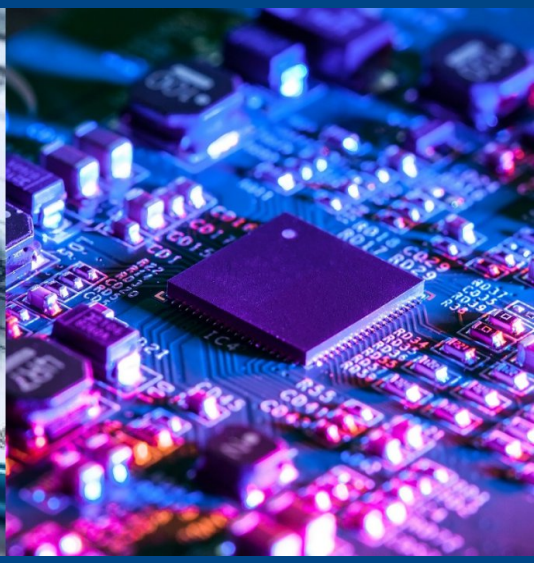
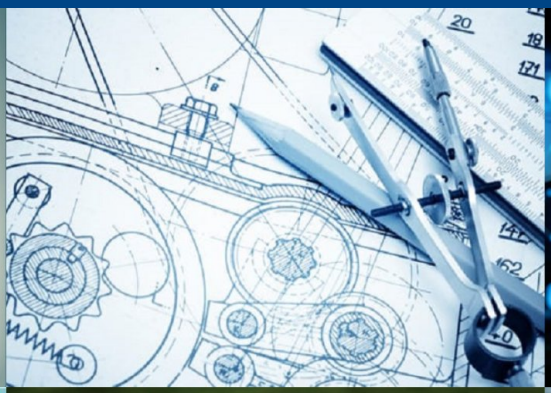
ISSN: 2582-7219

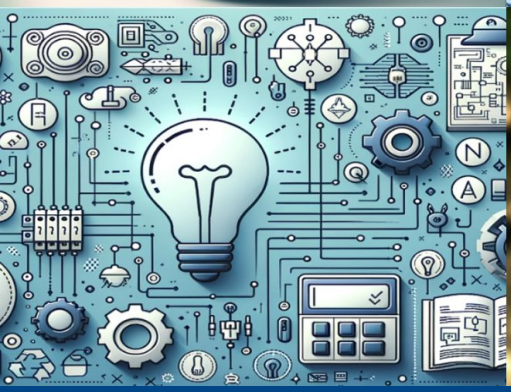




International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206 **Volume 9, Issue 4, April 2026**

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904366

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Image Encryption on Cloud Using Hybrid Algorithm

DR. K.jose reena[1], Zabir.N[2], Afrith rihan.M[3]

Assistant Professor, Department of Computer Applications, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[1]

Department of Computer Applications, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[2]

Department of Computer Applications, B.S. Abdur Rahman Crescent Institute of Science and Technology, Chennai, Tamil Nadu, India[3]

Abstract: Cloud storage services provide scalable and convenient solutions for storing digital media such as images. However, storing sensitive images directly in cloud environments introduces serious security risks including unauthorized access, data leakage, and privacy violations. Traditional encryption techniques alone may not provide sufficient protection when encryption keys are compromised or cloud servers are attacked. This paper proposes a secure cloud-based image storage system that combines AES-256 encryption with additive secret sharing to enhance data confidentiality. The proposed system encrypts images using AES in CTR mode and splits the encrypted image into multiple shares using additive secret sharing before uploading them to cloud storage. The system is implemented using Python Flask, Supabase cloud storage, and the Python cryptography library. During reconstruction, the shares are combined and decrypted to restore the original image. Experimental evaluation demonstrates that the proposed approach significantly improves security by preventing unauthorized access even if individual cloud storage components are compromised.

KEYWORDS: Cloud Security, Image Encryption, AES-256, Additive Secret Sharing, Secure Cloud Storage, Flask Web Application.

I. INTRODUCTION

Cloud computing has revolutionized the way digital data is stored, accessed, and managed. Cloud storage platforms enable users to store large volumes of data remotely while providing convenient access through web-based applications. Among different types of digital data, images represent a significant portion of stored content due to the widespread use of smartphones, social media, and digital documentation systems. Despite its advantages, cloud storage introduces several security challenges. Storing sensitive images in remote servers exposes them to risks such as unauthorized access, malicious attacks, and data breaches. In traditional cloud storage systems, data is typically encrypted before storage. However, if encryption keys are compromised or attackers gain access to encrypted data, the security of stored information can be threatened. To address these challenges, advanced cryptographic techniques can be combined with distributed storage mechanisms.

One such approach is secret sharing, where sensitive data is divided into multiple parts that dividually reveal no meaningful information. Only when the shares are combined can the original data be reconstructed.This paper proposes a secure cloud image storage system that integrates AES-

256 encryption and additive secret sharing. The encrypted image is split into multiple shares and stored in the cloud, ensuring that no single share contains useful information about the original image. This approach significantly enhances data security in cloud environments.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

II. RELATED WORK

Several studies have explored techniques for securing data stored in cloud environments. Encryption-based solutions remain the most commonly used approach for protecting sensitive information.Advanced Encryption Standard (AES) is widely used for secure data encryption due to its high level of security and computational efficiency. AES-256 provides strong protection against brute- force attacks and is widely adopted in cloud security systems. Research on digital image encryption using the **256-bit Advanced Encryption Standard algorithm** shows that AES can effectively protect multimedia data and ensure secure image transmission and storage (1). However, encryption alone may not fully protect data when attackers gain access to encrypted files or encryption keys.Secret sharing techniques such as Shamir's Secret Sharing have been proposed to improve data protection by dividing sensitive data into multiple parts. Each share contains partial information and requires collaboration with other shares to reconstruct the original data. Secure secret sharing approaches designed for cloud environments ensure that individual shares reveal no meaningful information unless the required shares are combined correctly (2).Recent research has also explored secure image sharing systems, where images are encrypted and stored in cloud environments to prevent unauthorized access. For example, frameworks developed for **secure medical image storage using advanced ciphertext algorithms in cloud computing** demonstrate how encryption techniques can be applied to protect sensitive healthcare data (3). These approaches improve security but may introduce computational overhead.In addition, verifiable secret sharing techniques have been proposed to enhance the reliability and integrity of distributed shares. Methods based on **Merkle tree structures** enable participants to verify the authenticity of shares before reconstructing the secret, preventing malicious users from submitting incorrect shares (4).However, many existing solutions rely either on encryption techniques or secret sharing methods individually. The proposed system improves security by combining encryption with secret sharing, ensuring that encrypted data itself is also distributed across storage systems.

III. EXISTING SYSTEM:

Most existing cloud image storage systems rely on simple encryption mechanisms to protect stored data. In these systems, users upload images that are encrypted and stored in cloud servers.Although encryption provides a level of protection, several limitations remain:

1. If attackers gain access to the encrypted data and encryption keys, the data can be decrypted.
2. Centralized storage increases the risk of data breaches.
3. Compromised cloud servers may expose encrypted files to attackers.
4. Many systems do not provide multi-layered security mechanisms.

These limitations highlight the need for a more robust security model that protects data even if cloud storage components are compromised.

IV. PROPOSED SYSTEM:

To overcome the limitations of existing cloud storage systems, this paper proposes a secure image storage framework that integrates AES encryption and additive secret sharing.

The proposed system works in two stages:

5. Image Encryption

Secret Share Generation and Cloud Storage First, the uploaded image is encrypted using the AES-256 encryption algorithm in CTR mode. This ensures that the image content is protected before being processed further.

Next, the encrypted image is divided into two shares using an additive secret sharing technique. Each share contains random values that individually reveal no information about the original encrypted image.The generated shares are then stored in cloud storage using Supabase, ensuring that the original encrypted image is never stored in a single location. During reconstruction, both shares are retrieved from cloud storage and combined to recreate the encrypted image. The AES decryption process then restores the original image.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904366

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

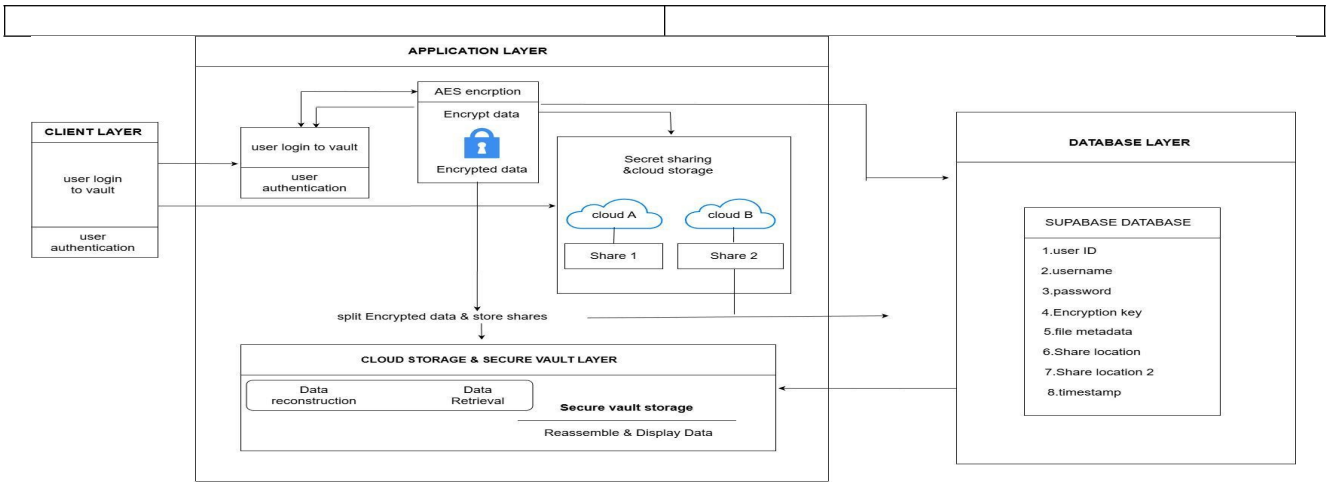
V. SYSTEM ARCHITECTURE:

The proposed system follows a client-server architecture consisting of three main components:
1. Client Interface
2.Application Server
3. Cloud Storage

Client Interface
The client interface is a web-based application that allows users to log in, upload images, view stored images, and reconstruct images. The interface is implemented using HTML templates integrated with the Flask framework.

Application Server
The application server is built using Python Flask and handles all processing tasks including authentication, encryption, secret sharing, and reconstruction. The server performs image processing using the Python Imaging Library (PIL) and numerical computations using NumPy.

Cloud Storage
The system uses Supabase cloud storage to store image shares. Each share is uploaded separately to ensure that no single stored file contains meaningful information about the original image.



VI. IMPLEMENTATION DETAILS:

The system is implemented using the following technologies:

component	technology
Backend	Python (flask)
Encryption	AES-256(CTR mode)
Secret sharing	Additive secret sharing
Image processsing	PIL and NumPY
Cloud storage	Supabae
Authentication	Supabase Auth

When a user uploads an image, the system performs the following steps:
6. The image is resized and converted to RGB format.
7. The image data is encrypted using AES-256 encryption.
8. The encrypted image is split into two shares using additive secret sharing.
9. The generated shares are uploaded to Supabase cloud storage.

© 2026 IJMRSET | Volume 9, Issue 4, April 2026 | DOI:10.15680/IJMRSET.2026.0904366

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

10. The initialization vector (IV) used for encryption is also stored securely.

During reconstruction:

1. Both shares are downloaded from cloud storage.
2. The shares are combined to recreate the encrypted image.
3. AES decryption is applied to obtain the original image.

VII. SECURITY ANALYSIS:

The proposed system provides multiple layers of security.

AES Encryption

AES-256 encryption ensures that image data remains protected even if stored data is intercepted.

Secret Sharing

The additive secret sharing mechanism ensures that individual shares do not reveal any information about the encrypted image.

Cloud Isolation

Shares are stored separately in cloud storage, reducing the risk of complete data exposure in case of server compromise.

Secure Authentication

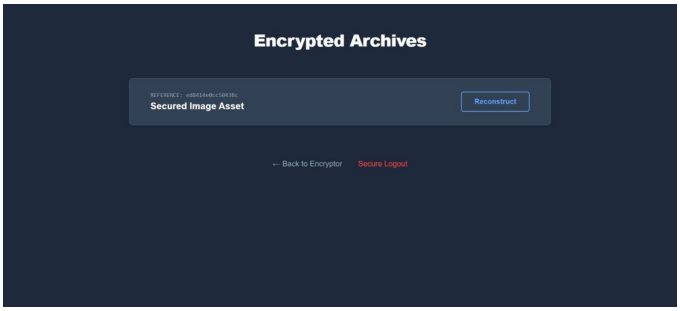
User authentication is handled through Supabase authentication services, ensuring secure access control.

Together, these mechanisms provide strong protection against unauthorized access and data leakage.

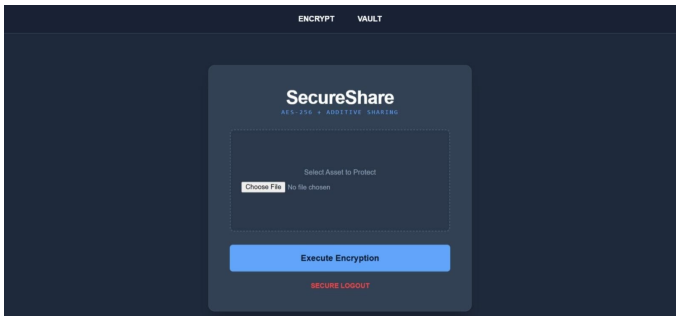
VIII. RESULTS AND DISCUSSION:

The system was successfully implemented and tested using multiple image files. Users were able to upload images securely through the web interface and store encrypted image shares in cloud storage. Experimental testing confirmed that:

Images were correctly encrypted using AES-256.



2,The additive secret sharing process generated two independent shares.



3. Individual shares did not reveal any information about the original image.
4. Reconstruction successfully restored the original image with no data loss.

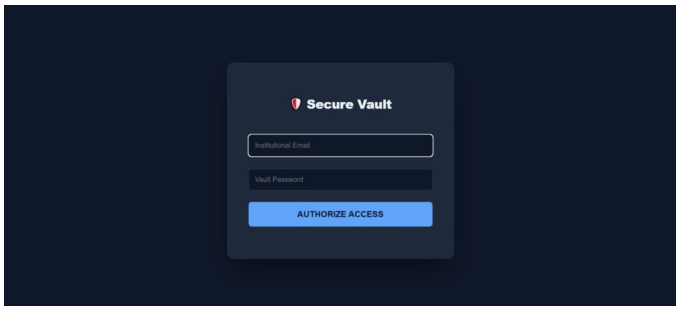
The system demonstrated reliable performance and improved security compared to traditional cloud image storage

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

approaches.



IX. CONCLUSION

This paper presented a secure cloud-based image storage system using AES encryption and additive secret sharing. The proposed system enhances data confidentiality by combining strong cryptographic encryption with distributed storage techniques.

By encrypting images and dividing them into multiple shares before cloud storage, the system prevents unauthorized access even if individual cloud storage components are compromised. The implementation using Flask, Supabase, and Python cryptographic libraries demonstrates the practicality of the proposed approach.

Future work may focus on extending the system to support multi-share secret sharing schemes, distributed cloud providers, and blockchain-based storage verification to further enhance system security and reliability.

REFERENCES

[1] J. Kala, J. Panda, and L. Tanwar, "Digital Image Encryption Using 256-bit Advanced Encryption Standard Algorithm," *2023 International Conference on Advancement in Computation & Computer Technologies (InCACCT)*, 2023.
[2] C.-C. Chang and C.-T. Li, "Secure Secret Sharing in the Cloud," *IEEE International Symposium on Multimedia*, 2017.
[3] Y. Fang, J. Liao, and Y. Lai, "Verifiable Secret Sharing Scheme Using Merkle Tree," *International Symposium on Computer Engineering and Intelligent Communications (ISCEIC)*, 2020.
[4] Author name(s), "A Novel Effective Framework for Medical Images Secure Storage Using Advanced Cipher Text Algorithm in Cloud Computing," *Journal / Conference Name*, Year.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com