CHAPTER 7

Implementation and Simulation

7.1 Implementation Scenario

We have implemented our proposed scheme and simulated it in local environment. However, it can be implemented in any network environment. The users can choose their usernames, biometrics and passwords freely. The registration center is a trusted third party who is trusted by both the user and the server. Here, registration center is involved in all the phases accept login and authentication phase. It can monitor the whole process and save necessary data if needed. It can halt any process at anytime if needed. The registration center keeps its private AES key secret and protects the key in any situation. The servers must register with registration center before starting its operation. The server keeps its private AES key secret and protects the key in any situation. The sensitive data are encrypted before saving into the database. The sensitive information of the messages is hashed before transmission. Only login and authentication phase uses insecure channel; all other phases use secure channel to exchange messages.

7.2 Implementation Tools

We simulated our work using HTML [32], CSS [33], JAVASCRIPT [34], PHP [35] and MYSQL [36]. We also used bootstrap [37], font-awesome CSS library [38] and jquery JAVASCRIPT library [39]. We also used Apache server [40] to run our simulation. We simulated the following phases: Server Registration Phase, User Registration Phase, Login and Authentication Phase, Password Change Phase, Password Recovery Phase, and Smart Card Recovery Phase. We also simulated following attacks: User Impersonation Attack, Server Masquerading attack, and Replay Attack. The prevention of other remaining attacks and weaknesses are theoretically discussed in chapter 6.