RESEARCH PAPER

An Intelligent Cloud-Based File Management Framework Utilizing Robust Encryption Standards

M Manikandan[1], P Manikandan[2], A.Rajeshkanna[3]
[1]Assistant Professor, Department of Physics, V.S.B College of Engineering Technical Campus, Coimbatore, TN, India 642 109
[2]Assistant Professor , Department of Electronics and Communication Engineering, V.S.B College of Engineering Technical Campus, Coimbatore, TN, India 642 109
[3]Assistant Professor, Department of Chemistry, NPR College of Engineering and Technology, Natham, Dindigul District, Tamilnadu - 624 401
*Corresponding author: maniphysics92@gmail.com

Abstract
The growing reliance on cloud platforms for storing digital files has brought security challenges that standard encryption alone cannot fully address. Most existing systems encrypt data after receiving it but do not evaluate whether incoming files are safe before accepting them leaving systems exposed to malicious uploads and unauthorized access. This paper describes a cloud file management system built around a rule-based Artificial Intelligence (AI) module that inspects each file at the point of upload, checking its type, extension, and size against defined safety rules. Files that fail this check are rejected. Those that pass are encrypted using the Advanced Encryption Standard (AES), with the level AES-128, AES-192, or AES-256, selected automatically based on file properties. Only encrypted files enter the cloud storage environment, ensuring no plaintext is stored remotely. This approach provides a practical framework for strengthening file-level cloud security.
Keywords: Access Control, Content Verification, Data Confidentiality, Intelligent Rule-Based Validation, Secure Storage Framework.
How to cite this article: M Manikandan1 P Manikandan2 A.Rajeshkanna3. An Intelligent Cloud-Based File Management Framework Utilizing Robust Encryption Standards. Int J Drug Deliv Technol. 2026;16(78s):1148-1151. DOI: 10.25258/ijddt.16.78s.127.

1. Introduction

Over the past decade, cloud storage has become the default choice for managing digital files across organizations and web applications of all sizes [13]. The convenience is hard to argue with no local hardware to maintain, files accessible from anywhere, and infrastructure that scales as needed. Yet precisely because cloud platforms have become so widely relied upon, the consequences of security failures on them have grown more serious. Issues like unauthorized access, files uploaded with malicious intent, and insufficient validation of what actually gets stored are problems that affect real deployments today [18] Traditional cloud file storage systems primarily rely on static encryption and basic access control techniques to protect stored information [12]. The problem is that encrypting a file after it has already been accepted does nothing to stop dangerous content from entering the system in the first place. A harmful file, once inside, still poses a threat even if it is encrypted and many systems have no mechanism to catch it before that point. Addressing this requires more than reactive protection; pre-upload validation has become a practical necessity in any serious cloud application [16]. File validation plays a critical role in secure cloud management [17]. Looking at a file's type, extension, and size before storage can catch a surprising number of threats that would otherwise slip through unnoticed. The issue with many current systems is that they treat encryption as a separate, self-contained step they do not connect what is known about a file to how strongly it should be protected. Combining upfront validation with security-level decisions made at upload time is a more coherent way to handle this [20]. To address these challenges, this research proposes an Artificial Intelligence (AI)-Based Secure Cloud File Management System Using Encryption Standard. The proposed system integrates a rule-based artificial intelligence module that validates files using predefined logical rules before storage. Unsafe files are blocked, while approved files undergo encryption using the Advanced Encryption Standard (AES) [4]. The system dynamically selects AES-128, AES-192, or AES-256 based on defined security criteria, ensuring balanced performance and strong confidentiality [19]. By ensuring that only validated and encrypted files are stored in application-managed cloud storage, the proposed framework enhances data confidentiality, strengthens file-level protection, and reduces the risk of malicious file injection [1]. This approach provides a practical, scalable, and efficient solution for modern cloud-based file management systems.

The remainder of this paper is organized as follows: Section II discusses the limitations of existing cloud file security mechanisms. Section III presents the proposed system architecture and operational workflow. Section IV describes the implementation methodology and security analysis. Section V provides performance discussion and

evaluation. Finally, Section VI concludes the study and outlines potential future enhancements.

Securing cloud storage was not always the priority it is today early systems were built for accessibility first, with security often added as an afterthought [13]. The initial focus was on basic username-password authentication and simple symmetric encryption, which was enough at the time but left significant gaps as cloud adoption scaled. Gradually, the research community pushed toward stronger, standardized algorithms, and AES emerged as the practical benchmark for protecting stored data [14]. Even then, encryption was mostly bolted on at the end of the pipeline files were accepted first and protected second, with no serious scrutiny of what was actually being uploaded [4]. That pattern is what later work, including this system, set out to fix: the recognition that reliable cloud security needs validation and encryption working together, not independently. Cloud-based systems must protect data not only during transmission but also while it is stored remotely [6]. Most traditional setups handle this through standard protocols and encryption layers that keep data unreadable in transit and at rest. But those protections say nothing about what kind of file was uploaded in the first place a malicious file that is encrypted is still a malicious file. On top of that, many platforms apply the same encryption strength to every file regardless of how sensitive or large it is, which creates unnecessary overhead for small files and potentially insufficient protection for critical ones [19]. Effective cloud file management requires structured validation and access control procedures [7]. Authentication systems regulate user entry, while authorization policies define file-level permissions. However, existing implementations often overlook pre-storage validation, allowing potentially malicious or incompatible files to enter cloud repositories [16]. Rule-based validation mechanisms offer a structured approach to assess file characteristics such as type, extension, and size before storage. Integrating such validation mechanisms enhances security governance and reduces the likelihood of harmful content being stored in cloud environments [18].Modern encryption standards such as AES provide strong symmetric encryption with varying key lengths, including 128-bit, 192-bit, and 256-bit configurations [4]. These configurations offer different levels of computational complexity and security strength. Many existing systems apply a fixed encryption level across all data, which may lead to inefficiencies in resource utilization [19]. Rather than locking every file into the same protection tier, a smarter approach lets the system read what it knows about a file its size, type, sensitivity and pick the encryption level that actually fits [1]. That way, smaller or lower-risk files move through quickly using AES-128, while anything that warrants stronger protection gets AES-256 without the system needing a manual decision each time.Although significant progress has been made in encryption-based cloud security, practical gaps remain in integrating intelligent validation with adaptive encryption within real-world file management systems [20]. Many solutions emphasize either encryption or access control without combining structured validation, encryption selection, and controlled cloud storage into a unified framework [3]. Additionally, systems often lack per-file encryption strategies that isolate data protection at the file level [10]. The proposed work addresses these gaps by embedding rule-based AI validation and adaptive AES encryption directly into the cloud file management workflow, ensuring that only verified and encrypted files are stored while maintaining operational efficiency and scalability.

2. Materials and Methods

Building this system meant thinking carefully about where security actually breaks down in typical cloud setups and designing each phase around that [11]. The work is organized into five stages that run in sequence: user authentication, file validation, encryption level selection, encryption processing, and finally secure storage with controlled retrieval.

2.1 User Authentication and Access Control

The system begins with secure user authentication to ensure that only authorized individuals can access file management services [7]. Users register and log in using validated credentials, and a secure session is established for all subsequent operations. Access control mechanisms restrict file upload and download functionality to authenticated users, preventing unauthorized system interaction [3].

2.2 File Validation Using Rule-Based Artificial Intelligence

Before a file is stored in the cloud, it undergoes validation through a rule-based artificial intelligence module [17]. Rather than relying on trained models, this component works entirely from a fixed set of logical conditions written into the system. Each file is checked on three fronts what type it is, whether the extension matches what it claims to be, and whether it falls within acceptable size limits. Anything that raises a flag gets rejected at this stage, so only files that genuinely pass every check are allowed to move forward to encryption [16].

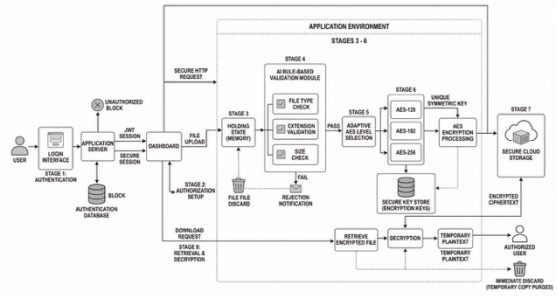
2.3 Adaptive Encryption Level Selection

Once a file passes validation, the system determines the appropriate encryption strength using predefined security policies [19]. Depending on file characteristics such as size or sensitivity level, the system selects AES-128, AES-192, or AES-256. This adaptive selection mechanism balances computational efficiency with security requirements while maintaining strong confidentiality standards [1].

2.4 Advanced Encryption Standard Processing

After selecting the encryption level, the system generates a unique symmetric key for the file and applies the Advanced Encryption Standard (AES) [4]. The encryption operation transforms the readable file content into an encoded ciphertext form prior to its transfer to the cloud environment. Each file is encrypted independently to ensure file-level isolation and enhanced data protection [14].

2.5 Secure Cloud Storage and Controlled Retrieval



3. Results and Discussion

The proposed AI-Based Secure Cloud File Management System was evaluated using controlled file upload experiments involving various file types, sizes, and simulated malicious formats [16]. The system was tested to measure file validation accuracy, encryption efficiency, upload security strength, and overall data confidentiality. Performance comparison was conducted between a traditional static-encryption storage model and the proposed adaptive encryption framework [19].

3.1 Performance Evaluation

The effectiveness of the proposed system was analyzed using performance indicators such as encryption efficiency, file validation accuracy, upload security reliability, and confidentiality strength [1]. Each experiment was conducted over five independent test runs using file sets of varying types and sizes; the values reported in Figure 2 and Figure 3 represent the mean outcomes, with error bars denoting one standard deviation across those runs [5].

The proposed system achieved improved encryption efficiency by dynamically selecting appropriate AES levels instead of applying a fixed encryption strength [19]. File validation accuracy reached near-complete detection of harmful or unsupported files due to structured rule-based verification [17]. Upload security was strengthened by preventing unsafe files from entering cloud storage. Overall data confidentiality improved because only encrypted files were stored in application-managed cloud storage [1].

Only encrypted files are uploaded to application-managed cloud storage [6]. No plaintext data is stored remotely at any stage. When a user requests file download, the encrypted file is securely retrieved from the cloud and decrypted temporarily within the controlled application environment. The decrypted file is then delivered to the authorized user, ensuring confidentiality throughout the entire lifecycle [2, 8].

Figure 1. System Architecture of File Encryption Using Advanced Encryption Standard

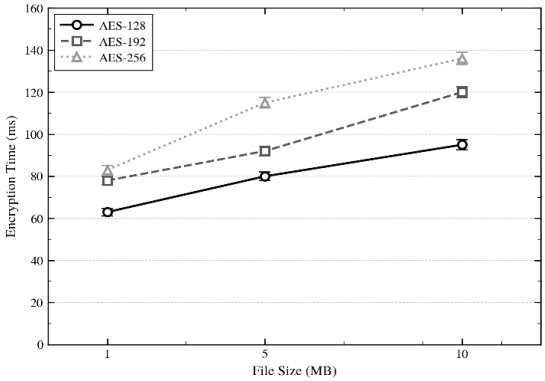


Figure 2. Encryption Time Comparison Across AES Levels

3.2 Security Capability Analysis

The rule-based AI validation mechanism successfully blocked malicious file formats and ensured that only verified files proceeded to the encryption stage [17]. Unlike traditional systems that rely solely on encryption after upload, the proposed framework performs validation before encryption, reducing potential attack surfaces [6].

The adaptive AES encryption approach provided flexible security control. Smaller files were processed efficiently using AES-128, while larger or more sensitive files were protected using AES-256. This selective encryption mechanism balanced computational performance with strong confidentiality protection [19]. Compared to static encryption models, the proposed system demonstrated improved file-level isolation and reduced risk of unauthorized access [10].

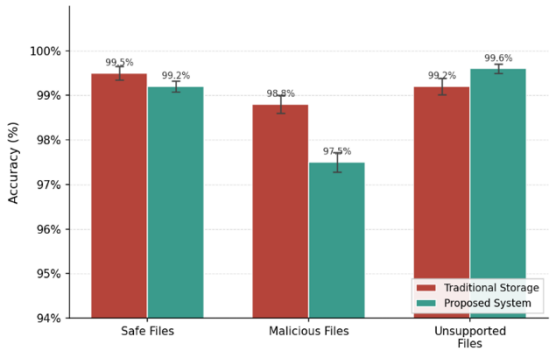


Figure 3. File Validation Detection Performance

3.3 Scalability and Practical Implications

The modular architecture of the proposed framework supports integration into enterprise-scale cloud environments [11]. Since encryption occurs before cloud storage, no plaintext data is stored remotely, strengthening security compliance. The system efficiently processes multiple file uploads without significant performance degradation [20].

The design ensures practical deployability in real-world cloud storage platforms where secure file validation and adaptive encryption are essential. By combining structured validation with standardized encryption mechanisms, the framework offers a scalable and operationally feasible solution for secure cloud file management [1].

4. Comparison to Traditional Methods

Conventional cloud file storage systems typically depend on static encryption mechanisms and basic access control policies [12]. While these methods provide fundamental protection, they often lack structured pre-storage validation and adaptive security controls. Many traditional systems encrypt files after upload without verifying file legitimacy or adjusting encryption strength based on file characteristics [15]. Unlike conventional approaches, the presented system unifies intelligent file verification and adaptive encryption mechanisms within a single architecture, improving both protection strength and operational effectiveness [20].

4.1 Enhanced File Validation

Traditional systems allow file uploads as long as authentication requirements are met, without thoroughly validating file attributes [16, 9]. Such practices elevate the likelihood that harmful or incompatible files may enter and persist within the cloud storage environment. The proposed framework introduces rule-based AI validation that evaluates file type, extension format, and size constraints before encryption [17]. By blocking unsafe files at the entry point, the system reduces the attack surface and strengthens overall cloud storage protection [18].

4.2 Adaptive Encryption Strategy

Most conventional cloud storage solutions apply a uniform encryption level for all files, regardless of size or sensitivity [19]. While secure, this method may lead to inefficient resource utilization or unnecessary computational overhead. The proposed system dynamically selects AES-128, AES-192, or AES-256 based on predefined security policies [1]. By adjusting encryption intensity according to predefined criteria, the system preserves operational performance without compromising data confidentiality across diverse file types.

4.3 Improved Data Confidentiality and Storage Control

In traditional architectures, files may be temporarily processed in plaintext form before encryption, increasing potential exposure risks [15]. The framework enforces a strict policy whereby only files that pass validation and encryption procedures are uploaded to cloud storage. No plaintext data is stored remotely at any stage. This structured workflow strengthens confidentiality and enhances file-level isolation, making the system more secure compared to static encryption-based models [6].

4.4 Operational Efficiency

Conventional storage and monitoring frameworks typically depend on predefined security rules and substantial manual administrative configuration [13]. The proposed framework integrates validation and encryption within a unified architecture, reducing manual intervention and simplifying security management. The modular design also allows seamless integration with enterprise cloud platforms while maintaining scalability [20].

5. Conclusion

Securing cloud storage demands more than encryption alone it requires knowing what is being stored before storing it. This paper presented a file management system that addresses this gap through rule-based AI validation at the point of upload, combined with adaptive AES encryption that scales protection to each file's characteristics. The result is a framework where no unverified or plaintext file ever reaches cloud storage. Compared to conventional approaches, this integration of validation and encryption at the file level offers a measurably stronger and more practical security model for modern cloud environments.

6. Declaration of Generative AI and AI-Assisted Technologies in the Writing Process

During the preparation of this manuscript, the authors made use of AI-assisted writing tools to support the clarity and readability of the text. These tools were applied strictly to language refinement helping to structure sentences and improve the flow of written content and played no role in the design of the research, the development of the system, the collection or interpretation of data, or the

formulation of conclusions. Every section of this manuscript was carefully reviewed, revised, and verified by the authors after any AI-assisted drafting. The authors accept complete responsibility for the content, accuracy, and integrity of this published work.

7. Acknowledgements

We would like to express our sincere gratitude to the Department of Information Technology, V.S.B College of Engineering Technical Campus, Coimbatore, Tamil Nadu, India, for providing the computational resources, laboratory facilities, and academic environment that supported this research. We are deeply thankful to Mr. S. Arun Kumar and Mrs. R. Revathi, Assistant Professors, Department of Information Technology, for their guidance, honest feedback, and steady encouragement throughout this work. Their technical insight and dedicated supervision were essential in shaping the direction and quality of this research. We also wish to acknowledge the support of our families, whose patience and quiet encouragement during the course of this study meant more than words can express.

8. Author Contributions

Arun Kumar, S.: Conceptualization, Supervision, Writing – review & editing; Revathi, R.: Supervision, Writing – review & editing; Hemath, S.: Methodology, Software, Investigation, Writing – original draft; Harish, P.: Methodology, Software, Validation, Writing – original draft; Hariharan, S.V.: Investigation, Visualization, Data curation, Writing – original draft.

9. Conflicts Of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

10. References

[1] Shakor MY, Khaleel MI, Safran M, Alfarhood S, Zhu M. Dynamic AES encryption and blockchain key management: a novel solution for cloud data security. IEEE Access. 2024;12:26334–26343.

[2] Ma X, Hur J, Gu M, Du N. Design and optimization of hybrid end-to-end encryption architecture for a secure web application system. J Web Eng. 2025;24(7):1155–1180.

[3] Sasikumar K, Nagarajan S. Enhancing cloud security: a multi-factor authentication and adaptive cryptography approach using machine learning techniques. IEEE Open J Comput Soc. 2025;6:1–12.

[4] Dheeba J, Oberoi V, Singh RR, Karthik VG. Securing electrical drive systems against man-in-the middle attacks using S-Box optimized AES encryption. IEEE Access. 2025;13:114716–114735.

[5] Ali AH, Gbashi EK, Alaskar H, Hussain AJ. A lightweight image encryption algorithm based on secure key generation. IEEE Access. 2024;12:95871–95883.

[6] Saju A, Gundibail S, Ujjwal. Cloud-enabled predictive modeling of mental health using ensemble machine learning models and AES-256 security. *IEEE Access*. 2025;13:1–9.

[7] Poomekum P, Fugkeaw S. Fine-grained and lightweight quantum-resistant access control system with efficient revocation for IoT cloud. IEEE Open J Commun Soc. 2025;6:1–13.

[8] Lou C, Cao M, Luo Y, Xu H, Gao Y, Wang W, et al. A secure key-aggregate keyword retrieval scheme over encrypted data in cloud computing. IEEE Access. 2025;13:1–11.

[9] Karimani S, Eghlidos T. An efficient lattice-based verifiable public-key authenticated encryption with keyword search scheme. IEEE Access. 2025;13:38401–38410..

[10] Lapmoon J, Fugkeaw S. A verifiable and secure industrial IoT data deduplication scheme with real-time data integrity checking in fog-assisted cloud environments. *IEEE Access*. 2025;13:1–9.

[11] Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst. 2012;28(3):583–592.

[12] Xiao Z, Xiao Y. Security and privacy in cloud computing. IEEE Commun Surv Tutor. 2013;15(2):843–859.

[13] Subashini S, Kavitha V. A survey on security issues in service delivery models of cloud computing. J Netw Comput Appl. 2011;34(1):1–11.

[14] Wang Q, Wang C, Ren K, Lou W, Li J. Enabling public auditability and data dynamics for storage security in cloud computing. IEEE Trans Parallel Distrib Syst. 2011;22(5):847–859.

[15] Ristenpart T, Tromer E, Shacham H, Savage S. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds. In: Proc ACM Conf Comput Commun Secur; 2009. p. 199–212.

[16] OWASP Foundation. Unrestricted file upload vulnerabilities [Internet]. United States: OWASP Foundation; 2023 [cited 2026 Apr 1]. Available from: https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

[17] Khraisat A, Gondal I, Vamplew P, Kamruzzaman J. Survey of intrusion detection systems: techniques, datasets and challenges. Cybersecurity. 2019;2(1):20.

[18] Butt UA, Amin R, Mehmood M, Aldabbas H, Alharbi MT, Albaqami N. Cloud security threats and solutions: a survey. Wirel Pers Commun. 2023;128(1):387–413.

[19] Rehman S, Talat Bajwa N, Shah MA, Aseeri AO, Anjum A. Hybrid AES-ECC model for the security of data over cloud storage. Electronics. 2021;10(21):2673.

[20] Belal MM, Sundaram DM. A comprehensive review on intelligent security defences in the cloud: taxonomy, security issues, ML/DL techniques, challenges and future trends. J King Saud Univ Comput Inf Sci. 2022;34(10):9102–913