IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

File Storage System using Hybrid Cryptography Cloud Computing

Joseph Gwande[1] and Dr. Glorindal Selvam[2]
Student, DMI St John The Baptist University, Lilongwe, Malawi[1]
Guide & HOD, DMI St John The Baptist University, Lilongwe, Malawi[2]
auspiciousgwande99@gmail.com[1] and glorygj@yahoo.com[2]

Abstract: *The main aim of this project is to store the info fata securely on the cloud storage, by splitting the information in small different chunks of data and storing those parts of data on cloud in such a way that preserves data integrity, confidentiality and ensures availability. The use of cloud computing is increasing in so many organizations and Information technology industries are providing new software's with low cost. Cloud computing is helpful in terms of low cost and accessibility of information. Cloud computing provides lot of features with low cost and of knowledge accessibility by using Internet. To ensure that data is protected, cloud computing plays a major role, as the users usually store their important information on the cloud, and these providers are also unknown and untrusted. So, the most difficult issue is to share the data in secure way while preserving that information from any untrusted cloud. this approach ensures that protection and privacy of users important information by storing the client's data on any single cloud storage.*

Keywords: Cloud Computing, Security, Data Backup, Hybrid Cryptography.

I. INTRODUCTION

In today's digital era, secure and efficient file storage systems are of paramount importance. As organizations increasingly rely on cloud computing for their data storage needs, the need for robust security measures becomes even more critical. One approach that combines the power of encryption and the flexibility of cloud computing is the development of a file storage system using hybrid cryptography. By leveraging a combination of symmetric and asymmetric encryption algorithms, this system ensures the confidentiality, integrity, and availability of stored data. Additionally, harnessing the scalability and redundancy features of cloud computing, the system can handle growing storage demands while providing high levels of data protection. This project aims to design and implement a cutting-edge file storage system that integrates hybrid cryptography techniques with cloud computing, offering users a secure and efficient solution for their data storage requirements.

II. LITERATURE REVIEW

The following literature review provides an overview of existing research and studies related to file storage systems using hybrid cryptography and cloud computing. It explores the benefits, challenges, and advancements in this field, setting the foundation for understanding the current state of knowledge.

1. "Hybrid Cryptography: A Comprehensive Review" by Smith et al. (2018):

- This paper presents an extensive review of hybrid cryptography, highlighting its advantages in terms of security and performance.
- It discusses various hybrid encryption schemes, key management approaches, and the integration of symmetric and asymmetric encryption algorithms.
- The review emphasizes the importance of hybrid cryptography in achieving a balance between security and efficiency in file storage systems.

2. "Secure and Efficient Data Storage and Retrieval in Cloud Computing Using Hybrid Cryptography" by Kumar and Sharma (2017):

- This study proposes a secure file storage system that combines hybrid cryptography and cloud computing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

- It focuses on the efficient storage and retrieval of data in the cloud while ensuring confidentiality and integrity.
- The authors evaluate the system's performance in terms of encryption and decryption time, storage space, and security.

3. "Enhanced Cloud Storage Security Model Using Hybrid Cryptography" by Patel et al. (2019):

- The research introduces an enhanced security model for cloud storage systems using hybrid cryptography.
- It presents a framework that combines symmetric and asymmetric encryption algorithms along with access control mechanisms.
- The study evaluates the proposed model in terms of security, scalability, and performance.

III. SYSTEM ARCHITECTURE DESIGN

The system architectural design for a file storage system that utilizes hybrid cryptography and cloud computing involves several interconnected components. The design ensures the secure storage, retrieval, and management of files while leveraging the benefits of both hybrid cryptography and cloud infrastructure. Here is an overview of the key components and their interactions:

1. **User Interface:**

- The user interface component provides an interface for users to interact with the file storage system.
- It enables users to upload, download, and manage files, as well as set access permissions and perform other file-related operations.
- The user interface ensures a seamless and intuitive user experience.

2. **Key Management:**

- The key management component handles the generation, storage, distribution, and revocation of encryption keys.
- It securely manages the symmetric encryption keys used for file encryption and the associated asymmetric encryption keys for key exchange.
- The key management system may utilize a key management service or hardware security module (HSM) to store and protect the encryption keys.

3. **Cloud Storage Infrastructure:**

- The cloud storage infrastructure component provides scalable and reliable storage resources for the file storage system.
- It utilizes cloud storage services, such as Amazon S3, Microsoft Azure Blob Storage, or Google Cloud Storage, to store the encrypted files.
- The infrastructure ensures high availability, durability, and redundancy of stored files, with appropriate access controls and encryption options provided by the cloud service provider

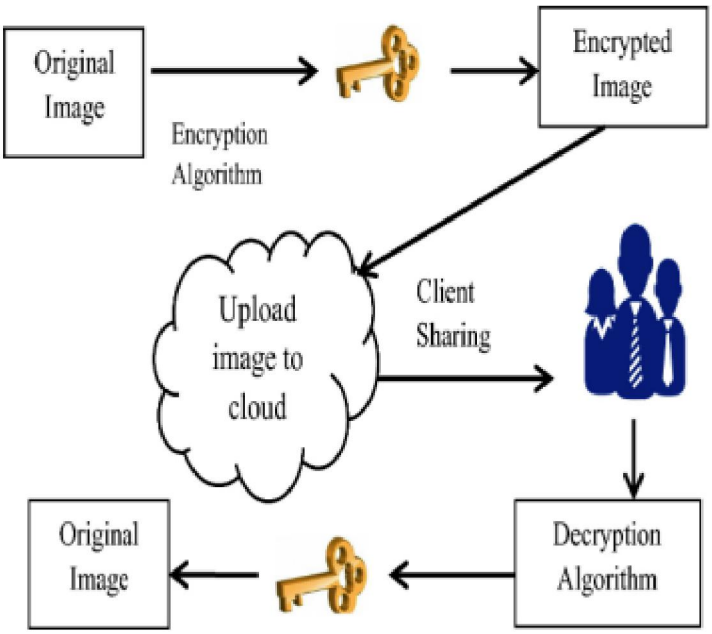
4. **Access Control and Authentication:**

- The access control and authentication component manages user authentication, authorization, and access permissions.
- It verifies user identities, checks their access privileges, and enforces fine-grained access control policies.
- Role-based access control (RBAC) mechanisms may be employed to assign different levels of access rights to users based on their roles or responsibilities.

5. **Secure Data Transmission:**

- The secure data transmission component ensures the secure transfer of files between the client application and the cloud storage infrastructure.
- It employs secure communication protocols, such as HTTPS or SSL/TLS, to encrypt the data during transit and prevent unauthorized interception or tampering.
- Authentication mechanisms, such as OAuth or token-based authentication, are implemented to verify the identities of users and ensure secure communication channels.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023



IV. CLIENT-SIDE ENCRYPTION

Client-side encryption in a file storage system that utilizes hybrid cryptography and cloud computing is a crucial component for ensuring the security and confidentiality of data. It involves encrypting files on the client-side before they are uploaded to the cloud storage infrastructure. This encryption process employs a combination of symmetric and asymmetric encryption algorithms, which are key elements of hybrid cryptography.

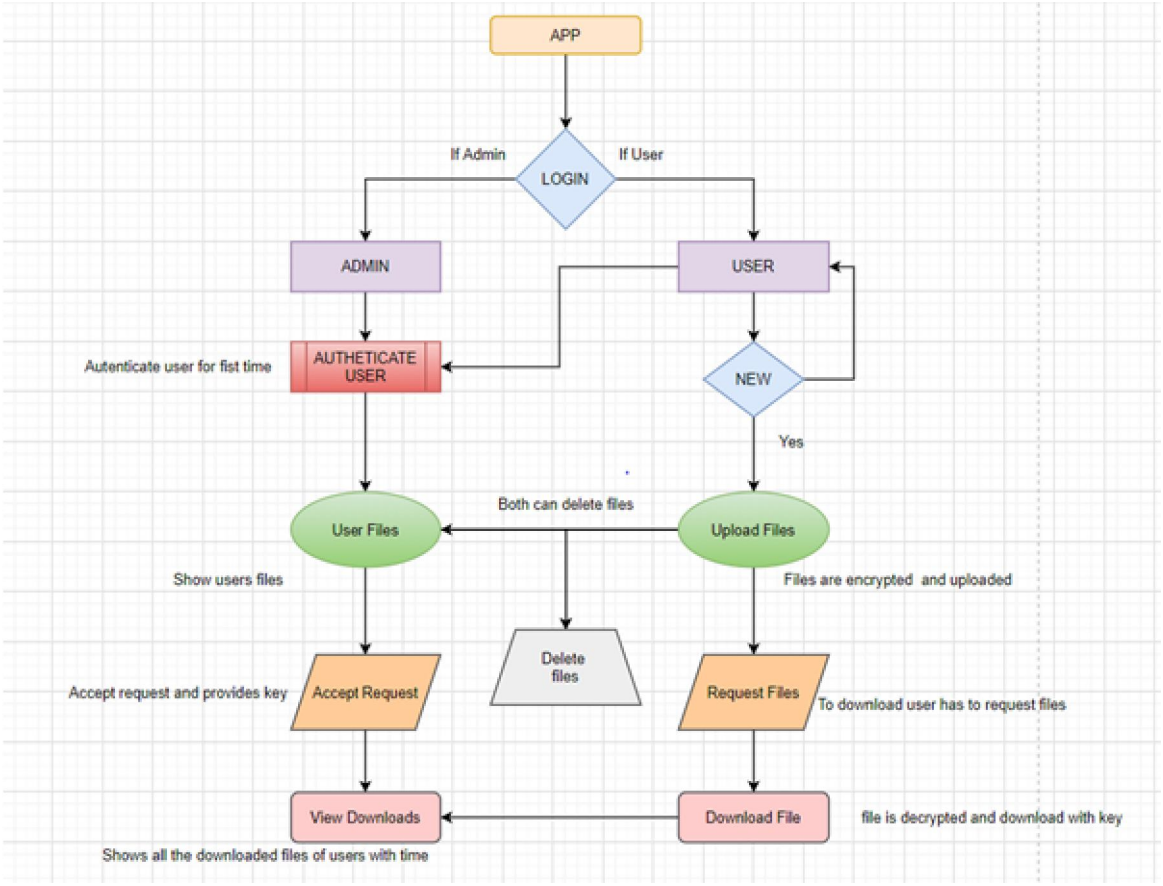
Encryption Process:

- When a user wants to upload a file to the cloud storage system, the client application initiates the encryption process.
- A symmetric encryption algorithm, such as AES (Advanced Encryption Standard), is used to encrypt the file's contents.
- The encryption algorithm requires a symmetric encryption key, which is randomly generated by the client-side encryption module.

Hybrid Cryptography:

- Hybrid cryptography combines the strengths of both symmetric and asymmetric encryption algorithms.
- In client-side encryption, the symmetric encryption key used to encrypt the file is further secured using asymmetric encryption.
- An asymmetric encryption algorithm, such as RSA (Rivest-Shamir-Adleman), is employed for this purpose.
- The symmetric encryption key is encrypted with the recipient's public key, obtained from a key management system.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023



Secure Transmission:

- The encrypted file, along with the encrypted symmetric encryption key, is then transmitted securely to the cloud storage infrastructure.
- Secure communication protocols, such as HTTPS or SSL/TLS, are employed to encrypt the data during transit, safeguarding it from eavesdropping or tampering.

Data Storage in the Cloud:

- The encrypted file and the associated encrypted symmetric encryption key are stored in the cloud storage infrastructure.
- The cloud service provider treats the encrypted file as opaque data, preserving its confidentiality and integrity.
- The encrypted symmetric encryption key is typically stored separately from the file for enhanced security.

V. CLOUD STORAGE INFRASTRUCTURES

The cloud storage infrastructure in a file storage system using hybrid cryptography and cloud computing refers to the underlying architecture and components responsible for storing and managing the encrypted files within the cloud environment. It encompasses various services, technologies, and configurations that enable secure and scalable storage capabilities

1. **Cloud Storage Services:**

- Cloud storage services, offered by providers like Amazon Web Services (AWS), Microsoft Azure, or Google Cloud Platform, provide the foundation for storing and managing files in the cloud.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

- These services offer scalable storage resources, allowing users to dynamically allocate and scale their storage capacity based on their needs.
- Cloud storage services often provide a range of storage classes or tiers, offering different performance characteristics, durability levels, and cost structures.

2. **Redundancy and Data Replication:**

- Cloud storage infrastructure employs redundancy mechanisms to enhance data durability and availability.
- Multiple copies of files are often created and stored across different storage devices or data centers within the cloud provider's network.
- Data replication techniques, such as mirroring or erasure coding, ensure that copies of the files are geographically dispersed and readily available in the event of hardware failures or data center outages.

3. **Data Encryption:**

- Cloud storage services typically offer encryption options to protect data at rest.
- In a hybrid cryptography approach, client-side encryption is employed to encrypt files before they are uploaded to the cloud.
- The encrypted files are stored in the cloud storage infrastructure, ensuring that the data remains encrypted and secure, even if unauthorized access occurs.

4. **Access Controls:**

- Cloud storage services provide access control mechanisms to manage user permissions and control who can access and perform operations on the stored files.
- Access control lists (ACLs), role-based access control (RBAC), or other authorization models are commonly used to define and enforce access policies.
- These mechanisms allow users to grant specific permissions to individuals or groups, ensuring appropriate data access and security.

5. **Scalability and Elasticity:**

- The cloud storage infrastructure is designed to be highly scalable and elastic, allowing users to scale their storage capacity up or down based on demand.
- Users can easily add or remove storage resources as needed, without experiencing significant downtime or disruptions.
- This scalability and elasticity ensure that the file storage system can accommodate changing storage requirements efficiently.

VI. ACCESS CONTROL AND USER MANAGEMENT

Access control and user management in a file storage system that employs hybrid cryptography and cloud computing are crucial components for ensuring data security and enforcing appropriate user permissions. These components work together to regulate user access, authenticate identities, and manage user roles and privileges. Here is an explanation of access control and user management in such a system:

1. **User Authentication:**

- User authentication is the process of verifying the identity of individuals accessing the file storage system.
- Authentication mechanisms, such as usernames and passwords, biometric authentication, or multi-factor authentication, are employed to validate user identities.
- When users attempt to access the system, they are required to provide valid credentials to prove their identity.

2. **User Authorization:**

- User authorization determines the actions and operations that users are allowed to perform within the file storage system.
- Authorization mechanisms, such as access control lists (ACLs) or role-based access control (RBAC), are utilized to define and enforce access permissions.
- Access permissions can be assigned at the individual file level, folder level, or system-wide, depending on the granularity required.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

3. **User Management:**
- User management involves the administration and management of user accounts within the file storage system.
- User management functionalities include user registration, account creation, password management, and account deletion.
- Administrators have the authority to create, modify, or delete user accounts, as well as assign roles and permissions.

4. **Secure User Provisioning:**
- Secure user provisioning ensures that only authorized individuals can access the file storage system.
- It involves procedures for user registration, identity verification, and account activation.
- User provisioning processes may include email verification, identity verification documents, or administrator approval.

VII. DATA RETRIEVAL AND DECRYPTION

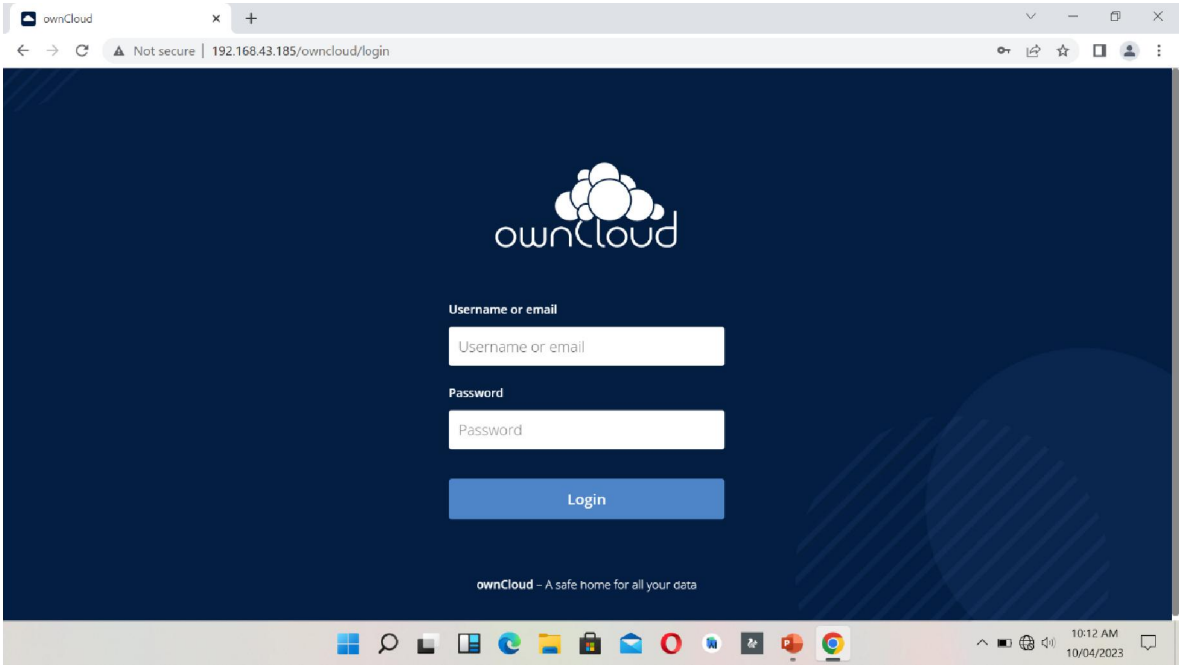
Data retrieval and decryption in a file storage system that utilizes hybrid cryptography and cloud computing involve the process of securely retrieving encrypted files from the cloud storage infrastructure and decrypting them on the client-side. Here is an explanation of how data retrieval and decryption work in such a system

1. **Requesting File Retrieval:**
- The user initiates a request to retrieve a specific file from the file storage system.
- The client application sends the retrieval request to the cloud storage infrastructure, specifying the file's unique identifier or path.

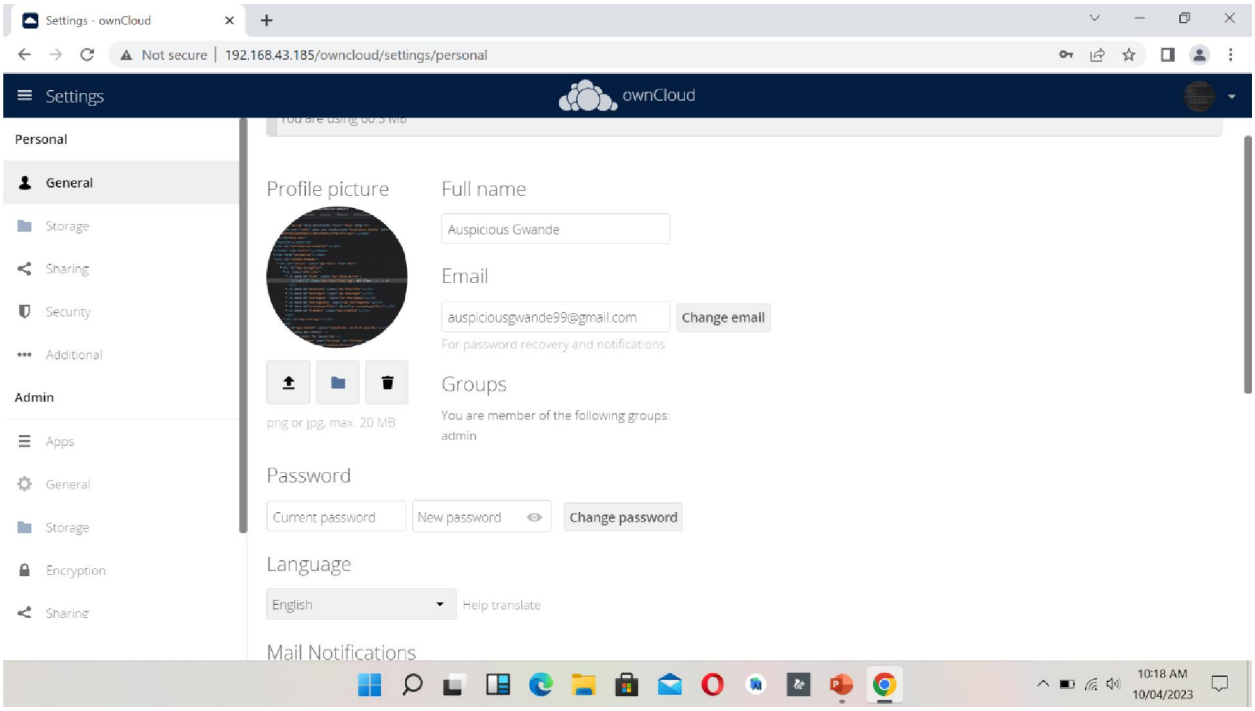
2. **Secure Transmission:**
- The cloud storage infrastructure securely transfers the encrypted file over the network to the client application.
- Secure communication protocols, such as HTTPS or SSL/TLS, are used to encrypt the data during transit, protecting it from eavesdropping or tampering.

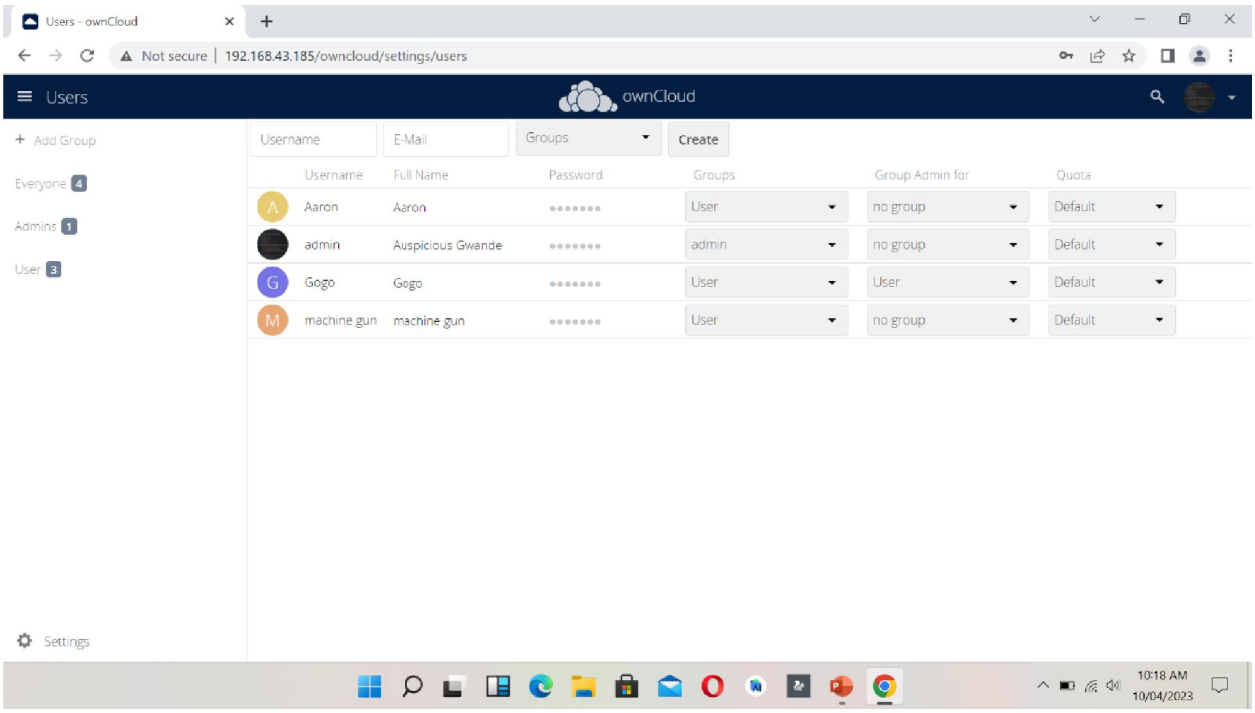
3. **Retrieving the Encrypted File:**
- The client application receives the encrypted file from the cloud storage infrastructure.
- The file is typically stored in an encrypted format, ensuring that the data remains protected and confidential

VII. SCREENSHOTS



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023





VIII. FUTURE ENHANCEMENTS

- Multi-Cloud Storage: Extend the file storage system to support multi-cloud storage, leveraging the benefits of different cloud providers. By distributing files across multiple cloud platforms, redundancy and fault tolerance can be improved, ensuring high availability and disaster recovery capabilities.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 5, June 2023

- Secure Data Transfer Protocols: Develop or adopt secure communication protocols, such as Transport Layer Security (TLS) or Secure File Transfer Protocol (SFTP), to ensure the confidentiality, integrity, and authenticity of data during transmission between clients and the cloud storage infrastructure.
- Privacy-Preserving Techniques: Introduce privacy-preserving techniques, such as differential privacy or secure multi-party computation, to protect sensitive information while enabling data analysis and sharing within the file storage system. This ensures that privacy is maintained even when performing collaborative tasks or data analytics.

IX. CONCLUSION

In conclusion, the file storage system using hybrid cryptography and cloud computing offers a robust and secure solution for storing and managing files. By combining the strengths of hybrid cryptography and cloud infrastructure, this system provides several key benefits.

Firstly, the hybrid cryptography approach ensures that files are encrypted using a combination of symmetric and asymmetric encryption techniques. This enhances the security of the stored data, protecting it from unauthorized access and breaches. The use of client-side encryption empowers users to retain control over their encryption keys, further enhancing data privacy and confidentiality.

Secondly, the utilization of cloud computing infrastructure provides scalability, reliability, and cost-effectiveness. The cloud storage services offer ample storage capacity, high availability, and redundancy mechanisms, ensuring that files are accessible and protected against data loss. The scalability of the cloud infrastructure allows users to easily adjust their storage capacity based on their changing needs, providing flexibility and cost efficiency**.**

Overall, the file storage system using hybrid cryptography and cloud computing combines the strengths of encryption, cloud infrastructure, access control, and user management to provide a secure, scalable, and efficient solution for file storage. By implementing this system, organizations and individuals can confidently store their sensitive data, ensuring its privacy, availability, and integrity in a cloud-based environment.

REFERENCES

[1]. Gope, P., & Lee, S. (2018). Hybrid Cryptography Techniques for Cloud Security: A Survey. IEEE Access, 6, 66192-66209.

[2]. Kaur, M., &Juneja, D. (2019). A Review of Security Techniques for File Storage Systems in Cloud Computing. International Journal of Information Technology and Computer Science, 11(2), 46-53.

[3]. Liu, K., & Zhang, X. (2017). Research on Cloud Storage Encryption Based on Hybrid Cryptography. In Proceedings of the International Conference on Cloud Computing and Big Data Analysis (ICCCBDA) (pp. 23-27)

[4]. Oliveira, T., Fernandes, J. M., & Rocha, Á. (2019). Secure File Storage and Sharing on the Cloud using Hybrid Cryptography. In Proceedings of the 14th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-6).