USER AUTHENTICATION SYSTEM WITH RC4 STREAM ENCRYPTION ALGORITHM

Karan Prabu Kandhaswamy

Abishek Lakshmirathan

Introduction:

Purpose:

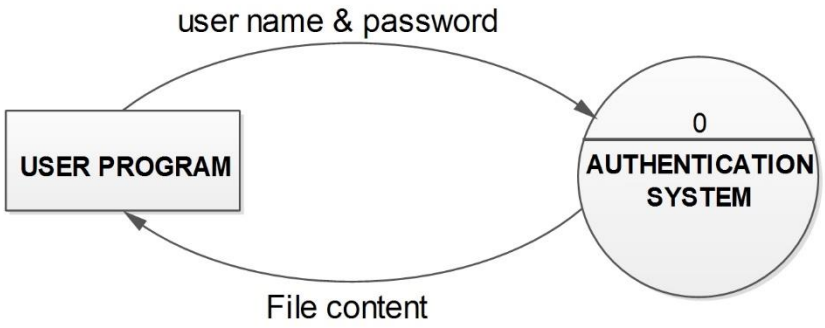
- Software to view a specified file from the Database by the Authenticated user.
- The document describes the following phases of the software:
  - Requirements
  - Analysis and feasibility
  - Design

Scope:

- The software is Authentication System.
- The software performs the authentication for the user to view the specified file as follows:
  - It allows the existing user to login to the application.
  - It allows registration for new users.
  - The software provides secure authentication to login application

High Level Design:

Level 0 Design Description:



Interface Description:

The user sends the username and password. The Authentication system validates the username and password and then system will provide the path of the file specified by the user.

Data Description

- **Username and password**
- **File name**
- **File content**

User name and password

The username and password provided by the user are used for authentication purposes.

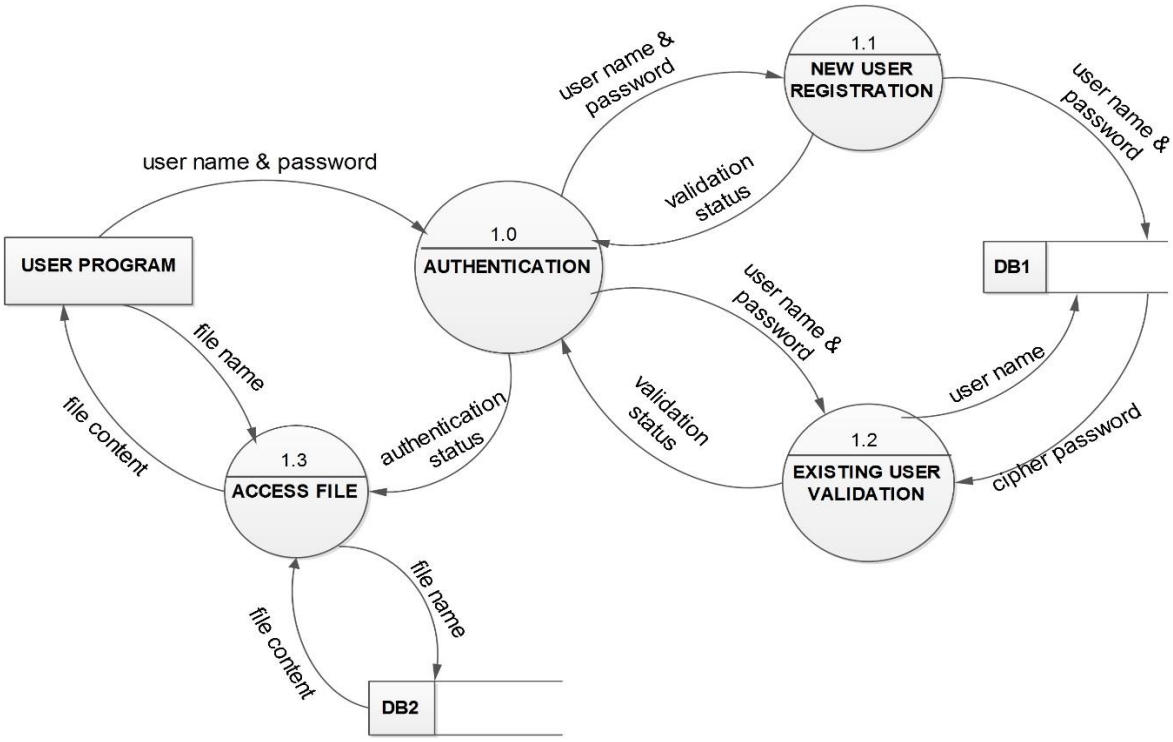
File name

File name is the name of the file the user wants to access.

File content

This is the content of the file requested by the user.

Level 1 Design Description:



Authentication System:

This module validates the username and password and provide the file path to the user.

Module Description:

Authentication

Authentication is the main module which accepts information from the user and processes it accordingly for authentication. Based on authentication status it will provide the file path to the user.

New user registration

This module will register the user. And store user information in the database.

Existing user validation

This module will check whether the username and password given by the user matches with the username and password stored in the database.

Access file

Based on the authentication status given by the authentication module, this module provides the file path to the user.

Data description

- **Username**
- **Password**
- **Registration status**
- **Validation status**
- **Ciphered password**
- **Authentication status**
- **File name**
- **File content**

User name

User name is used to identify the user.

Password

Password is the secret word that enables the user to access the file.

Registration status

This status will provide the result of new user registration process.

Validation status

This status tells whether the user is authenticated or not.

Ciphered password

It is the encrypted password stored in the database**.**

Authentication status

This status tells whether the user can access the file or not

File name

File name is the name of the file requested by the user.

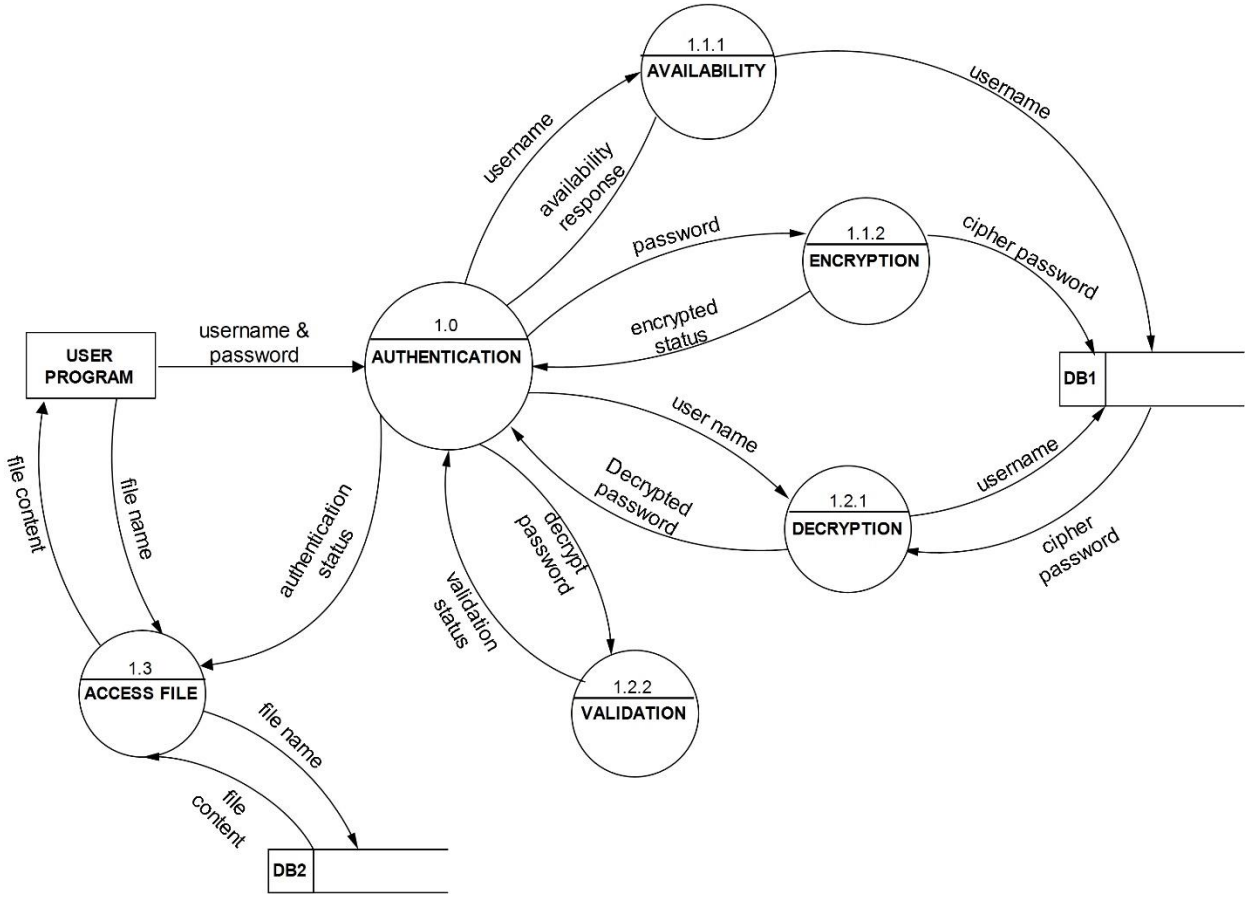
File content

This is the content of the file requested by the user.

Interface Description

The user information is given to the system which checks whether the user is new user or an existing user and validates the information. Based on the validation status the file requested by the user is displayed.

Level 2 Design Description:



New User Registration:

This module registers a new user by checking the username availability and the password is stored in encrypted format.

Module Description:

This module is further decomposed into the following two components **Availability** and **Encryption**.

- **Availability**
  This module checks whether the user name given by the user is available or not.
- **Data description**
  - Username
  - Availability response

- **User name**
  User name is used to identify the user.
- **Availability response**
  This returns whether the given username exists or not to the authentication module.

- **Encryption**
- This module will encrypt the password and store the username and the encrypted password in the database.

- **Data description**

    - **Password**
    - **Encrypted password**
    - **Encryption status**

- **Password**
  Password is the secret word that enables the user to access the file.
- **Encrypted password**
  The password given by the user is stored in the database in the encrypted form.
- **Encryption status**
  This returns the success or failure of encryption process to the system.

Existing User Validation:

This module checks whether the username and password given by a registered user is available in the database and return the authentication status to the system.

Module Description:

- This module is further decomposed into the following two components **Decryption** and **Validation**.
- **Decryption** module decrypts the encrypted password.
- **Validation** module checks the password given by the user matches with the decrypted password**.**

Decryption:

This module decrypts the encrypted password into plain text.

Module Description:

- **Decryption**
  This module retrieves the corresponding encrypted password from the database and decrypts it.

- **Data description**

    - **Username**
    - **Cipher password**
    - **Decrypted password**
- **User name**
  User name is used to identify the user.
- **Cipher password**
  The corresponding ciphered password for the given username is retrieved from the database.
- **Decrypted password**
  The retrieved encrypted password is decrypted and sent to the system.

Validation:

This module checks whether the password given by the user is same as that of decrypted password.

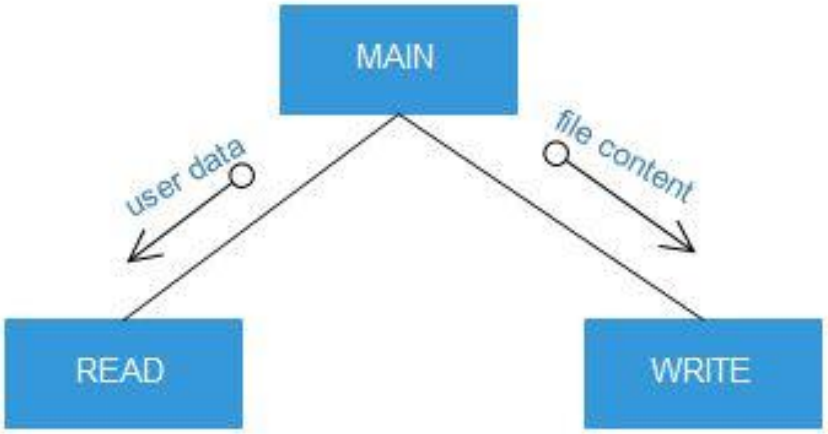
Data description

- **Decrypted password**
- **Validation Status**

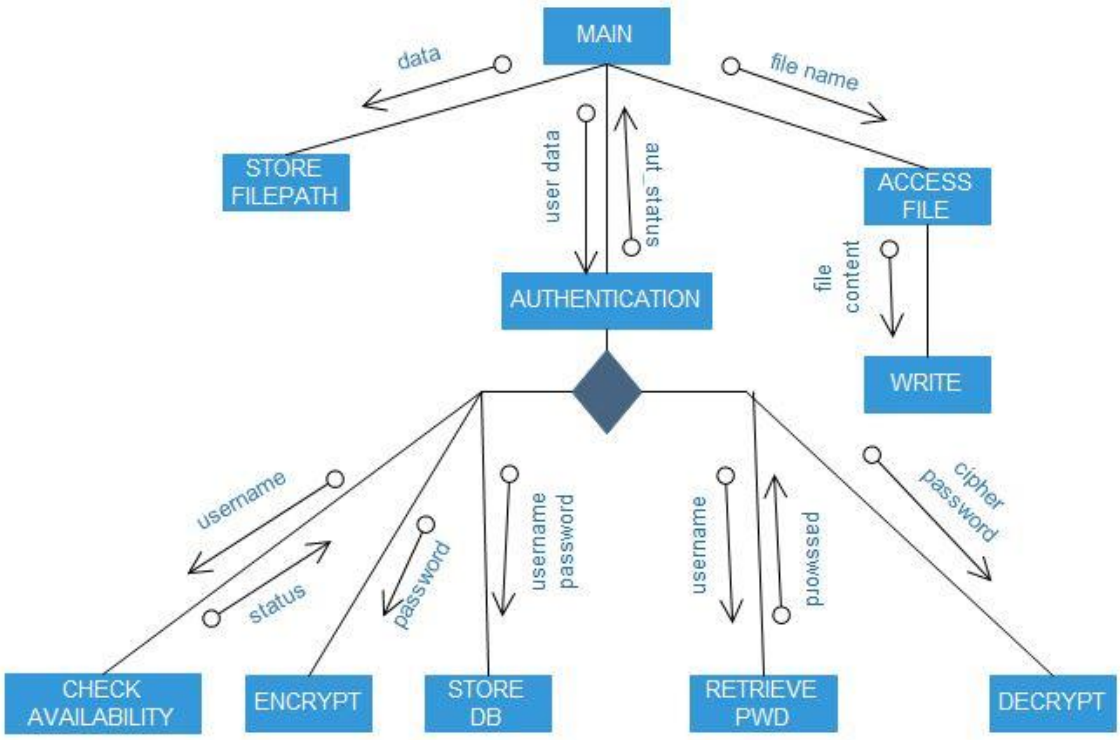
Decrypted password
The deciphered password is given to the validation process.
Validation status
This status will return whether the password given by the user matches with password given by the decryption process.

Structure Chart:

Client Side:



Server Side:



Scalability:

- The system is scalable. Every authenticated user can view the content of the requested file.
- The system provides login facility for the existing user.
- The system provides registration facility for the new user.

Hardware Requirements:

- Intel Pentium processor or equivalent clone.
- 256 MB RAM
- 2 GB hard disk

Software Requirements:

- Windows XP or windows 7
- GCC compiler