

A SYSTEMATIC REVIEW OF HYBRID CRYPTOGRAPHIC TECHNIQUES FOR ENHANCING SECURITY IN CLOUD DATA STORAGE

***Dr. Atuluku Amichi Ruth¹, Dr. Francis. B. Osang² & Enoch Jacob Dodo³**

^{1,2,3}Department of Information Systems and Technology, National Open University of Nigeria, Abuja, Federal Capital Territory, Nigeria

Corresponding Author: amichiruth@yahoo.com

ARTICLE INFO

Article No.: 0324

Accepted Date: 22/04/2026

Published Date: 07/05/2026

Type: Research

ABSTRACT

Cloud computing has revolutionised modern organisational operations by offering agility and cost-effectiveness. However, declining customer confidence due to frequent data breaches remains a significant barrier to adoption. Reports indicate that 99% of compromised data in recent years was unencrypted, underscoring the inadequacy of traditional security measures. This study explores the transition from single-method cryptographic approaches to hybrid models that combine symmetric and asymmetric algorithms. Through a systematic review of 51 contemporary studies, this paper identifies critical flaws in existing hybrid frameworks, including high computational complexity and limited support for diverse file formats like audio and video. The findings suggest that while hybrid models improve data confidentiality, significant gaps remain in multi-factor authentication and processing efficiency. This research provides a foundation for developing a high-performance hybrid cryptographic framework designed to restore executive and consumer trust in cloud storage environments.

Keywords: hybrid cryptography, cloud data security, performance metrics multi-format encryption, data integrity

Introduction

The ICT landscape is evolving rapidly, forcing organisations to adapt their business models to survive in a digitally driven climate. Cloud computing has emerged as a critical technology shift, fundamentally altering how resources like storage and processing power are provisioned (Dlamini et al., 2017). Despite these advantages (EZComputer Solutions, 2018), security and privacy concerns remain the primary obstacles for organisations considering the migration of sensitive data (Diaz et al., 2016; Ismail et al., 2016). Recent data breaches have eroded customer confidence, with evidence showing that only 1% of the 2.6 billion pieces of information compromised in 2017 were protected by encryption (Gemalto, 2018; Pandey, 2018).

Despite the growing body of research on cloud security and the increasing adoption of hybrid cryptographic approaches, there remains a lack of comprehensive, systematic synthesis of existing models, particularly in terms of their performance trade-offs, implementation architectures, and real-world applicability in cloud environments. Prior studies have largely focused on proposing individual hybrid schemes or evaluating specific algorithms in isolation, without providing a consolidated analysis that compares their efficiency, scalability, and resilience against emerging threat vectors. Furthermore, there is limited evidence on how these hybrid models perform across diverse data types and deployment scenarios, creating a gap in actionable insights for organisations seeking to adopt robust, integrated encryption frameworks.

As traditional single-method algorithms become insufficient against modern threats, scholars have proposed hybrid cryptography to combine the strengths of various algorithms (Mangalampalli et al., 2023). However, the practical application of these models faces persistent challenges in efficiency and resistance to advanced cyber-attacks (Prabhu et al., 2020).

Objectives of the Study

In alignment with the goal of strengthening cloud security posture, the specific objectives of this research are:

- To conduct a comprehensive literature survey on the security and privacy concerns associated with cloud computing.
- To analyse existing hybrid security algorithms to identify key security flaws and privacy violations.
- To evaluate the performance limitations of current models, focusing on processing time and computational complexity.
- To identify more resilient cryptographic options that can guide the design of future high-performance hybrid frameworks for sensitive data protection.

Methodology

A systematic literature review was used to find and analyse relevant studies on hybrid encryption models for cloud security. The process followed a structured protocol to ensure all gathered information was consistent and reliable.

1 Search Strategy

Searches were carried out across several academic databases known for technical and computer science research:

- **Web of Science and ACM Digital Library:** Used to capture a wide range of academic and grey literature.
- **ScienceDirect:** For high-impact peer-reviewed journals.
- **IEEE Xplore:** To access technical papers on cryptographic standards.
- **Scopus:** To ensure a comprehensive reach across global research.

To get the best results, specific keywords related to cloud security and encryption were combined using Boolean operators (AND, OR). The main search string used was:

- "Hybrid encryption" AND ("cloud security" OR "cloud storage") AND ("AES" OR "RSA" OR "ECC") AND ("confidentiality" OR "integrity" OR "performance").

The search was limited to documents published within the years 2018–2025 to ensure the findings reflect modern cloud threats and the latest cryptographic advancements. Only studies written in English were included.

2 Inclusion Criteria

To make sure the review only included high-quality and relevant work, the following criteria were used:

- **Focus:** Studies must specifically discuss the combination of two or more encryption algorithms (hybrid models) for cloud environments.
- **Publication Type:** Only peer-reviewed journal articles, conference papers, and official technical reports were selected.
- **Exclusion:** General papers on cloud computing that did not offer a specific security model or algorithm were excluded.

3 Data Extraction

Once the relevant studies were chosen, key details were pulled from each paper and organised in a spreadsheet. The information extracted included:

- Author(s) and year of publication.
- Specific cryptographic techniques used (e.g., AES, RSA, Blowfish).
- The main security issues being addressed.
- The strengths and weaknesses (gaps) of each proposed model.

4 Quality Assessment

Quality Assessment Procedure

To ensure the reliability and relevance of the selected studies, a structured quality assessment was conducted using a predefined scoring rubric. Each study was evaluated against key criteria focusing on methodological rigour, clarity, and practical applicability. The assessment criteria are outlined below:

QA1: Clarity of Research Objectives – Are the aims and scope of the study clearly defined?

QA2: Methodological Transparency – Is the research design, including cryptographic implementation and evaluation procedures, adequately described?

QA3: Performance Evaluation – Does the study provide measurable performance metrics (e.g., encryption/decryption time, throughput, resource utilisation)?

QA4: Real-World Applicability – Are experiments conducted using realistic datasets, cloud environments, or simulation scenarios that reflect practical use cases?

QA5: Comparative Analysis – Does the study compare the proposed approach with existing cryptographic methods or benchmarks?

Each criterion was scored using a three-point scale:

2 = Fully satisfied

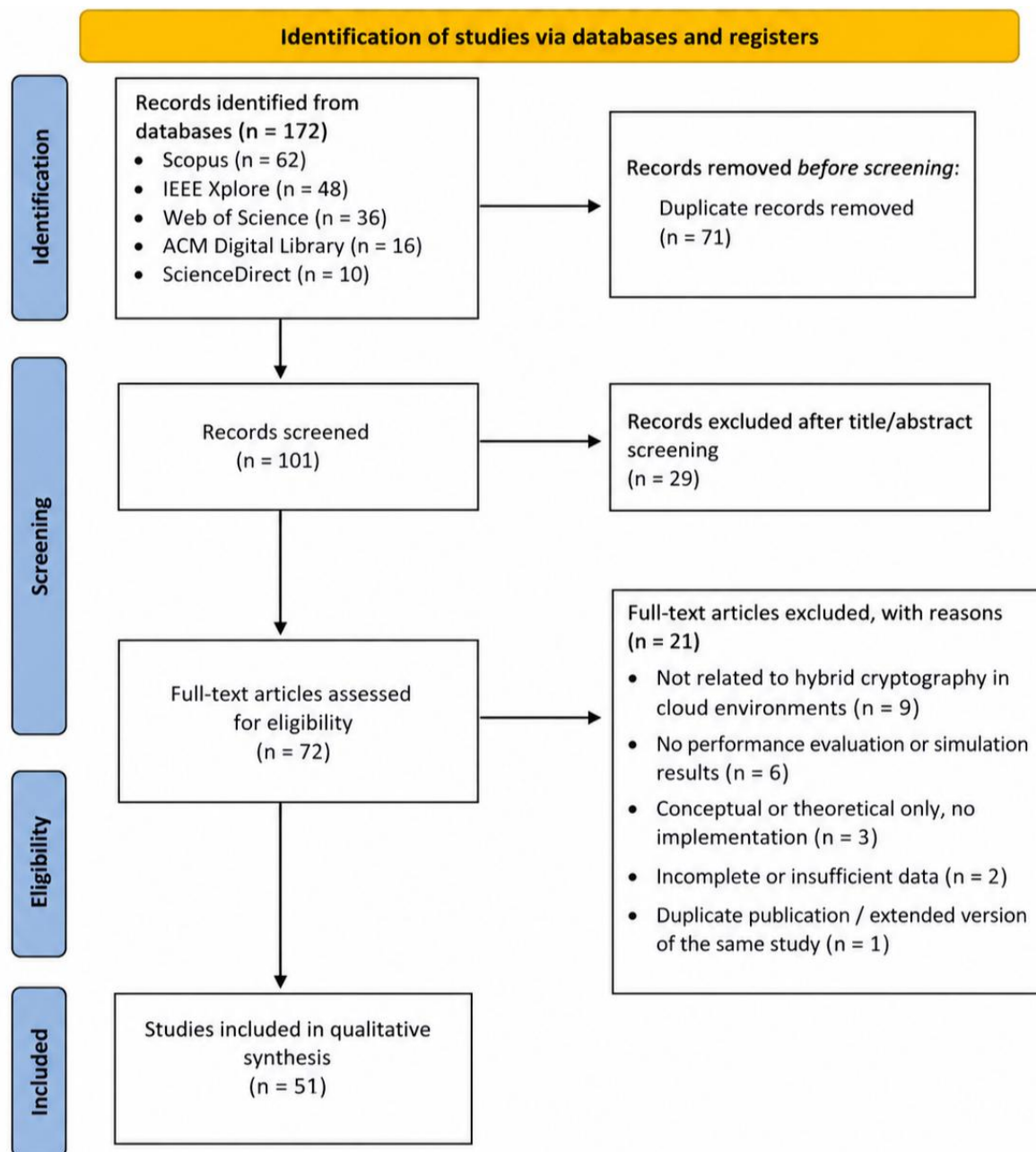
1 = Partially satisfied

0 = Not satisfied

The maximum achievable score for each study was 10. Studies scoring below a threshold of 5 were excluded to maintain the overall quality and credibility of the review. This systematic scoring approach enhances objectivity, reduces selection bias, and ensures that only studies with sufficient methodological rigour and practical relevance are included in the analysis.

Table 1: Summary of Studies by Year

Year	Number of Publications
2018	12
2019	7
2020	6
2021	7
2022	9
2023	5
2024	4
2025	1
Total	51 Entries (Note: Some authors appeared in multiple years/studies)


Fig 1. PRISMA Flow Diagram of Study Selection

Review of Related Works on Hybrid Encryption Models

1 Multi-Layer Symmetric and Asymmetric Combinations

The dominant theme across the 51 reviewed studies is the integration of symmetric encryption (AES, Blowfish, DES, RC4, RC6) with asymmetric techniques (RSA, ECC, ElGamal, Paillier) to achieve both efficiency and secure key management.

- AES–RSA and AES–ECC Integration:

A large proportion of studies adopt AES–RSA or AES–ECC combinations to balance speed and security. Studies such as Sa'idu (2022), Manoj et al. (2019), Mohammed and David (2022), Nair (2022), Kota (2022), Kanatt et al. (2020), Sam et al. (2019), Zinah et al. (2018), and Zhang et al. (2019) demonstrate that AES ensures fast encryption while RSA/ECC provides secure key distribution.

Further refinements were proposed by Abhishek and Asha (2021), Basapur (2021), El-Attar et al. (2021), and Souza and Ruby (2021), incorporating dynamic encryption, neural networks, and OTP-based authentication.

However, Vanaja et al. (2019) and Sam et al. (2019) highlight persistent challenges such as computational overhead and scalability limitations, while Kota (2022) and Abhishek and Asha (2021) identify vulnerabilities to replay and tampering attacks.

- Blowfish and Alternative Symmetric Hybrids:

Several studies explored Blowfish and other symmetric algorithms as alternatives to AES. Chinnasamy and Deepalakshmi (2018), Ponnuru and Sunitha (2018), Bijeta et al. (2020), Sajay et al. (2019) demonstrate that Blowfish offers faster encryption and effective mitigation of man-in-the-middle attacks when combined with RSA or Paillier. However, Chinnasamy et al. (2021) caution that reliance on older algorithms such as Blowfish may weaken long-term security. Similarly, Uttam and Jay (2020) note that DES and RC-based algorithms are outdated and introduce security vulnerabilities.

- ECC and Optimised Key Management:

To reduce computational overhead, several studies integrate ECC into hybrid models. Silki and Abhilasha (2018), Pradeep et al. (2019), Nair (2022), Lai and Heng (2022), Ranganatha and Sujatha (2023), and Sabitha et al. (2023) demonstrate that ECC achieves strong confidentiality with shorter key lengths and improved efficiency.

However, implementation complexity and scalability challenges remain key limitations (Sabitha et al., 2023; Lai & Heng, 2022).

2 Data Slicing and Concurrent Encryption

A major trend in hybrid cryptography is the use of data fragmentation and parallel encryption techniques to enhance security.

- Multi-Algorithm Data Slicing:

Mehul et al. (2018), Batra et al. (2018), Maria et al. (2022), and Uttam and Jay (2020) proposed models where data is divided into segments and encrypted using multiple algorithms such as AES, DES, and RC4/RC6. These approaches improve resistance to brute-force attacks and unauthorised access.

- Parallel and Multi-Cloud Security Frameworks:

Viswanath and Krishna (2020, 2021), and Shukla et al. (2024) extended this approach by introducing multithreading, block-level encryption, and multi-cloud storage architectures. These models enhance resistance to insider attacks, tampering, and Denial-of-Service (DoS) attacks.

Despite these advantages, most studies report increased computational overhead, higher resource consumption, and complex data reconstruction processes.

3 Integration of Steganography and Identity Management

Beyond encryption, several studies integrate steganography and authentication mechanisms to strengthen security.

- Steganographic Key Protection:

Mehul et al. (2018), Poduval et al. (2019), Bokhari et al. (2023), and Chatterjee et al. (2023) utilised Least Significant Bit (LSB) steganography to conceal encryption keys within media files. This approach enhances confidentiality by hiding the existence of keys and sensitive data.

- Authentication and Verification Layers:

Ugba et al. (2018) introduced a three-way security model using SMS verification, while Singh and Garg (2018) and Gurjeet and Mohita (2018) implemented OTP-based authentication mechanisms.

More advanced integrity and authentication frameworks were proposed by William et al. (2022), Varma et al. (2022), Souza and Ruby (2021), Pravin and Rahul (2021), and Adee and Mouratidis (2022), incorporating SHA-256, SHA-2, and identity-based encryption.

However, the use of MD5 in some models remains a critical weakness due to collision vulnerabilities, and multi-layer authentication increases system complexity and processing overhead.

4 Emerging Frameworks: Blockchain, AI, and Advanced Cryptographic Models

Recent studies extend hybrid encryption into **advanced and future-oriented architectures**.

- Blockchain and Decentralised Storage:

Wang et al. (2018) proposed a decentralised framework combining blockchain, attribute-based encryption (ABE), and IPFS for secure cloud storage, enabling fine-grained access control.

- Homomorphic and Advanced Encryption Models:

Kumar and Badal (2019), Zaineldeen et al. (2020), and Dutta et al. (2023) explored homomorphic encryption and NTRU-based systems for secure computation and data privacy in cloud environments.

- AI-Driven and Optimised Cryptography:

Ranganatha and Sujatha (2023), Sabitha et al. (2023), and Almalawi et al. (2024) introduced optimisation techniques such as lightweight ECC, Diffie–Hellman key exchange, and Ant Lion Optimisation (ALO) to enhance efficiency and intrusion detection accuracy.

- Next-Generation Hybrid Models and Performance Trade-offs:

Recent works by Rath et al. (2024), Anjana (2024), and Riyaz Fathima and Saravanan (2025) propose multi-layer hybrid models (e.g., AES–ChaCha20, RSA–ChaCha20–Poly1305) to improve resistance to cryptanalytic attacks. However, these models consistently suffer from high computational overhead, limited real-world validation, and lack of post-quantum readiness.

5 Summary of Reviewed Related Works on Hybrid Encryption Models

Table 2 provides a structured overview of security models developed for cloud environments. While many researchers have addressed cloud computing vulnerabilities, the following table presents a thematic meta-analysis of the most recent and relevant studies.

Table 2: Thematic Overview of Hybrid Security Algorithms for the Cloud

Theme	Key Authors	Primary Techniques	Strengths	Observations (Weaknesses/Issues)
Advanced Symmetric–Asymmetric Hybrids	Sa’idu (2022); Manoj et al. (2019); Mohammed & David (2022); Nair (2022); Kota (2022);	AES, RSA, ECC, ElGamal	High confidentiality, strong key management, efficient encryption	High computational overhead; replay/tampering vulnerabilities; scalability issues

	Kanatt et al. (2020); Sam et al. (2019); Zinah et al. (2018); Zhang et al. (2019); Abhishek & Asha (2021); Basapur (2021); El-Attar et al. (2021); Souza & Ruby (2021); Vanaja et al. (2019)			
Blowfish & Legacy Algorithm Hybrids	Chinnasamy & Deepalakshmi (2018); Ponnuru & Sunitha (2018); Bijeta et al. (2020); Sajay et al. (2019); Uttam & Jay (2020); Maria et al. (2022); Wani & Kumar (2022)	Blowfish, DES, RC4, RC6	Fast encryption, flexible hybridisation	Use of outdated algorithms; weaker long-term security
Multi-Tier & Data Slicing Models	Mehul et al. (2018); Batra et al. (2018); Uttam & Jay (2020); Viswanath & Krishna (2020, 2021); Shukla et al. (2024)	AES, DES, RC4, RC6, BRA	Strong resistance to attacks via segmentation	High processing time; increased resource consumption
Steganography & Obfuscation	Mehul et al. (2018); Poduval et al. (2019); Bokhari et al. (2023); Chatterjee et al. (2023)	AES, RSA, LSB Steganography	Concealed key transmission; enhanced secrecy	Limited scalability; performance constraints
Authentication & Integrity Layers	Ugba et al. (2018); Singh & Garg (2018); Gurjeet & Mohita (2018);	AES, SHA-256, MD5, OTP, IBE	Ensures data integrity and user verification	MD5 vulnerability; increased system complexity

	William et al. (2022); Varma et al. (2022); Souza & Ruby (2021); Pravin & Rahul (2021); Adee & Mouratidis (2022); Silki & Abhilasha (2018)			
Emerging & Intelligent Hybrid Models	Wang et al. (2018); Kumar & Badal (2019); Zaineldeen et al. (2020); Dutta et al. (2023); Ranganatha & Sujatha (2023); Sabitha et al. (2023); Almalawi et al. (2024); Rath et al. (2024); Anjana (2024); Riyaz Fathima & Saravanan (2025)	Blockchain, ALO, NTRU, AES, ChaCha20	Advanced security, decentralisation, optimisation	High cost, computational overhead, limited scalability, no post-quantum readiness

Results and Discussion

1 Study Selection

The selection process resulted in 51 primary studies that met all inclusion criteria. The distribution of these studies shows a strong focus on recent developments in hybrid security.

2 Study Characteristics

- **Recency:** Most of the reviewed papers were published between 2022 and 2024, reflecting the rapid changes in cloud security needs.
- **Technique Diversity:** The review found a wide variety of algorithms being used. While AES and RSA remain the most popular choices for hybrid models, there is a growing trend toward using newer methods like ChaCha20-Poly1305 and Edwards Curve Cryptography.
- **Validation Method:** Over 60% of the studies used Experimental methods, where the authors built a prototype and measured its speed and security against attacks.

3 Methodology Trends

The analysis reveals three dominant trends in the design of cloud security frameworks:

1. **Emphasis on Speed:** Many studies now focus on reducing the time it takes to encrypt data without losing security.
2. **Multi-Layered Defence:** There is a move towards "Three-Phase" or "Multi-Tier" models to make it harder for unauthorised users to access data.

3. **Integrity Checks:** More researchers are adding hashing (like SHA-256 or SHA-3) to their encryption models to ensure data is not changed during transit. Based on the 51 selected studies, the following table highlights the journals and conferences that contributed the most to this review.

Table 3: Top Publications by Article Volume

Publication Name	Number of Articles
IEEE (Access, Conferences, & Journals)	8
International Journal of Engineering Research & Technology (IJERT)	4
International Journal of Computer Science and Engineering	3
Sensors	3
International Journal of Scientific Research in Computer Science	2
Journal of Emerging Technologies and Innovative Research (JETIR)	2
International Journal of Applied Engineering Research	2
Wireless Personal Communications	2
Others (Single-article contributions)	25
Total	51

4 Analysis of Publication Trends

The distribution shows a high concentration of research within IEEE and specialised Engineering and Technology journals. This indicates that hybrid encryption is a major focus for technical development and practical implementation.

5 Observation on Methodologies

The quality assessment revealed that most of these studies used Experimental and Simulation methods. This means the literature is not just theoretical; most authors built and tested these hybrid models to prove their speed and security.

6 Key Synthesis of Findings

The review of the 51 studies reveals several critical insights regarding the current state of hybrid cloud security:

1. **The Performance-Security Trade-off:** Most modern models (2023–2025) achieve high security but suffer from computational overhead. For instance, the TPHC algorithm (Shukla et al., 2024) and the RSA-ChaCha20 scheme (Riyaz Fathima, 2025) provide excellent protection but are noted as being resource-intensive for low-power or real-time systems.
2. **Shift Towards Multi-Layering:** There is a clear move from simple dual encryption to multi-tier frameworks involving three or more algorithms. This "Optionality" in security layers allows for better defense against sophisticated attacks like pattern analysis.
3. **The Integrity Gap:** While confidentiality (encryption) is well-addressed, several older models (e.g., Kota, 2022; Manoj et al., 2019) failed to achieve robust authentication or authorisation, a gap being filled by more recent integrations of SHA-3 and 2FA.
4. **Outdated Algorithms:** A recurring weakness in some "hybrid" models is the continued inclusion of DES and RC2 (Selvanayagam et al., 2018). These are considered outdated and can compromise the overall security of the system, regardless of the other algorithms paired with them.

7. Research Gap

A critical analysis of the current literature reveals several significant gaps that hinder the effective adoption of hybrid security models:

i. High Processing Time and Computational Overhead:

Studies (e.g., Mangalampalli et al., 2023; Ranganatha & Sujatha, 2023; Viswanath & Krishna, 2021) show that although hybrid cryptographic models enhance security, they significantly increase encryption/decryption time and CPU usage, creating a persistent security–performance trade-off that limits scalability and real-time application.

ii. Weak Authentication Mechanisms:

Research (e.g., Gurjeet & Mohita, 2018; Singh & Garg, 2018; Maria et al., 2022) indicates reliance on basic authentication methods such as passwords or single OTP systems, with limited adoption of multi-factor or adaptive authentication, thereby weakening access control in cloud environments.

iii. Limited File-Type Coverage:

Most studies (e.g., Batra et al., 2018; Lai & Heng, 2022; Souza & Ruby, 2021) focus on text-based datasets, with few (e.g., Hernal & Chauhan, 2019; Dutta et al., 2023) addressing multimedia files, indicating poor generalisation to real-world data types.

iv. Insufficient Data Integrity Mechanisms:

While confidentiality is well addressed, fewer works (e.g., Rath et al., 2024) incorporate robust integrity checks such as hashing or authentication tags, leaving gaps in protection against data tampering.

v. Lack of Standardised Performance Evaluation:

Studies (e.g., Kanatt et al., 2020; Kumar & Bandal, 2019; Abhishek & Asha, 2021) often evaluate systems without standard benchmarking metrics like throughput, latency, and memory usage, limiting comparability and reproducibility of results.

8 Practical Implications

The findings of this review have serious implications for both cloud service providers and organisational leadership. For the provider, the inability to offer efficient, multi-format encryption leads to a loss of market share. For the executive, the primary implication is one of risk management; if only 1% of compromised data is encrypted (Gemalto, 2018), then the current "security-first" vision of many organisations is not being met by their technical implementation. Transitioning to more robust hybrid models is no longer just a technical option but a strategic necessity to ensure business continuity and protect digital assets.

9. Future Research Focus

Future investigations should move from "contributor with insight" to "enablers of success" by focusing on the following areas:

- Cross-Platform Usability: Developing hybrid models that are easy to deploy and configure across different cloud architectures.
- Multimedia Encryption: Creating algorithms specifically optimised for the high-speed encryption of video and audio files.
- Adaptive Key Management: Researching how artificial intelligence can be used to manage cryptographic keys dynamically to reduce computational overhead.
- Integrity-First Frameworks: Prioritising hashing and verification steps as a standard part of the encryption pipeline to prevent unauthorised data alteration.

Conclusion

Cloud computing offers immense potential for organisational growth, yet its full adoption is stifled by persistent security vulnerabilities. This study concludes that while hybrid cryptography represents a significant step forward, current implementations are often too slow, too complex, or too narrow in their file-type support. By addressing the identified gaps, particularly regarding processing efficiency and multi-factor authentication, organisations can

better align their IT posture with their strategic vision. Building a more secure cloud environment is essential to restoring declining user confidence and ensuring the long-term resilience of digital infrastructures.

This study successfully achieved its stated objectives. A comprehensive literature survey was conducted, revealing critical security and privacy concerns in cloud environments. Existing hybrid cryptographic models were analysed, exposing key weaknesses in their design and implementation. Performance limitations, particularly in terms of processing time and computational complexity, were systematically evaluated. Furthermore, the review identified more resilient cryptographic approaches, providing a foundation for the development of improved high-performance hybrid frameworks.

However, this study is not without limitations. The review was restricted to English-language publications between 2018 and 2025, which may have excluded relevant studies in other languages or outside this timeframe. Additionally, the quality assessment process was conducted by a single reviewer, and the final selection of 51 studies may not fully represent the entire body of research on hybrid cryptography in cloud environments.

Future research should focus on developing optimised hybrid models that balance security strength with computational efficiency, particularly for large-scale and real-time cloud applications. There is also a need for more empirical studies that evaluate these models across diverse data types and real-world deployment scenarios to enhance their generalisability and practical adoption.

References

- Abhishek, G., & Asha, A. (2021). Study of Data Security Using Hybrid Cryptographic Techniques. *Solid State Technology*, 63, 20714-20718.
- Adee, R., & Mouratidis, H. A. (2022). Dynamic Four-Step Data Security Model for Data in Cloud Computing Based on Cryptography and Steganography. *Sensors*, 22, 1109. <https://doi.org/10.3390/s22031109>.
- Almalawi, A., Hassan, S., Fahad, A., & Khan, A. (2024). A hybrid cryptographic mechanism for secure data transmission in edge AI networks. *International Journal of Computational Intelligence Systems*, 17. <https://doi.org/10.1007/s44196-024-00417-8>
- Anjana. (2024). An enhanced three layer cryptographic algorithm for cloud information security. *International Journal of Intelligent Systems and Applications in Engineering*, 12(17s), 615–627. <https://ijisae.org/index.php/IJISAE/article/view/4927>
- Basapur, S. B. (2021). A hybrid cryptographic model using AES and RSA for sensitive data privacy preserving. *Webology*, 18(Special Issue).
- Batra, M., Dixit, P., Rawat, L., & Khalkar, R. (2018). Secure File Storage In Cloud Computing
- Bijeta, S., Surjeet, D., Dac-Nhuong, L., Vivek, J., Neeraj, D., Akshat, A., Mayank, M. S., Deo, P., & Verma, K. D. (2020). Secure Cloud Data Storage System Using Hybrid Paillier–Blowfish Algorithm. *Computers, Materials & Continua*. <https://doi.org/10.32604/cmc.2021.014466>
- Bokhari, N., José, J., & Martínez, H. (2023). A Security Model for the Cloud, Applying a Hybrid of Cryptography and Steganography. *Journal of Emerging Technologies and Innovative Research*, 10(1).
- Chatterjee, P., Bose, R., Banerjee, S., & Roy, S. (2023). Enhancing Data Security of Cloud-Based LMS. *Wireless Personal Communications*, 2023, 1–17. <https://doi.org/10.1007/s11277-023-10323-5>.
- Chinnasamy, P., & P., Deepalakshmi (2018). Design of Secure Storage for Healthcare Cloud Using Hybrid Cryptography. *Proceeding of the 2nd International Conference on Inventive Communication and Computational Technology (ICICCT)*. ISBN: 978-1-5386-1974-2 PP. 1708-1711. <https://doi.org/10.1109/ICICCT2018.8473107>.
- Chinnasamy, P., Padmavathi, S., Swathy, R., & Rakesh, S. (2021). Efficient Data Security Using Hybrid Cryptography on Cloud Computing. *Inventive Communication and Computational Technologies, Lecture Notes in Networks and Systems* 145. https://doi.org/10.1007/978-981-15-7345-3_46.
- Diaz, M., Martin, C., & Rubio, B. (2016). State-of-the-art, challenges, and open issues in the integration of the Internet of things and cloud computing. *Journal of Network and Computer Applications*, 67, 99–117. <https://doi.org/10.1016/j.jnca.2016.01.010>.
- Dlamini, M.T., Eloff, J.H.P., Venter, H.S., Eloff, M.M., Henha E. R.P.S., and Mosola, N.N. (2017). Behavioural analytics: beyond risk-based MFA. *The 2017 Proceedings of the Annual Southern Africa Telecommunication Networks and Applications Conference (SATNAC 2017)*, Freedom of the Seas Cruise Liner, Royal Caribbean International, Barcelona, Spain, 3 – 10. ISBN: 978-0-620-76756-9.
- Dutta A, Bose R, Roy S, Sutradhar Sh. (2023).” Hybrid Encryption Technique to Enhance Security of Health Data in Cloud Environment. *Arch Pharm Pract*”. 2023;14(3):41-7. <https://doi.org/10.51847/raeh8fHBT6>.
- El-Attar, N. E., El-Morshedy, D. S., & Awad, W. A. (2021). A New Hybrid Automated Security Framework to Cloud Storage System. *Cryptography*, 5, 37. <https://doi.org/10.3390/cryptography5040037>.
- EZComputer Solutions. (2018). 6 things to consider before moving to the cloud, EZComputer Solutions, available online: <https://www.ezcomputersolutions.com/blog/tips-before-moving-to-cloud/>, accessed: [30 August 2023].

- Gemalto and Ponemon Institute. (2018). The 2018 Global Cloud Data Security Study. Retrieved from <https://www2.gemalto.com/cloud-security-research/>, accessed: [04/12/2023].
- Gurjeet S. and Mohita G. (2018). Enhanced Cloud Security using Hybrid Mechanism of RSA, AES and Blowfish Data Encryption with Secure OTP. *International Journal of Computers & Technology* Vol 18(2018) ISSN:2277-3061.
- Hernal, S., & Chauhan, R. K. (2019). Hybrid Cryptography base E2EE for Integrity & Confidentiality in Multimedia Cloud Computing. *International Journal of Innovative Technology and Exploring Engineering (IJITEE)*, 8(10), 918-924. DOI:10.35940/ijitee.J9001.0881019. ISSN: 2278-3075. www.ijitee.org.
- Ismail, S., Hassen, H. R., & Zantout, H. (2016). Open challenges in security of cloud computing. In *Proceedings of the International Conference on Big Data and Advanced Wireless Technologies*, BDAW 2016, Blagoevgrad, Bulgaria, 10 – 11 November 2016. [a62] Association for Computing Machinery (ACM). DOI: 10.1145/3010089.3016025.
- Kanatt, S., Jadhav, A., & Talwar, P. (2020). Review of Secure File Storage on Cloud using Hybrid Cryptography. *International Journal of Engineering Research & Technology (IJERT)*, 9(02), 16–20. <http://www.ijert.org>.
- Kota, C. (2022). Secure File Storage in Cloud Using Hybrid Cryptography. Available at SSRN: <https://ssrn.com/abstract=4209511> or <http://dx.doi.org/10.2139/ssrn.4209511>.
- Kumar, L., & Bandal, N. A. (2019). A Review on Hybrid Encryption in Cloud Computing. In *Proceedings of the 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)*, 1–6. doi:10.1109/IoT-SIU.2019.8777503.
- Lai, J.F. and Heng, S.H., (2022). Secure File Storage on Cloud Using Hybrid Cryptography. *Journal of Informatics and Web Engineering*, 1(2), pp.1-18.
- Mangalampalli, S.S.L., Virajitha, T., Divya, A.R., & Sree, B.S. (2023). A Security Framework for Data Storage in Cloud Computing by Using Cryptographic Approaches. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 9(4), 110-120. <https://doi.org/10.32628/CSEIT228659>.
- Manoj, T., Manish, M., & Bharat, M. (2019). Analysis and Implementation of AES and RSA for Cloud. *International Journal of Applied Engineering Research*, 14(20), 3918-3923. <https://dx.doi.org/10.37622/IJAER/14.20.2019.3918-3923>.
- Maria, J., Qamar, S., & Salman, A. (2022). Securing the Cloud Storage by Using Different Algorithms of Cryptography. *International Journal of Scientific Research in Computer Science and Engineering*, 10(2), 38-45.
- Mehul, B., Prayas, D., Lalit, R., & Rohini, K. (2018). Secure File Storage In Cloud Computing Using Hybrid Encryption Algorithm. *International Journal of Computer Engineering and Applications*, 9(6).
- Mohammed, A.B., & David, T.O. (2022). Secure File Storage on Cloud Computing Using Hybrid Cryptography. *International Journal of Science and Advanced Innovative Research*, 7(3).
- Nair, S. (2022). "Data security using a hybrid cryptographic approach in mobile cloud computing". Master's thesis, Dublin, National College of Ireland.
- Pandey, U.N. (2018). Data Breach Statistics 2017: See What is the Status of Cloud Security? LetToKnow. Retrieved from <https://lettoknow.com/data-breach-statistics-2017-status/> [Accessed: 30 August 2023].
- Poduval, A., Doke, A., Nemade, H., & Nikam, R. (2019). Secure File Storage on Cloud Using Hybrid Cryptography. *International Journal of Computer Science and Engineering Open Access*, 7(1), EISSN: 2347-2693, 587-591.

- Ponnuru, S., & Sunitha, K.V.N. (2018). Enhancing the Data Security In the Cloud Using Hybrid Algorithm. *International Journal of Pure and Applied Mathematics*, 120(6), 3669-3680.
- Prabhu, K., Ganapathy, B., Kanimozhi, S., & Kannan, U.A. (2020). An Enhanced Security Framework for Secured Data Storage and Communications in the Cloud Using ECC, Access Control, and LDSA. *Wireless Personal Communications*, 115(2), 1107-1135. DOI: 10.1007/s11277-020-07613-7.
- Pradeep, K.V., Vijayakumar, & Subramaniaswamy, V. (2019). An Efficient Framework for Sharing a File in a Secure Manner Using Asymmetric Key Distribution Management in Cloud Environment. Hindawi, *Journal of Computer Networks and Communications*, Volume 2019.
- Pravin, S., & Rahul, M. (2021). A Hybrid Cloud Security Model for Securing Data on Cloud. *CEUR Workshop Proceedings (CEUR-WS.org)* Vol.1.2889.
- Ranganatha, B.R., & Sujatha, B. (2023). A hybrid elliptic curve cryptography (HECC) technique for fast encryption of data for public cloud security. Measurement: *Sensors*, 29(100870). <https://doi.org/10.1016/j.measen.2023.100870> .
- Rath S.B., Priyadarshini S. B., Patel D. K., Sahu P. K., Jagadev N., Panda M., Patra N., & Sahoo S. (2024). AES-RSA: An Innovative Hybrid Security Framework for File Authentication, Integrity, and Data Secrecy Model. *International Journal of Intelligent Systems and Applications in Engineering*, 12(18s), 303–312. Retrieved from <https://ijisae.org/index.php/IJISAE/article/view/4974>.
- Riyaz Fathima Abdul, & Saravanan, A. (2025). A novel data transmission model using hybrid encryption scheme for preserving data integrity. *Advances in Technology Innovation*, 10(1), 15–28. <https://doi.org/10.46604/aiti.2024.14114>
- Sabitha, R., Shaik, J.S., Karthik, S., & Kavitha, M.S. (2023). Secure Data Storage on Cloud Using Hybrid Cryptography Methods. *EasyChair Preprint no.* 10126.
- Sa'idu, S. (2022). An Improved Cryptographic Scheme Using AES & RSA Algorithms for Maximum Security in File Encryption and Decryption. *International Journal of Scientific Development and Research (IJS DR)*, Volume 7 Issue 6.
- Sajay, K.R., Sasidhar, S.B., & Vijayalakshmi, Y. (2019). Enhancing the security of cloud data using a hybrid encryption algorithm. *Journal of Ambient Intelligence and Humanized Computing*. <https://doi.org/10.1007/s12652-019-01403-1>.
- Sam, N., Jianbiao, Z., Edna, T., & Harold, B.D. (2019). Enhancing User Data and VM Security Using the Efficient Hybrid of Encrypting Techniques. *Journal of Theoretical and Applied Information Technology*, Vol.97, No 15.
- Selvanayagam, P., Singh, A., Michael, J., & Jeswani, J. (2018). Secure File Storage on the Cloud using Cryptography. *International Research Journal of Engineering and Technology (IRJET)* Vol. 05, No. 03.
- Shukla, D. K., Khalaf, O., Vallabhaneni, R., Srivastava, S. K., & Algburi, S. (2024). A three-phase hybrid cryptography algorithm: Utilized in public sensor network for data security with an enhancement of hashing algorithm. *International Journal of Computing and Digital Systems*, 15(1), 1–13. <https://doi.org/10.12785/ijc ds/150101>
- Silki, J., & Abhilasha, V. (2018). An improved security framework for cloud environment using ECC algorithm. *International Journal for Research in Applied Science & Engineering Technology*, vol. 6, no. 1.
- Singh, J., & Mansotra, V. (2019). Factors affecting cloud computing adoption in the Indian school education system, *Education, and Information Technologies*, 24(4), pp. 2453–2475.

- Souza, D' R.B., & Ruby, D. (2021). Secure file storage on cloud using enhanced hybrid cryptography. *International Research Journal of Engineering and Technology (IRJET)*, 8(3), 294–298.
- Ugba T. P, Eze C. Onyebuchi, Ogidi P. Chinasa, Ekle F. Adoba (2018). “A Cloud-Based Data Security System using Advanced Encryption (AES) and Blowfish algorithms”. *Journal of Scientific and Engineering Research*, 2018, 5(6):59-66.
- Uttam K. & Jay P. (2020). “Secure File Storage on Cloud Using Hybrid Cryptography Algorithm”. *International Journal of Creative Research Thoughts (IJCRT)*. Volume 8, Issue 7.
- Vanaja, M., Raman, D., & Kumar, A. (2019). A Novel Data Security Framework in Distributed Cloud Computing. pp. 373-378. DOI: 10.1109/ICIIP47207.2019.8985941.
- Varma, V., Patil, M., Patil, S., Patil, M., & Kadam, A. (2022). Data Storage Security in Cloud Computing Using AES Algorithm and MD5 Algorithm. *International Journal for Research in Applied Science and Engineering Technology*, 10(5), pp.5052-5055.
- Viswanath G. and Krishna P. V., (2020). Hybrid encryption framework for securing big data storage in a multi-cloud environment. *Evol. Intell.*, no. 0123456789, doi: 10.1007/s12065-020-00404- w.
- Viswanath, G.; Krishna, P.V. (2021). Hybrid encryption framework for securing big data storage in a multi-cloud environment. *Evol. Intell.* 14, 691–698. [CrossRef].
- Wang, S., Zhang, Y., and Zhang, Y, (2018). A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems, *IEEE Access*, 6, 38437–38450.
- William, P., Choubey, A., Chhabra, G.S., Bhattacharya, R., Vengatesan, K. and Choubey,S., (2022). Assessment of Hybrid Cryptographic Algorithm for Secure Sharing of Textual and Pictorial Content. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)* (pp. 918-922). IEEE.
- Zaineldeen, S., & Ate, A. (2020). Improve the security of transfer data file on the cloud by executing hybrid encryption algorithms. *Indonesian Journal of Electrical Engineering and Computer Science*. 20. 521-527. 10.11591/ijeecs. v20.i1. pp521-527.
- Zhang, F., & Chen, Y. & Meng, W. & Wu, Q. (2019). Hybrid Encryption Algorithms For Medical Data Storage Security in Cloud Database. *International Journal of Database Management Systems*. 11. 57-73. 10.5121/ijdms.2019.11104.
- Zinah R.S, Zakiah A, Nurul A., Mohd. R.B., (2018). Improved Cloud Storage Security by Using Three Layers Cryptography Algorithms. *International Journal of Computer Science. Intelligence*, 14(1), 691–698.