TEAM 27 report:

**Team number:**

YANG Shu: 23098979d

WANG Jinghan: 23099359d

WANG Jiawen 23109973d

LIN Hao:

**contribution table**

|  |  |  |
| --- | --- | --- |
| Student name | Student ID | Overall Contribution |
| YANG Shu | 23098979d |  |
| WANG Jinghan | 23099359d |  |
| WANG Jiawen | 23109973d |  |
| LIN Hao |  |  |

**Abstract:**

Our project is to do a data delivery system, the client can do the transmission system to the server, to provide message encryption transmission function, to ensure the confidentiality,integrity, tamperability of the message. The server could store the data to database system

**Introduction:**

Our project is going to do a client-server storage system. User could deliver the data from client to server, which should should the data in the database system. The system implement the Client-server architecture:

Client: Interface with user. Access the provided data. Do data encryption. Connect and communicate with the server.

Server: Access data from client. Store the data from client to database.

encryption method: RSA

Thread Model:

Adversaries:

1. Passive Adversary:Identities: the admin or attacker who can see the data from server

Ability:

1. Read the data from server, including the encrypted data and the database
2. Network communication between client and server can be monitored
3. But it can not change the data and return fake response
4. User attacker: User who use the program but try to attack

Ability:

1. Operate but don't admit it,
2. use share or other functionality to access other user’s data
3. Man in middle: Like network Eavesdropper, Public Wi-Fi listeners, ISPs or intermediate nodes.

Ability:

Intercepting plaintext communications between clients and servers

Designed Algorithms to implement functionalities:

1. User Management
2. Register a user by username and password:

i: Theoretical Design:

ii: Technical Details:

1. Data Encryption
2. Access Control
3. Log Auditing
4. General Security Protection
5. Multi-Factor Authentication(Email)