

Bachelor of Computer Science

(Digital Systems Security)

Final year project – Proposed system solution

(CSCI321)



A location based document locking application

Table of Contents

[Project Team structure 1](#_Toc488844100)

[Market Survey 2](#_Toc488844101)

[Conclusion 4](#_Toc488844102)

[Project Scope 5](#_Toc488844103)

[Project purpose 5](#_Toc488844104)

[Target Users 5](#_Toc488844105)

[Proposed features 6](#_Toc488844106)

[Programming development methodologies 8](#_Toc488844107)

[Waterfall 8](#_Toc488844108)

[Prototyping model 8](#_Toc488844109)

[Agile model 9](#_Toc488844110)

[System Architecture 11](#_Toc488844111)

[Design principles of the application: 11](#_Toc488844112)

[The proposed application will have the following quality: 11](#_Toc488844113)

[Risk List 13](#_Toc488844114)

[References 14](#_Toc488844115)

# 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 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 must 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 they are 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: -

### Login

The user has to login to access the files. The location is verified only after the user logins. The password and user data will be hashed to using a collision resistant, pre-image resistant and second pre-image resistant. A good hash function would be SHA-256.

#### Password Recovery

The user can set a password recovery location with a small radius for password recovery. The user needs to be at this location to change password. The must set a challenge question with an appropriate answer. The user can set change their password recovery settings when they are logged in.

### PDF Viewer

A PDF viewer for user to view his documents in the vault. The pdf viewer will only be accessible after the user has been authenticated and if the user is within the radius of the location stored in the database. The pdf viewer will close when the user moves out of this zone.

### Encryption and decryption

Files are encrypted using secure cryptographic algorithm such as Advanced Encryption standard. The file will not have the same name as the original file after encryption, the original name will be stored in the database along with the new name. The user will be able delete the file in the vault after authentication. The user can import files from local directory to a secure directory. They may wish to delete the original file.

The database containing the user data and file meta data is encrypted using secure cryptographic algorithm.

### Migration

The user may wish to move to a new device, the app saves data into a folder so the user can copy the encrypted file to the new phone reinstall application, specify the folder containing the data and he will be good to go.

These are the key features that will be included in the application. Further enhancements such as support for more file types will be added if these basic requirements are met.

### Highest level use case diagram

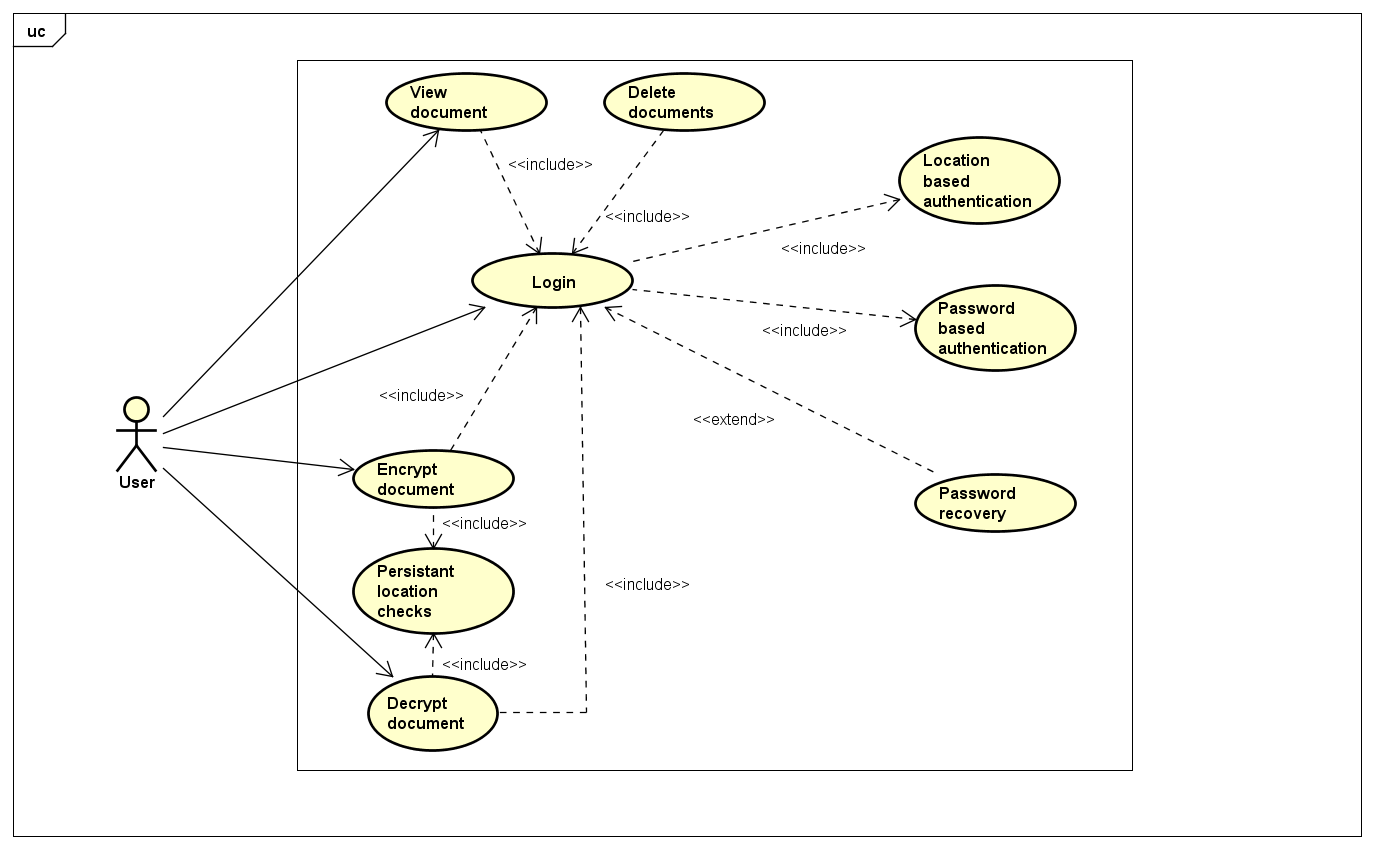


Figure 1: highest level use case diagram

# Programming development methodologies

## Waterfall

This is a legacy model for software development projects. The development cycle is linear and not capable of supporting challenges faced by modern software development domain such as changing user requirements and adaptations. There is high amount of risk and uncertainty using [6].



Figure 2: water fall model

## Prototyping model

Under this model the requirements are gathered from user and a prototype is build based on it for evaluation before refining requirements. This iteration repeats until final design is confirmed before final construction of the product itself. This model may be inappropriate for this project as there are no rapid changes that may need iterative prototyping. Prototyping also require active involvement of end user which is not possible for this project [7].

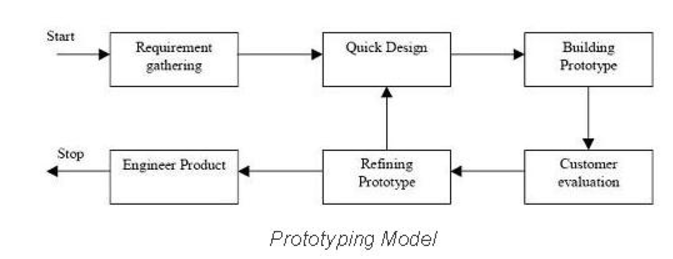


Figure 3: prototyping model

## Agile model

Agile methodologies include Extreme Programming (XP), Scrum, Crystal, Dynamic Systems Development Method (DSDM), Lean Development, and Feature-Driven Development (FDD). They all are based on a common principle of iteration and continues feedback that it provides to successively refine and deliver a software system. This method also requires active involvement of end-users and may track off the user is not sure about the outcome they want. There is also lack of emphasis on necessary designing and documentation. Hence agile model may not suitable for this project [8].



Figure 4: agile model

Rational Unified processing

Rational unified processing model provide a disciplined approach to assigning task and respocibilities within the development organisation. The development is divided into 4 sections:-

Inception – The project scope is defined along with requirements gathering and Risk analysis.

Elaboration – Coming up with detailed design of the system.

Construction – The actual development of the system.

Transition – Testing and deployment of the system.

There may be more than one iterations for each of the above stages and the also provide a flexibility to make changes to requirement deep into the development cycle [9].



Figure 5: Rational Unified Processing

After considering above different models we have decided RUP is the most suitable for this project as it allow us to decide the business case, need less involvement of end user and gives flexibility to make changes during later part of the development process.

# System Architecture

The architecture adopted by the application will be standalone. Standalone means that the application will operate independently by itself without having to rely on or being a part of another system. Since the main purpose of the application is to secure the user’s data, standalone would be the best option to have the best security and reliability. It is because the data stays within the application itself and it does not have to depend on other system to operate.

Other architecture that have been considered are client-server and web-based. Client-server opens more possibilities for the application to have more interesting features, however it also raises more threats such as network attacks. In addition, there would be a cost to set up the server and maintenance of the server itself. All of this can apply for web-based architecture too since it uses a server. Additionally, web-based is less desirable due to its performance issue because there is no local storage for the application so the performance is very dependent on network connection to access the data.

## Design principles of the application:

### Modularity

separating the functionality of a program into independent, interchangeable modules, such that each contains everything necessary to execute only one aspect of the desired functionality.

### High Cohesion

**E**ach module has functions and elements that are strongly related, only to fulfil one particular purpose or task

### Low Coupling

modules are loosely coupled and independent so that a change in one module do not affect the other modules

### Standardization

Implementation will conform to standard that has been established and agreed by different parties, this is crucial for things like security

## The proposed application will have the following quality:

### Extensibility

The proposed application can add additional functionality without changing or damaging much of the current system. New data types can be added as long as it is supported by the android

### Maintainability

Following the design principles of high cohesion and low coupling, small modifications will not be a problem. Changing one module will not affect other modules significantly.

### Performance

The response time will be in acceptable manner even with the huge amount of data that are processed. Efficient encryption algorithm is used as well as other processing algorithm

### Usability

Adapting KISS (Keep It Simple Stupid) principle in designing interfaces will give user easier times in learning and figuring out the proposed application. It lets user to take less time to perform a certain task.

### Compatibility

The proposed application will be able to run in various type of android devices as well as different version of android.

### Security

Data are kept safe by encryption and login is required to have access. Security measures like protection against SQL injection or encryption algorithm will follow standard

# 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. |

# References

|  |  |
| --- | --- |
| [1] | dSwizz, “SecureSafe,” dSwizz, [Online]. Available: https://www.securesafe.com/fr/. [Accessed 2017 July 23]. |
| [2] | Passible, “Home page,” Passible, 10 Oct 2016. [Online]. Available: http://www.passible.com/#security. [Accessed 23 July 2017]. |
| [3] | M. Wojas, “File Locker,” Marcin Wojas, 6 May 2014. [Online]. Available: https://play.google.com/store/apps/details?id=com.mwgo.filelocker. [Accessed 23 July 2017]. |
| [4] | Innorriors, “File locker - Lock any File,” Innorriors, 15 June 2017. [Online]. Available: https://play.google.com/store/apps/details?id=inno.filelocker. [Accessed 23 July 2017]. |
| [5] | Legendary Software Labs LLC, “Private Photo Vault,” Legendary Software Labs LLC, 11 July 2017. [Online]. Available: https://play.google.com/store/apps/details?id=com.enchantedcloud.photovault. [Accessed 23 July 2017]. |
| [6] | “What is Waterfall model- advantages, disadvantages and when to use it?,” ISTQB EXAM CERTIFICATION, [Online]. Available: http://istqbexamcertification.com/what-is-waterfall-model-advantages-disadvantages-and-when-to-use-it/. |
| [7] | ISTQB EXAM CERTIFICATION, “What is Prototype model- advantages, disadvantages and when to use it?,” ISTQB, [Online]. Available: http://istqbexamcertification.com/what-is-prototype-model-advantages-disadvantages-and-when-to-use-it/. |
| [8] | I. E. CERTIFICATION, “What is Agile model – advantages, disadvantages and when to use it?,” ISQTB, [Online]. Available: http://istqbexamcertification.com/what-is-agile-model-advantages-disadvantages-and-when-to-use-it/. |
| [9] | P. Christensson, “RUP,” TechTerms, 2006. [Online]. Available: https://techterms.com/definition/rup. [Accessed 25 July 2017]. |