Secure Cloud Simulator Using Cryptography and Python

Submitted by - Mallem Anil Kumar *O180677*

Under the Guidance of -

Mr. Mallikarjuna Nandi

Assistant Professor

Abstract -

The project, "Secure Cloud Simulator using Cryptography and Python," focuses on enhancing **Data Security** for users interacting with **Cloud Storage**. The application utilizes **Encryption Algorithms**, including Fernet and AES, to secure files before uploading them to AWS S3. It also incorporates a web app with features for file encryption, secure upload to the cloud, download, and decryption. The project leverages Python, Flask, Cryptography algorithms, and AWS cloud services. The primary goal is to provide users with a user-friendly and secure environment for managing their files in the cloud through effective encryption and decryption processes.

Purpose -

The purpose of my project, "Secure Cloud Simulator using Cryptography and Python," is to create a **User-friendly** and **Secure environment** for managing files in the **cloud**. By employing encryption algorithms like Fernet and AES, the application ensures that users can protect their sensitive data before uploading it to cloud storage, specifically **AWS S3**. The project aims to provide a seamless experience, allowing users to encrypt, upload, download, and decrypt files with ease while leveraging the capabilities of Python, Flask, cryptography algorithms, and AWS cloud services. The overarching goal is to enhance data security for users interacting with cloud storage platforms.

Technologies Used -

- Frontend - HTML, CSS, JS
- Backend - Flask, Python
- Cryptography - AES, Fernet
- Cloud - AWS S3

WorkFlow –

Simplified workflow of "Secure Cloud Simulator using Cryptography and Python":

- **User Registration and Login**
- **File Encryption**
- **Cloud Upload**
- **Cloud Storage**
- **Download from Cloud**
- **File Decryption**
- **Key Management**

Encryption Algorithms

Advanced Encryption Standard (AES) -

Widely utilized for its strength and efficiency, AES surpasses DES and triple DES. It operates as a **Block cipher** with key sizes of 128/192/256 bits, encrypting data in 128-bit blocks. AES relies on the substitution-permutation network principle, involving a series of linked operations that replace and shuffle input data, providing robust security.

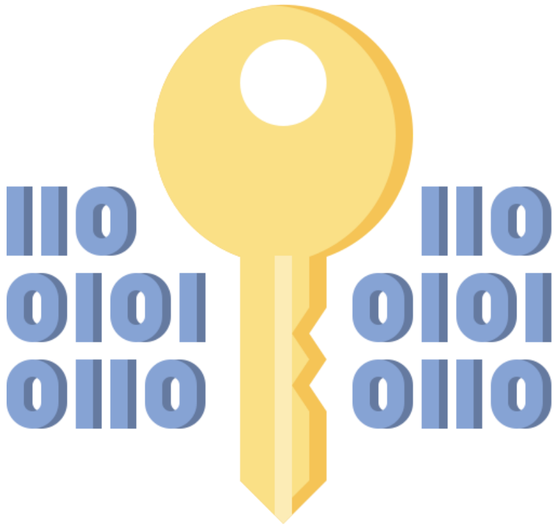
Fernet Algorithm -

The Fernet module in the cryptography package offers built-in functions for key generation, plaintext encryption to ciphertext, and ciphertext decryption to plaintext. It ensures that encrypted data remains secure and cannot be manipulated or read without the corresponding key.

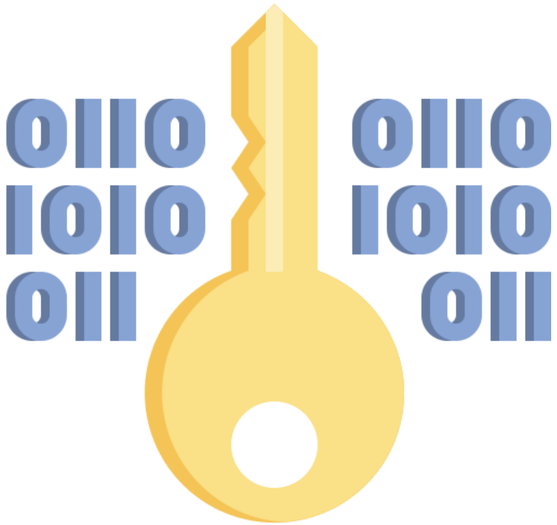
Cloud Integration-

In our project's cloud integration, we're connecting to **AWS** (Amazon Web Services) for secure file storage and retrieval. This is done through the **Boto3** library in Python, the official **AWS SDK**. You configure Boto3 with your AWS credentials (Access Key ID and Secret Access Key) and the AWS region. Using Boto3, you upload encrypted files to AWS S3 (Simple Storage Service) and download them as needed. This integration ensures that your application seamlessly interacts with the cloud for secure storage and retrieval of encrypted files.

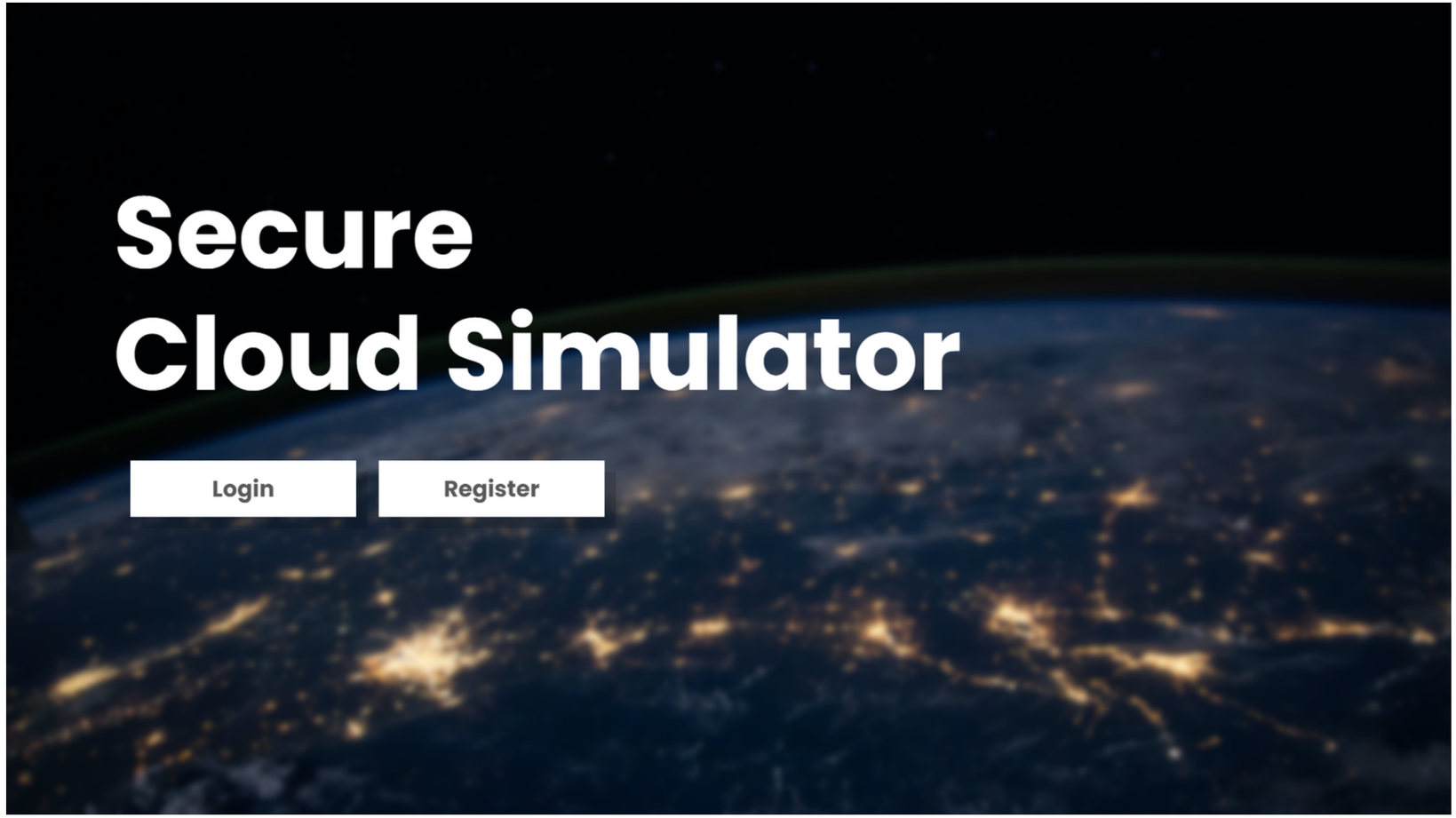
Input -



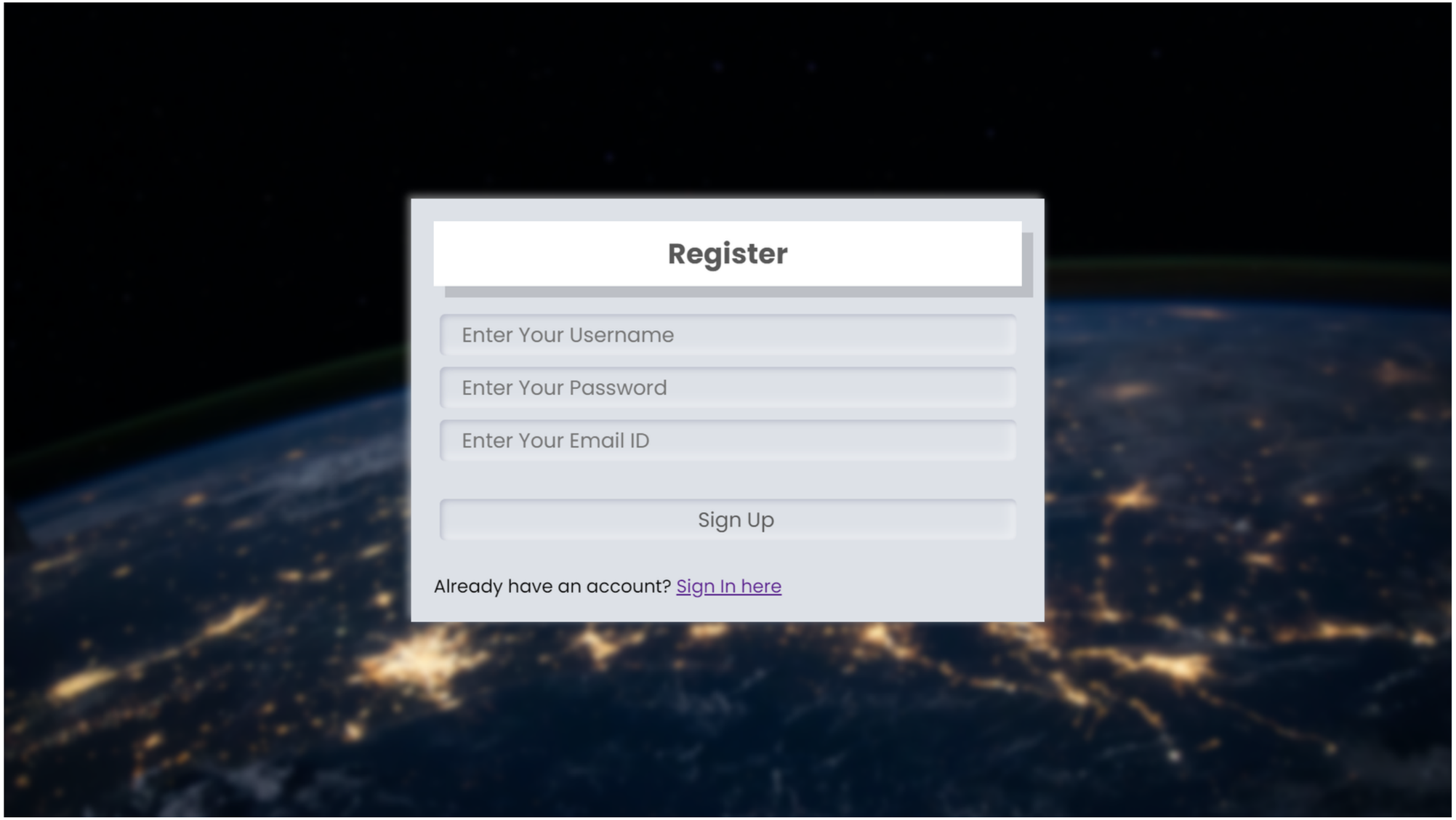
Output -



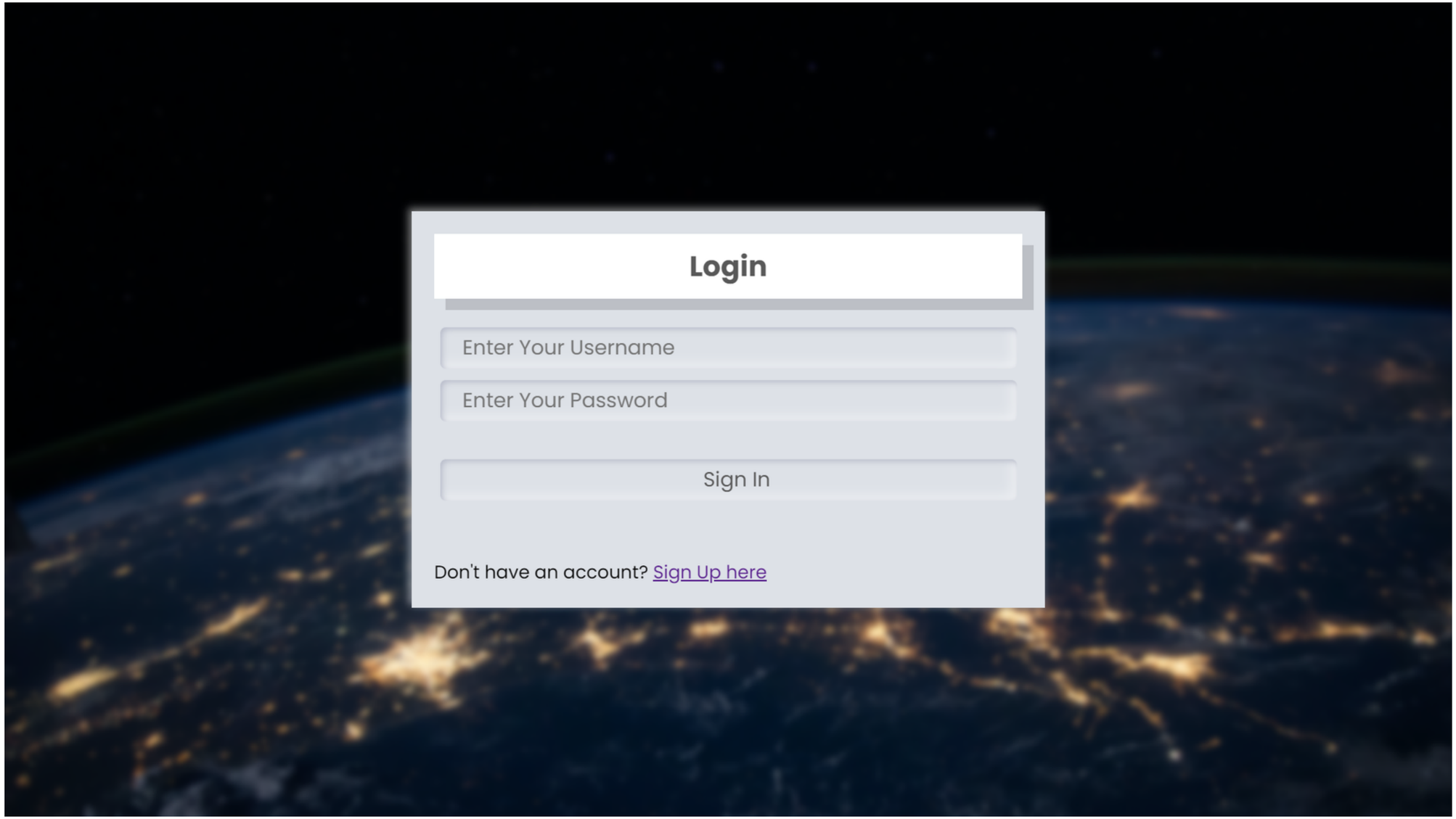
Screenshots



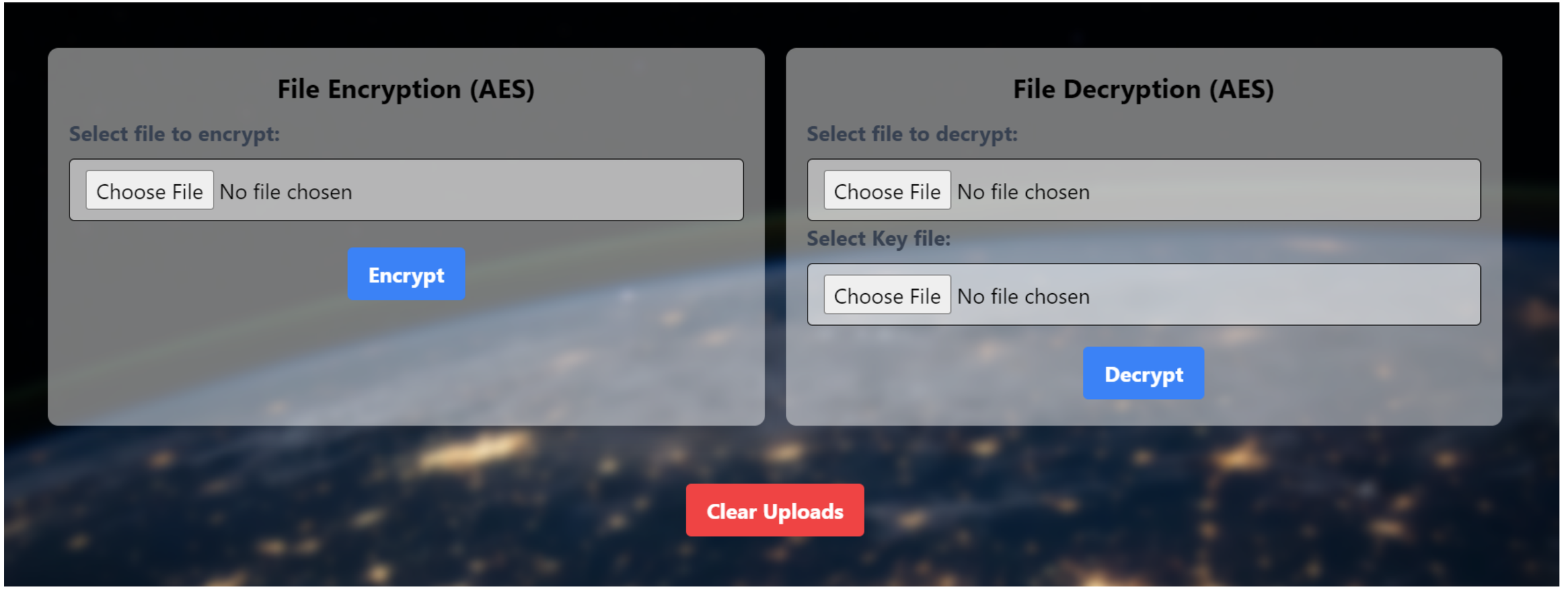
Home Pge



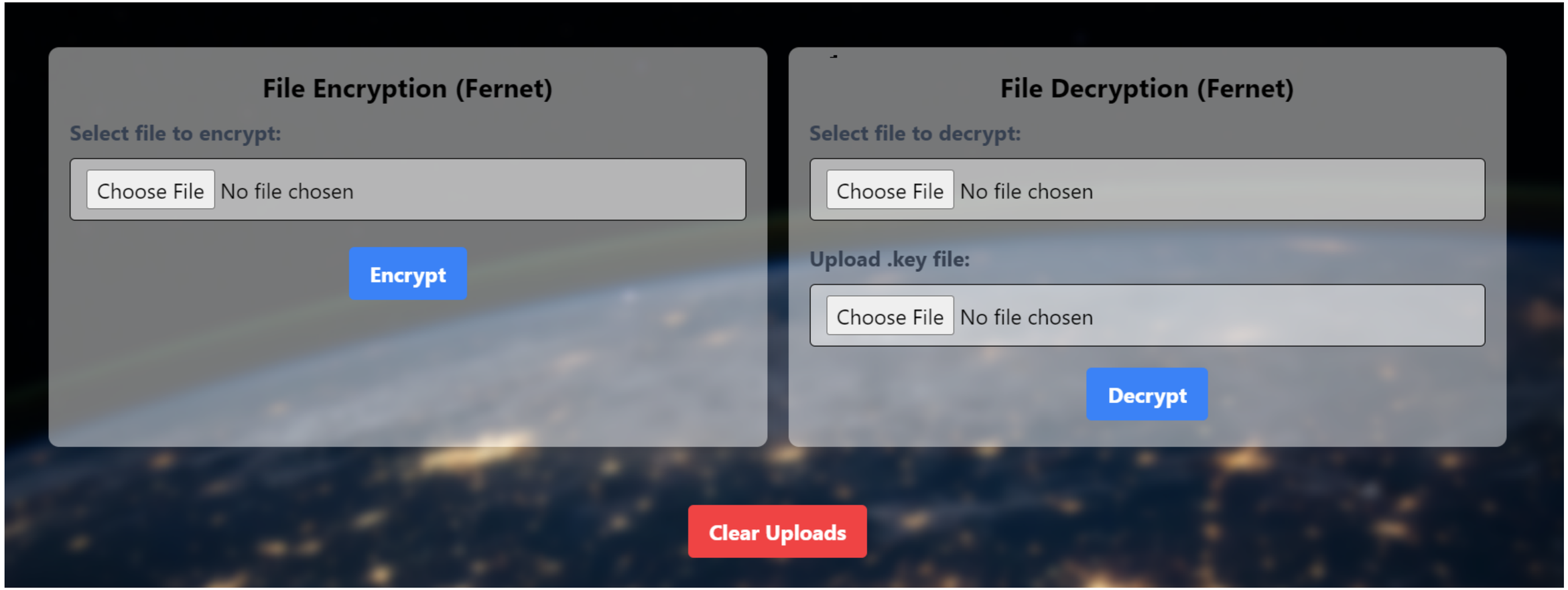
Register Pge


Login
Enter Your Username
Enter Your Password
Sign In
Don't have an account? Sign Up here

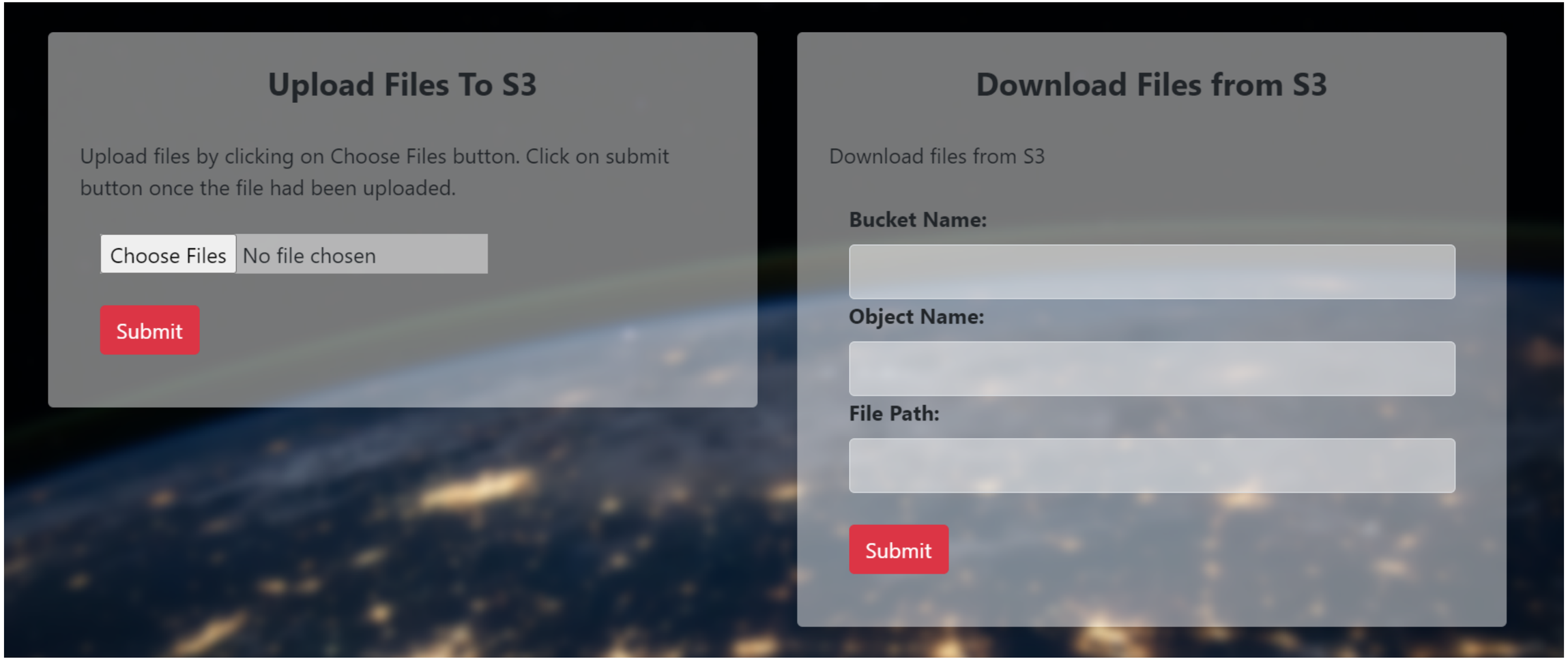
Login Page



File Encryption and Decryption (AES)



File Encryption and Decryption (Fernet)



Cloud Integration (AWS S3)

Conclusion

The project, "Secure Cloud Simulator using Cryptography and Python," successfully creates a secure and user-friendly platform for efficient file management in the cloud. Robust encryption algorithms, Fernet and AES, safeguard user data during upload and download processes to and from AWS S3. The integration of Python, Flask, cryptography algorithms, and AWS services ensures both efficiency and security, achieving the project's goal of enhancing data security in cloud storage. The well-designed and cohesive system provides users with a reliable and protected environment for their file management needs.

Thank You !!