iJRASET
International Journal For Research in Applied Science and Engineering Technology

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

**Volume:** 12 **Issue:** V **Month of publication:** May 2024

**DOI:** https://doi.org/10.22214/ijraset.2024.61491

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 12 Issue V May 2024- Available at www.ijraset.com*

# Implementation of Personal Cloud using Cryptography

Aman Jain[1], Prof. Ritu[2], Chirag Saini[3]
*Department of CSE, Chandigarh University, Mohali, Punjab, India*

***Abstract:*** ***This Python-based personal cloud application leverages Flask and cryptography to establish a secure file storage system. Employing the Fernet encryption algorithm, the server encrypts uploaded files, ensuring data confidentiality. Users can securely upload, store, and download files, with each file automatically encrypted upon upload and decrypted for download. While this example prioritizes simplicity, a production-ready system should include robust user authentication, access controls, and further security enhancements. The abstract encapsulates the project's essence, highlighting its focus on file security within a personal cloud environment while acknowledging the need for additional features in a real-world deployment.***
***Keywords: Python, Flask, Cryptography, Personal Cloud, File Encryption, Fernet Algorithm, Secure File Storage***

## I. INTRODUCTION

In an age dominated by digital interactions and data-centric lifestyles, the demand for secure and accessible personal cloud solutions has become increasingly paramount. This project introduces a sophisticated Python-based personal cloud application, adeptly integrating the Flask web framework and cutting-edge cryptography techniques, with a specific emphasis on the Fernet algorithm.

The central objective of this application is to establish a robust and secure file storage system within the personal cloud paradigm. Leveraging the Flask framework, the application provides a user-friendly interface for seamless file uploads and downloads. The cryptography component, employing the Fernet algorithm, plays a pivotal role in ensuring data confidentiality. Every file uploaded to the cloud undergoes automatic encryption, guaranteeing that sensitive information remains shielded from unauthorized access. Correspondingly, files are decrypted seamlessly for download, providing users with a streamlined and secure experience.

While the project prioritizes simplicity for instructional purposes, it serves as a foundational framework for more comprehensive and production-ready personal cloud environments. The discussion underscores the imperative need for additional security features, including robust user authentication mechanisms and granular access controls. Recognizing the evolving landscape of digital security, the project lays the groundwork for the development of a secure, user-centric, and feature-rich personal cloud, addressing the nuanced demands of modern data storage and accessibility. Through this initiative, the intersection of Flask, cryptography, and personal cloud technology emerges as a promising avenue for secure and tailored file management solutions.

## II. LITERATURE SURVEY

In this research study, the author makes the argument that cloud computing's inability to protect user privacy and security Three key factors that clients lately took into consideration while signing up for cloud computing services are accessibility, keenness, and secrecy. Security lapses and instances of illegal access have been reported by several open and private cloud administrators. This document suggests that users encrypt their data before uploading it to a cloud storage platform such as Google Drive, Microsoft, Amazon, CloudSim, etc. The suggested cryptography computation was carried out on the advantage of Amazon S3 cloud space and is based on symmetric key cryptography demonstration.

This research study proposes a novel parallel cryptography protocol that reduces the time complexity by using DNA atomic structure, one-time-pad plot, and DNA collection method. The Internet of Things (IoT) could be a collection of web-enabled objects that use stationary sensors to collect and correlate data. In today's IT environment, cloud computing and the Internet of Things (IoT) are the key advancements achieving significant impact. Due to their intelligence and resemblance to all computing devices, they tend to use them more frequently in sophisticated situations. The stage known as IoT cloud is created by combining these developments. There is a need for information security regarding the devices that these advancements connect, as a result of their widespread use. There are various concepts that been proposed for security of information.

In this paper, the creator proposes a ponder of half breed cryptography has been performed from 2015 to early 2019. Papers related to the issue were looked and almost 20 were considered on the premise of sifting in this consider. Of these, eight (8) are based on a userfriendly unthinkable study and 12 are indepth overviews.

The most point of this review paper is to supply increasingly data to the modern analysts, understudies in this field conjointly unpracticed in cryptography. The inquire about hole recognized are ignoring of client verification and disgraceful usage of the cross breed calculations.

In this paper, a multilevel cryptography based cloud computing security framework was suggested. The method used in the demonstration is a hybrid of symmetric and deviated key cryptography computations. In order to provide multilevel encryption and unscrambling at both the sender and collector sides, RSA and the Data Encryption Standard (DES) are used in this, increasing the cloud's security. In order to reduce security risks, this security demonstration provides clarity to cloud clients and cloud service providers. The suggested demonstration is implemented using the cloudsim cloud test system device and Java. In comparison to the current framework, this demonstration increases information security to an unprecedented degree and speeds up the upload and download of content records.

This paper presents Cross breed (RSA & AES) encryption calculation to defend information security in Cloud. Security being the foremost vital factor in cloud computing needs to be managed with extraordinary safety measures. This paper basically centers on the three key tasks-secure Transfer of information on cloud, secure download of information, appropriate utilization and sharing of the open, private and mystery keys included for encryption and decoding. The utilize of a single key for both encryption and unscrambling is exceptionally inclined to pernicious assaults. But in crossover calculation, this issue is unraveled by the utilize of three isolated keys each for encryption as well as decoding. Moreover, the key era method utilized in this paper is one of a kind in its possess way. This has made a difference in dodging any chances of rehashed or excess key.

In this paper, the creator proposes a framework, at whatever point the proprietor transfers a record, it is named with a set of properties that incorporates office, work profile, department, involvement which is called as get to structure. After this time interim, date and area too included. The client can decode and download the record in the event that the time interim, date area and traits matches with the proprietor set traits. Some time recently this, specialist will check whether client is authorized to get to any of the record. To realize more security record is part into numerous parts concurring to record estimate and stored on different hubs rather than being put away on a single hub. The framework has made a confirmable calculation, an authorized client get to and point by point approach. It moreover gives us the ensure of the rightness of the designated computer comes about.

This term paper proposes that cloud computing is the most recent innovation within the field of disseminated computing. It gives different online and on-demand administrations for information capacity, arrange administrations, stage administrations, etc. Numerous organizations are apathetic approximately utilizing cloud administrations due to information security issues as the information dwells on the cloud administrations provider's servers. To address this issue, there have been a few approaches connected by different analysts around the world to fortify the security of the put away information on cloud computing. The Bi-directional DNA Encryption Calculation (BDEA) is one such information security method. Be that as it may, the existing procedure centers as it were on the ASCII character set, disregarding the non-English client of cloud computing. Hence, this proposed work centers on upgrading the BDEA to utilize with the Unicode characters.

PROBLEM FORMULATION:

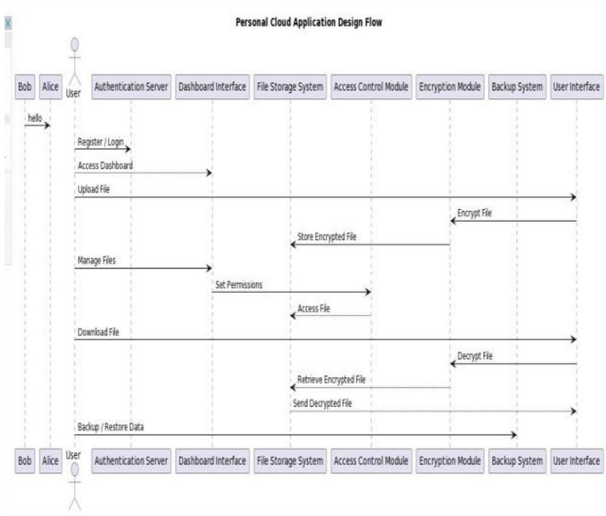
In contemporary digital environments, the absence of readily available, secure, and usercentric personal cloud solutions poses a significant challenge for individuals seeking to manage and access their files remotely. Existing cloud platforms often lack comprehensive security measures, exposing sensitive data to potential breaches. Moreover, the complexity of implementing encryption and authentication mechanisms hinders the seamless integration of these features into personal cloud applications. Consequently, there is a pressing need for a robust and accessible personal cloud system that combines the simplicity of use with state-of-theart cryptography to ensure data confidentiality. This project aims to address these challenges by developing a Python-based personal cloud application that employs the Flask web framework and Fernet cryptography for secure and efficient file storage, emphasizing userfriendly functionalities while maintaining a strong focus on data security and privacy.

## III. METHODOLOGY

### *A. Design Flow of the Model*

The design flow for the personal cloud application entails a seamless process beginning with user authentication through the Authentication Server. Upon login, users access the Dashboard Interface, which provides an intuitive overview of available features for file management. Files are uploaded securely via the User Interface and encrypted for confidentiality using the Encryption Module before storage in the File Storage System.

Access control is facilitated by the Access Control Module, allowing administrators to manage permissions and restrict file access. Users can collaborate by sharing files, and downloading files is facilitated through the User Interface, with decryption occurring before retrieval from storage. Automated backups and data recovery options are provided by the Backup System to ensure data integrity. With a user-friendly interface and robust security measures, including encryption, authentication, and access controls, the design flow prioritizes user experience and data security throughout the personal cloud application's functionalities.




## IV. OBSERVATION

The design flow outlined for the personal cloud application demonstrates a comprehensive and user-centric approach to addressing key functionalities required for effective file management in a cloud environment. The flow begins with user authentication, ensuring secure access to the application's features. The Dashboard Interface provides an intuitive overview, simplifying navigation for users. Encryption is employed to maintain data confidentiality during file upload and storage, enhancing security. Access control mechanisms offer administrators granular control over user permissions, ensuring data privacy. Collaboration features such as file sharing facilitate seamless teamwork among users. Additionally, the provision for file download and data backup contributes to a robust data management strategy, promoting data integrity and availability. The user interface is designed with usability in mind, prioritizing ease of use and navigation. Overall, the design flow effectively addresses the diverse needs of users in managing their files securely within a personal cloud environment.

## V. FUTURE SCOPE

1) Enhanced Security: Implement advanced encryption, multi-factor authentication, and intrusion detection.
2) Scalability: Optimize architecture for scalability and improve performance with caching and load balancing.
3) Collaboration: Enable real-time collaboration features and integration with IoT devices.
4) Cross-Platform Compatibility: Develop mobile and desktop applications for iOS, Android, and web browsers.
5) Blockchain Integration: Explore blockchain for decentralized storage and enhanced security.
6) AI-driven Features: Implement AI for intelligent file organization and security enhancements.
7) User Experience: Continuously refine UI/UX based on feedback and add personalized features.
8) Compliance: Ensure compliance with data protection regulations like GDPR and HIPAA.
9) Monitoring and Maintenance: Establish a robust monitoring and maintenance strategy for reliability and security.

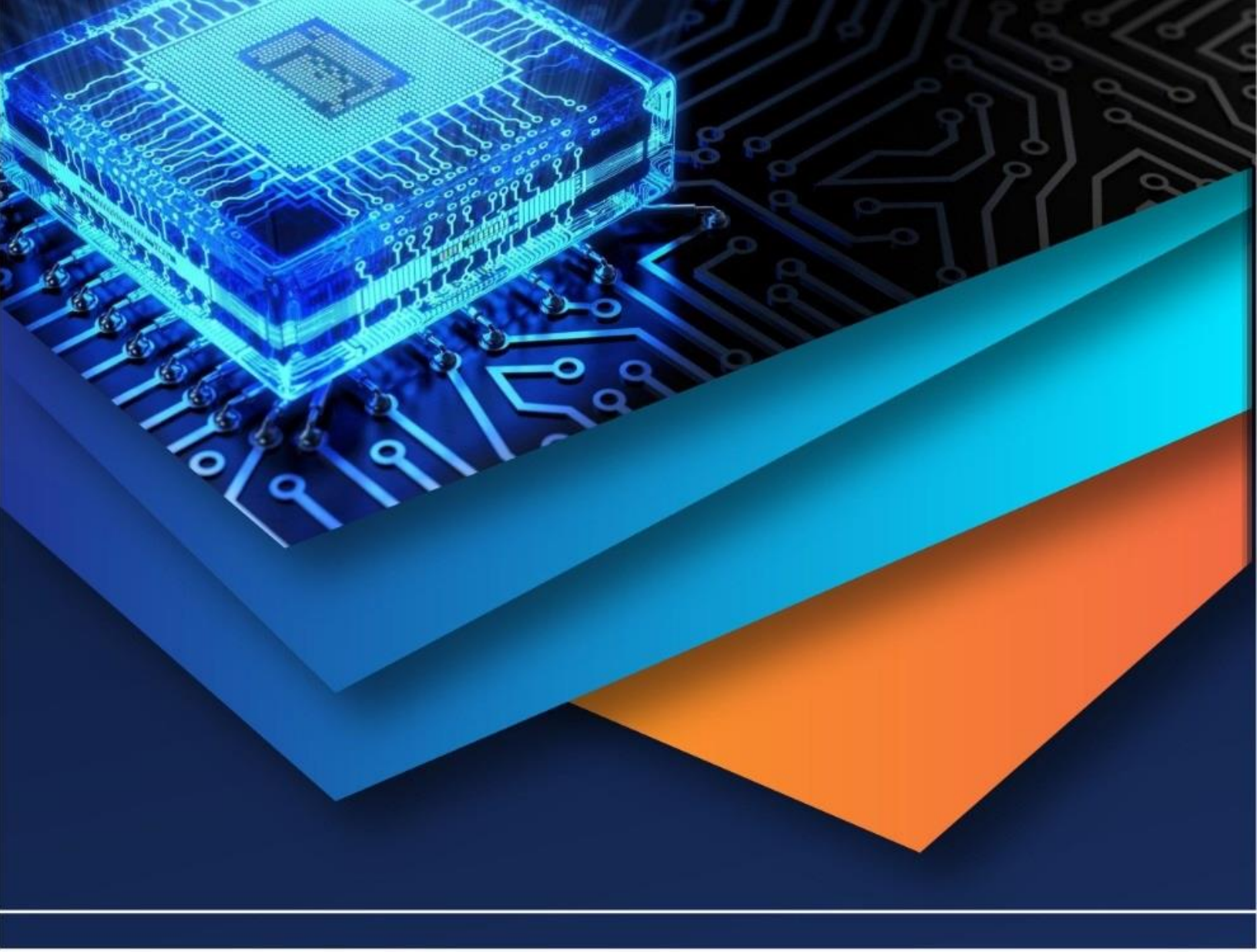
## VI. RESULT AND CONCLUSION

The design flow for the personal cloud application encapsulates a comprehensive approach to address the diverse needs of users in managing their files securely within a cloud environment. Key functionalities, including user authentication, file upload and storage, access control, collaboration features, and data backup, have been successfully integrated into the application's architecture. Security measures, such as encryption, authentication, and access controls, have been implemented to safeguard user data and ensure confidentiality. The user interface has been designed to prioritize usability and provide a seamless experience for users navigating the application.

The design flow presents a robust foundation for the development of a personal cloud application that meets the requirements of modern users in securely managing their files. By incorporating essential features and prioritizing security and usability, the application aims to enhance user productivity and data management efficiency. Moving forward, further enhancements and optimizations, such as scalability improvements, advanced security measures, and integration with emerging technologies, can be explored to continually enhance the application's functionality and meet evolving user needs. Overall, the design flow sets a solid framework for the development of a reliable, secure, and user-friendly personal cloud application.

## REFERENCES

[1] In the 2020 International Conference on Computing and Information Technology (ICCIT-1441), Tabuk, Saudi Arabia, pp. 1-4, S. A. Nooh, "Cloud Cryptography: User End Encryption," doi: 10.1109/ICCIT144147971.2020.9213745.
[2] Pandey, Gyan Prakash, Socket Programming and New Approach to Secure Cloud Data: Implementing DNA Cryptography in Cloud Computing and Using Huffman Algorithm (August 7, 2019). Accessible via SSRN at http://dx.doi.org/10.2139/ssrn.3501494
[3] In the 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-6, S. A. Ahmad and A. B. Garko, "Hybrid Cryptography Algorithms in Cloud Computing: A Review," doi: 10.1109/ICECCO48375.2019.9043254.
[4] "Cloud Security using Hybrid Cryptography Algorithms," S. Kumar, G. Karnani, M. S. Gaur, and A. Mishra, 2021 (doi: 10.1109/ICIEM51511.2021.9445377), 2nd International Conference on Intelligent Engineering and Management (ICIEM), London, United Kingdom, pp. 599–604.
[5] In the 2014 International Conference on Power, Automation and Communication (INPAC), Amravati, India, pp. 146-149, doi: 10.1109/INPAC.2014.6981152, V. S. Mahalle and A. K. Shahade, "Enhancing the data security in Cloud by implementing hybrid (Rsa & Aes) encryption algorithm."
[6] S. B. Javheri and S. Kute, "Implementation of Secure File Storage on Cloud with OwnerDefined Attributes for Encryption," in Proceedings of the Fourth International Conference on Computing, Communication Control and Automation (ICCUBEA), Pune, India, 2018, pp. 1-6, doi: 10.1109/ICCUBEA.2018.8697792.
[7] "LockNKey: Improvised Cloud Storage System using Threshold Cryptography Approach," A. Vats, P. Jimmy, A. Mishra, and A. D., 2022, 2nd International Conference on Emerging Smart Technologies and Applications (eSmarTA), Ibb, Yemen, pp. 1-6, doi: 10.1109/eSmarTA56775.2022.9935488.
[8] In the 2016 International Conference on Computer Communication and Informatics (ICCCI), Coimbatore, India, pp. 1-6, Prajapati
[9] Ashishkumar B. and P. Barkha, "Implementation of DNA cryptography in cloud computing and using socket programming," doi: 10.1109/ICCCI.2016.7479930.
[10] "Research and design of cryptography cloud framework," S. Lei, W. Zewu, Z. Kun, S. Ruichen, and L. Shuai, 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA), Chengdu, China, 2018, pp.147-154, doi: 10.1109/ICCCBDA.2018.8386503.
[11] Using hybrid cryptography and steganography, M. S. Abbas, S. S. Mahdi, and S. A. Hussien improve cloud data security (pp. 123–127; doi: 10.1109/CSASE48920.2020.9142072). 2020 International Conference on Computer Science and Software Engineering (CSASE),Duhok, Iraq, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

# INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY