International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 08 | August - 2023 SJIF Rating: 8.176 ISSN: 2582-3930

# Efficiently Encryption Decryption schema for Secure File Storage System in Cloud Computing

**Mrs.Pooja Sameer Bhondve, Ms.Supriya Sathe**

*[1]Assistant Professor Computer Engineering Department, D Y Patil College Of Engineering Akrudi, Pune*
*[2] Assistant Professor Computer Engineering Department , D Y Patil College Of Engineering Akrudi, Pune*

---

**Abstract-** Cloud computing finds applications in different industries, providing various services and data storage capabilities. While data stored in the cloud can be retrieved based on user requests, data security remains a primary concern. To address these security concerns, a proposed system employs the combined strength of the Triple Data Encryption Standard (AES) and Blowfish algorithms. The lack of robust and efficient secure file storage systems in cloud computing poses significant risks to data confidentiality and integrity.Existing solutions often lack strong encryption mechanisms and reliable server-side encryption and decryption capabilities. This research aims to develop a secure file storage system that leverages server encryption and decryption techniques to ensure data confidentiality, integrity, and access control in cloud environments. The objective is to design a system that effectively protects sensitive files during storage, transmission, and processing, while maintaining efficient data access and retrieval for authorized users.

***Key Words*:** Server-Side Encryption, Secure Key Storage Decryption, Encryption, Secure File Storage, Blowfish

## 1. INTRODUCTION

A secure and reliable file storage system in the cloud is provided as part of the secure file storage system in cloud computing project based on server encryption and decryption techniques.it protects files from unauthorized access by encrypting them before storing them and decrypting them when authorized users need to access them .with server-side encryption, files are encrypted prior to storage and decrypted when authorized users need to access them. Using the convenience and scalability of cloud storage, this project addressing the growing need for secure file storage in cloud computing The increasing industries on cloud storage for storing sensitive files has raised concerns about data security, unauthorized access, and privacy violations. Organizations and individuals require a robust solution that ensures the confidentiality and integrity of their data while taking advantage of the scalability and convenience offered by cloud computing. The problem addressed by the Secure File Storage System in Cloud Computing project using server encryption and decryption lies in the need for a secure file storage solution that effectively protects sensitive data stored in the cloud from unauthorized access, interception, and data breaches. This project aims to develop a system that implements server encryption and decryption techniques to address these concerns and provide a reliable and efficient solution for secure file storage in the cloud.

## 2. LITERATURE REVIEW

Shrikant Tangade,IEEE(2020) implement Trust Management Scheme Based on Hybrid Cryptography for Secure Communications. VANETs are susceptible to a number of security attacks from malicious entities. To secure the network against these attacks, most of the researchers have proposed various security schemes based on cryptography and trust management.

Tianfield ,Akhil Bedi (2020) introduced Cloud Security Concerns. The cloud security requirements in terms of the fundamental issues, i.e confidentiality, security issues in cloud computing is discussed. It focused on developing a comprehensive cloud-aware security strategy that can meet the aforesaid research challenges.

Nilesh Mangtani and Sukadha Bhingarkar (2021) open Source Cloud Environment. It discussed various open source cloud environment available that provides a substi- tute for the users that do not hope to use a commercially provided cloud. The public, private, hybrid cloud sometime difficult to be created by Open Nebula. It provides IaaS with more diversified and powerful functionalities.

Sonali Mishra,2018 introduced Hybrid Encryption and Decryption using Cryptography and Watermarking Technique for High Security Applications Detail presentation of a hybrid technique to implement data security in communication. In insecurity to data, are also being developed to look into the issues related to hacking, unethical sharing etc.

Elza Jintcharadze 2020 implementation Hybrid of Twofish, AES, ElGamal and RSA Cryptosystems Author have proposed the implementation and analysis of new hy- brid cryptosystems. Main objectives of this paper are to emphasize on better performance, maximum speed of an algorithm, checking effectiveness and comparison with other algorithms .At the decryption process follows opposite difficult order of the encryption process.

## 3. PROPOSED SYSTEM

Secure Record Capacity Framework in Cloud Computing utilizing cryptography emerges from the expanding dependence on cloud administrations for record capacity and collaboration. With the multiplication of information breaches and security concerns, organizations and people require a arrangement that guarantees the secrecy, judgment, and controlled get to of their put away records. By leveraging cryptographic methods such as encryption and unscrambling, the framework ensures touchy information from unauthorized get to, secures record transmission, and avoids altering. It too consolidates strong get to controls, key administration hones, and review trails to uphold authorized get to and keep up information security. The Secure Record Capacity Framework gives a dependable and secure arrangement that addresses the require for information security, compliance with controls, and relieving dangers related with putting away records within the cloud.

### 3.1 Data design

The database within the Secure Record Capacity Framework in Cloud Computing utilizing cryptography serves as a central store for putting away metadata, client accreditations, get to control information, encryption keys, and review logs. It safely stores file-related data, encourages client confirmation, upholds get to control, oversees encryption keys, and keeps up a record of framework occasions. The database guarantees information astuteness, privacy, and proficient record recovery, supporting the by and large security and usefulness of the framework.

### 3.2 System Modules

#### 3.2.1 User Module

1. User Authentication:
This module confirms the character of clients getting to the framework, guaranteeing that as it were authorized people can perform operations. It may include login accreditations, multi-figure confirmation, or biometric confirmation strategies to upgrade security.
2. File Encryption:
This module empowers clients to scramble their records some time recently uploading them to the cloud. Clients can select encryption calculations, key sizes, and create encryption keys for securing their records. The module ought to give an instinctive interface for selecting records, indicating encryption parameters, and starting the encryption prepare.
3. File Transfer and Download:
This module encourages the consistent exchange of records between the user's gadget and the cloud capacity. It ought to give an instinctive interface for selecting records to transfer or download, showing advance, and guaranteeing the keenness of exchanged records.
4. Key Administration:
This module helps clients in overseeing their encryption keys safely. It may incorporate choices for producing and putting away encryption keys, as well as pivoting or denying keys when vital. Clients ought to be able to get to and oversee their encryption keys through a user-friendly interface.
5. File Metadata and Organization:
This module makes a difference clients oversee and organize their records viably. Clients ought to be able to include metadata, such as record portrayals, labels, or names, to encourage looking and categorization of records. It may incorporate highlights like record versioning, organizer creation, and record sharing alternatives.
6. Secure Sharing and Collaboration:
This module permits clients to safely share records with other authorized people. Clients ought to be able to set consents and get to levels for shared records, guaranteeing controlled and secure collaboration. Highlights like secure record joins, watchword protection, and close dates for shared records can improve security.
7. File Keenness Checking:
This module empowers clients to confirm the judgment of their records put away within the cloud. Clients can start judgment checks to distinguish any unauthorized adjustments or tampering of their records. The module ought to give notices or cautions when keenness issues are identified.
8. User Get to Control:
This module permits clients to oversee get to authorizations for their put away records. Clients can characterize who can get to, see, alter, or erase their records, guaranteeing granular control over information get to. It ought to give an natural interface for overseeing client permissions and get to rights

#### 3.2.2 Developer Module

1. Encryption and Decoding Module:
This module actualizes the encryption and decoding calculations, such as AES or RSA, to convert records between plaintext and cipher text. It gives capacities or classes to perform n keys. The module ought to handle the fundamental scientific operations and guarantee the keenness and privacy of the information.
2. Key Administration Module:
This module centres on the era, capacity, and administration of encryption keys. It incorporates capacities or classes for creating solid and irregular encryption keys of different key sizes. The module ought to give secure capacity components for encryption keys, guaranteeing their accessibility when required for encryption and decoding forms. Key turn, key disavowal, and key dissemination instruments may too be actualized in this module.
3. Authentication and Authorization Module:
This module handles client verification and authorization forms. It incorporates capacities or classes for approving client accreditations, such as usernames and passwords. The module coordinating with confirmation frameworks, such as LDAP verify user identities client personalities. It moreover oversees client parts and authorizations, guaranteeing that as it were authorized clients can get to and adjust records.
4. Cloud Capacity Integration Module:
This module empowers interaction with the cloud capacity benefit where records are put away. It incorporates capacities or classes to transfer, download, and oversee records inside the cloud capacity. The module handles secure communication with the cloud capacity supplier, guaranteeing the privacy and judgment of information amid exchange. It may actualize APIs or SDKs given by the cloud capacity supplier to coordinate the framework with the chosen cloud stage.
5. Error Discovery and Adjustment Module:
This module centres on guaranteeing information keenness and unwavering quality. It executes blunder discovery and adjustment codes, such as CRC or Reed-Solomon codes, to distinguish and recoup from information debasement or blunders. The module gives capacities or classes to encode

and translate information utilizing blunder redress codes, guaranteeing the judgment of put away records**.**

**3.3Architectural Design**

The engineering plan for the Secure Record Capacity Framework in Cloud Computing utilizing cryptography incorporates components such as the client interface, encryption module, key management, cloud capacity integration, decoding module, get to control and verification, security checking and review, and compliance contemplations.

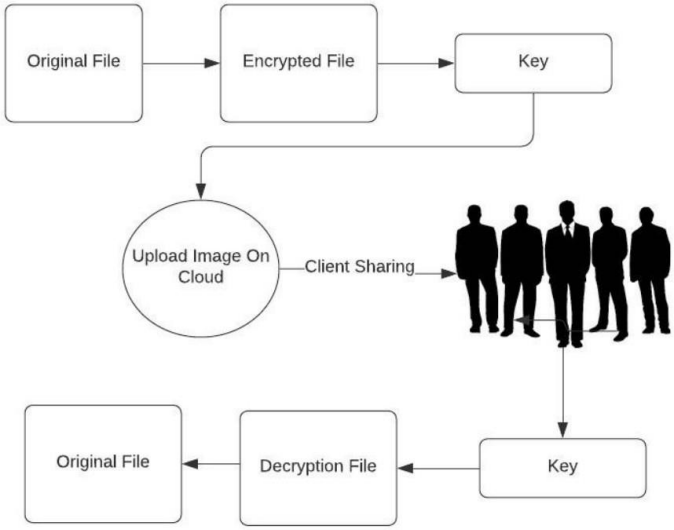


Fig 1: System Architecture

It gives a user-friendly interface for secure record transfer and download, scrambles records utilizing solid encryption algorithms, oversees encryption keys safely, coordinating with cloud capacity suppliers, decodes records for authorized clients, implements get to control and verification, screens security and logs exercises, and guarantees compliance with information security controls.

**4. Algorithms**

**4.1 Advanced Encryption Standard (AES)**

The Advanced Encryption Standard (AES) is a widely used symmetric encryption algorithm that is capable of securing sensitive data. It was selected by the U.S. National Institute of Standards and Technology (NIST) as a replacement for the older Data Encryption Standard (DES) algorithm. AES operates on blocks of data and uses a secret key to perform encryption and decryption. The algorithm works by applying a series of substitution and permutation operations on the input data using the key. It consists of several rounds, with the number of rounds depending on the key size. AES supports key sizes of 128, 192, and 256 bits. Here is a high-level overview of the AES encryption process:

1. Key Expansion: The original key is expanded into a set of round keys. The number of round keys generated depends on the key size.
2. Initial Round: The input data is XORed with the first round key.
3. Rounds: AES performs a series of rounds, each consisting of four main operations:

a. SubBytes: A non-linear substitution is performed on each byte of the data using a substitution box (S-box).

b. ShiftRows: The bytes in each row of the data are shifted cyclically.

c. MixColumns: A mixing operation is applied to the columns of the data.

d. AddRoundKey: The round key for the current round is XORed with the data.

4. Final Round: The final round omits the MixColumns operation.

5. Output: The resulting data after all the rounds is the encrypted data.

The decryption process is essentially the inverse of the encryption process, using the same round keys but applied in reverse order.

**4.2 Blowfish**

The Blowfish algorithm is a symmetric key block cipher designed by Bruce Schneier in 1993. It is a fast and secure algorithm used for encryption and decryption of data. Blowfish operates on fixed-size blocks of data (64 bits) and supports key sizes ranging from 32 bits to 448 bits, with 64-bit increments. Here's a high-level overview of the Blowfish algorithm:

1.Key Expansion: Blowfish uses the input key to generate a series of subkeys. The key expansion process involves applying the Blowfish encryption function multiple times to produce the subkeys.

2. Encryption/Decryption Rounds: Blowfish employs a Feistel network structure, which consists of multiple rounds. Each round consists of the following operations:

a. Data Split: The input block is split into two equal halves: the left half (L) and the right half (R).

b. Data Mixing: The data mixing step involves applying the Blowfish encryption function to the right half of the data (R) and XORing the result with the left half (L).

c. Swapping: After the data mixing, the left and right halves are swapped. This ensures that the left half becomes the new right half for the next round.

3. Final Round: The final round is a modified version of the encryption/decryption rounds without any swapping operation.

4. Output: The resulting data after all the rounds is the encrypted or decrypted data.

The core of the Blowfish algorithm is the Blowfish encryption function, which consists of several subroutines including data lookup in S-boxes, modular addition, and XOR operations. The S-boxes are precompiled and depend on the subkeys generated during the key expansion process. Blowfish is widely used in various applications, including secure file transfer, password hashing, and virtual private networks (VPNs). However, it has been largely replaced by newer algorithms such as AES in many security-sensitive systems**.**

## 3. CONCLUSIONS

The Secure Record Capacity Framework in Cloud Computing utilizing cryptography gives a vigorous and secure arrangement for putting away delicate information within the cloud. By utilizing encryption calculations and compelling key administration, it guarantees information privacy, astuteness, and genuineness. This framework offers improved

information security, compliance with controls, and farther record gets to whereas keeping up control over delicate information. The chosen AES and Blowfish calculations offer solid cryptographic properties and have been demonstrated to be dependable in securing information. By scrambling records locally some time recently transmission and utilizing secure communication conventions, the framework guarantees that information remains secret and secured from unauthorized get to amid transmission. Extend offers a strong arrangement for securing delicate information. By leveraging AES and Blowfish calculations, actualizing secure key administration, and conducting thorough security testing, organizations can unquestionably store and access their records within the cloud whereas moderating security dangers and protecting information secrecy and judgment.

## REFERENCES

[1] Tingyuan Nye and Tang Zhang ”An investigation of DES and Blowfish encryption al- gorithm, in Proc. IEEE Region 10 Conference, pp. 1-4 , 2021

[2] Rewagad, P., Pawar, Y. Use of Digital Signature with Diffie Hellman Key Exchange and AES Encryption Algorithm to Enhance Data Security in Cloud Computing. 2013 In- ternational Conference on Communication Systems and Network Technologies. 2013

[3] Kumar, A., Lee, B. G., Lee, H., Kumari, A. (2012). Secure storage and access of data in cloud computing. 2012 International Conference on ICT Convergence (ICTC).

[4] Jitendra Singh Adam et al.,” Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm” , International Journal of Advanced Research in Com- puter Science and Software Engineering ,vol. 2,Aug. 2012.

[5] Identity-based Encryption to Implement AntiCollusion Information Sharing Schemes in Cloud Computing Second International Conference on Applied Artificial Intelligence and Computing (ICAAIC 2023)IEEE Xplore Part Number: CFP23BC3-ART; ISBN: 978-1-6654-5630-2

[6] Boon Chian Tea, Muhammad Rezal Kamel Ariffin, Muhammad Asyraf Asbullah, Identity-Based Encryption Schemes – A Review, Journal of Multidisciplinary Engineering Science and Technology (JMEST) ISSN: 2458-9403 Vol. 6 Issue 12,

[7] [9] Ping, Z. L., Liang, S. Q., Liang, L. X. (2011). RSA Encryption and Digital Signa- ture. 2011 International Conference on Computational and Information Sciences.

[8] Enhancing Data Access Security in Cloud Computing using Hierarchical Identity Based Encryption (HIBE), IJSER journal, ISSN 2229-5518.

## BIOGRAPHIES

Mrs.Pooja Sameer Bhondve
Assistant Professor
Computer Engineering Department,
D Y Patil College Of Engineering
Akrudi, Pune

Ms.Supriya Sathe
Assistant Professor
Computer Engineering Department,
D Y Patil College Of Engineering
Akrudi, Pune