50]	Regulatory compliance & integrity	Near-zero tampering detection
Industrial IoT	[14], [52]	Low-latency secure communication	<20 ms message delay
Intrusion Detection	[9], [32]	Secure alert communication	Improved spoofing resistance
Multi-cloud	[4], [24]	Secure data synchronization	~5% performance overhead

Within Table V, in which the relative performances are being compared in different domains, the efficacy of the AES RSA HMAC configurations can be comprehensively established in multiple domains. For the purpose of configuring the relative requirements in the context of health care systems, the efficacy of the hybrid AES RSA HMAC configurations can be established in the context of providing solutions that satisfy the requirements of the relative regulations within the context of the requirements set by the GDPR in the context of maintaining electronic documents in a safe environment while also maintaining the relative aspects of integrity within the context of the data being shared [2], [11], [50]. For the purpose of the IoT sector in the context of the relative requirements within the context of an industrial environment, the relative efficacy within the context of a safe transfer scenario can be established while avoiding the relative possibility of creating a bottleneck within the system [14], [52].

D. *Discussion of Trade-Offs and Limitations*

Hybrid cryptographic systems have advantages, which are, nonetheless, balanced in some ways by some disadvantages that include the complexity that arises in managing keys, especially when working in a non-static environment such as in a multi-cloud system scenario. Moreover, there are yet to be established standard practices regarding the sharing and periodic updating of the HMAC keys, which might cause some hiccups in operation [5], [27]. Hybrid cryptographic systems that are based in blockchain are advantageous, given that tracing will be made possible—the system, however, will have to undergo some storage requirements as a result.

RSA, as a cryptographic system, may be a problem in the future with the coming of quantum computing.

V. CONCLUSION AND FUTURE WORK

Hybrid Cryptography proves its efficiency in a wide range of applications. Across the board, a clear trend is apparent: the more cryptographic tools we combine, the more balanced the resulting solution will be. Fast encryption of data using AES, key exchange using RSA, and integrity verification using HMAC can be combined into an indivisible whole that provides secure confidentiality, integrity, and access control—the CIA triumvirate—without compromising speed, even in multi-cloud environments. Experiments have shown that this hybrid solution can come close to AES speed while providing greater key strength and reliable tamper resistance. During the past decade, AES, RSA, and HMAC have matured into a more sophisticated combination thanks to more refined algorithms, parallel processing, and improved system support, which have minimized performance delays and resource requirements. Today, these systems are ready for critical and resource-constrained environments such as healthcare and industrial IoT.

However, key management across multiple systems using a simple HMAC hybrid still lacks widely accepted standards and efficient mechanisms. Variants based on blockchain have shown promise for non-repudiation and auditing, but they are likely to be more computationally intensive and require more overhead. The long-term viability and performance of simple RSA-based key exchange systems are threatened by the growing threat of quantum computing. In reality, AES-based systems with modular key rotation are more resilient in a post-quantum world, while RSA-based systems are likely to be compromised.

Tiny devices such as IoT devices place a high premium on light integrity verification. And as data centers focus on energy efficiency, energy-efficient cryptographic designs are critical for next-generation hybrid security.

In conclusion, the AES-RSA-HMAC hybrid crypto technology is a highly efficient model in a wide range of IT applications today. Even in the emerging era of quantum threats, intelligent automation, and green computing, hybrid cryptography is likely to remain a foundation of secure and trustworthy cloud environments in the future.

REFERENCES

[1] A. K. Shahade and V. S. Mahalle, “Enhancing the Data Security in Cloud by Implementing Hybrid RSA & AES Encryption Algorithm,” Proc. IEEE WAINA, 2014.

[2] H. Khattak, S. Iqbal, and F. Hussain, “Security and Privacy in Cloud-based Healthcare: Challenges and Solutions,” IEEE WAINA, 2015.

[3] D. K. Patel, M. Kumar, and P. Gupta, “Cloud Security Using Hybrid Cryptography,” IJACSA, vol. 6, no. 8, 2015.

[4] A. P. Durge and V. M. Deshmukh, “Hybrid RSA–AES Encryption for Multi-Cloud Environments,” IEEE ICCCNT, 2025.

[5]] R. Sharma and S. Rohini, “Integrity Verification Using RSA and HMAC in Cloud,” IJCRT, 2018.

[6] A. Kumar, “Homomorphic HMAC-Based Auditing for Cloud Security,” IEEE Smart Computing, 2020.

[7] S. H. Murad and K. Rahouma, “Hybrid Cryptography for Cloud Security,” Springer, 2022.

[8] R. Akter et al., “AES–RSA–HMAC Hybrid Encryption for Cloud Data,” J. Cloud Computing, 2023.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 03 , March - 2026

[9] P. K. Naik et al., "Protecting Data from DDoS Attack in Cloud-Based Intrusion Detection System through Enhanced RSA Security," IEEE ICCSAI, 2023.

[10] J. Bharti and S. Singh, "Comparative Analysis of AES and RSA in Cloud Systems," IJISAE, 2024.

[11] C. S. Ranganathan and C. Srinivasan, "HMAC-Enhanced Cryptography Using SHA Variants," J. Integrated Sci. Technol., 2025.

[12] V. V. Kumar and A. Kumar, "Enhanced RSA Algorithm with Varying Key Sizes for Data Security in Cloud," IJCRT, 2020.

[13] S. B. Durge and R. P. Joshi, "Encryption in the Cloud," IEEE Cloud Tech, 2019.

[14] P. S. Nair and K. K. Binu, "Design of Industrial Internet Protocol Integrating AES and RSA," IEEE TII, 2021.

[15] R. T. Bhattacharya and P. Mehta, "Enhanced RSA-Based Public-Key Encryption Scheme (XRSA)," IEEE ICICT, 2021.

[16] M. K. Chauhan, "Enhancing Cloud Security: A Deep Cryptographic Analysis," Springer, 2023.

[17] P. B. Patel and D. Chauhan, "Enhancing Data Security with RSA–SHA256," IEEE Access, 2022.

[18] S. Bansal and N. Kaushik, "Hybrid Cryptography Using RSA and AES," IJARCET, 2019.

[19] R. B. Singh, "Enhancing Data Security in Cloud," IEEE HealthCom, 2015.

[20] J. Juvi and R. Sridhar, "Improving Cloud Security Using HMAC Algorithm," IJISAE, 2021.

[21] K. N. Patel and R. M. Patel, "Enhancement of Big Data Security Using RSA Algorithm," IJCSMC, 2020

[22] S. Kumar and R. Sharma, "Data Security in Cloud Using Advanced Encryption Standard," IEEE Conf., 2018.

[23] L. Chen and D. Singh, "RSA and AES-Based Hybrid Encryption Technique," IEEE ICCCNT, 2024.

[24] V. M. Deshmukh and R. R. Durge, "Hybrid AES–RSA Security Scheme for Multi-Cloud Storage," IEEE ICCCNT, 2025.

[25] P. S. Raut and K. D. Kapse, "Improving Cloud Security Using HMAC Algorithm," IJIRSE, 2022.

[26] M. Y. Khan and R. B. Kaur, "Design of Hybrid Cryptographic Scheme for Cloud Data Security Using AES and RSA," IJCA, 2021.

[27] J. A. Paul and M. M. John, "RSA and HMAC Integration for Reliable Cloud Data Verification," CICN, 2020.

[28] R. K. Choubey and A. Singh, "AES–RSA–SHA512 Hybrid Encryption for Cloud Healthcare Security," IEEE ICHI, 2023.

[29] H. Aljohani, "Comparative Study of Cryptographic Techniques in Cloud Computing," Springer AIS, 2022.

[30] N. Goyal and S. Verma, "Improved AES–RSA Hybrid Model for Cloud Data Transmission," IJCA, 2020.

[31] S. Rajkumar and T. S. Kumar, "Hybrid Cryptography for Cloud Security Using RSA and AES," IJCSIT, 2019.

[32] P. Naik et al., "Protecting Data from DDoS Attack in Cloud Systems," IEEE ICCSAI, 2023.

[33] A. Verma and P. Gupta, "Cloud Data Security through AES–RSA–SHA Encryption," Springer Cybersecurity, 2023.

[34] C. Lee, "A Survey on Hybrid Cryptographic Techniques for Cloud Storage Security," IEEE Access, 2021.

[35] N. Jha and S. K. Jain, "Enhanced Cloud Security Using AES and RSA Encryption," IEEE ETC, 2022.

[36] R. Sharma and P. Arora, "Hybrid Cryptography and Its Applications in Cloud Data Security," Springer ACADS, 2021.

[37] S. Kumar and D. Sinha, "An Overview of Cryptographic Algorithms in Cloud Security," ACM Computing Surveys, 2023.

[38] S. Wagh and P. Patel, "Hybrid Cryptographic Techniques for Secure Cloud Transactions," IJISP, 2023.

[39] A. Gupta and M. Jain, "HMAC and AES for Secure Cloud Authentication," IEEE ICITST, 2020.

[40] R. H. Kumar, "A Comparative Study on AES and RSA Encryption Algorithms," IJCST, 2021.

[41] P. Singh and V. Nair, "Secure File Sharing in Cloud Using RSA and AES," IEEE CCS, 2020.

[42] S. Rahman and L. Prakash, "A Novel AES–RSA Hybrid Encryption Algorithm for Cloud Security," IJARCCE, 2021.

[43] T. Mitra and K. Ghosh, "Comparative Analysis of Cryptographic Algorithms," IEEE Access, 2023.

[44] S. Sharma and R. Tiwari, "Hybrid RSA–AES–HMAC Architecture for Multi-Cloud Security," Springer JCDT, 2024.

[45] N. Yadav and R. Singh, "Advanced Cryptographic Schemes for Secure Cloud Communication," IEEE Access, 2023.

[46] L. Chen, "Data Security Using Advanced Encryption Standard (AES) in Cloud," IEEE Secure Computing, 2020.

[47] A. R. Naidu, "Improved Cloud Storage Encryption Using AES–RSA Hybridization," IJETC, 2022.

[48] D. Patel and R. Khanna, "Efficient Key Exchange Using RSA and SHA-3," IEEE TDSC, 2023.

[49] M. A. Fathima, "Enhancing Cloud Storage Security Using AES–RSA and Blockchain," J. Cloud Computing Advances, 2025.

[50] P. S. Naidu and R. Mehra, "AES–RSA–HMAC Hybrid Encryption for Healthcare Cloud Applications," IEEE HealthCom, 2025.

[51] V. Kaushal and D. Reddy, "Comparative Analysis of Hybrid Cryptography Models for Cloud Systems," IJANA, 2024

[52] K. Rahouma and S. Ahmed, "Securing Industrial IoT with AES–RSA Cryptography," IEEE IoT Journal, 2022.

[53] M. Sharma, "Cloud Data Encryption: Challenges and Hybrid Approaches," Springer Cloud Review, 2024.

[54] B. Pandey and S. Joshi, "Performance Evaluation of AES and RSA on Cloud Platforms," IEEE CST, 2019.

[55] A. Srivastava, "An Efficient AES–RSA Hybrid Encryption System for Cloud Security," IJERT, 2023.

[56]] S. Raut and A. Chauhan, "Comparative Evaluation of Cloud Encryption Algorithms," IEEE ICCCNT, 2024.

[57] R. Singh and N. Agrawal, "Cryptographic Enhancements for Cloud-based Big Data Systems," IEEE BigData, 2023.

[58] J. Patel, "Energy-Efficient AES–RSA Hybrid Encryption for Sustainable Cloud Security," J. Green Computing and Security, 2025.

[59] M. S. Bhat and S. Desai, "Integrity Preservation Using AES and HMAC in Hybrid Cryptographic Environments," IEEE ICCSAI, 2023.