JNIESTRT'S

SMT. INDIRA GANDHI COLLEGE OF ENGINEERING

GHANSOLI, NAVI MUMBAI – 400709

(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)

COMPUTER SCIENCE ENGINEERING (AI&ML) DEPARTMENT

ACADEMIC YEAR :- 2021-22 (Odd SEM)

Initial Project Document (IPD)

Title of the Project: Secure File Storage Using Hybrid Cryptography Algorithms	
Group No. 12	**Name of Student 1: SHRUTI KAMBALI**
	Name of Student 2: POORVA PADAVE
	Name of Student 3: POORVA PATIL
	Name of Student 4: GHANSHYAM GADEKAR
Name of the Supervisor: Prof. SWATI VYAS	

Abstract

This proposed hybrid algorithm can be made much more powerful and secure by increasing the number of iterations in the encryption algorithm to suit the level of security required. An inverse policy of reducing the number of iterations for lower security can also be employed.

Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms.

The idea of splitting and merging adds on to meet the principle of data security. This system can be implemented into banking and corporate sectors to securely transfer confidential data in the world of data being the key asset, safeguarding our asset is primary responsibility.

Communications, databases, infrastructure, transactions, knowledge; an organization's data is arguably its most valuable asset. It is in a business' best interests to keep its information safe, regardless of legal or regulatory requirements. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled. Cryptography technique translates original data into unreadable form.

Cryptography technique is divided into symmetric key cryptography and public key cryptography. This technique uses keys for translate data into unreadable form. So only authorized person can access data from cloud server. Cipher text data is visible for all people.

It works on 9 stages:-

1) User Selects file
2) Encrypt using AES, DES, IDEA or Blowfish
3) Generate key
4) Upload same or another file
5) User Search File
6) View File & Send request
7) Enter Key
8) Decrypt using Key
9) Download file

Objectives of the Project

(Every purpose / feature of project should be enumerated point wise.)

1. The stored image file is completely secured, as the file is being encrypted not by just using one but four encryption algorithm which are AES, DES, Blowfish, IDEA and RC6.
2. The key is also safe as it embeds the key in image using LSB.
3. The system is very secure and robust in nature.
4. Data is kept secured on cloud server which avoids unauthorized access.
5. A system which stores data after encryption.
   - This prevents data leak if a breach occurred.
   - Any form of data can be stored.
   - It ensures data confidentiality to users.
   - The primary goal of the system is to provide and simulate a solution to face the challenges and solve security issues that exists.

Hardware / Software Platform used:

❖ Software Requirements:

- Windows 7 or above
- Visual Studio 2010
- Python IDE
- Python
- Flask
- HTML
- CSS
- JavaScript

❖ Hardware Components:

- Processor – Core i3
- Hard Disk – 160 GB
- Memory – 2GB
- Computer/laptop
- Intel i3 6th Gen or higher/4gb Ram
- Internet Connection

Group Members / Roll Nos. / Signature

1. **SHRUTI KAMBALI-29**

Shruti.

2. **POORVA PADAVE-43**

Poorva

3. **POORVA PATIL-49**

Patil

4. **GHANSHYAM GADEKAR-16**

Ghanshyam