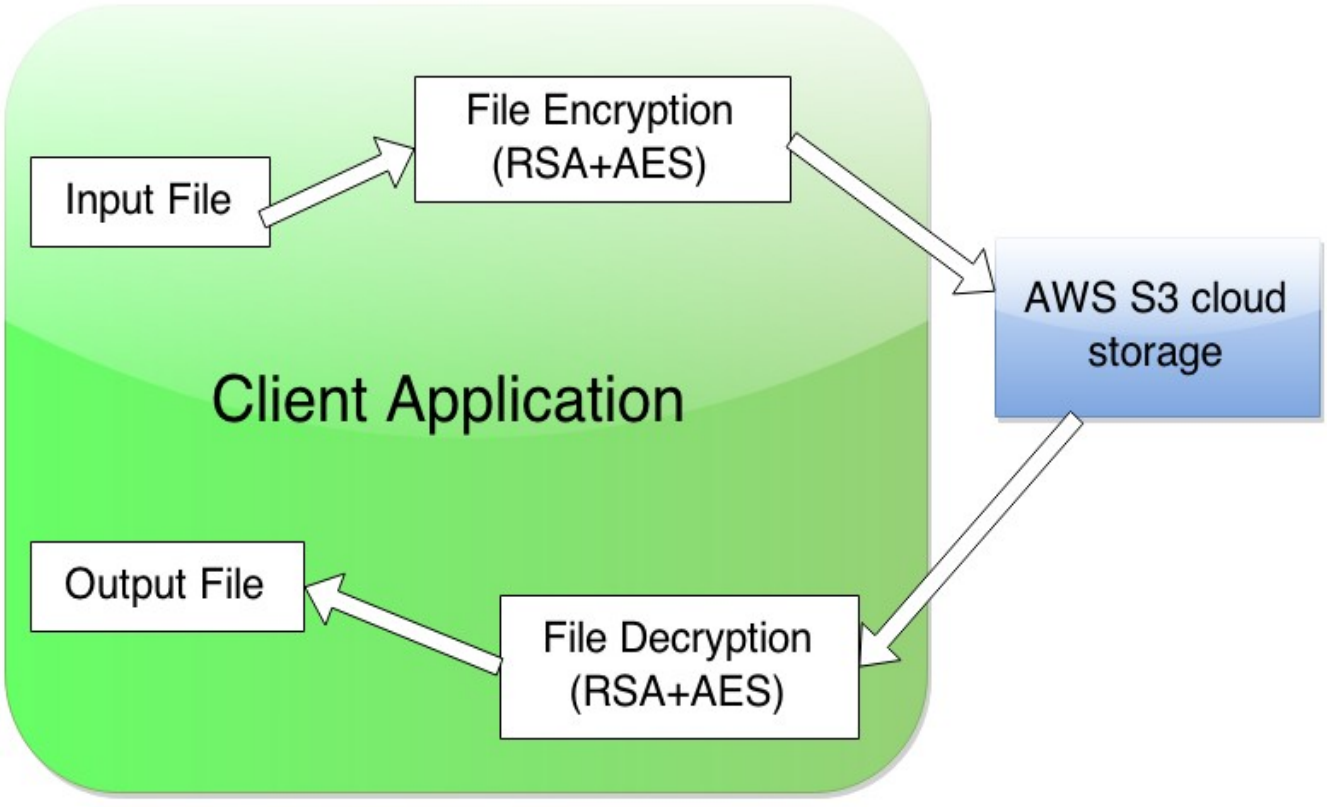
CSL707 | Assignment #4

Entry No.	Name
2012csb1002	Aditya Abhas
2012csb1005	Akshay Prasad Singh
2021csb1020	Mohit Garg

We have developed an application which stores and retrieves file/directory from local directory to AWS S3 cloud storage. The files are properly protected so that the cloud vendor may not view the contents or other information about the files being stored. For protection, RSA and AES based encryption is used.

Solution Design



File Encryption: Combination of RSA and AES encryption is used to encrypt the files. Whenever a user gives command to upload a file to the cloud storage, application first encrypts the file and then upload it to the cloud storage. Also, if directory is selected to upload, every file is encrypted recursively and then uploaded on the cloud.

The need for using AES arose because RSA Key can encrypt only those files which consists of lesser number of bytes than the RSA key. Also, RSA encryption is slow. AES encryption is much faster than RSA. When we encrypt the files using AES Key and encrypt the AES key using RSA, the files stored on the cloud is secure.

Encryption Steps:

1. User provides the RSA encryption key pair.

2. Application generates a random AES and encrypt the input file using that AES key.

3. This AES key is encrypted using the public RSA key given by the user.

4. The RSA encrypted AES key is attached in the beginning of the file and the file is sent to the cloud.

5. To avoid confusion, we add “.enc” at the end of the filename of every file encrypted by our application.

Decryption Steps:

1. First few bytes (256 bytes, in our case) of encrypted AES

key and the remaining file is separated.

2. The encrypted AES key is decrypted by the private RSA key given by the user.

3. Now, the obtained AES key is used to decrypt the file and the original file is restored.

Interaction with AWS Cloud: Java AWS SDK is used for interacting with the bucket created on the cloud. The SDK removes the complexity out of coding by providing Java APIs for many AWS services including Amazon S3. All the files are uploaded on the bucket `'csl707-mohit-garg'.` Whenever a directory is uploaded, the same path as present in the user's directory is created on the cloud for the all the files.

GUI: User interface is made such that user can choose file or folder to upload on the cloud. Also, user can view the uploaded files on the cloud in form of a list view in the application and double click on the file name to download it. The progress of upload/download are shown using a progress bar.

The app gives five options for the user:

i. Choose File: This will open a dialog box to choose a file to upload on cloud. On selecting the file, file upload starts and its progress is shown.

ii. Choose Folder: This will open a dialog box to choose a directory to upload on cloud. The directory and all the files and directories contained it are uploaded on the cloud.

iii. List Object on S3: This will show a list of all files present on the S3 storage. To download a file, double click on the file name and choose the location to download the file. Then, download will start and its progress is shown.

iv. Provide RSA Keys: On clicking this button, two dialog box will get opened one after other asking the user to give the public key and private key respectively.

V. Generate RSA Keys: On clicking this button, our application will automatically generate the public key and private key and will ask the user to save them.

Proxy Settings: The application can run also run through network proxy. The various attributes of proxy settings are specified in the 'proxy.properties' file.