UNIVERSITY OF WOLLONGONG AUSTRALIA

SIM GLOBAL EDUCATION

Bachelor of Computer Science (Digital System Security)

CSCI321 – Final Year Project

Project Proposal

Project Particulars

Supervisor	Dr Ta Nguyen Binh Duong
Project Group	SS18/1F
Project Title	Two Factor Authentication

Project Team's Particulars

Student Number	Student Name	Email Address
5363536	Koh Hong Wei	hwkoh003@mymail.sim.edu.sg
5710923	Chua Han Ming Adler	hmachua002@mymail.sim.edu.sg
5711356	Ong Wei Hao	whong012@mymail.sim.edu.sg

go2FA

A secure file locking application

Document Control

Title: Project Proposal

Document Name: FYP_ProjectProposal

Distribution List

Name	Title/Role	Where

Record of Revision

Revision Date	Description	Section Affected	Changes Made By	Version after Revision	Notes
23/01/18	Initial Setup of project proposal	-	Adler	1.0	
24/01/18	Populating Data into project proposal	-	Team	1.1	
26/01/18	Finalizing Project Proposal	-	Hong Wei	1.2	Individual Parts collated and compiled together.

Table of Contents

Project Team Structure

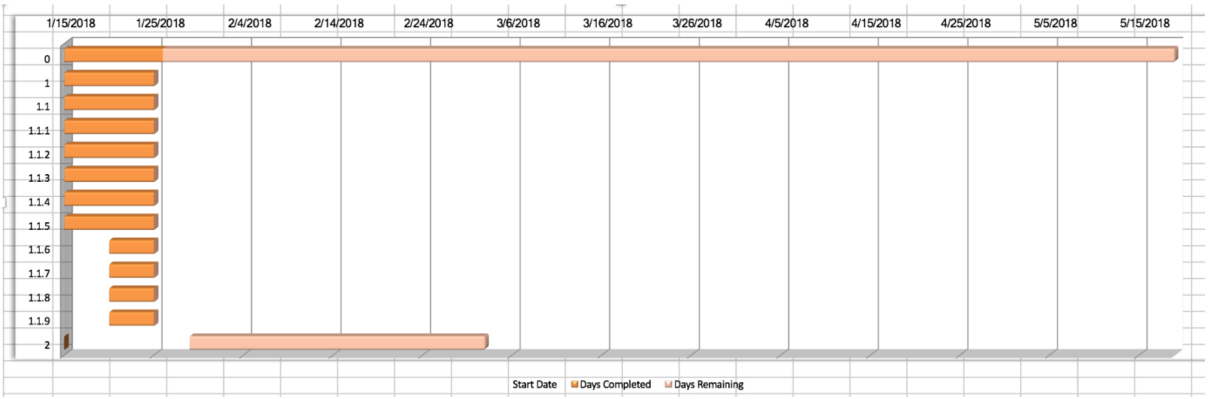
Name	Email	Roles
Koh Hong Wei	hwkoh003@mymail.sim.edu.sg	Manager, Tester
Chua Han Ming Adler	hmachua002@mymail.sim.edu.sg	Implementer, Documenter
Ong Wei Hao	whong012@mymail.sim.edu.sg	Designer, Documenter

The above team structure is implemented to clearly distinguish the area each member of the team is to focus on but it does not infer that he/she will be the only one involved in doing that task.

SmartSVN and a private GitHub repository will be use as version controlling and team collaboration tool. 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.

Meeting minutes will be noted down during every meeting summarising the content of the meeting and what actions to be taken.

Project Gantt chart



	Task Name
0	Full Project Time Line
1	Inception Phase 1
1.1	Project Proposal
1.1.1	Background introduction
1.1.2	Defining project scope
1.1.3	Market Research on Current Product
1.1.4	Target User
1.1.5	Proposed Features
1.1.6	Highest Level Use Case
1.1.7	Comparison 1: Application Develop Language
1.1.8	Comparison 2: Database
2	Inception Phase 2

1. Introduction

1.1. Background

This project proposal was written to document the research and proposed idea for the Final Year Project entitled “Two Factor Authentication”. Impersonating others has always been an issue when it comes to cyber threat. As technology advances, using password alone is no longer as effective as before. Attackers tends to develop new ways to breech security and obtain sensitive data.

Our group is tasked to develop a two factor authentication to enhance current security authentication that are already implemented in current applications, systems or devices.

In this proposal, we will bring you through on our market research and our proposed idea.

1.2. Project Purpose

This project aims to provide the following to users:

- To enhance security on file management
- Provides 2 factor authentication to unlock files
- A secure vault that only allows intended users to access files

1.3 Target Users

According to our market research, we found our application suitable for the following group:

1. Employees in a workplace that wants to keep documents with different security level confidential from other employees using the same machine.
2. Student using school machine for assignment or homework and wants to keep it confidential from other students who might use the same machine after.
3. General public using shared machine with documents or information saved on such machine.
4. Family using a shared PC to keep their files safe and secure.

2. Market Survey

2.1. Market Research and Current Products

Below are a few ways of user authentication that are already in the market and example of products in the market that are using them.

Application	Platform	Description	Security	Features
1Password	Android	This application remembers all your passwords for the user, the user would need a master password or using fingerprint authentication before being able to access the rest of the passwords	Login using master password or fingerprint authentication Lock the app automatically to ensure data is protected, even if device is lost or stolen	Create strong, unique passwords for all online accounts Fill usernames and passwords into websites and apps Access information on all user's mobile devices and computers Share passwords securely with family or company Unlock using fingerprint unlock
Authenticator Plus	Android	Authenticator Plus generates 2-step verification to protect accounts with your password and phone/tablet	Secure – 256-bit AES encryption and Pin lock for security Automatic back/restore- accounts are automatically backed up to cloud Fingerprint support – Unlock the app through fingerprint	Generates a 6 digit OTP after scanning QR code generate from facebook or other site. This OTP serves as a second authentication factor before being able to access to the account Organize – group accounts with categories and re-order frequently used accounts to top

App Lock: Fingerprint Password	Android	A secure and easy-to-use application locker with pin, pattern or fingerprint password protection	Second authentication factor even though the user's phone is unlock. App Lock able to prevent others from opening locked apps, deleting or purchasing anything while on the user's phone	Put a Pin, Pattern or fingerprint lock in front of any app on your phone like Facebook, Snapchat. When opening a protected app, App Lock will ask to confirm password the user have set to let the user in
Google Authenticator	iOS, Android, website	A software token that implements two-step verification using Time-based One-time algorithm and HMAC-based algorithm.	Google account (username and password) Implements algorithm specified in RFC 6238 & 4226	Uses QR code to register account One google account to manage multiple 2FA applications Password Managers File hosting services
Hardware token		A keychain sized security token which generates OTP. Each time user logs in, user will press the button on the token to generate the OTP and the OTP will be displayed on the screen of the token.	Only generates OTP when user press on the button on the token	OTP is generated based on time and last for a certain amount of time before a new OTP will be generated upon request.
SMS OTP	Mobile with SIM card	SMS containing OTP will be sent to mobile phone registered. OTP sent whenever user log in with Username and Password	OTP is sent to registered mobile number.	OTP is sent via SMS to user. OTP last a certain amount of time
Yubikey	NFC devices/ computer	Touch the button to trigger security based on public-key cryptography: works instantly, no need to re-type passcodes from a device — replacing SMS texts, authenticator apps, legacy tokens, and similar devices	Only allow accessing when the key is plugged in or detected by NFC.	Can be used for any accounts, by NFC or USB form. Key allows 2FA done when accessing account-based sites(fb/gmail)

3. Proposed Solution

After conducting our market research, we propose a 2FA product that provides the following:

- To use this product, users are required to have a smart phone equipped with a camera.
- Each users are to initialize an account with our application.
- On the mobile application, users will be prompt to login using his/her fingerprint.
- To lock a file on the computer, run the desktop application and login using the username and password.
- Select file that the user wish to lock. A unique QR code will be produced and users are required to scan the QR code with their mobile phone.
- Using a unique cryptographic algorithm, the mobile app will produce a unique OTP that will be used to lock the file on the desktop.
- To unlock, the user does the same steps as above.

3.1 Proposed Features

Setting up an account

- Users will be allowed to set-up an account with us using their email address.
- Select a unique username and a password to complete registration.

Locking of File/Folder

- Files can only be locked upon logging into his/her account.
- Scanning of the QR code produced on the application with the mobile phone will produce a unique OTP.
- Enter the OTP into the application to securely lock the application

Unlocking of File/Folder

- Alike locking a file, if the user wish to unlock the file, login into the application.
- Scan the QR code produced and enter the OTP from the mobile phone to unlock the file

Secure Cryptographic Computation

- The back end of our application is securely encrypted with a cryptographic algorithm that is hard to break. Thus, allowing users to have the assurance that their files are only available to intended users.

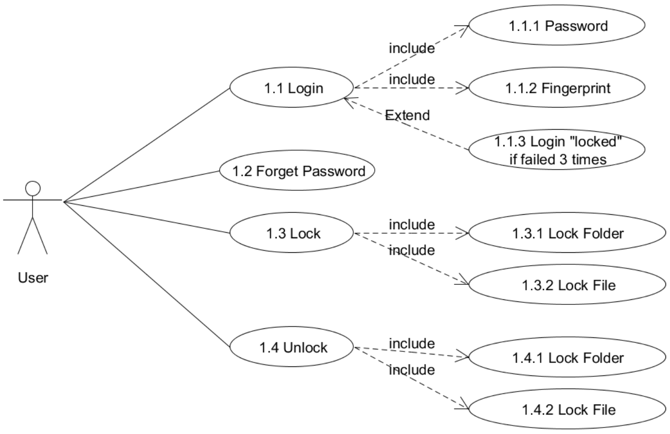
Account Recovery

- In the unlikely event of forgetting the password, users will be able to reset their account credentials.

Trusted Users

- Users with the file rights will be able to authorize other users to access the files.

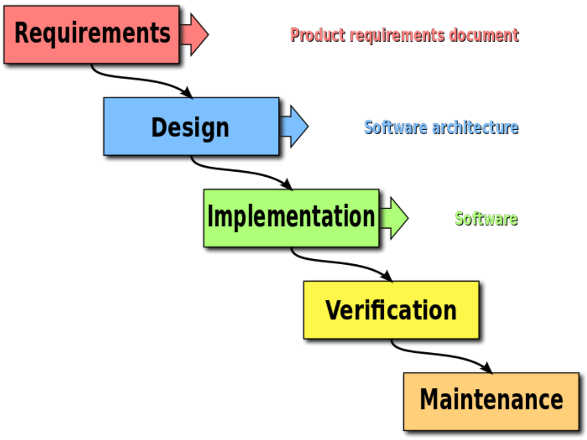
3.2 Proposed Use Case



4. Development Methodologies

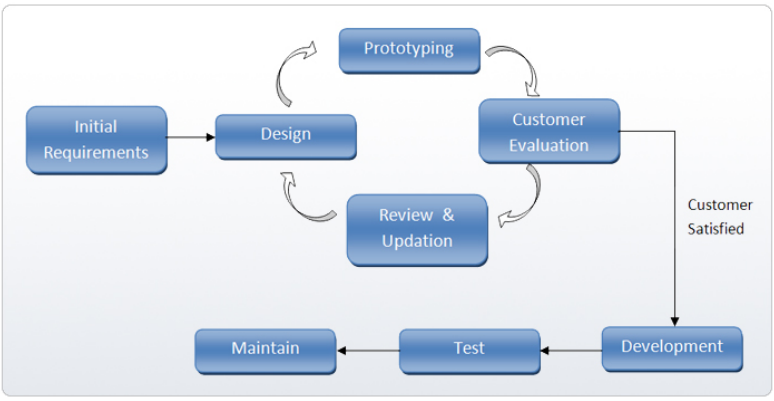
4.1 Waterfall Model

The waterfall model is a relatively linear sequential design development methodology. It tends to be one of the less iterative and less flexible approach to adopt. As its name suggest, it is a downwards model that flows through the different phases. By adopting this model, it is challenging and more costly to support changes once its phase has passed.



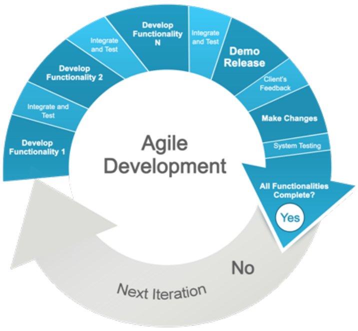
4.2 Prototyping Model

This model is based on requirements gathered from a user. A prototype is then built based on requirements gathered. Prototype is reviewed by the user an a new prototype is built again. This iteration repeats until the final design is confirmed and accepted by the user.



4.3 Agile Model

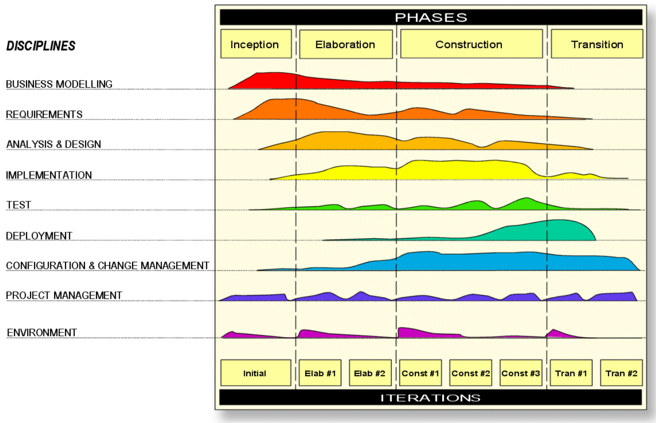
The initial planning and analysis is kept at a high level, just enough to outline the scope. After every iterations, an end product is released. At every iteration, product is refined.



4.4 Rational Unified Process

RUP is an iterative software development framework. It consists of 4 main stages:

- Inception
  In this phase, the scope of the project is defined.
  Requirements are gathered.
  Mitigate the key risk items identified through analysis.
- Elaboration
  Develop detailed design of the system with diagram aids (use case diagram, activity diagram etc)
- Construction
  In this phase, the actual product is being developed.
- Transition
  Primary objective is to transit from development phase into production, making it ready for the market. This phase includes testing the system and providing training to its user.



RUP allows more than one iterations for each of the 4 stages, providing flexibility when changes are required during development phase.

After much considerations, we have decided to adopt the RUP development methodology.

5. Comparison

5.1 Application Development Language

Language	**IDE**	**Description**
C++	QT	C++ is a general purpose object oriented programming language. Provides a collection of predefined classes. Android applications can also be developed using C++ using QT libraries. However, the size required for the package will be significantly larger
Java	Android SDK, Eclipse	Android applications are usually developed in Java or Kotlin. Java is also the official programming language for using android studio

5.2 Database

Relational Database	**Non Relational Database**
Structured Query Language (SQL)	No SQL
Fixed Schema	No fixed schema
Table relationships makes queries more resource intensive (foreign keys)	Stores as individual entries.
Able to handle complicated querying and database transactions	Does not handle transactions

6. Risk Assessment

Risks	Description
Project delay	Bugs and error along the way during the implementation
Anyone is able to unlock the file/folder	QRCODE is universal so it is open for use by anybody with a QRCODE scanner
App crash	Application unable to open and thus unable to start and run to scan
Leaking of information	As QRCODE is encrypted with username and password, if the QRCODE is decrypted when hacked, the username and password will be known
Database stop working	Database SQL may have its services stop or crash and unable to carry on further actions.

References

https://en.wikipedia.org/wiki/Google_Authenticator#Pseudocode_for_one-time_password_(OTP)

https://www.csa.gov.sg/gosafeonline/go-safe-for-me/homeinternetusers/2fa-the-use-of-otp-token

https://www.yubico.com/products/yubikey-hardware/fido-u2f-security-key/#toggle-id-10

https://www.computerworld.com/article/3063544/android/android-apps-fingerprint-support.html

https://play.google.com/store/apps/details?id=com.agilebits.onepassword

https://play.google.com/store/apps/details?id=com.mufri.authenticatorplus

https://play.google.com/store/apps/details?id=com.getkeepsafe.applock

https://www.pluralsight.com/blog/software-development/relational-non-relational-databases