ENHANCING CLOUD STORAGE SYSTEM FOR DYNAMIC CLOUD SECURE STORAGE APPLICATION

Mr. DINESH P S[1], AKSHYA SRI S[2], SAI PRASATH S[3], NISHA S[4]

[1] Assistant professor III, Computer Science and Engineering, BIT, Tamil Nadu, India
[2] Student, Electronics and Communication Engineering, BIT, Tamil Nadu, India
[3] Student, Computer Technology, BIT, Tamil Nadu, India
[4] Student, Computer Science and Technology, BIT, Tamil Nadu, India

ABSTRACT

The project "Enhancing Cloud Storage System for Dynamic Cloud Secure Storage Applications" aims to revolutionize the landscape of cloud storage by addressing the growing need for secure, dynamic, and efficient storage solutions in the era of digital transformation. In an increasingly interconnected world, where data is the lifeblood of businesses and individuals alike, the demand for flexible and secure cloud storage systems has never been greater. This project seeks to meet this demand by enhancing existing cloud storage infrastructure to cater to the evolving needs of dynamic cloud secure storage applications.

By leveraging cutting-edge technologies and innovative approaches, this project endeavors to optimize the performance, reliability, and security of cloud storage systems. Through the implementation of advanced encryption techniques, access control mechanisms, and dynamic data management protocols, the enhanced cloud storage system will provide a robust and resilient platform for storing sensitive and mission-critical data. Moreover, the project will focus on accommodating the dynamic nature of modern cloud applications, allowing for seamless scalability and adaptability to varying workloads and user demands.

Furthermore, the project aims to streamline the user experience by introducing intuitive interfaces and simplified management tools, empowering users to effortlessly navigate and administer their data within the secure cloud environment. With a focus on enhancing data integrity, confidentiality, and availability, this project endeavors to set new standards for cloud storage systems, ensuring that organizations and individuals can confidently embrace the benefits of cloud technology without compromising on security or performance.

In summary, the "Enhancing Cloud Storage System for Dynamic Cloud Secure Storage Applications" project represents a pivotal step towards shaping the future of cloud storage, offering a comprehensive and state-of-the-art solution to meet the evolving needs of secure and dynamic data storage in the cloud.

Keywords: *Dynamic storage systems, Encryption techniques, Data security, Hybrid cryptography, Data integrity, Data confidentiality, Cloud computing, Secure file storage, Data privacy.*

1. MODULE DESCRIPTION LOGIN/LOGOUT

In the module, the user can login by using their unique username and graphical password.

The login module verifies the user-given username and password with the stored username and password in the cloud.

Once the username and password are matched the user can access the resources

If it does not match the user is not allowed to access the resource.

1.1 UPLOAD/DOWNLOAD

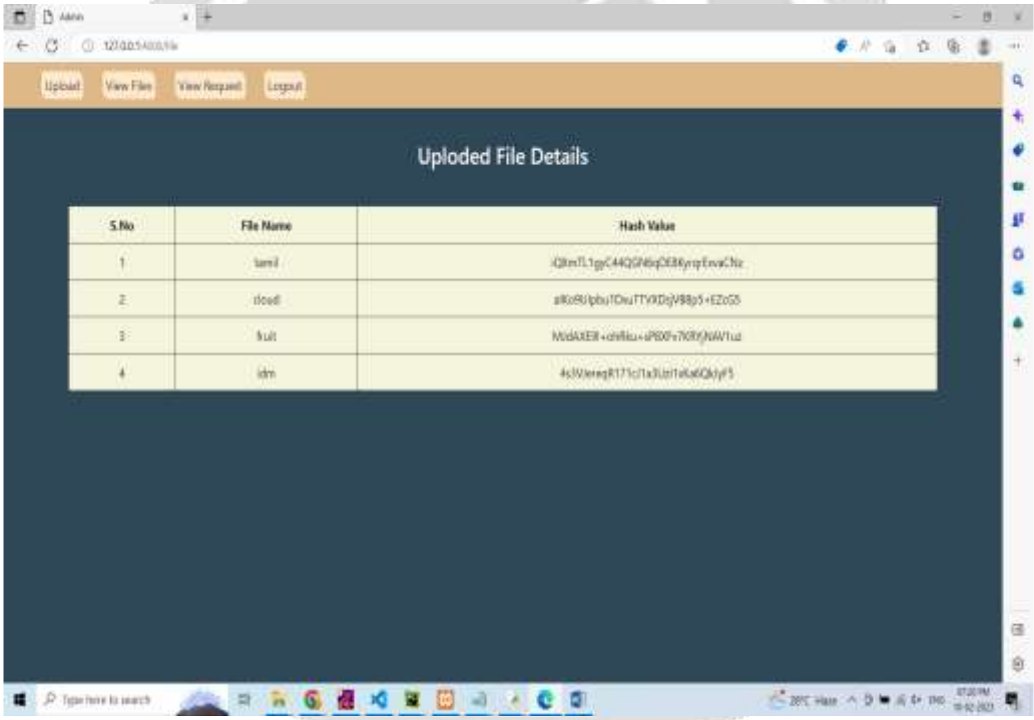
In this module, the buyer and seller can post the ads and also able to download the data that are posted by other sellers.
This module is mainly used to upload and also download big data files.

1.2 DATA DISPERSION

Two data sets can have the same mean but they can be entirely different thus to describe data, one needs to know the extent of variability.
This is given by the measures of dispersion. Range, interquartile range, and standard deviation are the three commonly used measures of dispersion.

1.3 ENCRYPTION

There are two basic encryption algorithms for cloud-based data: Symmetric encryption: The method is most commonly used for bulk data encryption.



Uploded File Details

S.No	File Name	Hash Value
1	tamil	iQltmTL1gyC44QGN6qDE8KyrqpEvaCNz
2	cloud	a8Ko9UlpbuTDwuTTVXDsjV8Bp5+EZoG5
3	fruit	MJdAXEB+chRku+iPB0Fv7KRYjNAW1uz
4	idm	4s3WereqR171c/1a3Uzi1eKa6QkdyF5

Chart -1: ENCRYPTION

2. PROPOSED METHODOLOGY

The main objective of the proposed mechanism is to secure cloud storage against data breaches, which may be the result of targeted attacks or management negligence in case hackers even some malicious administrators can steal user data.
Using a cloud secure storage mechanism named CSSM to store in the cloud.
CSSM uses data dispersion to divide uploaded files into several parts, and each part is called a fragment.
In the proposed secure user data using encryption technique. To reduce time overhead, 128 bit AES symmetric encryption algorithm is selected to implement the encryption and decryption for user data.

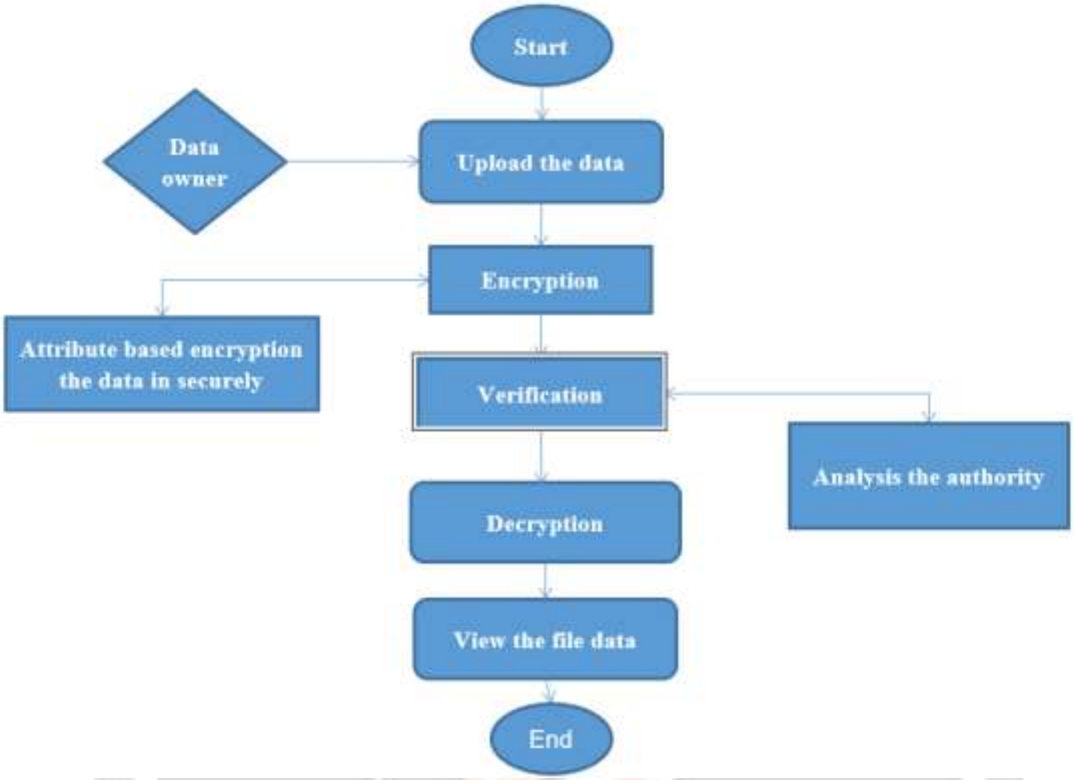


Chart -2: ENCRYPTION OF DATA

The first step is to create a page login user and the client can share the document and protect the document using CSSM.

The data owner (client) can upload the data using an ID and password. After verifying that they can upload the document, request for encryption. Encrypt by AES using CSSM model on AES. Which helps in more security.

After decryption by generating the same key and can view the file.

2.1 EFFECTIVE UTILIZATION OF MODERN TOOL

H/W SYSTEM CONFIGURATION:-

processor - Pentium – IV

RAM - 4 GB (min)

Hard Disk - 20 GB

S/W SYSTEM CONFIGURATION:-

Operating System: Windows 7 or 8

Software: python Idle

2.2 FEASIBILITY ANALYSIS

Feasibility analysis is an essential step in assessing the viability and potential success of a project. In the context of a study or project on cloud storage management with blockchain integration, a feasibility analysis would typically encompass various dimensions. Here are key aspects to consider in a feasibility analysis:

With a thorough feasibility analysis across these dimensions, project stakeholders can gain a comprehensive understanding of the project's viability, potential challenges, and opportunities

2.3 TECHNICAL ANALYSIS

Technical feasibility for a Cloud Secure Management System involves evaluating whether the proposed system can be effectively designed, developed, implemented, and integrated from a technical standpoint. Here are key aspects to consider

Evaluate the proposed architecture for the Cloud Secure Management System. Ensure that the architecture supports the required security features and scalability

Evaluate the effectiveness of security mechanisms such as encryption, access controls, and identity management.

Assess how well the system protects data both at rest and in transit.

3. RELATED WORK

The idea of hybrid cryptography is used to secure cloud storage systems. The differences between less secure and more secure systems are demonstrated using two alternative methods. The first method makes use of the RSA and AES algorithms; text or data encryption is done using AES and key encryption with RSA. The AES and Blowfish algorithms are employed in the second, or more secure, method. In contrast to the previous method, this one offers higher security since it uses two algorithms to give double encryption across both data and keys.

[1] Elliptic Curve Cryptography, or ECC, is used to secure centrally located cloud storage. With this method, encryption and decryption are done using a single key, and the client handles the entire process. This process includes the following steps: a. authentication; b. key creation; c. encryption; and d. decryption.

[2] The Elliptic Curve Cryptography (ECC) technology is used to secure centralized cloud storage. This method entails a single key for both encryption and decryption, with the client handling the entire operation. Steps including authentication, key generation, encryption, and decryption are all carried out by this process.

[3] combination of the MD5 and RSA algorithms to ensure several security features, including nonrepudiation, data integrity, and confidentiality. It generates encrypted keys using the RSA key generation technique for the encryption and decryption processes. The MD5 digest is used to process inputs up to 128 bits in length and produce padded outputs for use in the encryption and decryption processes.

[4] Cache manager is used in the implementation of a trusted storage system that uses the Encrypted File System (EFS) and NTFS file system disc to secure data files. Cryptographic systems are automatically used by EFS to encrypt stored files. The procedure is as follows: an application writes files to NTFS first, then caches the files and returns them to NTFS.

Following this, NTFS directs EFS to encrypt files before sending them to the disc.

[5] Three distinct servers are used to deliver the Cloud Storage Security Service: User Input, Data Storage, and User Output.

To make sure that the data is not harmed by a server failure, three separate servers are employed. The purpose of the User Input server is to store user files and input data while ensuring that no unauthorised parties can access the data by granting user authentication. The user input server receives the encrypted files once they are sent from the data storage server, which is where AES encryption is used to secure user input. The user output server is where users obtain their output files, or decrypted files, to be used for other purposes.

3.1 COMPARATIVE STUDY OF CLOUD STORAGE SYSTEMS

NO	TITLE	METHODOLOGY	LIMITATIONS
1	Secure storage and access of data in cloud computing	ECC (Elliptic curve cryptography) algorithm. Performs authentication, key generation, encryption, and decryption.	uses a single key for both encryption and decryption, reducing security.

2	Using a digital signature along with the Diffie-Hellman key exchange and the AES encryption technique to improve cloud computing data security	Diffie Hellman key exchange is used. The Digital Signature system provides authentication, and files encrypted with AES are the final step.	lengthy process because three distinct processes must be completed utilizing various ways.
3	RSA Cryptography and Electronic Signature.	Utilizing the RSA method in conjunction with MD5 Digest to guarantee cloud data security	Together with MD5, the RSA method only offers key encryption; it does not support multiple-text encryption.
4	File sharing and storage that is safe.	Functions for input, storage, and output are handled by different servers. Better security is provided by maintaining distinct modules.	There may be synchronization and connectivity issues because three separate servers are being used.

4. CONCLUSIONS

To sum up, the project "Enhancing Cloud Storage System for Dynamic Cloud Secure Storage Applications" is a big step forward in solving the ever-changing problems associated with dynamic and safe cloud data storage. The project focuses on improving access control mechanisms, dynamic data management protocols, and encryption techniques to strengthen the cloud storage infrastructure and guarantee data availability, confidentiality, and integrity. The project aims to enable businesses and individuals to safely store and manage their data in a dynamic cloud environment while easily adjusting to shifting workloads and user demands through the application of cutting-edge technologies and creative ways.

5. REFERENCES

[1]. Chinnasamy, P. and Deepalakshmi, P., 2018, April. Design of secure storage for health-care cloud using hybrid cryptography. In 2018 second international conference on inventive communication and computational technologies (ICICCT) (pp. 1717-1720). IEEE.

[2] Cao, S., Zhang, X. and Xu, R., 2020. Toward secure storage in cloud-based eHealth systems: a blockchain-assisted approach. IEEE Network, 34(2), pp.64-70.

[3] Ren, Y., Leng, Y., Qi, J., Sharma, P.K., Wang, J., Almakhadmeh, Z. and Tolba, A., 2021. Multiple cloud storage mechanism based on blockchain in smart homes. Future Generation Computer Systems, 115, pp.304-313.

[4] Zhou, Y. and Tang, Y., 2018, April. Application of Cloud Computing Technology on Computer Secure Storage. In 2018 3rd International Workshop on Materials Engineering and Computer Sciences (IWMECS 2018) (pp. 110-113). Atlantis Press.

[5] Sharma, S., Singla, K., Rathee, G. and Saini, H., 2020. A hybrid cryptographic technique for file storage mechanism over cloud. In First international conference on sustainable technologies for computational intelligence (pp. 241-256). Springer, Singapore.