**Developing and securing of cloud (CS 6301)**

**Project proposal**

**Secure File Storage Using Hybrid Cryptography**

**Team Members** –

Arjun Hegde

Sravya Kurra

Suraj R Vadvadgi

**Literature** –

Brute force approach:

Encrypting the file once it is uploaded on server with the key and later the same key will be used by the user to decrypt the file for downloading. This approach has cons like risk of third-party eaves dropping where the entire file will be accessed to attacker if he gets the key.

Our approach:

We designed the system, where the file is divided into N parts once it is uploaded on the server. These N files will be then encrypted with different encryption algorithms using a key(this key will be further secured using some algorithm for added level of security). And finally, this key servers as a public key for the user to download the file contents abiding to CIA of security.

**Programming Environment** –

Python

Flask

**Intended implementation –**

This implementation can be explained in two parts

Encryption phase (generates a key for the user)

* Load the file on the server.
* Dividing the uploaded file into N parts.
* Encrypting all the parts of the file using any one of the selected algorithms (Algorithm is changed with every part in round robin fashion).
* The keys for cryptography algorithms are then secured using a different algorithm and the key for this algorithm is provided to the user as public key.

Decryption phase (this public key helps to decrypt the file for the download)

* Load the key on the server.
* Decrypt the keys of the algorithms.
* Decrypt all the N parts of the file using the same algorithms which were used to encrypt them.
* Combine all the N parts to form the original file and provide it to the user for downloading.

**Tentative Schedule** –

April 7th – April 12th

* Collect, read, understand related papers/article/blogs/resources.

April 13th – April 18th

* Design/research on the libraries, input, output, algorithm, programming environment to be used

April 19th – April 24th

* Develop frontend, backend

April 25th - May 30th

* Test/Debug the developed application
* Make a report and presentation on the project

**Conclusion** –

To store data on cloud we have to face many issues. To provide the solution to these issues there are n number of ways. Cryptography and steganography techniques are more popular now a day's for data security. Use of a single algorithm is not effective for high level security to data in cloud computing. The proposed model efficiently secures the file/data on cloud.