Smart India Hackathon 2017

Ministry Category : **Indian Space Research Organisation (ISRO)**

Problem Statement : **Storing emails on mailbox server in encrypted format accessible only to owner of the email**

Problem Code : **#ISR1**

Current AICTE Application No. : 1-3328528908

Team Leader Name : **Anup Kumar Panwar**

IDEA

Our idea is to develop a SECURED & ENCRYPTED EMAIL SERVICE. Normally Email services provide STORAGE LEVEL ENCRYPTION which are decrypted on-the-fly and that too with a SINGLE KEY. So, we have tackled the drawbacks in this ON-THE-FLY DECRYPTION and SINGLE KEY approach:-

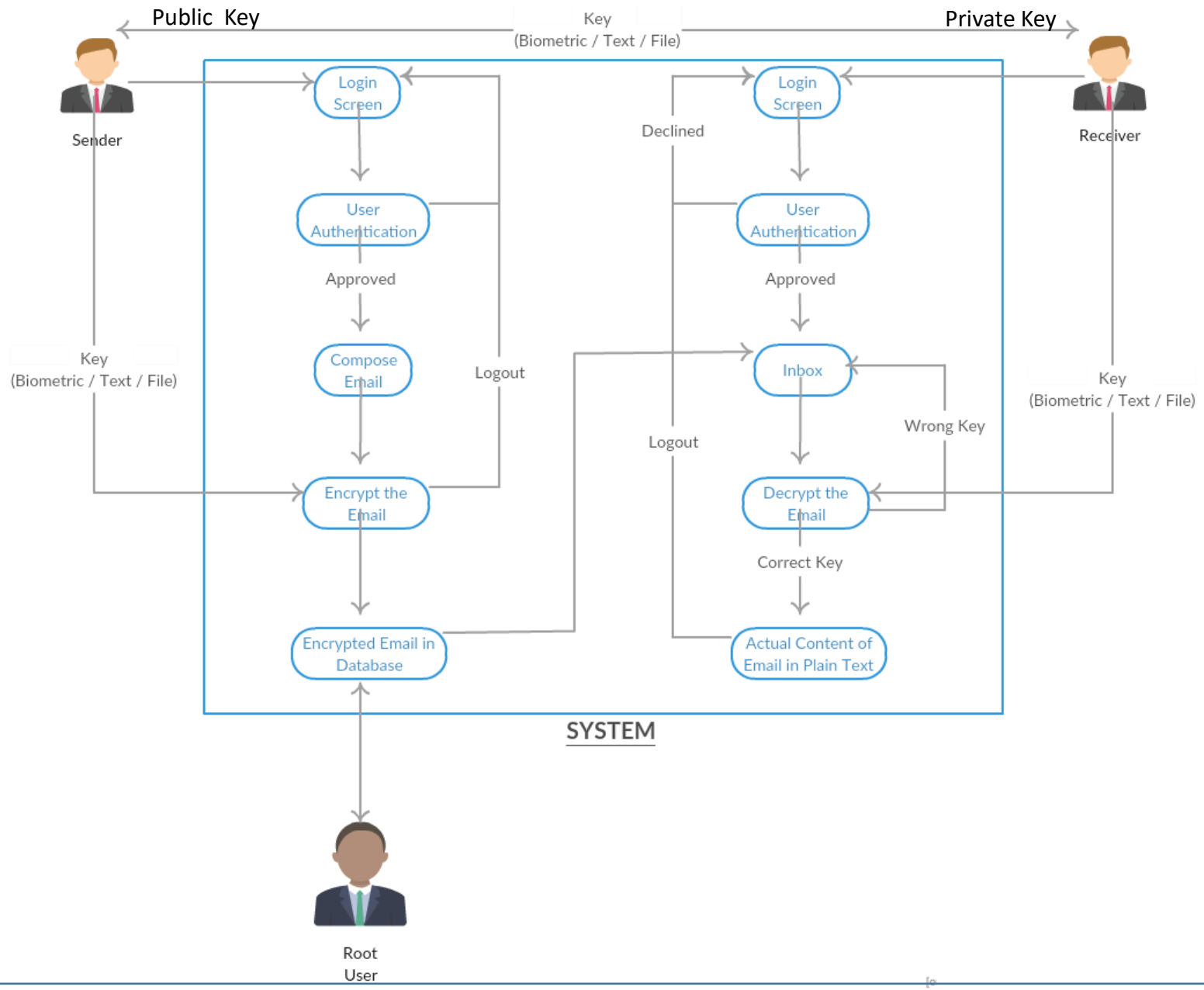
1. The sender will provide a KEY to lock the Email Content; This key can be anything the BIOMETRICS, a STRING or a FILE. For example, any ISRO research paper can be encrypted with a photo of "Ganesh Ji". Thereafter that research paper can be opened only if the user has that same "Ganesh Ji" photo with him. But mostly our approach is based on encrypting the content with FINGER PRINTS of the users.
2. A RANDOM SALT will be generated under MD5 ENCRYPTION ALGORITHM and SERVER TIMESTAMP;
3. The KEY(Ex: Thumbprint) + SALT will be used to generate an INITIALIZATION VECTOR (IV) that will again undergo MD5 ENCRYPTION;
4. Then this INITIALIZATION VECTOR will be used to encrypt the email content using AES 128 BIT ENCRYPTION TECHNIQUE;
5. This Encrypted content will be BASE64 ENCODED and stored in the database. (NOTE : The key provided by the sender is NEVER STORED anywhere in any form)
6. The recipient of the email will see the content of the email in encrypted form which no one can understand. To read the actual content he has to provide his FINGER PRINTS. This decryption is temporary and at the VIEW LEVEL ONLY . Once the user has read the actual content, as soon as he redirects from the web page. The temporary decryption will vanish.
7. Now a question might be "Does the receiver needs to remember 100s of passwords for deciphering 100s of emails?" The answer is NO.
8. Once the recipient has successfully deciphered the email. The key will be stored in user's LOCAL STORAGE or CACHE, providing DEVICE LEVEL SECURITY as well.
9. Moreover the sender of the email will get a notification if number of wrong password attempts exceeds a preset value(say 3).The sender and receiver both get an option to delete the email permanently from the server (Even from the receiver's inbox for the sake of security).

Thus an email service with 3 LAYERS security and encryption : USER AUTHENTICATION, ENCRYPTED STORAGE & DEVICE BASED SECURITY

Technology Stack

HTML, CSS, Material Design Light (MDL), JavaScript, Angular.js, jQuery, PHP, MySQL DB, Mcrypt, AJAX, OpenSSL, Asymmetric Encryption, MD5 Encryption Algorithm, AES 128 bit Encryption Algorithm, PHP Mailer, P2P communication channel, APACHE server, WAMP/LAMP, Web sockets, Ionic Framework, ng-Cordova

USE CASE



DEPENDENCIES

Android Device with Finger Print Scanner and Minimum SDK version 23, Biometric Scanner, Internet Connection, A computer