# Project 2

## (Cryptography: confidentiality, integrity detection, and replay attack detection for your data)

Presented by:

Archana Purushothama (ap4095)
Prashanth Tekal Venkateshprasanna (ptv207)

## Data Processing Application

- Party1 stores on and later retrieve files from a cloud server,

# Analysis of possible attacks :

- Data Eavesdropping :

Data in transit can be intercepted by the hackers and eavesdroppers, either by directly listening or sniffing any kind of communication.

# Securing Data in Transit

- SSL: Provide a secure communication channel.
- Identification and Authentication: Exchange of certificates to avoid man-in-the-middle attacks.
- OpenSSL library is used to create certificates and SSL implementation.

openssl req -x509 -nodes -days 365 -newkey rsa:1024 -keyout mycert1.pem -out mycert1.pem

# Securing Data at Rest

- Server Side Encryption
- Each file uploaded into the server is encrypted using AES-256 bit cipher using a key.

# Message Integrity

- HMAC SHA 1 is used to check for Message Integrity.
- Once any file is uploaded into a server, HMAC of the file is created and stored at client side.
- When the client requests for the file to be downloaded, server responds by sending the file, the contents of the file are then cross-checked with the HMAC contents present at client side to ensure message Integrity.

# Replay Attack

- When a client requests for a file to be downloaded, server sends across a random session number to the client.
- Session number is then appended to the file name at the client and sent to the server.
- Server then diligently checks if the session number is valid(already used) and allows the file to be downloaded only if the session number is valid.

# Conclusion

- All the cloud storage services are using the best cryptographic algorithms available to keep up with the competitors.
- User’s data is always in a vulnerable state in the cloud storage services supporting server side encryption.
- Try to use clouds that are less popular but use strong ciphers for encryption. Hackers keep their eyes on services that are popular in the market.
- Example : Dropbox
  - AES-256 bit cipher for Server side encryption and storage.
  - SSL to secure data in transit.

# THANK YOU