Cryptographic system

Project Supervisor

Madam Alina Munir

Submitted by

2021-CS-688 : Muhammad Zain-ul-Abideen

2021-CS-679 : Aleena Mazhar

Table of Contents

Content **Page no.**

Introduction - - ----------2
Abstract - - ----------2
Vision - ----------2
Scope - - ----------3
Project Statement - - ----------3
Requirements - ----------3
Data structures - - ----------4
Functionality- - ----------4
Design - - ----------4
Flow Diagram - - ----------

Introduction

Cryptographic systems are used to keep data secure and safer during transmission so that it cannot be accessed by any other individual other than the receiver of that data. It is very commonly used in almost every aspect of life where there is a need to share data with other people. It helps users to keep their data secure by using end to end encryption at both the sender and receiver end.

Abstract

Cryptography is very commonly used in almost every aspect of life where there is a need to share data with other people. It protects the data which have to be shared. Data will be encrypted before transmission, encrypted data will be transmitted and then decrypted after transmission and received by the receiver.

But most hackers hack the data which is less secured and encrypted using simpler techniques.

Our cryptographic system helps the users to keep their data secure by using safer and difficult encrypting techniques which cannot be easily understood by hackers.

Vision

Our vision is to facilitate companies in which millions of data is to be shared on a daily basis. We will provide safer encryption techniques which have been applied to the transmitted data before its transmission and also the receiver can check if there is any change in the data during transmission.

Scope

Our system is made for transmission ends so that senders can send their data privately without having access to other users or any other individual. It is easy to use and handle. User will only send the data and this system is used at both the sender and receiver end so that data will be encrypted and decrypted accordingly.

Project Statement

Developing a cryptographic system which automatically encrypts the data using the key provided by the user and also decrypts that data using the encryption key. Users also don't know the technique of encryption and decryption of data.

Requirements

Our cryptographic system has the following requirements.

- ➔ Users must provide the data which has to be sent.
- ➔ Users must provide their own id and also receiver id.
- ➔ Users must provide the key which has been used for encryption.
- ➔ Users don't know the technique of encryption.

Data Structures

Following data structures have been used by our cryptographic system.

- ➔ Hash tables
- ➔ Linked lists
- ➔ Trees
- ➔ Queues

Functionality

Our system can perform the following operations.

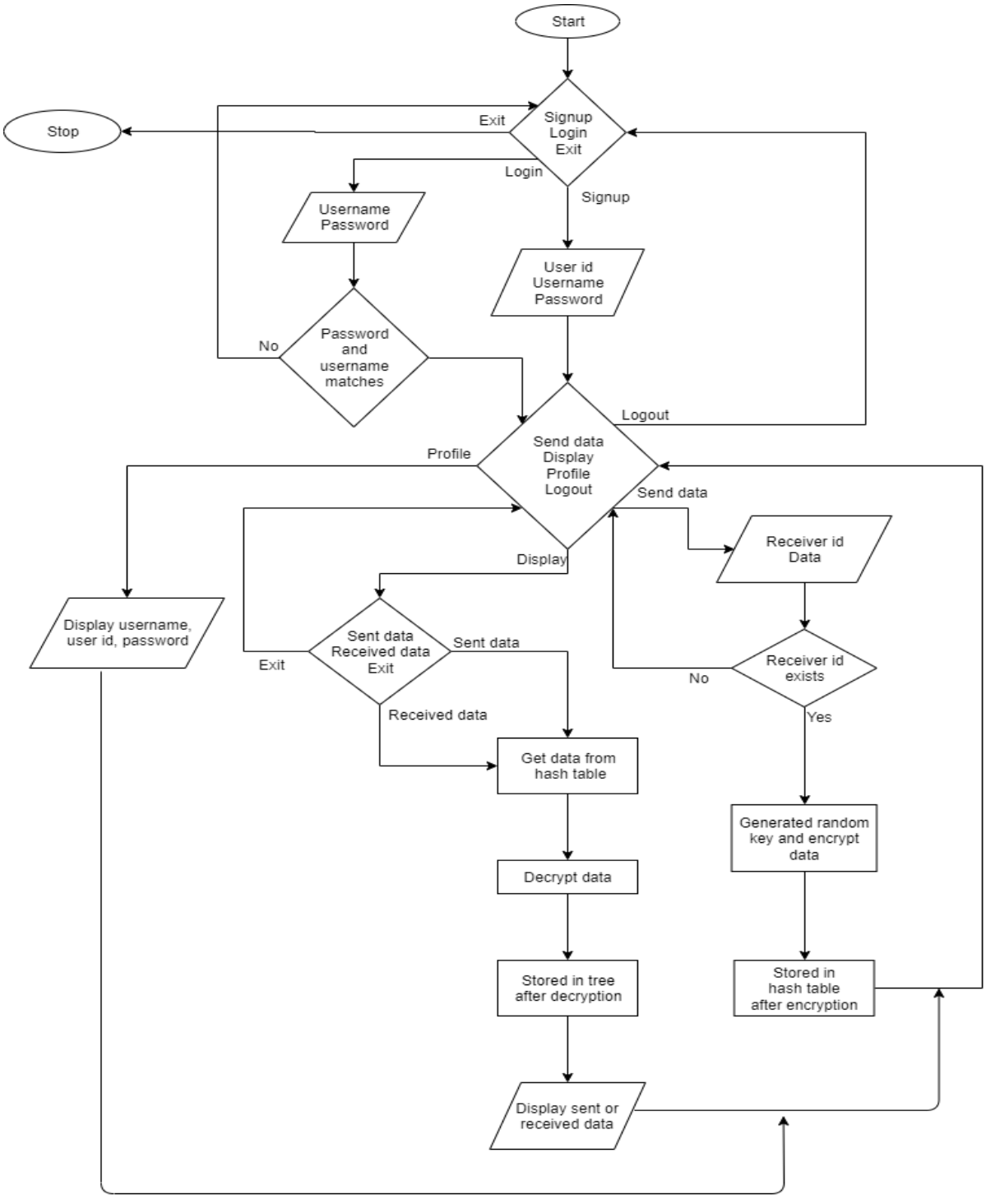
- ➔ Signup
  - ◆ User id
  - ◆ Username
  - ◆ Password

  Go to menu
- ➔ Login
  - ◆ Username
  - ◆ Password

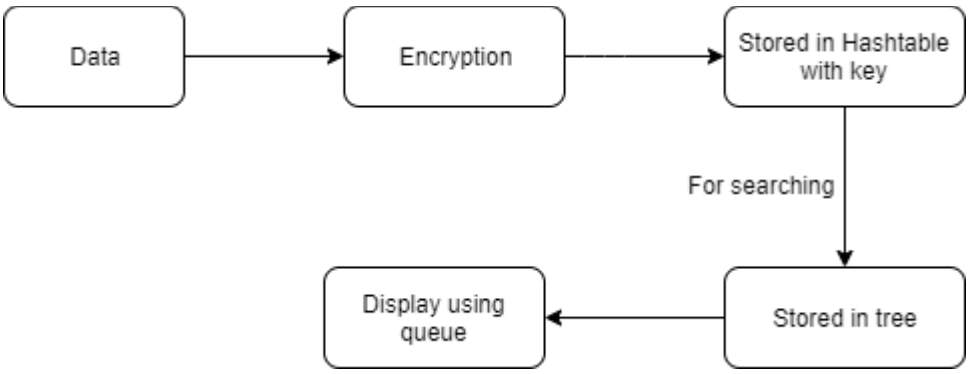
  If user exists, go to menu

- ➔ Menu
  - ◆ Send data
    - Get receiver id and data to be sent from user
    - If receiver id matches, encrypt data and stored in hash table and go to menu
  - ◆ Display
    - Display sent data
      - Get that user data from hash table
      - Store in tree after decryption
      - Display sent data
    - Display received data
      - Get that user data from hash table
      - Store in tree after decryption
      - Display sent data
  - ◆ Profile
    - Display username, user id , password
  - ◆ Logout
    - Go to login signup

Flow diagram



Design


Data
Encryption
Stored in Hashtable with key
For searching
Stored in tree
Display using queue