Secure File Storage With Hybrid Cryptographical And Fragmentation System

Mr. K. Krishna Reddy[1*], Sirikonda Srutha Sri[2], Lingagiri Srithajana Alwar[3], Murthy Kruthika Reddy[4], Soogoor Meghana[5],

[1*]Assistant Professor, Dept of CSE, Sreyas Institute of Engineering and Technology, krishnareddy@sreyas.ac.in
[2]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[3]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[4]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.
[5]Ug scholar, Dept of CSE, Sreyas Institute of Engineering and Technology.

***Corresponding Author:** Mr. K. Krishna Reddy
*Assistant Professor, Dept of CSE, Sreyas Institute of Engineering and Technology, krishnareddy@sreyas.ac.in

Abstract
When you are storing data in a public cloud, securing our data becomes a big challenge. Our data will be stored in remote cloud servers. We can access our cloud remotely. In this case, we must obey the provider license agreements. We need to trust the providers blindly. So, it is very important to secure our data with encryption. We are implementing a secure cloud storage system with AES, Triple DES, Blowfish algorithms by applying the fragmentation. The secret agencies can use our systems to share the information. In our project, we have the modules named Administrator, Data Owner, Data User and Cloud Server. The administrator will manage the data owner accounts, data user accounts, file access permissions. The administrator can monitor uploads and downloads. The data owner will upload the files into the system. We are applying double encryption on the file. The generated cipher text is going to be divided into seven fragments. These fragments will upload into the firebase cloud. The user can download the files by requesting the file key. The use will receive the key through email after a request processed by the data owner. If the key is valid the file will be downloaded. While downloading the seven fragments will combine as a single fragment and double description will apply on the file. The plain text will be downloaded as a text file. The cloud can track the uploads and downloads, the cloud can view data owners and data users details.

Keywords: Cryptography, Encryption, Cloud Computing, AES, Triple DES, Blowfish.

INTRODUCTION

In the digital era, the need for secure and reliable file storage solutions has become increasingly crucial. Confidential and sensitive information must be protected from unauthorized access and potential data breaches. To address these concerns, a secure file storage system that combines hybrid cryptographic techniques and fragmentation can provide enhanced security and privacy. The objective of this study is to propose a secure file storage system that utilizes a combination of cryptographic algorithms and fragmentation techniques to protect files from unauthorized access. By employing hybrid cryptography, the system ensures that files are encrypted using a combination of symmetric and asymmetric encryption algorithms, providing a multi-layered approach to data protection.

The system also incorporates fragmentation, which involves dividing files into smaller fragments and distributing them across multiple storage locations. This fragmentation process adds an additional layer of security by dispersing file fragments across different locations, making it challenging for attackers to retrieve the complete file even if they gain access to one or more fragments. The proposed system involves several key components and steps. Firstly, the file is encrypted using a symmetric encryption algorithm, which uses a single secret key to encrypt and decrypt the file. This ensures the confidentiality of the file's content. Next, the symmetric encryption key itself is encrypted using an asymmetric encryption algorithm, which employs a public-private key pair. The public key is used to encrypt the symmetric key, while the private key is kept securely by the file owner.

Additionally, the system fragments the encrypted file into smaller parts, each containing a portion of the original file. These fragments are distributed across different storage locations, such as cloud servers or decentralized storage networks. The fragmentation process can be customized based on specific security requirements, such as the number of fragments and their distribution across storage locations. To retrieve the original file, the authorized user must possess the private key associated with the asymmetric encryption algorithm. They can decrypt the symmetric key using the private key, and subsequently decrypt the file using the symmetric key. The retrieval process ensures that only authorized users with the proper encryption keys can access and reconstruct the original file.

The proposed system offers several advantages. Firstly, the hybrid cryptographic approach combines the strengths of symmetric and asymmetric encryption, providing robust security and efficient encryption and decryption processes.

Secondly, the fragmentation technique disperses file fragments, minimizing the risk of unauthorized access to the complete file even if some fragments are compromised. Lastly, the system can be tailored to specific security requirements, allowing customization of fragmentation parameters and storage location choices. In conclusion, the proposed secure file storage system with hybrid cryptographic and fragmentation techniques provides a comprehensive solution to protect files from unauthorized access and potential data breaches. By combining the strengths of encryption algorithms and fragmentation, the system ensures the confidentiality and integrity of stored files, enhancing overall data security in the digital environment.

LITERATURE SURVEY

Menezes, A. J., van Oorschot, P. C., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press. This comprehensive handbook provides an overview of various cryptographic techniques and their applications, including symmetric and asymmetric encryption algorithms. It serves as a valuable resource for understanding the fundamentals of cryptography. Zhang, R., Liu, L., & Sun, X. (2012). A Hybrid Encryption Scheme for Secure File Storage. In 2012 8th International Conference on Computational Intelligence and Security (pp. 926-929). IEEE. This paper proposes a hybrid encryption scheme for secure file storage that combines symmetric and asymmetric encryption algorithms. It presents an experimental evaluation of the proposed scheme and demonstrates its effectiveness in terms of security and performance. Zhang, Y., & Fu, S. (2018). Secure data storage based on hybrid cryptography and fragmentation technology. Future Internet, 10(10), 97. This research article proposes a secure data storage system that combines hybrid cryptography and fragmentation technology. It discusses the implementation details and evaluates the system's performance in terms of security and efficiency. Luo, C., Li, W., & Li, G. (2019). Research on Secure File Storage Technology Based on Hybrid Encryption and Fragmentation Technology. In Proceedings of the 2nd International Conference on E-Business and Internet (EBI 2019) (pp. 51-54). ACM. This conference paper presents a research study on secure file storage based on hybrid encryption and fragmentation technology. It discusses the design and implementation of the proposed system and provides insights into the security aspects and performance evaluation.

Wang, Q., Tang, Y., & Xiong, N. N. (2020). Secure file storage scheme based on hybrid encryption. Journal of Physics: Conference Series, 1661(1), 012076.

This article presents a secure file storage scheme based on hybrid encryption, combining symmetric and asymmetric encryption algorithms. It discusses the system architecture, encryption process, and performance analysis. Dasgupta, R., & Shrivastava, N. (2017). Secure file storage using hybrid cryptography. In Proceedings of the International Conference on Communication and Information Processing (pp. 134-139). Springer. This conference paper introduces a secure file storage system using hybrid cryptography. It discusses the encryption techniques employed and evaluates the system's security and efficiency.

Gencel, C., & Basaran, C. (2020). Enhanced secure file storage and retrieval mechanism with hybrid cryptography. Journal of Ambient Intelligence and Humanized Computing, 11(9), 4011-4022. This research article presents an enhanced secure file storage and retrieval mechanism with hybrid cryptography. It proposes a novel encryption scheme and evaluates the system's security and performance through experimental analysis. Jyothi, R., Prasad, M. V. N. K., & Naidu, M. S. (2020). Secure File Storage and Retrieval in Cloud Computing using Hybrid Cryptography. In 2020 6th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 422-427). IEEE. This conference paper focuses on secure file storage and retrieval in cloud computing using hybrid cryptography. It discusses the design and implementation of the proposed system and evaluates its security features and performance.

Parak, V., & Gondara, V. R. (2016). A survey on various data encryption algorithms. International Journal of Computer Applications, 145(4), 29-35. This survey article provides an overview of various data encryption algorithms, including symmetric and asymmetric encryption techniques. It offers insights into the strengths and weaknesses of different encryption algorithms, which can be relevant in the context of secure file storage systems. Wang, C., Xing, C., & Fang, Y. (2020). Secure file storage based on hybrid cryptography in cloud computing. Wireless Communications and Mobile Computing, 2020, 1-8. This research article presents a secure file storage system based on hybrid cryptography in the context of cloud computing. It discusses the system architecture, encryption mechanisms, and security analysis. These references provide a range of studies and research papers on secure file storage systems employing hybrid cryptographic and fragmentation techniques. They cover aspects such as encryption algorithms, system architecture, implementation details, and performance evaluation, offering insights into the design and effectiveness of such systems.

PROPOSED CONFIGURATION

Sharing data files on cloud becomes more complex as the access privileges increases and access restrictions becomes more difficult due to the sensitivity of data. A normal solution helps the data owner by using the public key encryption. This solution is not secure as the data owner needs to encrypt the data file once for each user who has being granted access then upload the cipher into cloud. The data users will take the encrypted parts of the file and use their private key for decryption. This method ensures that no unprivileged data user will gain access. Even then public key encryption becomes inefficient due to many encryptions and large storage. Therefore, we need to provide data owners with secure, and privilege-based method that allows them to share their data file among many data users while reducing cloud storage space to store encrypted data Nowadays clouds have become a very common platform in the internet world. Cloud computing provides many services in which storage as a service is one. When you are storing our data in a public cloud, securing the data becomes a big challenge. Our data will be stored on remote cloud servers. We can access cloud remotely. In this case, we have to obey the providers license agreements.

We need to trust providers blindly. So, it is very important to secure our data with encryption. We are implementing a secure cloud storage system with AES, Triple DES and Blowfish algorithms by applying fragmentation. The students and professors can use our system to share files securely.

In existing framework single calculation is utilized for information encode and unravel reason. Yet, utilization of single calculation isn't achieved elevated level security. On the off chance that we utilize single symmetric key cryptography calculation than we need to confront security issue on the grounds that in this kind of calculation applies a solitary key for information encode and interpret. So key transmission issue happens while sharing key into multiuser climate. Public key cryptography calculations achieve high security however most extreme postponement is required for information encode and translate.

Selectively sharing data files on the cloud becomes a burden on the data owner as the hierarchy grows (the access privileges increase in number) and/or as the access restrictions become more complex due to an increase in the sensitivity of the file segments. A trivial solution involves the data owner to use public key encryption. This solution would require the data owner to encrypt the same part of the data file once for each data user being granted access then upload the resulting cipher texts to the cloud. The data users would then fetch their uniquely encrypted parts of the file from the cloud and utilize their private keys to decrypt them. This method ensures that no unprivileged data user will gain access to any part of the data file even if that user is able to download the cipher texts from the cloud. However, on a large scale, public key encryption becomes an inefficient solution due to the increase in the number of encryptions and large storage spaces required. Therefore, the challenge is to provide the data owners with an efficient, secure and privilege-based method that allows them to selectively share their data files among multiple data users while minimizing the required cloud storage space needed to store the encrypted data segments.

- Requiring less network communication.
- We present multiple data file partitioning techniques and propose a privilege-based access structure that facilitate data sharing in hierarchical settings.
- A new security layer is added to encrypt the data of the task before transferring to the cloud side by using AES and Triple DES encryption technique.

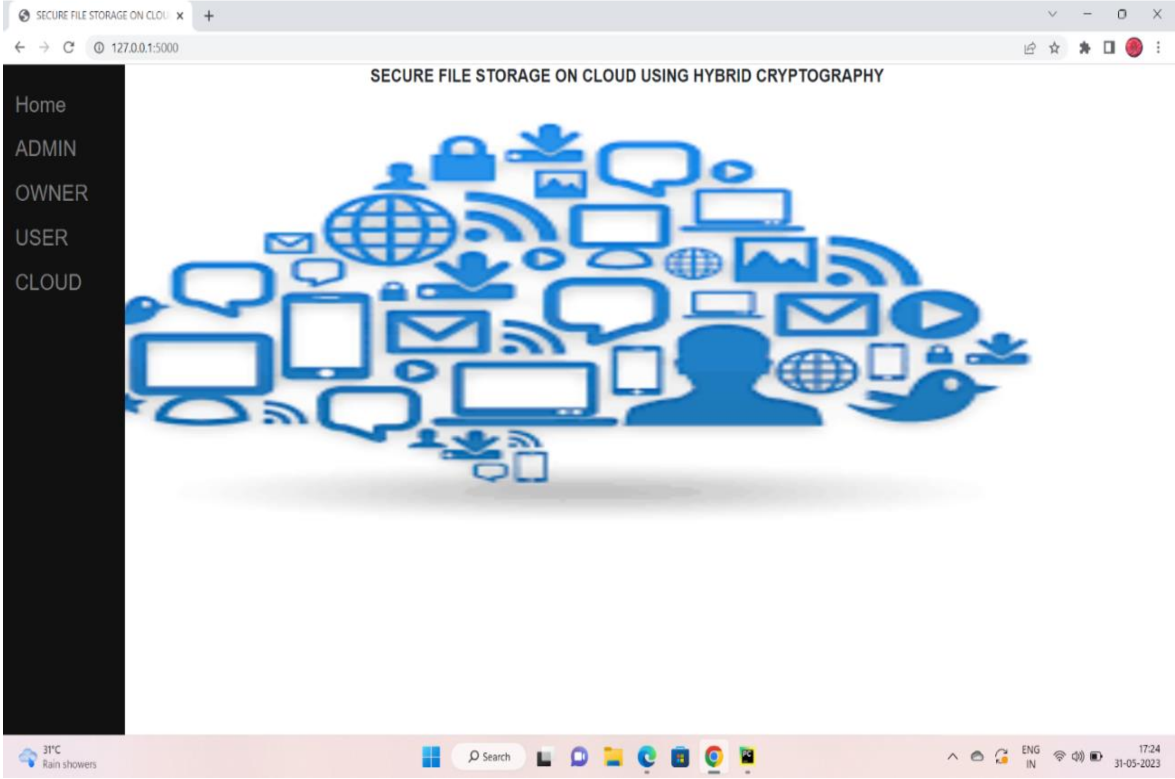
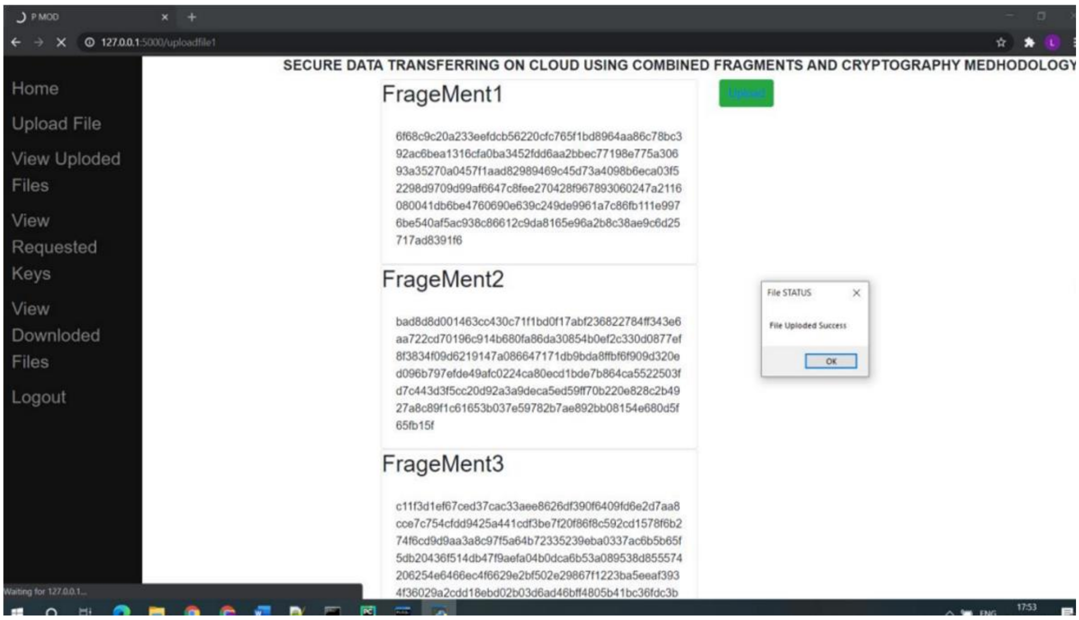

SECURE FILE STORAGE ON CLOU
127.0.0.1:5000
SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY
Home
ADMIN
OWNER
USER
CLOUD
31°C
Rain showers
Search
ENG
IN
17:24
31-05-2023

FIG 1. HOME PAGE



SECURE DATA TRANSFERRING ON CLOUD USING COMBINED FRAGMENTS AND CRYPTOGRAPHY MEDHODOLOGY

FrageMent1

```
6f68c9c20a233eefdcb56220cfc765f1bd8964aa86c78bc3
92ac6bea1316cfa0ba3452fdd6aa2bbec77198e775a306
93a35270a0457f1aad82989469c45d73a4098b6eca03f5
2298d9709d99af6647c8fee270428f967893060247a2116
080041db6be4760690e639c249de9961a7c86fb111e997
6be540af5ac938c86612c9da8165e96a2b8c38ae9c6d25
717ad8391f6
```

FrageMent2

```
bad8d8d001463cc430c71f1bd0f17abf236822784ff343e6
aa722cd70196c914b680fa86da30854b0ef2c330d0877ef
8f3834f09d6219147a086647171db9bda8ffbf6f909d320e
d096b797efde49afc0224ca80ecd1bde7b864ca5522503f
d7c443d3f5cc20d92a3a9deca5ed59ff70b220e828c2b49
27a8c89f1c61653b037e59782b7ae892bb08154e680d5f
65fb15f
```

FrageMent3

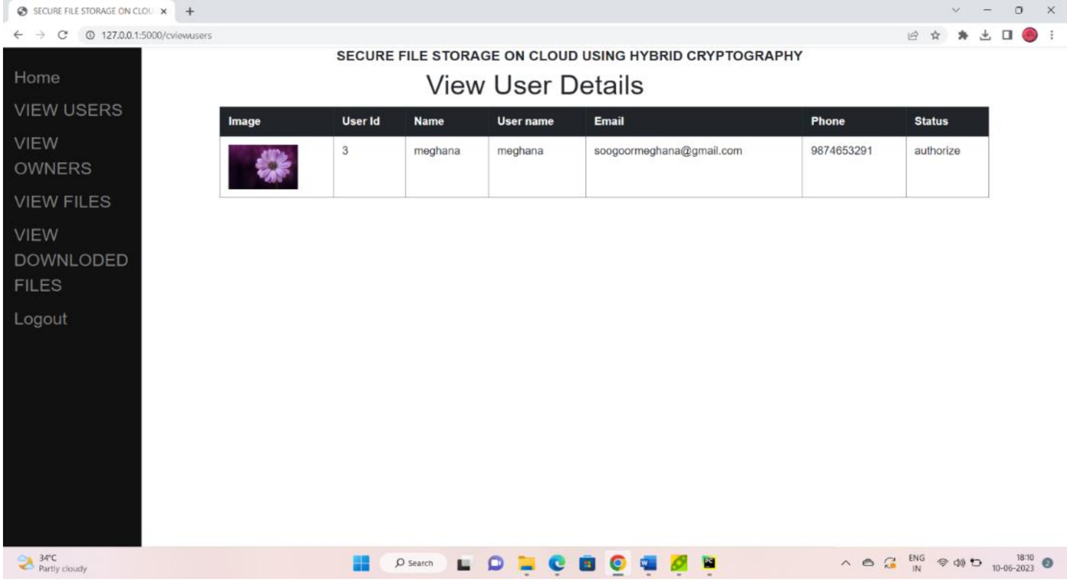
```
c11f3d1ef67ced37cac33aee8626df390f6409fd6e2d7aa8
cce7c754cfdd9425a441cdf3be7f20f86f8c592cd1578f6b2
74f6cd9d9aa3a8c97f5a64b72335239eba0337ac6b5b65f
5db20436f514db47f9aefa04b0dca6b53a089538d855574
206254e6466ec4f6629e2bf502e29867f1223ba5eeaf393
4f36029a2cdd18ebd02b03d6ad46bff4805b41bc36fdc3b
```

File STATUS

File Uploded Success

OK

FIG 2. OWNER FILE UPLOAD SUCCESS

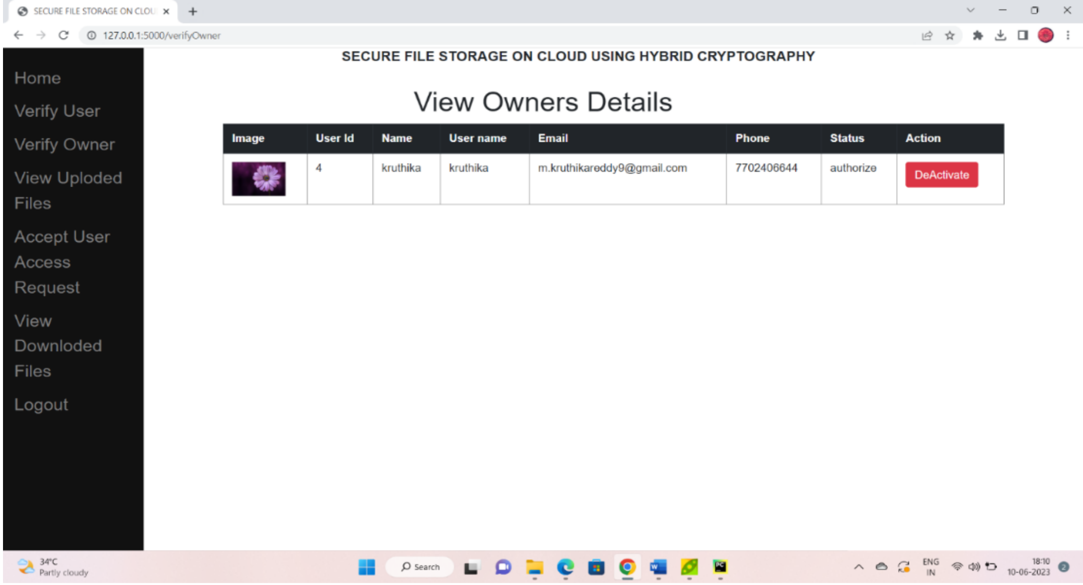


SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

View User Details

Image	User Id	Name	User name	Email	Phone	Status
	3	meghana	meghana	soogoormeghana@gmail.com	9874653291	authorize

FIG 3. CLOUD HOME PAGE

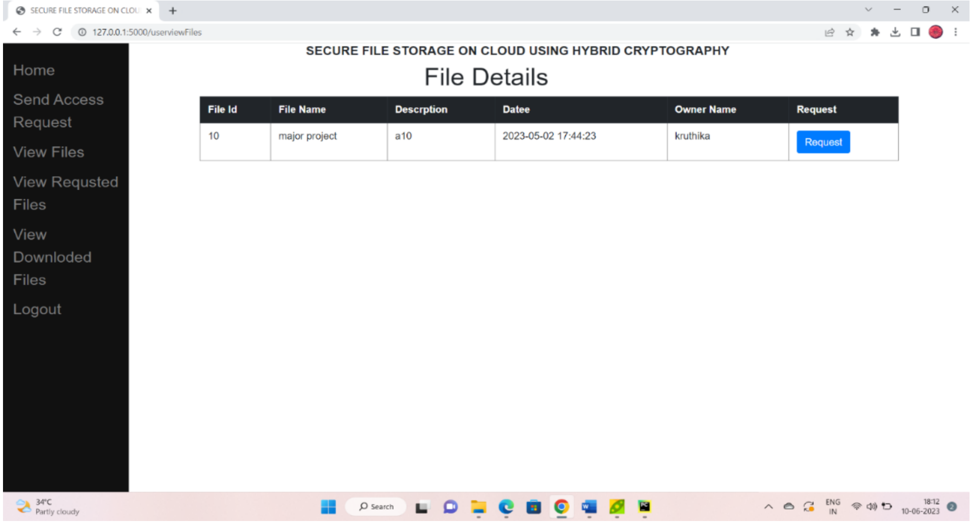


SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

View Owners Details

Image	User Id	Name	User name	Email	Phone	Status	Action
	4	kruthika	kruthika	m.kruthikareddy9@gmail.com	7702406644	authorize	DeActivate

FIG 4. ADMIN HOME PAGE

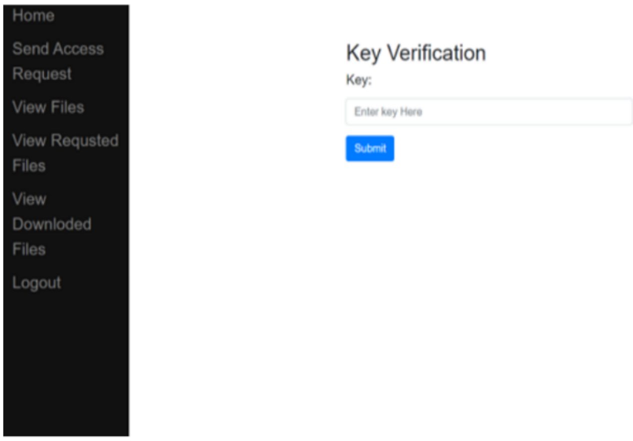


SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

File Details

File Id	File Name	Descrption	Datee	Owner Name	Request
10	major project	a10	2023-05-02 17:44:23	kruthika	Request

FIG 5. USER HOME PAGE

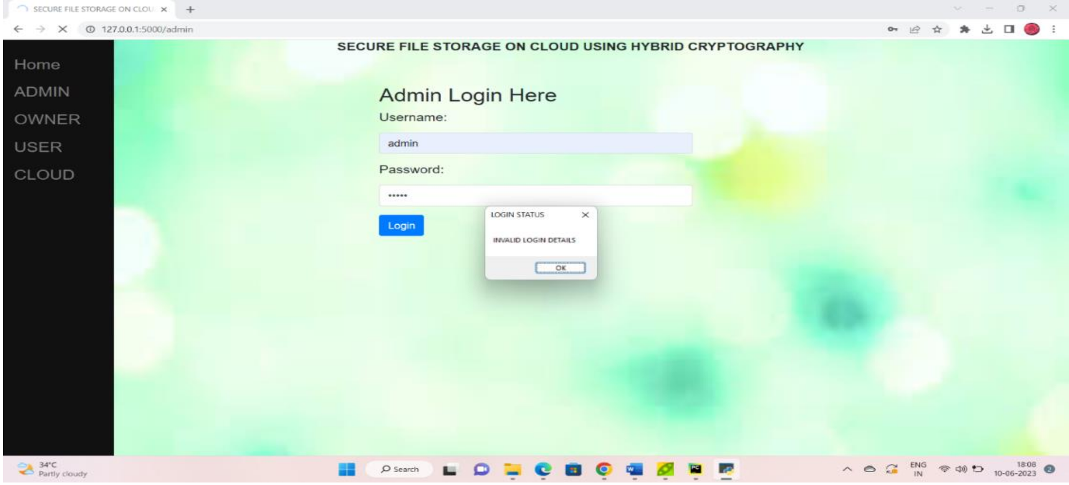


Key Verification

Key:

Enter key Here

FIG 6. KEY VERIFICATION TO DOWNLOAD THE FILE



SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

Admin Login Here

Username: admin

Password: •••••

LOGIN STATUS

INVALID LOGIN DETAILS

FIG 7. INVALID LOGIN DETAILS

ADVANTAGES OF PROPOSED SYSTEM

- More data storage needs turning over to the cloud, finding a secure and efficient data access structure has become a major research.
- Security techniques are applied in the protection of offloaded data from attacks.
- Once uploaded and shared, the data owner will not loses control over the data, opening the door to authorized data access

CONCLUSION

Our security model proves that we can provide hybrid security while storing the data in the public cloud. With this, irrespective of the cloud policies we can maintain security from our end. We can completely stop the hacking with conditional based double encryption. The key which we are providing for data users will work only for the particular user and particular file. We are not sharing original keys to the users and we are not storing the keys in the cloud. We are storing the file keys in our local database which we are using as mysql. So there is no chance of keys being stolen. our system will be suitable for a secret agency to share the information with the users. Our system is suitable where the security matters.

REFERENCES

1. Li, Y., & Chen, J. (2014). A hybrid cryptographic and fragmentation-based storage system for cloud computing. In 2014 IEEE 34th International Conference on Distributed Computing Systems Workshops (pp. 89-94). IEEE.
2. Qureshi, B., & Gupta, B. B. (2016). Secure storage in cloud computing using hybrid cryptography. In 2016 2nd International Conference on Next Generation Computing Technologies (NGCT) (pp. 251-256). IEEE.
3. Soh, B., Kumar, N., & Zhang, K. (2017). A hybrid cryptographic technique for secure file storage in cloud computing. Journal of Information Security and Applications, 34, 1-11.
4. Sharma, P., Sharma, A., & Sood, S. K. (2020). Hybrid Cryptography with Fragmentation for Secure File Storage. In 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 328-334). IEEE.
5. Parashar, M., & Singhal, S. (2019). Hybrid cryptographic algorithm with fragmentation for secure file storage in cloud computing. In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 29-33). IEEE.
6. Rani, R., & Bansal, R. (2020). Secure storage of data using hybrid cryptographic and fragmentation technique. In 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1426-1430). IEEE.
7. Kumar, A., & Rathore, N. S. (2017). Hybrid Cryptographic Approach with Fragmentation Technique for Secure File Storage. International Journal of Advanced Research in Computer Science, 8(5), 1477-1481.
8. Bahl, S., & Dahiya, K. (2021). A hybrid cryptographic approach for secure file storage using cloud computing. Journal of Ambient Intelligence and Humanized Computing, 12(3), 4007-4022.
9. Mittal, S., Aggarwal, M., & Khurana, R. (2016). Hybrid encryption technique for secure file storage in cloud computing. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 2344-2348). IEEE.
10. Sharma, S., & Jain, A. (2017). Secure file storage in cloud using hybrid cryptographic approach. International Journal of Computer Applications, 166(5), 32-36.
11. Saxena, S., & Verma, M. (2016). Secure file storage using hybrid cryptography in cloud computing. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom) (pp. 1065-1069). IEEE.
12. Verma, N., & Kumari, S. (2016). Hybrid cryptographic technique for secure file storage in cloud computing. International Journal of Advanced Research in Computer Science, 7(2), 244-248.
13. Sivakumar, V., & Sridhar, R. (2018). Hybrid encryption and fragmentation approach for secure file storage in cloud computing. In 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 183-187). IEEE.
14. Rana, S., Gahlot, M., & Kaushik, V. (2017). Secure file storage using hybrid cryptography with fragmentation in cloud computing. In 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
15. Patel, M. P., Patel, S. P., & Joshi, H. A. (2019). Secure file storage in cloud using hybrid encryption and fragmentation technique. In 2019 International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI) (pp. 1944-1949). IEEE.
16. Verma, K., & Bansal, M. (2020). Secure file storage in cloud computing using hybrid encryption and fragmentation. In 2020 International Conference on Smart Electronics and Communication (ICOSEC) (pp. 1-5). IEEE.
17. Nair, S. R., & Abraham, A. (2016). Hybrid cryptosystem with data fragmentation for secure file storage in cloud computing. In 2016 International Conference on Intelligent Systems and Signal Processing (ISSP) (pp. 71-76). IEEE.
18. Gupta, N., & Jain, R. (2016). Hybrid cryptographic algorithm for secure file storage in cloud computing. In 2016 3rd International Conference on Signal Processing, Computing and Control (ISPCC) (pp. 249-252). IEEE.
19. Pandey, S., & Malik, M. (2016). A hybrid cryptographic approach for secure file storage in cloud computing. In 2016 International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT) (pp. 199-202). IEEE.
20. Asadullah, S., & Ali, A. (2021). Secure file storage in cloud using hybrid cryptography and fragmentation technique. In 2021 International Conference on Advances in Computing, Communication Control and Networking (ICACCCN) (pp. 1-6). IEEE.