**Description of the Project:**

Problem Statement:

To design a bank system which ensures that compromise of any one server storing the password, never gives away the entire password of the user.

Objective:

The objective is to develop an app for a banking system where the user enters his password which is never completely stored anywhere. The Bank server splits the hashed password given to it into different pieces and stores these in geographically different locations. Nowhere does the Bank server or the Servers storing the pieces of password get to know what the complete password is. Hence compromise of the servers would never give away the users password as it is. The adversary would require multiple points of attacks in order to break the password.

Deliverables:

User end Application

* The end user interface of the application. This is what is displayed to the user.
* Handling authentication of the user by the server.

Algorithms

* Implementation of splitting of password and recovery.[2]
* Introducing a system which makes the application device specific.
* Generation of public and private keys, assymetrical encryption, hashing passwords.

Inter Machine Communication

* Secure Communication between the Device-specific Application and the Main Server.
* Secure Communication between the Main Server and the Servers containing pieces of the password sent

Timeline:

* Feasibility Report - Literature survey, architecture of System.
* Phase 1 - Communication between bank and split servers, Basic layout of the app, partial implementation of splitting of password.[2]
* Phase 2 - Communication between app and bank server, development of login page of the app, issue of keys and securing communication along with hashing.
* Phase 3 - Optimisation and end case testing of communication, development of sign up page, generation of location pass and making app device specific.
* Phase 4 - Integration of application with the servers.
* Final Presentation - Validation of results by simulation.





