



SOCIAL HAVALDAR



PROBLEM STATEMENT

A Desktop Utility meant to provide security by creating folders with to user information like videos, folders, photos and private wallet information.

ABSTRACT

Social Havalдар is a program that acts as a bank vault, or safe, where you can keep your private information or files hidden and secure. Everything in the vault is protected with an advanced encryption, and requires a password (your password) to open the vault to access the information.

Files and file structures can be added to the vault by a simple drag and drop operation. It is also possible to create picture passwords which is the part of GUA and which is the uniqueness of our system.

To open a file stored in vault the user can decrypt it from the vault and this sets the file permissions of the selected file to default. The software enables the user to store information about credit/debit cards which are highly confidential and can be accessed only by the authorized user.

The software also keeps track of the intruders into the system by taking an image of user on three wrong password entries.

Scope and objective

The primary purpose of this project is to protect the confidentiality of digital data stored on computer systems.

The application of this desktop utility is widespread. As security is a major concern in today's world, this utility can be put to use in almost every field to secure any kind of information.

Some fields are as follows:

- ▶ Banking
- ▶ Military
- ▶ Hospitals
- ▶ Scientific experimental data
- ▶ Personal use

It can be efficiently extended to any platform.

FEATURES

Improved Graphical User Interface

The system provides an easy way to store private information into the system providing improved GUI.

Graphical User Authentication

The system provides a unique feature that allows the user to set up a unique picture password that unlocks only on clicking the image at particular spots for particular number of times. This feature provides additional security to the folders containing personal files.

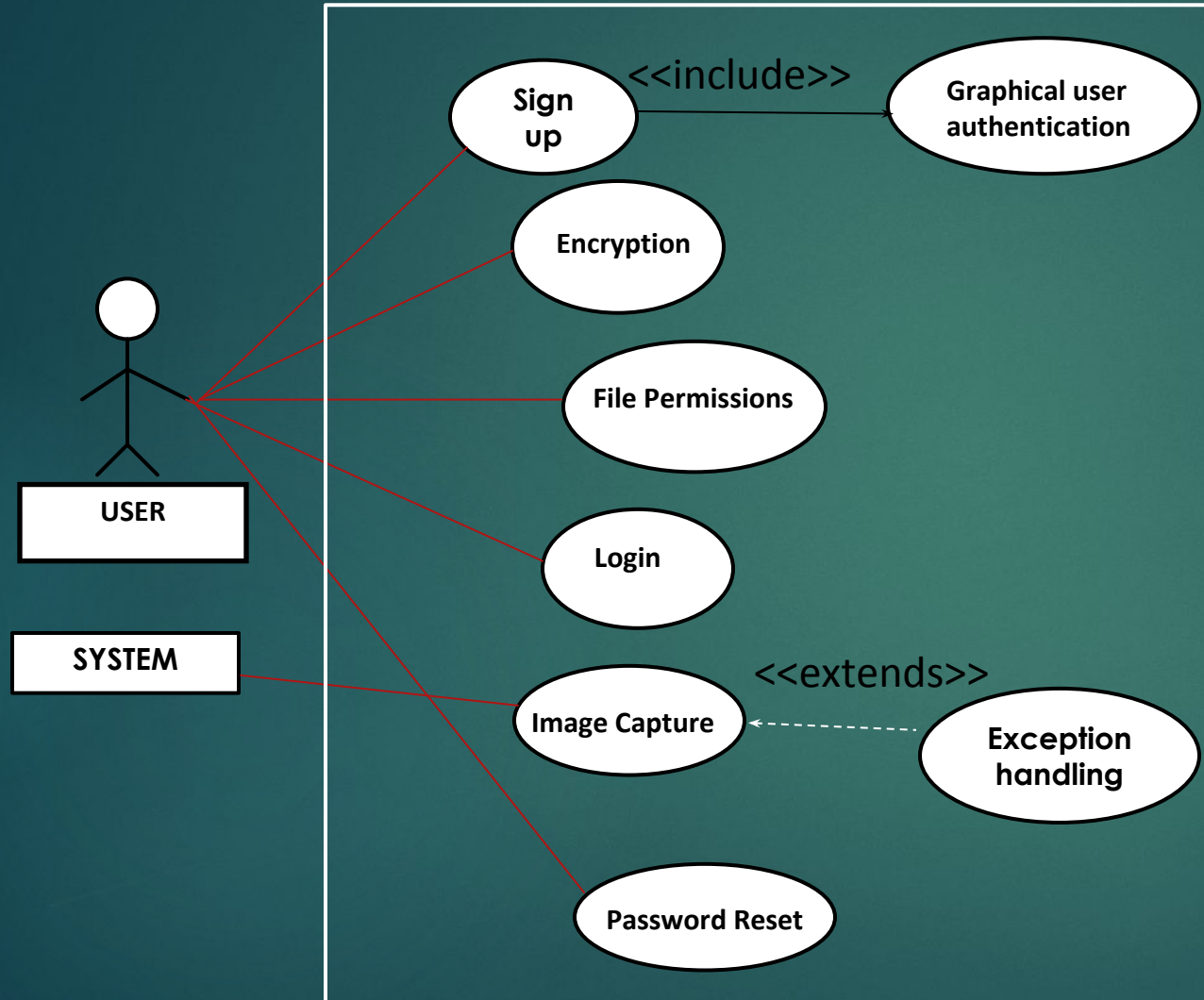
Mail Recovery of passwords

The system also provides the user with the option of email recovery of passwords in case the password is forgotten.

FUNCTIONAL REQUIREMENTS

Req-ID	Functional Requirement	Priority
1	The user shall be able to sign up to the system. The user can select either one or both of the security options. 1.1 The user shall be able to set a character password. 1.2 The user shall be able to set a picture password.	High
2	The user shall be able to encrypt any file in the computer through the system either by drag and drop or by browse method	High
3	The user shall be able to set file permissions to the selected file. The file shall be 3.1 Read only 3.2 Hidden	Medium
4	The user shall be able to login to the system any time by entering the previously set character password and/or picture password.	High
5	The system shall take a picture of the user on entering the password wrongly for continuous three times.	Medium
6	The user shall be able to reset password.	High
7	The user shall be able to email recovery of password in case password is forgotten.	High

USE CASE DIAGRAM



3.3.1 Use case: Sign Up

- Actors: Users.
- Pre condition:
 - The application must be launched.
 - The application must be in a state to save new password.
 - In case of GUA, there must be valid images available that can be set for password.
- Post condition:
 - The user password is saved.
- Success scenario:
 1. The user installs the application.
 2. For GUA, the background image is chosen.
 3. The application allows the user to prioritize the objects shown in the image.
 4. Thus a pattern is created to unlock.
 5. The other option is to set character password.
 6. The user selects a set of characters in a particular sequence that is saved as password.
 7. The user clicks on 'Save' button to save the created password.
- Exception scenario:
 - 6: Character password does not satisfy minimum length requirement.
 - 2: The background image resolution isn't appropriate for processing.
 - 7: The user does not happen to save the newly created password.

3.3.2 Use case: Encryption

Actors: Users.

Pre condition:

- The application is launched and password is entered.

- The application must display option “Browse” to search the files that the user wants to encrypt

- The application must also accept files that have user drags and drops into the application for encryption

Post condition:

- The user chooses browse option to select file , or

- The user chooses drag and drop to select file

Success scenario:

1. The user chooses browse option and selects a file or drag-drop option and drops a file into the application.
2. The application determine the format of the file.
3. The applications encrypts the selected file using format specific encryption algorithm .
4. Encryption successful message is displayed.

Exception scenario:

- 2: The application fails to determine format of the file and cant encrypt it.

- 3: The application does not have a specific encryption algorithm for the determined format.

3.3.3 Use case: File Permissions.

Actors: Users.

Pre condition:

The application is launched and user successfully logs in.

User sets the required file permissions as per his needs to a particular file.

Post condition:

The file permissions are successfully applied to the file chosen by the user.

Success scenario:

1. The application is opened and user is asked for password.
2. User inputs the password.
3. Then the submit button is pressed.
4. User is successfully logged in.
5. User sets the necessary file permissions.

Exception scenario:

- 5: (i) After selecting the File Permissions if the user fails to Press the OK button then default permissions would still exist on the file.
- 5: (ii) Admin authentication required to change file permissions.

3.3.4 Use case: Login

- Actors: Users.
- Pre condition:
 - The application is launched.
 - The application must be in state to accept the password given to it.
 - The application must be in state to recognize the wrong password.
- Post condition:
 - The entered password is accepted and the application is opened.
- Success scenario:
 1. The application is opened and user is asked for password.
 2. User inputs the password.
 3. The screen is displayed wherein the set pattern(password) is drawn.
 4. Then the submit button is pressed.
 5. The appropriate message is displayed.
- Exception scenario:
 - 2: Password is incorrect.
 - 3: If Password is not recognized .

3.3.5 Use case: Image Capture

- Actors: Users.
- Pre condition:

The application is launched.

The application must be in state to accept the password given to it.

The application must be in state to recognize the wrong password.

The application must have permission to access WEB cam on the respective system.
- Post condition:

A Image is captured of the user, no three wrong password tries.
- Success scenario:
 1. The application is opened and user is asked for password.
 2. User inputs the password.
 3. Then the submit button is pressed.
 4. On three continues wrong tries, image is captured of the user.
 5. The image is displayed on next successful login.
- Exception scenario:
 - 4: System permission to access WEBCAM is denied.
 - 5: If there's no WEBCAM on the system, this feature doesn't work.

3.3.6 Use case: Password Reset

Actors: Users.

Pre condition:

- The application is launched.

- The application must prompt the user to enter the password.

- The application must display options for the user to reset password.

Post condition:

- The user chooses to reset password using master reset.

- The password is set to new password.

Success scenario:

- The user chooses Reset password.

- User changes old password to new password according to his preference.

- The user enters new password again.

- The password is set to new password.

Exception scenario:

- 2: The new password set has less than minimum number of characters.

- 3: The new password re entered does not match with new password entered first.

3.3.7 Use case: Email Recovery

- Actors : Users
- Pre conditions:
 - The application is launched.
 - The user has opened log in window.
- Post conditions:
 - The password is mailed to the email ID of user stored during sign up.
- Success scenario:
 1. The user tries to login into the software.
 2. The user forgot the password.
 3. The user clicks on 'Forgot password?' button.
 4. The previously set password is mailed to the email ID of user that was entered during the sign up.
- Exception Scenario:
 - 4: The password is not mailed due to network connection problems.

NON – FUNCTIONAL REQUIREMENTS

3.3.3.1 Performance: Login to the software requires 2sec on average and 4sec maximum for completion. At a time only one user can login and whenever the system is degraded by some unexpected errors the user cannot have access to certain files until the user completes re-login.

3.3.3.2 Safety : If the system fails catastrophically the data stored will be lost permanently.

3.3.3.3 Security: The system is secure from brute force hacking.

3.3.3.4 Reliability: Performs encryption and decryption of files with consistent efficiency.

3.3.3.5 Availability: The software is available in working condition for 98% of times, can be used continuously without any functional issues for 98% of login.

Software and Hardware Requirement Specifications

3.4.1 Minimum Hardware Requirements

3.4.1.1 System should have an inbuilt camera.

3.4.1.2 Core 2DUO processor

3.4.1.3 1GB of free space

3.4.1.4 2GB RAM

3.4.2 Software Requirements

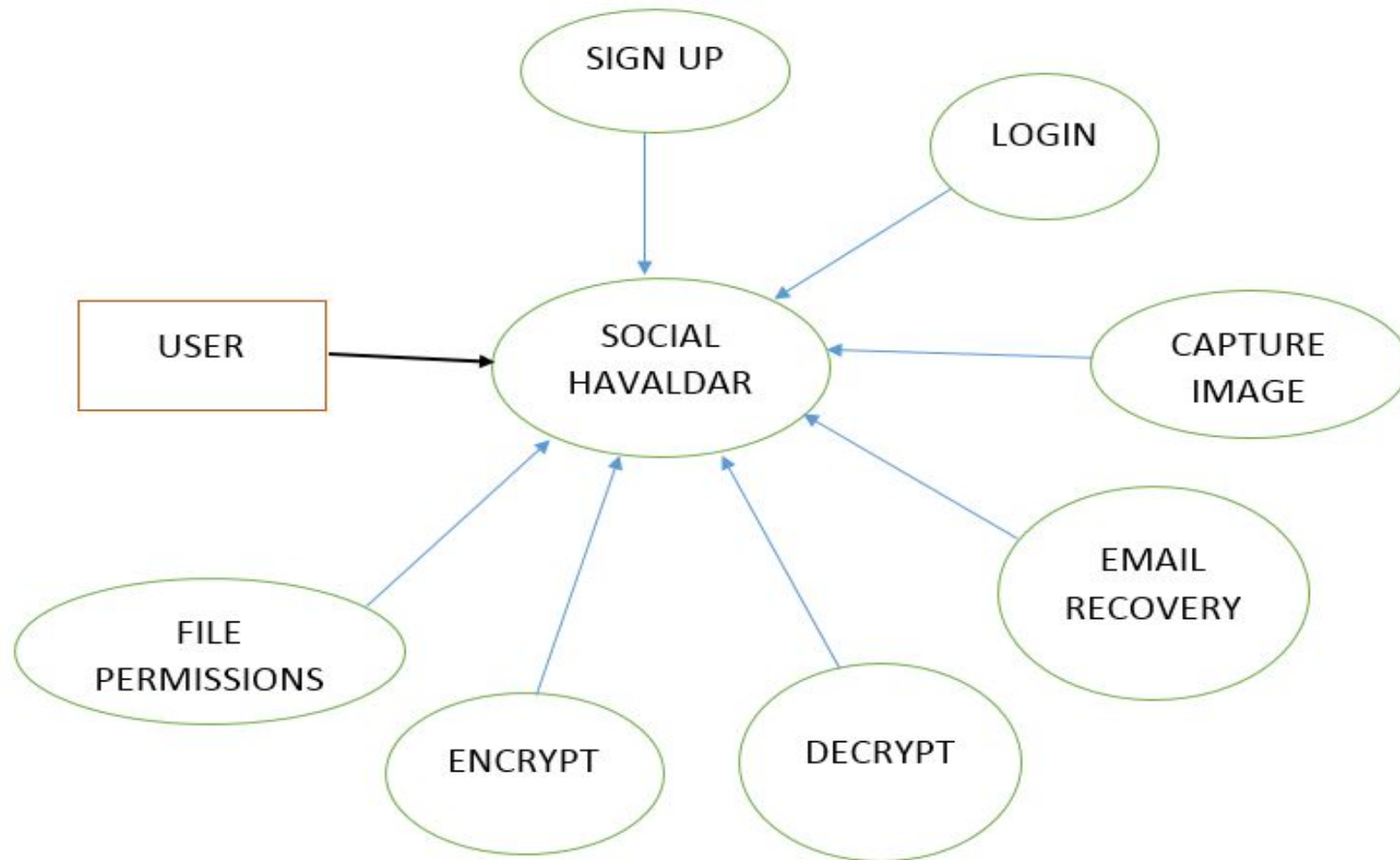
3.4.2.1 JDK version 1.4 onwards.

ACCEPTANCE TEST PLAN

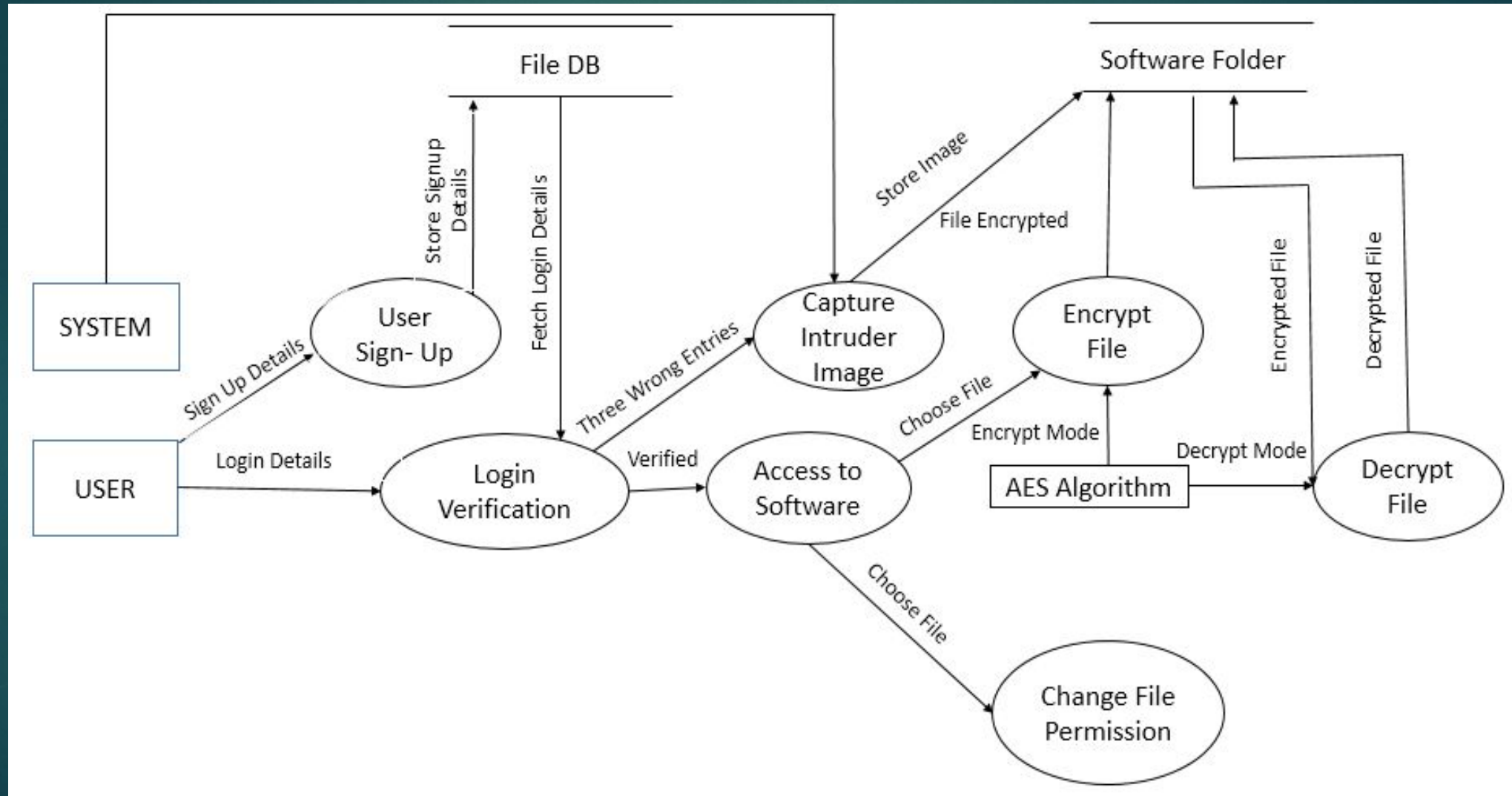
Test ID	Requirements ID	Input Description	Expected Output	Actual Output
3.7.1	1	User Sets valid password	Password saved message displayed.	Password saved message is displayed.
3.7.2	1	User Sets password and Password length insufficient.	Password length insufficient message displayed.	Password not set message is displayed.
3.7.3	2	File chosen using browse option/ drag-drop	File Encrypted	File encrypted message is displayed.
3.7.4	2	Invalid File chosen using browse option/ drag-drop	File format not detected.	File doesnot exist message displayed
3.7.5	3	File Permission chosen by user for the file	File permission changed	No message displayed but file permissions changed.
3.7.6	3	Unauthorized File Permission chosen by user for the file	Admin authentication required to change file permissions.	No message displayed and file permissions donot change.
3.7.7	4	User enters genuine password	Successfully logged in	Login complete message displayed.
3.7.8	4	User enters wrong password	Wrong password. Please re-enter password	Invalid username or password message displayed.

3.7.9	5	User enters 3 wrong password	Image captured	Invalid username or password message displayed and image is captured.
3.7.10	5	User enters 3 wrong password in system that doesn't have a WEBCAM	Image not captured	Invalid username or password message displayed and image is not captured.
3.7.11	6	User chooses password reset option	The password is set to new password.	Password successfully changed message is displayed.
3.7.12	6	User chooses password reset option and enters invalid password.	Password reset failed, new password is not activated.	Password reset failed message is displayed.
3.7.13	7	User chooses email recovery of password.	Username and password is mailed to the stored email ID of user.	Password successfully mailed message is displayed and username and password are mailed.
3.7.14	7	User chooses email recovery of password when there is no internet connection.	Username and password is not mailed to the user.	Password could not be mailed message is displayed and username and password is not mailed.

Level 0 DFD



Detailed DFD



Class diagram



Module Test Plan and Test

Cases

6.2.1 Sign up

Test ID	Input Description	Expected Output
1	User Sets valid password	Password saved message displayed.
2	User Sets password and Password length insufficient.	Password length insufficient message displayed.
3	User doesn't enter email ID during signup.	Sign up incomplete message displayed.

6.2.2 Login

Test ID	Input Description	Expected Output
1	User enters genuine password	Successfully logged in message displayed.
2	User enters wrong password	Invalid username and password message displayed.
3	User enters wrong username.	Invalid username and password message displayed.

6.2.3 Image capture

Test ID	Input Description	Expected Output
1	User enters 3 wrong password	Image captured , no message displayed.
2	User enters 3 wrong password in system that doesn't have a WEBCAM	Image not captured no message displayed.
3	User enters wrong username or password twice.	No image captured. Only message displayed.

6.2.4 Encryption

Test ID	Input Description	Expected Output
1	File chosen using browse option/ drag-drop	File encrypted message shown and encrypted file is stored.
2	Invalid File chosen using browse option/ drag-drop	File doesn't exist message displayed.

6.2.5 Mail Recovery

Test ID	Input Description	Expected Output
1	User chooses password reset option	Unique ID mailed
2	User chooses password reset option when there is no proper connectivity.	Mail not sent, password recovery failed message displayed.

RESULTS

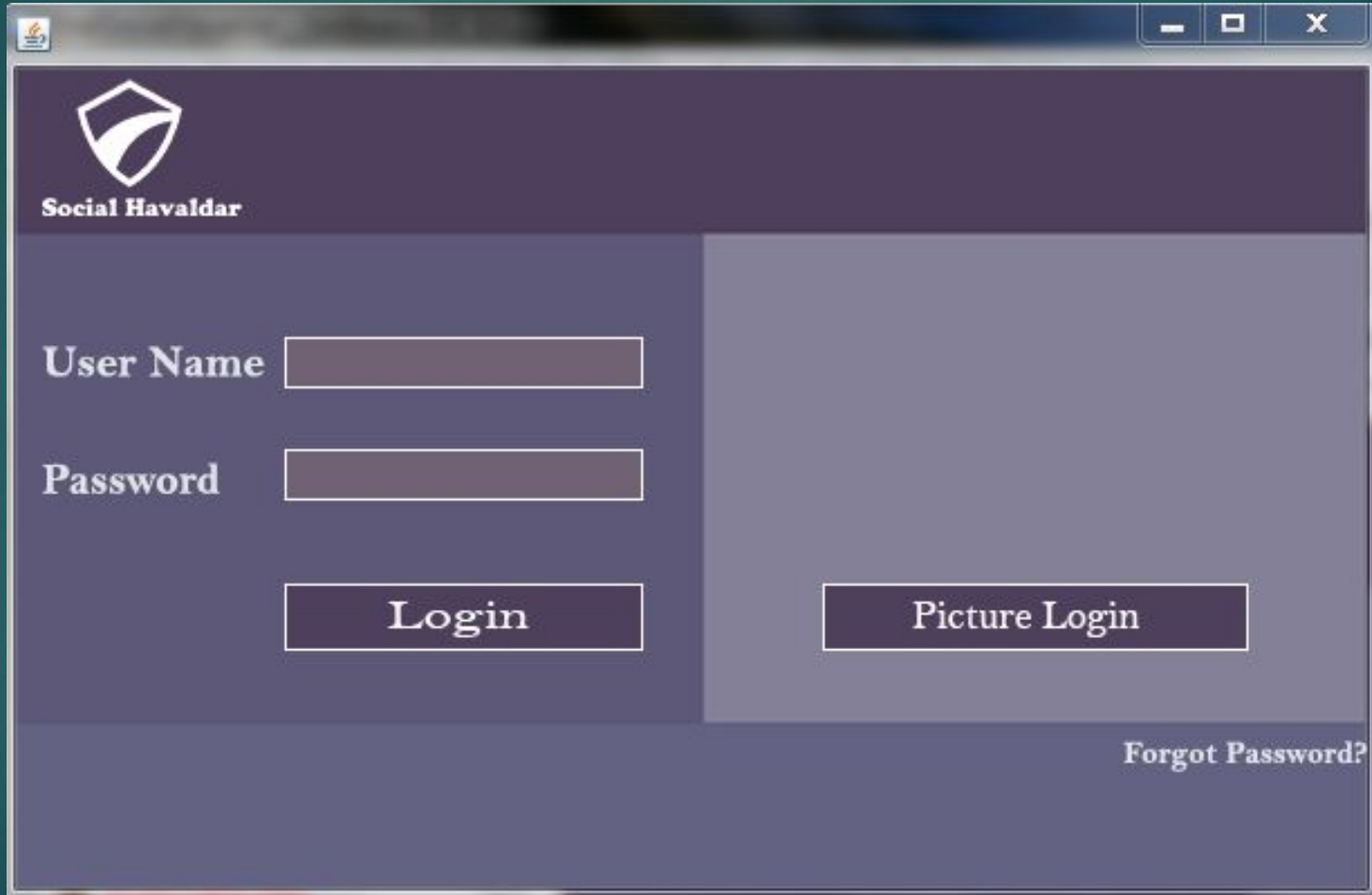
The Social Havalдар system is activated for the first time when the user performs Sign up operation successfully. The following screen appears when the user signs up for the first time.




The screenshot shows a web application window titled "Social Havalдар". The window has a dark purple header with a white shield logo on the left and the text "Social Havalдар" next to it. Below the header, the main content area is a lighter shade of purple. It contains four input fields arranged vertically, each with a label to its left: "User Name", "Password", "Confirm Password", and "Email". At the bottom of the form, there are two buttons: "Picture Password (Optional)" and "Sign Up". The "Sign Up" button is larger and more prominent.

User Name	<input type="text"/>
Password	<input type="password"/>
Confirm Password	<input type="password"/>
Email	<input type="text"/>

Once the user signs up into Social Havalдар by setting valid username and password, and/or picture password the use can login into the system. The following screen appears when the user wants to login into Social Havalдар.

A screenshot of a web application window titled "Social Havalдар". The window has a dark purple header with a white shield logo on the left and the text "Social Havalдар" next to it. The main content area is divided into two columns. The left column contains a "User Name" label followed by a text input field, a "Password" label followed by a text input field, and a "Login" button. The right column contains a "Picture Login" button. At the bottom right of the window, there is a link labeled "Forgot Password?". The window has standard Windows-style window controls (minimize, maximize, close) in the top right corner.

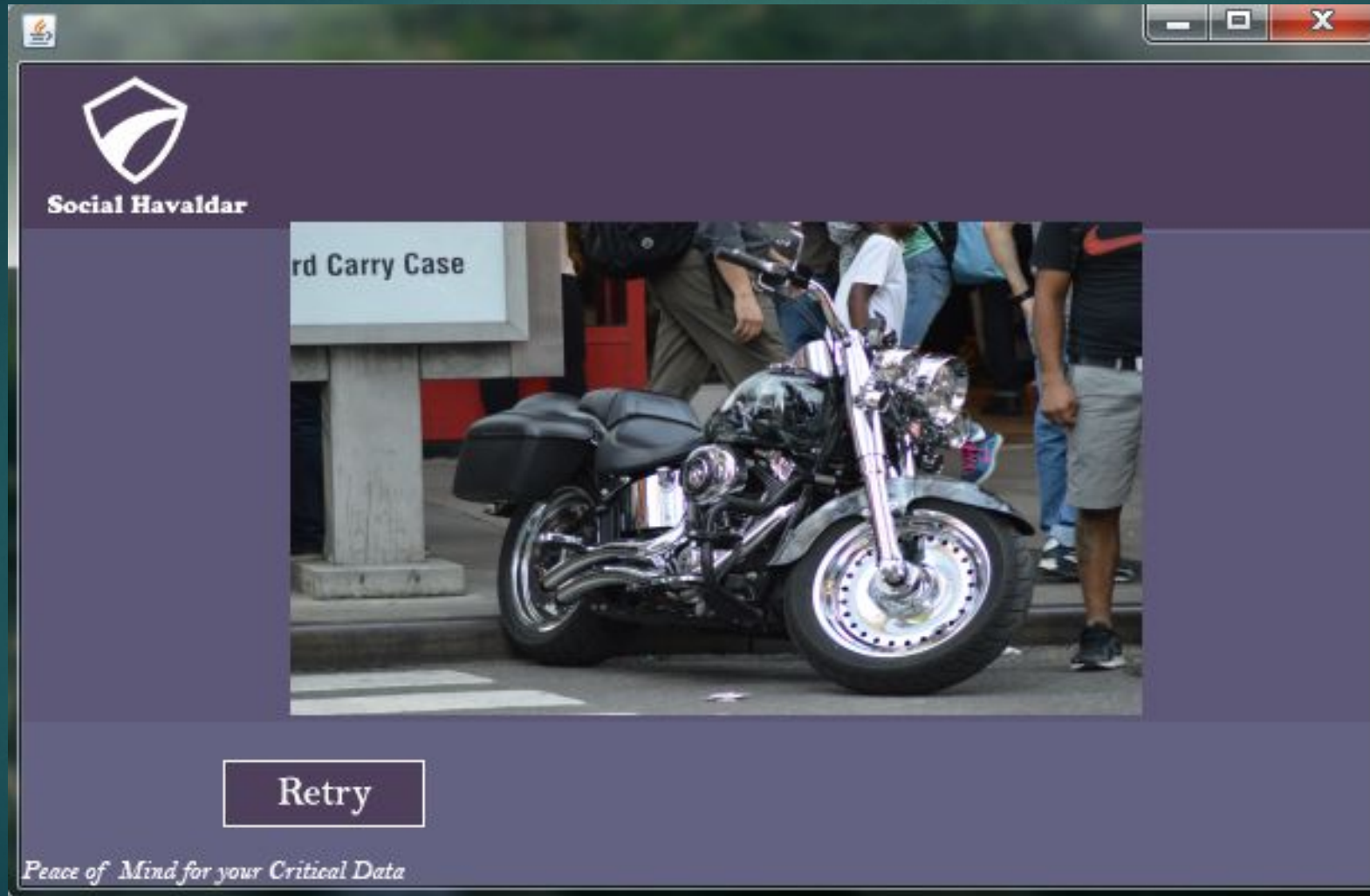
 **Social Havalдар**

User Name

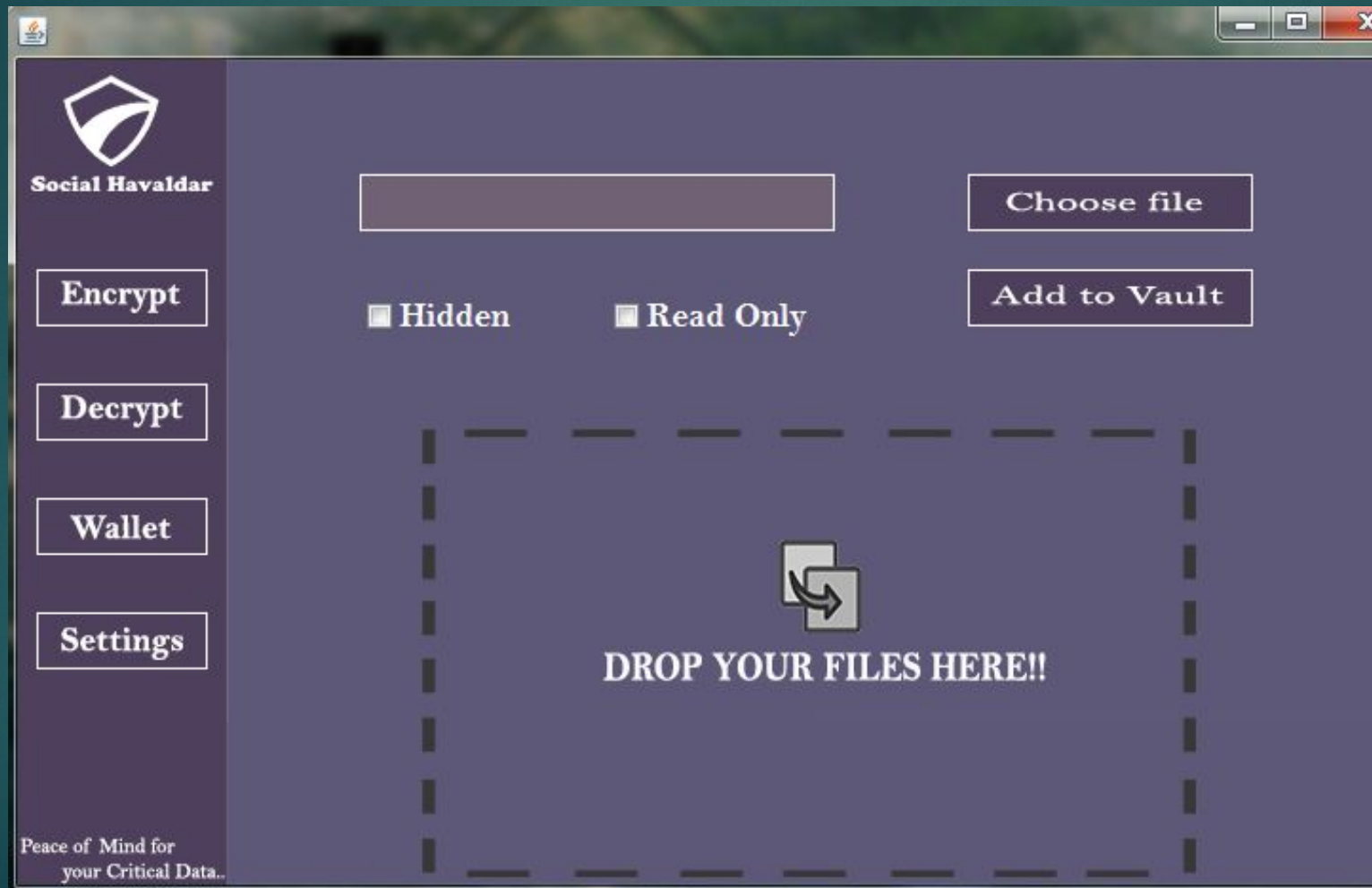
Password

[Forgot Password?](#)

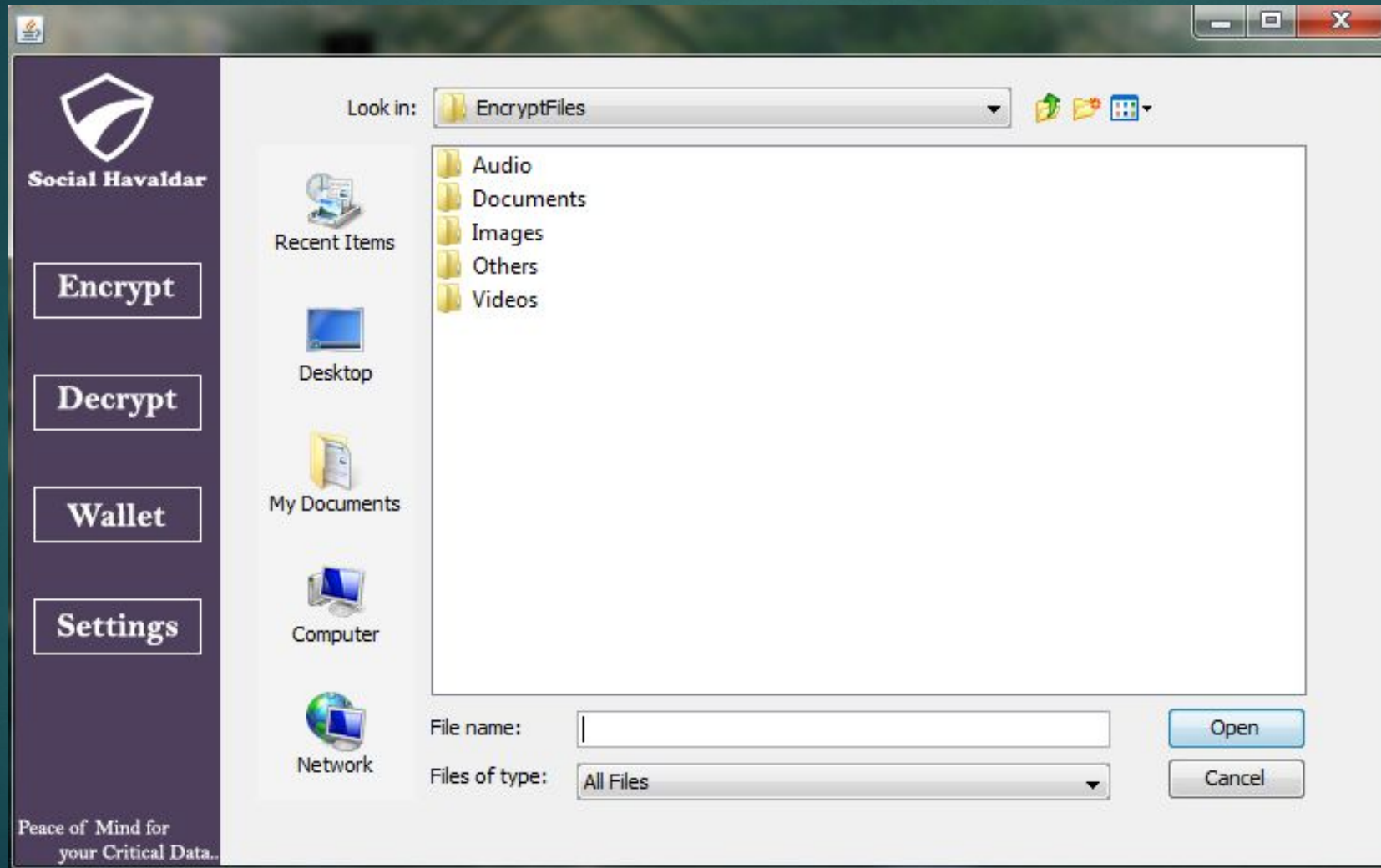
The picture password which is the part of GUA is also an option for security of the folder. The following window appears when the user selects picture password.



Once the user performs the login operation successfully by entering correct username and password and/or picture password, user can choose any file they desire either by browse option or by drag and drop option and encrypt it. The user can also set file permissions to the selected file. The following screen appears for encryption.



The user can also decrypt the encrypted files anytime from the encrypted files folder. The following screen appears for decryption of encrypted files.



In addition to all the functional requirements mentioned above in the SRS section, Social Havaladar also provides the feature to store information regarding wallet or credit/debit cards so that only user can access these private wallet information whenever required in any transactions. The following are the screens that appear for wallet storage.

Card Name

Card Number

Expiry Month

Expiry Year

CVV

Add

Cancel

Social Havaladar

Encrypt

Decrypt

Wallet

Settings

Peace of Mind for
your Critical Data..

Add new Card to your Wallet here

YOUR WALLET

CARD NO4214567489012347

EXPIRY MONTH/YEAR22016

CVV123

VISAMaestroCirrus

NEXT CARD