iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VI **Month of publication:** June 2023

DOI: https://doi.org/10.22214/ijraset.2023.54089

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VI Jun 2023- Available at www.ijraset.com

A Survey on Hybrid Cryptography for Secure File Storage on the Cloud

Ankit Chaudhari[1], Dr. P. R. Bhaladhare[2]
[1]*Sandip University, School of Computer Science & Engineering, Nashik, India*
[2]*HOD, Sandip University, School of Computer Science & Engineering, Nashik, India*

Abstract: ***This paper suggests the use of hybrid cryptography for safe cloud file storage and gives a software to implement it. To establish higher security measures, the application mixes symmetric and asymmetric encryption algorithms. The data is encrypted using symmetric encryption, and the symmetric key is encrypted using asymmetric encryption, guaranteeing that the data is encrypted using a unique key for each user while also protecting the key itself.***
The Advanced Encryption Standard (AES) algorithm is used for symmetric encryption, whereas the Rivest-Shamir-Adleman (RSA) method is used for asymmetric encryption. It has functions like user authentication, file upload/download, and key management. This study illustrates the efficacy of hybrid cryptography for protecting cloud-stored information and gives a framework for implementing it.
Keywords: Hybrid cryptography, cloud storage, file security, symmetric encryption, asymmetric encryption, Advanced Encryption Standard (AES), Rivest-Shamir-Adleman (RSA), key management.

I. INTRODUCTION

Hybrid cryptography is an encryption method that combines symmetric and asymmetric cryptographic methods to improve security and efficiency. In this study, we suggest the use of hybrid cryptography for safe cloud file storage. Because of its cost-effectiveness and simplicity, the cloud storage concept has grown in popularity in recent years. Yet, the security of data kept in the cloud remains a big worry, as unauthorized individuals can access the data if it is not adequately safeguarded.

The proposed system makes use of the strengths of both symmetric and asymmetric encryption to enable safe and efficient cloud file storage. To begin, the data is encrypted with a symmetric key technique, which delivers rapid and efficient data encryption and decryption. The symmetric key is then encrypted with an asymmetric key method, which increases security by guaranteeing that only authorized users have access to the key. This two-step encryption procedure maintains the efficiency of symmetric cryptography while providing a high level of security.

The suggested solution is intended to enable safe cloud file storage while simultaneously solving critical administrative concerns. The same key is used for both data encryption and decryption in classical symmetric key encryption. To prevent unwanted access to the data, the key must be kept hidden and safeguarded at all times. The symmetric key, on the other hand, is only utilized for encryption in the proposed system, and the encrypted key is kept on the cloud. This method ensures that the key is not kept in plain text and is safeguarded against unwanted access.

Overall, the suggested hybrid cryptography-based system offers a viable option for secure cloud file storage. The employment of a mix of symmetric and asymmetric encryption gives a high degree of security while retaining symmetric cryptography's efficiency. The method also addresses key management concerns by keeping the encrypted symmetric key in the cloud.

II. HYBRID CRYPTOGRAPHY

Hybrid cryptography is a technology that combines the advantages of both symmetric and asymmetric encryption methods in order to deliver a more secure and efficient data encryption solution. The same key is used for both encryption and decryption in symmetric cryptography, which implies that anybody with the key may decrypt the data. Asymmetric cryptography, on the other hand, employs two keys, one for encryption and the other for decryption.

Hybrid cryptography encrypts data with symmetric cryptography and employs asymmetric cryptography to securely exchange the symmetric key between the sender and recipient. This method offers the security benefits of asymmetric cryptography without the performance penalty of encrypting huge volumes of data. The symmetric key is only used once and then discarded, adding an additional layer of security.

In hybrid cryptography, the combination of symmetric and asymmetric cryptography gives a better degree of encryption and allows for the safe transfer of sensitive information. This method is widely employed in applications such as secure file transmission, email encryption, and online transactions. Hybrid cryptography is widely employed in modern cryptography and is regarded as one of the most effective data encryption methods.

A. Benefits of Hybrid Cryptography

1) Enhanced security
2) Efficient key management
3) Improved efficiency
4) High scalability
5) Flexibility and interoperability

B. File Storage using Hybrid Cryptography

The system is made up of three components: Flask, SQL server, and encryption techniques. Flask is used to provide a user-friendly, appealing, and convenient interface. The system runs on a cloud server, which stores and manages all files, user data, and accounts. For file security, they are encrypted with a hybrid technique, making it impossible for anybody to attack the files and assuring data protection.

The system operates by receiving requests from the Flask-created user interface. When a user makes a request, the data is encrypted with the cross-breed technique and delivered to the SQL server for storage. The SQL server is in charge of handling and storing all user data, including encrypted files. When a user requires access to the stored data, a request is made to the SQL server, and the encrypted data is obtained and decrypted using the cross-breed method. This method guarantees that the data is protected and that unauthorized persons cannot access it.

To summarize, the system employs Flask, SQL server, and encryption methods to create a user-friendly interface for securely managing and storing data on a cloud server. The data is encrypted with a hybrid technique, making it harder for unauthorized individuals to access it. The SQL server is in charge of maintaining and storing all data, ensuring that the data of the users is safe and quickly available when needed.

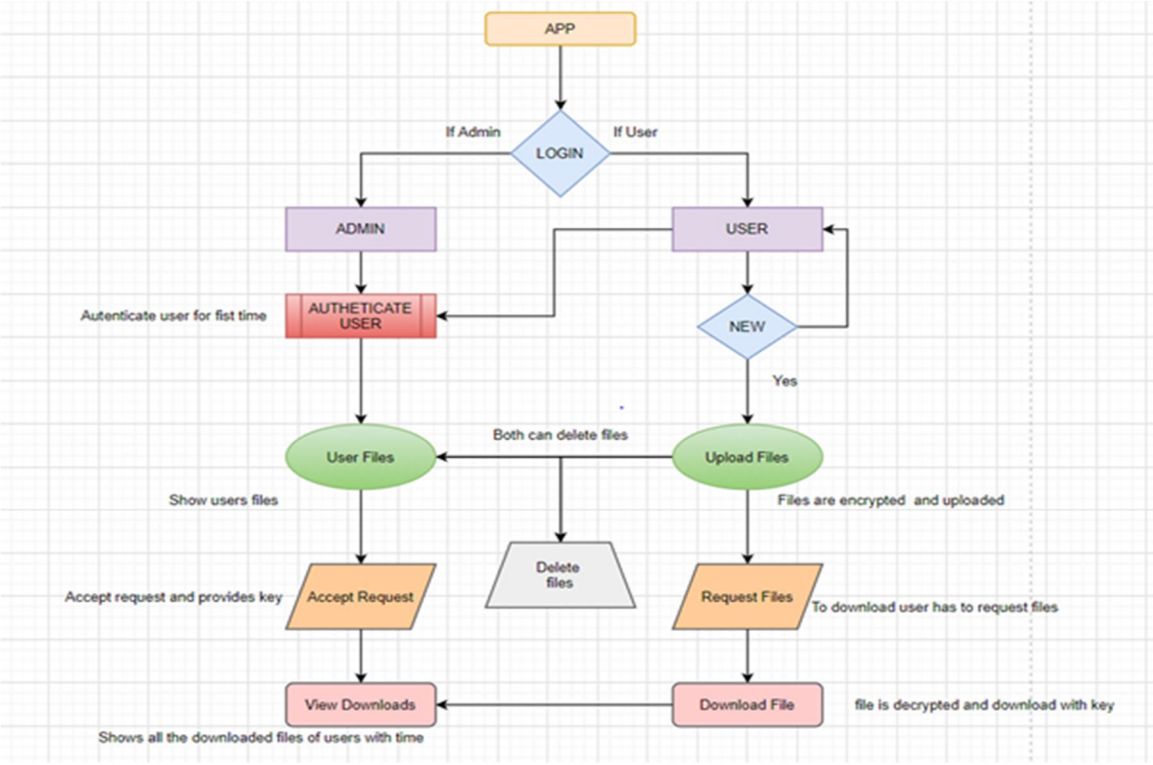


Fig. 1.1 Flowchart of system

III. HARDWARE/SOFTWARE USED

1) *Computer or Server:* A computer or server is required to host the hybrid cryptography system for secure file storage on the cloud.
2) *Storage Device:* Sufficient storage capacity is necessary to store the encrypted files securely. This can include hard drives, solid-state drives (SSDs), or cloud-based storage services.
3) *Network Infrastructure:* A stable and reliable network connection is essential to enable communication between the system and the cloud storage service.
4) *Operating System:* The system should be compatible with a preferred operating system such as Windows, macOS, or Linux.
5) *Web Server:* A web server software like Apache or Nginx is needed to host the application and provide access to users over the internet.
6) *Programming Language:* The chosen programming language, such as Python, should be installed on the system to develop the hybrid cryptography application.
7) *Development Framework:* Frameworks like Flask or Django can be utilized to facilitate the development and deployment of the system.
8) *Database Management System:* A database management system (DBMS) such as MySQL, PostgreSQL, or SQLite is required to store user credentials and metadata associated with encrypted files.
9) *Encryption Libraries:* Libraries or frameworks like OpenSSL or Cryptography can be employed to implement the hybrid encryption algorithms and cryptographic operations.
10) *Cloud Storage APIs:* APIs provided by the selected cloud storage service (e.g., Amazon S3, Google Cloud Storage) should be accessible to interact with the cloud storage infrastructure.
11) *Email Services:* If email confirmation or notifications are required, an email service provider like SMTP or SendGrid may be utilized.

IV. CONCLUSION

Hybrid cryptography provides a highly promising option for safe cloud file storage, successfully resolving cloud storage security problems. This technique delivers solid security, efficiency, and user-friendliness by combining the characteristics of symmetric and asymmetric encryption. It is a versatile and portable solution since it can be smoothly applied across numerous file types and cloud storage services that enable API-based file upload and download functions.

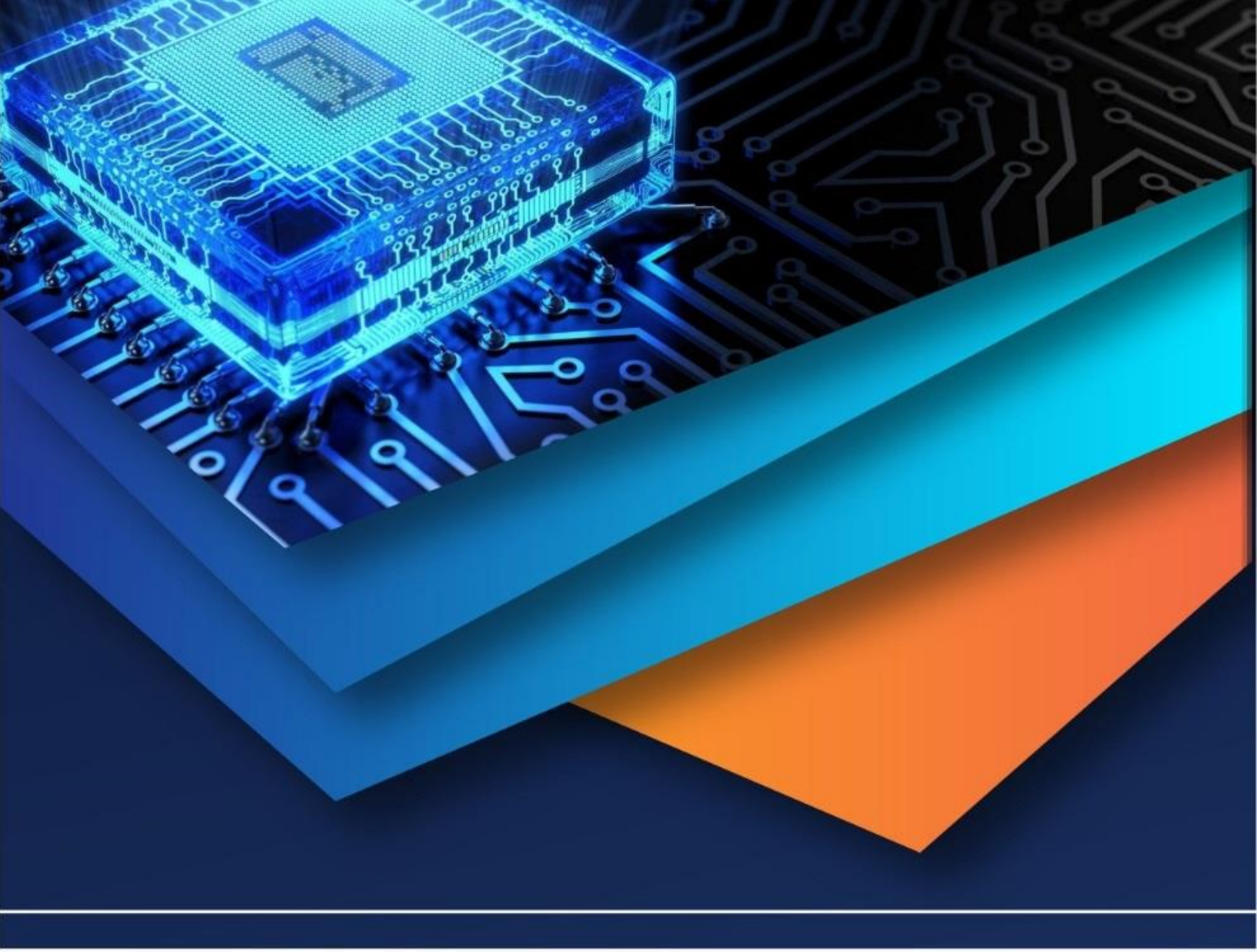
The solution provides a user-friendly interface, dependable storage, and safe encryption by using technologies such as Flask, SQL server, and sophisticated encryption algorithms. This protects data confidentiality and integrity, giving consumers and organizations confidence in cloud storage as a safe and trustworthy solution for their data storage needs.

Looking ahead, the future of hybrid cryptography for secure cloud file storage has promising promise. When combined with blockchain technology, an immutable record of data exchanges may be created, ensuring the authenticity and integrity of stored information. Incorporating multi-factor authentication may boost the approach's security even further, while employing machine learning algorithms allows for the monitoring of user behavior and the discovery of abnormalities, reinforcing protection against unauthorized access.

These developments will surely improve hybrid cryptography's security and efficiency, establishing its status as a trustworthy and trusted alternative for securely storing sensitive data in the cloud.

REFERENCES

[1] “A Hybrid Cryptography Approach Using Symmetric, Asymmetric and DNA Based Encryption” by Vikas Yadav, Manoj Kumar, 2023 3rd International Conference on Intelligent Communication and Computational Techniques (ICCT)
[2] “Secure File Storage using Hybrid Cryptography” by Putta Bharathi; Gayathri Annam; Jaya Bindu Kandi; Vamsi Krishna Duggana; Anjali T., 2021 6th International Conference on Communication and Electronics Systems (ICCES)
[3] “Secure File Storage on Cloud using Hybrid Cryptography” by Vivek Sharma; Abhishek Chauhan; Harsh Saxena; Shubham Mishra; Sulabh Bansal, 2021 5th International Conference on Information Systems and Computer Networks (ISCON)
[4] “Hybrid Cryptography for Cloud Computing” by Heena Kausar Khan; Rubika Pradhan; B. R. Chandavarkar, 2021 2nd International Conference for Emerging Technology (INCET)
[5] “Secure file storage in cloud computing using hybrid cryptography algorithm” by Punam V. Maitri; Aruna Verma, 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET)
[6] “A Secure Storage Service in the Hybrid Cloud” by Surya Nepal; Carsten Friedrich; Leakha Henry; Shiping Chen, 2011 Fourth IEEE International Conference on Utility and Cloud Computing



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY