

Bachelor of Computer Science

(Digital Systems Security)

Final year project – Proposed system solution

(CSCI321)



A location based document locking application

# Project Team structure

|  |  |  |
| --- | --- | --- |
| Name | Email | Role |
| Abhi Jay Krishnan | [ajk126@uowmail.edu.au](mailto:ajk126@uowmail.edu.au) | Manager, Designer |
| Durrah Afshan | [durrahafshan@gmail.com](mailto:durrahafshan@gmail.com) | Documenter |
| Rivaldo Erawan | [rivaldo.erawan97@gmail.com](mailto:rivaldo.erawan97@gmail.com) | Implementer |
| Kim Heoncheol | [effectmix@gmail.com](mailto:effectmix@gmail.com) | Tester |

The above team structure is implemented in order to clearly distinguish the area each team member is to focus on and it does not mean he/she will be the only one involved in doing that task. This is to have a pair of eyes watching each aspect of solution development.

We have decided to use a private GitHub repository for version controlling and team collaboration. Each team member will have local repository which will then be merged with the central repository. All members will be working on different part of the project at a given point in time to prevent clashes when committing to central repository. All documents and source codes will be stored in this central repository.

Each project meeting will have a project dairy summarising the content of the meeting and what actions have to be taken.

# Market Survey

We have done a bit of a research on the currently available applications in the market before defining the project scope. Here are the apps, their features and somethings that are they missing out.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **App** | **Platform** | **Description** | **Security** | **Features** | **Short-comings** |
| **Secure Safe** [1] | iOS, Android, Desktop (Mac) | App for online file storage & password management. Unique service as it provides double encryption, triple data storage and zero knowledge architecture, which ensures very high level of data security and privacy protection. | * Automatic logout upon exiting the program * Encryption is done using AES-256 and RSA 2048 * Files are decryptable only by the user itself * Communication between client-server is secured using https * Passwords are encrypted for maximum security * Support 2-factor authentication (SMS token) for premium users | * Login includes password and id (email) * Save texts, images, documents (scans), and videos * Scans (similar like pictures and convert to pdf) * Email system * Import/export data | * Connection independent (slow connection leads to slow access to data) * Need internet connection, offline mode can only access passwords * Allow multiple login attempts with wrong password/id * No password recovery |
| **Passible** [2] | iOS | A password management app which is redesigned for fast and simple experience while entering website’s logins and credit cards. | * Automatic logout after exit from program * AES-256 encryption * Does not allow multiple login attempts (timeout 5 minutes for 3 consecutive wrong attempts; after that each wrong attempt will get a 5-minute timeout) * Encryption with key and random string | * Login using 4-digit pins * Support Touch-ID (fingerprint) * Save account credentials and credit card details * Analyzing password strength features * Support offline mode * Private web browser | * Does not support import/export data * No password recovery |
| **File Locker** [3] | Android | App to protect your content against unauthorized reading, playing, watching, etc. The application encodes the file and makes it unreadable. | * Fast way to lock huge files (like movies) by hashing just both beginning and ending of file (optional). * Tracks temporary unlocked files by notification, to keep in mind you left unprotected docs. * Encodes the content and file names as well. | * Involves Android Media Scanner automatically after change to make file visible by other applications. * Smart looking through directories for documents, locked and unlocked files. * Opens documents directly from app. * Notifies about forgotten unlocked files, which were left by user. | * No password recovery as password is not stored anywhere. * Only one-way encryption. |
| **File Locker – Lock any file** [4] | Android | App that keeps all files secure and private with file locker. File Lock lets you password-protect your personal files (ex: photos, videos, documents, etc) in android phones. | * Encrypts file and save in secret location in SD Card so that file is completely secure. * Import files from SD Card / Phone Memory * Password protected app entry with a numeric code or Pattern lock. | * Unlimited files can be locked. * Optimized for HD tablets. * Fastest lock process with multi-select feature to import hundreds of files quickly. * Intuitive interface for a great experience. * Hide sensitive videos and pictures. * Opens documents directly from app. * Password recovery option is available | * Encryption and decryption is not location based. |
| **Private Photo Vault** [5] | iOS, Android | A photo safe that keeps all private pictures and videos hidden behind a password. | * Automatic logout after exit from program. * Login using 4-digit pin/pattern lock. * Import/export data * Pass recovery (email) | * Save photo and videos * Support offline mode * Private browser | * Allow multiple login attempts with wrong pins |

## Conclusion

The table above shows a comparison between 5 software applications available in the market. This survey shows the different types of platform the application can run on. It provides information on the features that have been used. The most common feature in all these app is that they use encrypted password for securing files such as images, videos, documents, etc. Major drawback noted from the table is the lack of password recovery and the encryption/decryption of files is not location based.

# Project Scope

## Project purpose

This project aim to provide user a way to store confidential documents in mobile devices and access it only in the area he/she find it is safe. By including two factor protections, one being password (what the user knows) and second being the location (where the user is currently), we will be able to provide a better solution compared to the applications currently in the market (based on market survey).

These are few ways a document in a mobile device may be compromised: -

* The documents stored in mobile device may end up in the wrong hands if the device itself is stolen.
* The user may lend the device to someone who intern may wish to gain access to these documents.
* The documents may be accessed remotely by penetrating device through network.

Our solution aim to provide a secure vault for document storage so the it does not get into wrong hands even if the device is compromised.

## Target Users

There are several applications for this solution in the market, here are few of them:-

1. Employees working in defense industry may have to handle highly secretive documents that should not be taken of the secure premises.
2. Most of the large firms these days have documents that are their intellectual property and wish to keep them from getting into wrong hands.
3. General public may want to store their personal information and keep it within their safe zone such as their home.
4. Governmental authorities may wish to keep their confidential documents within the country or within the restricted area.
5. A hospital may wish to keep the patient’s document within the campus but at the same time giving staff the freedom to view it while moving around.
6. A school may want to let the authorized staff to review an exam paper on the move while keeping the document within the restricted zone.

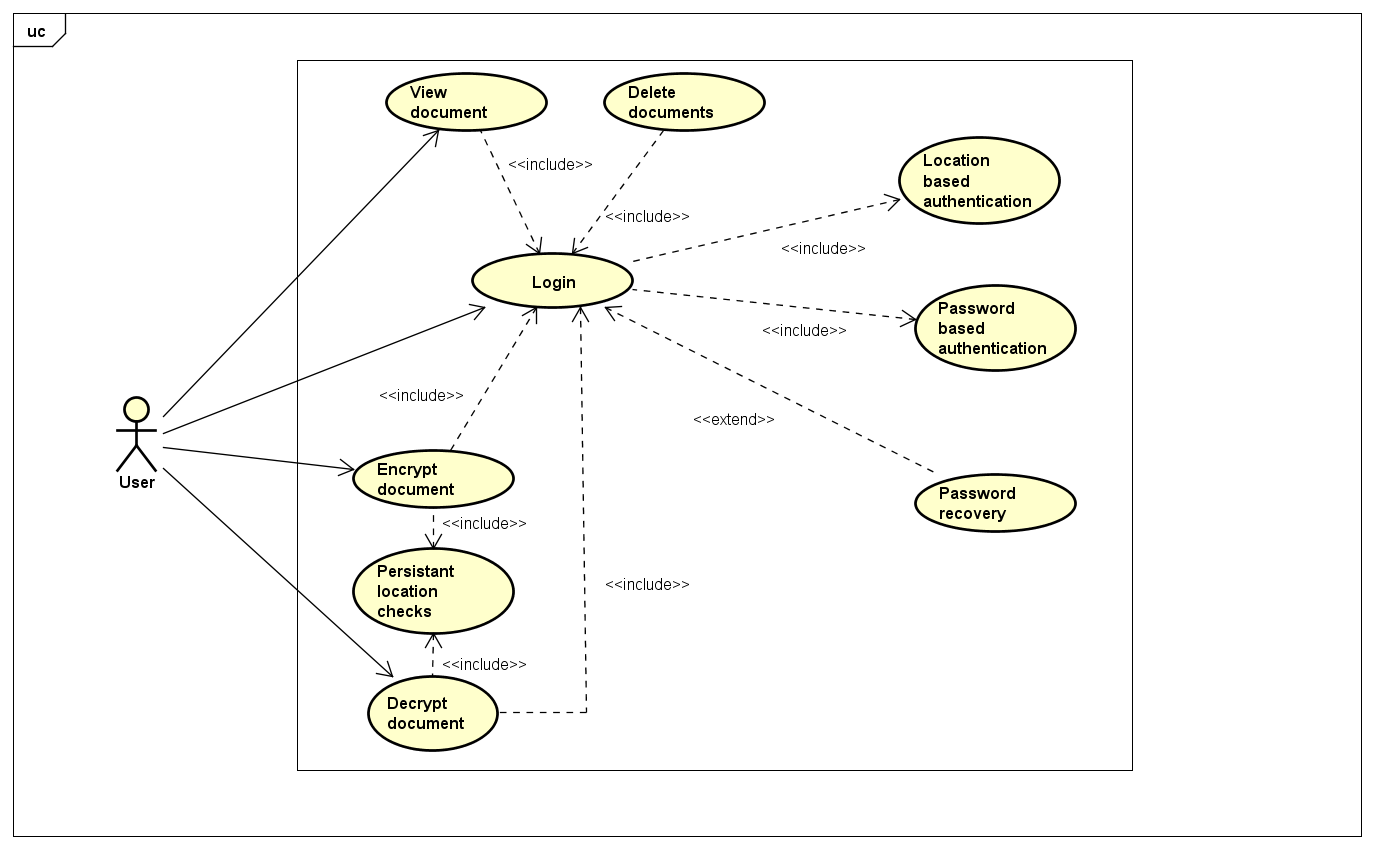
## Proposed features

The proposed solution is an android based app with following features: -

Highest level use cases

* Login
* PDF viewer
* Encryption and Decryption
* Import or archive pdf from local directory
* Delete existing files
* Move the imported files to a secure directory (ask user if they wish to delete the original document)
  + Files in secure folder are encrypted
  + SQLite database contain encrypted metadata and user details will be backed up here.
* Password recovery based on trusted location and challenge questions.
* Persistent location check to make sure that the user is within predefined secure radius.
* Notification to tell user that user is leaving the safe zone.
* Further Enhancements:
  + Inclusions of more file types and viewers.
  + Ability to access same document at multiple locations.

### Highest level use case diagram



# Risk List

|  |  |
| --- | --- |
| **Risks** | **Actions** |
| Sudden growth in requirement as the project progress. | Readjust project time line to accommodate the changes. |
| Team members unable to contribute to the project due to health or other valid reasons. | Distribute workload among remaining members. Making use of GitHub repository will help the team member who is not able to come for meeting to contribute remotely. Also using other means such as skype calls and TeamViewer. |
| Estimation and scheduling of development time is done on initial stage and there may be glitches along the way that will set back the project timeline. | Project plan can be revisited and adjusted to fit within the given deadline. |
| Usage of new and ever-changing products in the market will lead to bugs in software that is being developed. | Proper research and training is critical when using a new tools, techniques, protocol or systems. |
| System performance may be compromised when having substantial number of features. | Usage of good programming practices and threading. |
| Selecting an unsuitable design architecture | Doing a good research and developing a good picture of the end goal based on past experiences (market survey). |
| Loosing support for API (Application programming interface) used while making the solution. | Usage of good object oriented or modular programming architecture will help in transiting from one API to another with minimal work. |